DEPARTAMENTO DE INFORMÁTICA

PROYECTO FIN DE CARRERA

DELITOS INFORMÁTICOS: MALWARE, FRAUDES Y ESTAFAS A TRAVÉS DE LA RED Y CÓMO PREVENIRLOS

AUTOR: ALBERTO GALLEGO YUSTE

TUTOR: MIGUEL ÁNGEL RAMOS

Leganés, Octubre de 2012

Título: Delitos informáticos: Malware, fraudes y estafas a través de la red y cómo prevenirlos
Autor: Alberto Gallego Yuste
Director: Miguel Ángel Ramos

EL TRIBUNAL

Presidente: _____

Vocal: _____

Secretario: _____

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día __ de _____ de 20__ en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de

VOCAL

SECRETARIO PRESIDENTE

AGRADECIMIENTOS

Agradezco en primer lugar el esfuerzo realizado por mi tutor, Miguel Ángel Ramos, por guiarme durante todo el proyecto, animándome en los momentos más delicados pero también mostrando los puntos a mejorar y proponiéndome nuevas soluciones, manteniendo durante todo el desarrollo del trabajo un gran interés y atención y estando siempre disponible para cualquier consulta.

En segundo lugar, quiero agradecer la paciencia y el apoyo incondicional a mi familia y amigos, sin los cuales no hubiera podido finalizar mis estudios, y con toda seguridad no hubiera realizado este proyecto.

Por último, deseo agradecer el apoyo mostrado a mis compañeros Álvaro Casado y Javier Díez, pues al encontrarnos realizando nuestros respectivos proyectos en el mismo espacio de tiempo, nos hemos ido apoyando y animando mutuamente para poder lograr nuestros objetivos académicos.

RESUMEN

El presente documento desarrolla una completa visión sobre los delitos y fraudes informáticos que han tenido lugar desde que comenzaran a aparecer los primeros ordenadores personales hasta la actualidad, así como una completa descripción de las herramientas software y las técnicas más comunes que empleaban y emplean los delincuentes para perpetrar los delitos. El objeto de este documento es comprender los mecanismos y procesos que utilizan estos infractores y proponer en todo momento al usuario acciones preventivas, técnicas de protección o pautas a seguir para poder evitar ser víctima de cada una de las amenazas informáticas que se exponen en este documento, detallando los aspectos legales que rigen actualmente las leyes que versan sobre esta problemática y proponiendo medidas de acción a los usuarios afectados por alguna de estas infracciones.

En paralelo, también se podrá ir comprobando la evolución de los ciberdelitos desde su primera etapa hasta la actualidad, tanto en los procesos o mecanismos de los que se valen los infractores, como las motivaciones de los mismos para perpetrar las infracciones, los cambios de objetivos que persiguen, etc.

En la última parte del documento se realiza una previsión sobre las futuras amenazas informáticas que se estima que serán los principales focos de delincuencia informática en la próxima década, recopilando datos e indicadores que muestran el ascenso de estos nuevos tipos de infracciones y explicando el porqué de estas nuevas amenazas y las medidas de seguridad que se han de tomar al respecto.

ABSTRACT

This project develops a complete approach to Computer offense and fraud since the first Personal Computer until today. It also describes the variety of software tools and other techniques which have made it happen. The document aims to understand the processes and procedures employed by the offenders. It proposes the user a range of preventive actions, protection techniques and other measures in order to avoid becoming a victim. A focus on legal criteria is included as well to help the user to act consequently.

Yet at the same time, the project analyzes the historical evolution of cyber offenses, not only by their technical aspect but also by the psychological background of the action and the actors.

The last part is dedicated to the future predictions about informatics menaces which are to be the most important issues of cyber offense in the next decade. The project pays special attention to the existent data in order to explain why these are real menaces and how and to what extent we can react to them.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Introducción

Hoy en día se está produciendo un espectacular incremento tanto del comercio electrónico como de todo tipo de movimientos bancarios y actividades financieras a través de Internet. El auge de esta nueva herramienta de trabajo implica una serie de beneficios tanto para el usuario (comodidad, disponibilidad, etc.) como para las empresas y vendedores particulares (nueva plataforma de venta de productos, interacción con sus clientes, etc.). Todo esto nos ha servido para poder entrar en una nueva era de comunicación entre los clientes y las empresas hasta ahora desconocida, donde el comercio es instantáneo y no necesariamente hemos de conocer previamente al comprador o al vendedor. Sencillamente, para hacernos una idea del cambio producido, la cuota de mercado de cualquier negocio ha cambiado de su rango local o nacional para pasar a ser mundial, al obtener la oportunidad de vender sus productos globalmente mediante una sencilla página web.

Podemos hacernos una idea del potencial de este nuevo sector con sólo un dato: el año pasado (2011), en el denominado "Black Friday"[1] que se lleva a cabo por todo EEUU justo después del día de "Acción de Gracias", el 24,3% de las transacciones se realizaron a través de Internet, lo cual supuso un montante total de 3.697 millones de dólares, en tan solo 24 horas. Con esto, podemos observar la enorme cantidad de dinero que se mueve a diario por Internet y, entre toda esta oferta y demanda, esta compra-venta de artículos, al usuario medio le puede resultar difícil discernir entre lo que es una buena oferta, de lo que realmente es un fraude.

De hecho, esta nueva forma de interrelacionarnos nos ha permitido abrir la ventana al comercio global, pero también ha atraído a un buen número de personas y entidades que intentan mediante todo tipo de mecanismos, estafar a los usuarios desprevenidos, ingenuos o muy confiados que navegan a través de las webs y que desean obtener productos, realizar actividades financieras de forma ágil, etc. Este nuevo tipo de usuarios ha pasado a ser el objetivo de engaños, estafas y fraudes de todo tipo.

A lo largo de todo este documento se van a abordar la mayoría de tipos de estafas y fraudes que se cometen actualmente en Internet, partiendo desde las primeras estafas que existieron en los inicios de la denominada como "red de redes", hasta las que se están cometiendo actualmente y las que se piensa que en un futuro se cometerán, tratando de aportar una serie de pautas y procedimientos para que los usuarios puedan evitar ser estafados y puedan estar protegidos ante los numerosos fraudes que nos podemos encontrar hoy en día navegando por la red.

Así, se enumerarán y expondrán ejemplos de los fraudes y estafas, los cuales representan amenazas latentes para la seguridad de los usuarios de Internet, explicando las técnicas más comunes utilizadas por los infractores que tratan de obtener información personal, beneficio económico, etc. y cómo evitar ser víctima de estos fraudes.

Posteriormente, se explicará qué hacer en caso de haber sido objeto de una estafa por internet, cómo actuar, y cuáles son los derechos que tienen los usuarios a la hora de reclamar una posible indemnización.

Para finalizar, se expondrá hacia dónde van a ir enfocados los ciberdelitos en los próximos años, así como las nuevas amenazas a las que la comunidad de usuarios se tendrá que enfrentar y cómo evitarlas.

1.2 Objetivos

El objetivo principal de este documento es la prevención de los delitos informáticos, poniendo en alerta a la comunidad de usuarios acerca de las amenazas que se ciernen sobre ellos al utilizar cualquier tipo de sistema informático. Sobre este objetivo principal, se proponen los siguientes sub-objetivos:

- Repasar la historia de la delincuencia informática, desde sus inicios hasta la actualidad, indagando en sus motivaciones y su problemática para los usuarios.

- Comprender cada uno de los procesos y mecanismos con los que los infractores perpetran los fraudes y delitos informáticos, prestando especial atención al software que se utiliza para estos casos, para una mejor comprensión de los puntos a vigilar por parte de los usuarios.

- Entender el marco legal en el que se hallan este tipo de delitos, las organizaciones y entidades gubernamentales que los persiguen, y las entidades en donde el usuario puede reclamar o informar si ha sido víctima de cualquier tipo de delito informático.

- Recopilar todos los procesos y medidas de seguridad necesarias por parte de los usuarios, imprescindibles para una buena protección de sus sistemas.

- Entender las nuevas amenazas que se ciernen sobre los usuarios y proporcionar a los mismos la suficiente información y medios como para poder estar protegidos ante este nuevo tipo de amenazas.

2 DELITOS INFORMÁTICOS EN INTERNET: EL INICIO DE UNA NUEVA AMENAZA PARA LOS CONSUMIDORES

Actualmente, vivimos en una sociedad que se comunica e interrelaciona en gran medida a través de las telecomunicaciones y las diferentes tecnologías de las que disponemos, las cuales han ido progresivamente aumentando su público y que hoy en día están al alcance de casi cualquier persona. Esta situación ha representado un avance en la mejora de las comunicaciones entre las personas, inimaginable hace pocos años, pero de igual forma ha llevado consigo una serie de nuevas amenazas en forma de intentos de estafa, suplantación de identidades y demás problemas potencialmente peligrosos para los usuarios de estas nuevas tecnologías. Estas actividades fraudulentas que se perpetran mediante herramientas informáticas son los denominados como delitos informáticos.

Existe una gran cantidad de autores y organismos que han definido los delitos informáticos, existiendo multitud de opiniones, llegando incluso algunos expertos a concluir que no se han de diferenciar los delitos informáticos de los delitos comunes, ya que la única diferencia entre ellos es el medio por el cual se llevan a cabo, pero como el resultado final es el mismo, no cabe diferencia alguna.

En este documento definiremos el concepto de delito informático como "los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos", tal y como se expone en el Convenio de Ciberdelincuencia Europeo.

2.1 Características de los delitos informáticos

Existen una serie de características comunes a todos los delitos informáticos y que los diferencia del resto de infracciones, como la gran dificultad de demostrarlos ante un tribunal, ya que en ocasiones es mucho más difícil seguir la pista a un delincuente informático que a uno "común", la facilidad y rapidez con la que éstos se pueden llevar a cabo, pudiéndose cometer estos delitos en

apenas unos segundos y desde cualquier parte del mundo, y por último, su constante evolución y proliferación, que hacen que sean un tipo de delitos especialmente difíciles de detectar y perseguir para las autoridades.

Atendiendo a estas características, resulta evidente lo extraordinariamente difícil que puede llegar a ser el detectar este tipo de delitos, subsanarlos, y encontrar a los responsables de los mismos, por lo que los usuarios han de realizar grandes esfuerzos en la prevención de los mismos, y ser precavidos a la hora de suministrar cierto tipo de información a través de Internet, tanto en transacciones financieras como a la hora de proporcionar sus datos personales.

2.2 Clasificación de los delitos informáticos

Existen múltiples clasificaciones en torno a los delitos informáticos. En este documento, se recogerán las clasificaciones establecidas por el "Convenio sobre la Ciberdelincuencia", la Brigada de Investigación Tecnológica de la Policía Nacional Española y la Organización de las Naciones Unidas (ONU).

2.2.1 Clasificación según la ONU

La Organización de las Naciones Unidas (ONU) define tres tipos de delitos informáticos:

1. Fraudes cometidos mediante manipulación de computadoras.
2. Manipulación de los datos de entrada.
3. Daños o modificaciones de programas o datos computarizados.

A su vez, los fraudes cometidos mediante manipulación de computadoras pueden clasificarse en:

- Manipulación de los datos de entrada o sustracción de datos.
- La manipulación de programas: modificación de programas existentes en un sistema o la inserción de nuevos programas.

- Manipulación de los datos de salida.
- Fraude efectuado por manipulación informática: también conocido como la "técnica del salami"[2], aprovecha las iteraciones automáticas de los procesos de cómputo.

Los fraudes realizados mediante la manipulación de los datos de entrada pueden darse:

- Como objeto: alteración de los documentos digitales.
- Como instrumento: uso de las computadoras para falsificar documentos de uso comercial.

Técnicas empleadas para realizar daños o modificaciones de programas o datos computarizados:

- Sabotaje informático: acción de eliminar o modificar funciones o datos en una computadora sin autorización, para obstaculizar su correcto funcionamiento.
- Acceso no autorizado a servicios y sistemas informáticos.
- Reproducción no autorizada de programas informáticos de protección legal: piratería.

Ilustración 1: Clasificación de los delitos informáticos según la ONU

2.2.2 Clasificación según el "Convenio sobre la Ciberdelincuencia"

Firmado el 1 de Noviembre de 2001 en Budapest, se creó con el fin de definir un marco de referencia en el campo de las tecnologías y los delitos para la Unión Europea. En este convenio se propone una clasificación de los delitos informáticos en cuatro grupos:

- **Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:**
    - Acceso ilícito a sistemas informáticos.
    - Interceptación ilícita de datos informáticos.
    - Interferencia en el funcionamiento de un sistema informático.
    - Abuso de dispositivos que faciliten la realización de delitos.

Algunos ejemplos de este grupo de delitos son: el robo de identidades, la conexión a redes no autorizadas y la utilización de spyware[3] y de keylogger[4].

- **Delitos informáticos:**
    - Falsificación informática mediante la introducción, borrado o supresión de datos informáticos.
    - Fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.

El borrado fraudulento de datos o la corrupción de ficheros son ejemplos de delitos de este tipo.

- **Delitos relacionados con el contenido:**
    - Producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos.

- **Delitos relacionados con infracciones de la propiedad intelectual y derechos afines:**

    - Un ejemplo de este grupo de delitos es la copia y distribución de programas informáticos, o piratería informática.

Con el fin de criminalizar los actos de racismo y xenofobia cometidos mediante sistemas informáticos, en enero de 2008 se promulgó el "Protocolo Adicional al Convenio de Ciberdelincuencia del Consejo de Europa" que incluye, entre otros aspectos, las medidas que se deben tomar en casos de:

- Difusión de material xenófobo o racista.
- Insultos o amenazas con motivación racista o xenófoba.
- Negociación, minimización burda, aprobación o justificación del genocidio o de crímenes contra la humanidad.

Ilustración 2: Clasificación de los delitos informáticos según el Convenio sobre la Ciberdelincuencia

Conviene destacar que en el "Convenio sobre la Ciberdelincuencia" se recomienda a cada país que tome las medidas necesarias para tipificar como delito en su derecho interno cada uno de los apartados descritos en cada categoría.

2.2.3 Clasificación según la Brigada de Investigación Tecnológica (BIT) de la Policía Nacional Española

- **Ataques que se producen contra el derecho a la intimidad:**

  Delito de descubrimiento y revelación de secretos mediante el apoderamiento y difusión de datos reservados registrados en ficheros o soportes informáticos.

- **Infracciones a la Propiedad Intelectual a través de la protección de los derechos de autor:**

  Especialmente la copia y distribución no autorizada de programas de ordenador y tenencia de medios para suprimir los dispositivos utilizados para proteger dichos programas.

- **Falsedades:**

  Concepto de documento como todo soporte material que exprese o incorpore datos. Extensión de la falsificación de moneda a las tarjetas de débito y crédito. Fabricación o tenencia de programas de ordenador para la comisión de delitos de falsedad.

- **Sabotajes informáticos:**

  Delito de daños mediante la destrucción o alteración de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos.

- **Fraudes informáticos:**

  Actos de estafa a través de la manipulación de datos o programas para la obtención de un lucro ilícito.

- **Amenazas:**

  Realizadas por cualquier medio de comunicación.

- **Calumnias e injurias:**

  Cuando se propaguen por cualquier medio de eficacia

semejante a la imprenta o la radiodifusión.

- **Pornografía infantil:**

  Entre los delitos relativos a la prostitución al utilizar a menores o incapaces con fines exhibicionistas o pornográficos.

  La inducción, promoción, favorecimiento o el facilitar la prostitución de una persona menor de edad o incapaz.

  La producción, venta, distribución, exhibición, por cualquier medio, de material pornográfico en cuya elaboración hayan sido utilizados menores de edad o incapaces, aunque el material tuviera su origen en el extranjero o fuera desconocido.

  El favorecimiento de las conductas anteriores (la persona que facilitara la producción, venta, distribución, exhibición...).

  La posesión de dicho material para la realización de dichas conductas.

Ilustración 3: Clasificación de los delitos informáticos según la Brigada de Investigación Tecnológica

2.3 Actores dentro de un delito informático

Existen dos tipos de actores o personas involucradas en una actividad informática delictiva:

I. Sujeto activo: aquella persona que comete el delito informático.

II. Sujeto pasivo: aquella persona que es víctima del delito informático.

2.3.1 Sujeto activo de los delitos informáticos.

Actualmente, sabemos que se cometen numerosos delitos y fraudes informáticos de forma diaria, pero el anonimato que ofrece Internet y las diferentes tecnologías informáticas que se usan para realizar los delitos informáticos, hacen extremadamente difícil el conocer quiénes son realmente los autores de estos delitos. En este apartado se tratará de dar una descripción de algunas características comunes a todos los delincuentes informáticos, sus motivaciones, o las metas que persiguen al realizar este tipo de actividades delictivas.

2.3.1.1 Características

Primeramente, se comenzará enumerando algunas características comunes relativas a las conductas, acciones y motivaciones de estos delincuentes que suelen reflejarse en la mayor parte de los delitos informáticos:

- Al ser acciones muy concretas y técnicas, sólo son capaces de desarrollarlas personas con un nivel elevado de conocimientos tanto teóricos como prácticos, por lo que estas conductas son denominadas como "conductas criminales de cuello blanco".

- En multitud de ocasiones estos delitos se cometen en el entorno laboral o cuando el infractor se halla trabajando.

- Se suelen aprovechar debilidades, fisuras o brechas de seguridad en los sistemas informáticos, por lo que se las

denomina como "acciones de oportunidad".

- Detrás de estas acciones suele existir una motivación económica, y muchas veces se pueden llegar a producir grandes pérdidas económicas a la víctima.

- Se pueden cometer sin necesidad de que el infractor se encuentre físicamente presente en el lugar donde se perpetra la infracción y en un espacio muy breve de tiempo (en ocasiones, segundos).

- Generalmente no son denunciados (por diversos motivos como imagen de la compañía, que la víctima no es consciente del delito, o por simple dejadez), por lo que los delitos no son detectados por las autoridades y el infractor en muchas ocasiones no es detenido.

- Son relativamente frecuentes en el ámbito militar.

- Resulta muy difícil su demostración ante un tribunal, dado su carácter técnico.

2.3.1.2 Tipos de sujetos activos

Existen diferentes tipos de sujetos activos, diferenciándose principalmente por la naturaleza de los delitos cometidos. Así, en la calificación de sujetos activos pueden entrar desde usuarios que acceden a sistemas informáticos de forma ilegítima pero sin intenciones delictivas, hasta empleados que roban información sensible de su propia empresa para sacar un beneficio económico.

A todo este tipo de infractores en un principio se les denominó comúnmente como "Hackers", pero la realidad es que los que hoy se denominan como "Hackers" apenas constituyen una pequeña parte de todos los delincuentes informáticos.

Para diferenciar unos infractores de otros, hemos de tener en cuenta las diferencias implícitas que lleva su modo de actuar y las consecuencias del mismo, ya que las actividades de estos infractores llegan a ser muy diferentes las unas de las otras, y

responden a distintas motivaciones y momentos en el desarrollo computacional. Ya en los primeros pasos en el desarrollo de Internet, la información restringida y confidencial atrajo a los primeros delincuentes informáticos. Por entonces, los infractores eran definidos según los objetivos que perseguían:

- Sombrero Negro: infractores con amplios conocimientos en bases de datos, se infiltraban en los sistemas para extraer documentación de forma ilícita para posteriormente venderla.
- Sombrero Gris: personas inquietas cuya motivación no era económica, sino simplemente intelectual. Se introducían en los sistemas de forma ilícita pero solo como un reto personal, sin la intención de crear daño alguno.
- Sombrero Blanco: personas que simplemente estudiaban los sistemas de seguridad de las organizaciones y empresas y advertían a las mismas de las brechas de seguridad, debilidades y demás errores, proponiendo ellos mismos soluciones a los problemas que encontraban.

A medida que se fue desarrollando Internet, el "pirateo" fue alcanzando cotas cada vez más altas, ya que los programas fueron puestos a disposición de todos los usuarios a través de la propia red. Así, se pueden distinguir multitud de infractores, que se clasifican según sus comportamientos, intenciones, radio de actuación o conocimientos. A continuación se expondrán cada uno de estos subgrupos y sus características principales.

2.3.1.3 HACKER:

Persona que generalmente muestra un elevado interés en el funcionamiento de sistemas operativos y nuevas tecnologías. Sus infracciones son denominadas como hacking, y, por lo general, simplemente le gusta investigar las nuevas herramientas tecnológicas y su desarrollo, de una forma discreta y silenciosa, teniendo como objetivo final llegar a conocer el funcionamiento de cualquier sistema informático, tomando estas actividades como desafíos intelectuales. Lejos de pretender producir daños, los hackers poseen un código ético:

- El acceso a los ordenadores y a cualquier cosa que pueda enseñar cómo funciona el mundo, debería ser ilimitado y total.
- Toda la información deberá ser libre y gratuita.
- Desconfía de la autoridad. Promueve la descentralización.
- Los Hackers deberán ser juzgados por sus hacks[5], no por criterios sin sentido como calificaciones académicas, edad, raza, o posición social.
- Se puede crear arte y belleza en un ordenador.
- Los ordenadores pueden mejorar tu vida.

Evidentemente, esta visión de los hackers choca frontalmente con las legislaciones vigentes ya que en ocasiones el hecho de infiltrarse en un sistema constituye un delito.

Los hackers son auténticos expertos en el manejo de equipos informáticos, y se oponen a un uso ilícito de sus conocimientos, si bien frecuentemente intentan acceder a cualquier máquina conectada a la red, o a una Intranet[6] privada, siempre basan estas acciones en un afán de adquirir nuevos conocimientos, descubrir las posibles debilidades de los sistemas a los que intentan acceder y por último, obtener la satisfacción personal de haber logrado sobrepasar las barreras de seguridad de grandes empresas. Finalmente, muchos de ellos comunican a sus propias víctimas las debilidades encontradas en la seguridad y en algunos casos sugieren cómo corregirlas.

2.3.1.4 CRACKER:

Se dedican a romper las protecciones y otros elementos de seguridad de los programas comerciales, en su mayoría con el fin confeso de sacar provecho de los mismos en el mercado negro. Un Cracker debe conocer perfectamente las dos caras de la tecnología, esto es la parte de programación y la parte física de la electrónica, para poder crear códigos para utilizarlos en la copia de archivos. Sus acciones pueden ir desde la destrucción de información (ya sea a través de virus u otros medios) hasta el robo de datos y posterior venta.

El resultado evidente de estas actividades fraudulentas son el ingente número de archivos y soportes digitales que contienen

software pirata y que se distribuyen bien a través de la red, o bien mediante un soporte físico (generalmente CD´s y DVD´s) entre vastas comunidades de usuarios, algunos de los cuales ni siquiera llegan a sospechar que parte del software que tienen en sus máquinas, incluso con certificados de garantía de procedencia, es craqueado. Tiene dos variantes:

- Los crackers que se adentran en un sistema informático para robar información o producir destrozos en el mismo.
- Los que se dedican a desproteger todo tipo de programas.

El mayor problema de este tipo de infractores, es que pese a los grandes esfuerzos que las empresas realizan para proteger sus productos, la experiencia dice que los crackers siempre encuentran algún modo de romper las protecciones y poder craquear el software. Además, toda vez que se descubre la forma de saltarse una protección, generalmente ésta es difundida por Internet, por lo que si un infractor logra saltarse una protección y lo difunde, el número potencial de infractores aumenta exponencialmente desde ese mismo momento, por lo que resulta un problema de muy difícil solución.

En la actualidad es habitual ver como se muestran los cracks[7] de la mayoría de software de forma gratuita a través de Internet. El motivo de que estos cracks formen parte de la red es por ser difundidos de forma impune por otro grupo de infractores, que será detallado más adelante en este mismo documento.

Las herramientas de este tipo de infractores permiten "desamontonar" los programas, lo que se conoce como ingeniería inversa[8]. El proceso permite eliminar las protecciones del programa, que generalmente se basan en reglas temporales (sobre todo en los programas de prueba) de tal forma que se puedan seguir usando los programas aun habiendo expirado la fecha límite que se dictaba en un inicio y evitando pagar por continuar haciendo uso del mismo.

2.3.1.5 PHREAKER:

Un phreaker generalmente tiene amplios conocimientos en el ámbito de los sistemas telefónicos, (tanto terrestres como móviles) aparte de amplios conocimientos sobre informática, ya que

actualmente el control de centralitas es la parte más importante de la telefonía, y su desarrollo está basado en la informática.

Tienen como objetivo la eliminación de la protección en redes públicas y corporativas de telefonía, evitando así pagar por el servicio usado, y en algunos casos, obtener un beneficio económico mediante la falsificación de las tarjetas de prepago para llamadas telefónicas, cuyos códigos obtienen al lograr el acceso mediante técnicas de "hacking" a sus servidores. Los Phreakers a lo largo de los años han ido elaborando las denominadas "cajas de colores", sistemas que trabajan a determinadas frecuencias y que permiten realizar actividades enfocadas a entorpecer el normal funcionamiento de los sistemas de telefonía y obtener beneficios por ello.

Dentro de las actividades que comprende el phreaking podríamos distinguir:

- **Shoulder-surfing:** basada en la observación del código secreto de la víctima. En el momento en que el infractor conozca esa información podrá usar el servicio telefónico de la víctima.
- **Call-sell operations:** el infractor obtiene un código identificador de un usuario víctima, y de esta forma el montante económico pasa a la cuenta de la víctima, dada la baja seguridad en este aspecto en los dispositivos móviles.
- **Diverting:** penetración ilícita a centrales telefónicas privadas. Es frecuente que al acceder a estas centrales se realicen llamadas de larga distancia o llamadas de alta tarificación. Los infractores siempre buscarán empresas en las que este tipo de llamadas sean habituales, para poder pasar más desapercibidas estas actividades.
- **Acceso no autorizado a sistemas de correos de voz:** el infractor centra su ataque sobre las máquinas que soportan el almacenamiento de mensajes telefónicos de los usuarios suscriptores de un servicio.
- **Monitoreo pasivo:** El agente intercepta ondas radiales[9] y permanece a la escucha, pudiendo obtener información que se transmita por esas frecuencias usadas por los dispositivos móviles de forma ilícita.

2.3.1.6 LAMMERS:

Son infractores con escasa o nula capacidad para poder romper barreras de seguridad o protecciones de productos informáticos. Simplemente se dedican a intentar penetrar en sistemas o cometer infracciones a partir de los conocimientos que exponen otros usuarios en la red. Si el objetivo que intentan vulnerar les plantea algún tipo de problema adicional, generalmente no poseen la capacidad suficiente como para superar el escollo. Por regla general, son despreciados por los auténticos hackers ya que los lammers buscan el beneficio propio gracias al esfuerzo de usuarios más preparados intelectualmente. La mayoría de usuarios que hoy día intentan cometer algún tipo de infracción o penetrar en algún sistema pueden encuadrarse en esta categoría.

2.3.1.7 GURÚS:

Son los denominados como maestros y generalmente ayudan y forman a los futuros hackers. Se trata de usuarios que poseen amplios conocimientos y experiencia acerca de sistemas informáticos, y se dedican a transmitir sus experiencias y a aconsejar a las personas que se están iniciando en el dominio de los sistemas informáticos. Son personas muy respetadas por sus dilatadas trayectorias y normalmente sólo enseñan los conceptos más básicos, dejando a los hackers para el desarrollo propio y la investigación los aspectos más complejos.

2.3.1.8 BUCANEROS:

Son las personas que se dedican a la venta de los productos craqueados anteriormente. Evidentemente, no tienen por qué poseer ningún tipo de conocimiento acerca de la informática, simplemente capacidad para poder generar una serie de ventas a partir del producto craqueado. Son más comerciales y vendedores que delincuentes informáticos. Normalmente el bucanero compra al CopyHacker[10] y revende el producto.

2.3.1.9 NEWBIE:

Usuarios que se interesan por las técnicas de hacking y conocimientos informáticos en general, y comienzan a aprender teniendo como referencia unas cuantas páginas web y foros que les

sirven de guía. Serían el conjunto de aprendices que toma sus primeros contactos en el hackeo intentando introducirse en sistemas sencillos, aunque por lo general su conocimiento no va mucho más allá de seguir las pautas y procedimientos que les proponen webs expertas. Son considerados novatos en el ámbito del hacking, aunque con el paso del tiempo y a medida que crezca su interés y amplíen sus conocimientos podrán llegar a convertirse en expertos y alcanzar la categoría de auténticos hackers.

2.3.1.10 TRASHING:

Se basa en la obtención de información secreta o privada a partir del estudio de datos desechados o descartados por una persona o entidad, con la finalidad de cometer actividades delictivas valiéndose de esta información.

Estas actividades pueden tener como objetivo la realización de espionaje, coacción o simplemente el lucro mediante el uso ilegítimo de códigos de ingreso a sistemas informáticos que se hayan obtenido en el análisis de la basura recolectada.

2.3.2 Sujeto pasivo de los delitos informáticos.

El sujeto pasivo básicamente es la víctima del delito, el elemento que sufre las consecuencias de las acciones del sujeto activo. En el caso de los delitos informáticos las víctimas pueden ser cualquier ente (individuos, instituciones crediticias, gobiernos, etc.) que use sistemas automatizados de información, generalmente conectados a otros.

En el sujeto pasivo recae especial importancia ya que éste es en la mayor parte de los casos el primero en dar la alarma y denunciar infracciones que, por lo general, hasta ese momento son desconocidas. Por lo tanto, es muy importante que el sujeto pasivo que se haya percatado de que ha sido objeto de un fraude o un delito, denuncie el hecho para que pueda ser estudiado por las autoridades competentes, y al mismo tiempo, se pueda poner en sobre aviso al resto de la comunidad de usuarios. Sin el aviso del sujeto pasivo, sería extraordinariamente difícil detectar y eliminar las miles de amenazas que diariamente circulan por la red.

Generalmente, los delitos informáticos se descubren de forma casual, ya que en un primer momento se desconocen los métodos de acción de los infractores, por lo que el testimonio de los sujetos pasivos obtiene especial relevancia para tratar las nuevas amenazas. Así, se puede concluir que los sujetos pasivos son la principal herramienta en la lucha contra los delitos informáticos y la denuncia sistemática de cualquier sujeto pasivo que haya sido objeto de algún tipo de fraude o delito de esta índole permite poner en alerta a las autoridades competentes sobre posibles nuevos sistemas o procedimientos fraudulentos.

Por el contrario, la situación actual es que el grueso de los delitos informáticos no son descubiertos o no son denunciados por los sujetos pasivos, por lo que resulta imposible poder saber con certeza la verdadera magnitud de los mismos. Una de las posibles causas de la falta de denuncias reside en el temor por parte de empresas que hayan sido objeto de algún tipo de fraude informático de denunciar este tipo de infracciones (por el posible desprestigio que esto pudiera ocasionar a la misma y las consecuentes pérdidas económicas y de imagen ante la sociedad) teniendo que recurrir a la denominada como "cifra negra"[11] para poder valorar las estadísticas sobre este tipo de conductas.

Por lo tanto, en la búsqueda de la prevención de los delitos informáticos, se deben definir las necesidades de protección y los puntos y fuentes potencialmente peligrosos para los sistemas informáticos, poniendo como bases el conocimiento por parte de los usuarios de las diferentes técnicas de manipulación y las diferentes formas en las que pueden aparecer las amenazas en cualquier sistema informático.

Se puede afirmar que a través de la comunicación y la alerta sobre estas conductas ilícitas y creando una adecuada legislación que proteja a las víctimas, otorgando una formación amplia y completa para el personal que atiende e investiga estas conductas y ejecutando resoluciones similares a las realizadas por los organismos internacionales (basadas en educar a la comunidad de víctimas y estimular la denuncia de los delitos) se podría poner freno a estas técnicas y conductas ilegales.

2.4 Estadísticas de los delitos informáticos

Con el fin de poder extraer una relación numérica entre los casos más comunes y para saber con qué frecuencia aparecen en el entorno tanto empresarial como doméstico ciertos delitos informáticos, se pasará a exponer las estadísticas obtenidas en 2011 por la empresa de seguridad informática "Recovery Labs". Fijando como base la clasificación propuesta por el "Convenio sobre la Ciberdelincuencia" (del cual ya se ha hablado en puntos anteriores en este mismo documento), se ha elaborado una estadística con los porcentajes de delitos que más se han repetido durante el año 2011 respecto a las solicitudes del servicio de peritaje informático recibidas por esta empresa, obteniendo los siguientes resultados:

- Un 46,71% son delitos informáticos como la falsificación o fraude informático mediante la introducción, borrado o supresión de datos informáticos, o la interferencia en sistemas informáticos.

- Un 43,11% son delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos. Dentro de esta categoría las conductas que más se repiten son con un 63,89% delitos relacionados con el acceso ilícito a sistemas informáticos, y con un 36,11% todas aquellas conductas delictivas relativas a la interferencia en el funcionamiento de un sistema informático.

- Un 10,18% son delitos relacionados con el contenido, como la producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos.

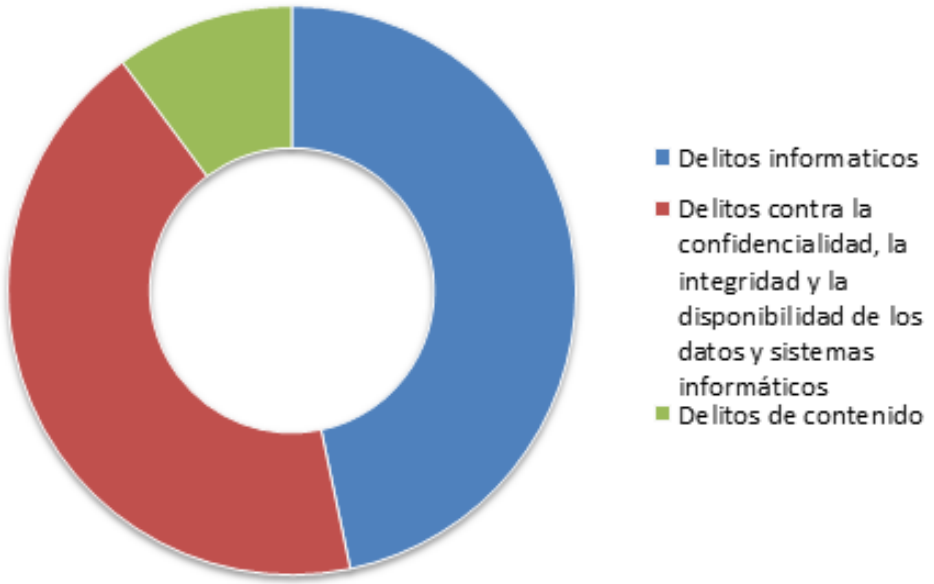


Ilustración 4: Gráfico sobre los delitos informáticos cometidos en 2011

Se puede concluir por lo tanto, que los delitos informáticos y contra la confidencialidad, integridad y disponibilidad de los datos son los más representativos. Se puede pensar que por ello que son los más cometidos, aunque cabe la posibilidad de que no sea tanta la diferencia entre el número de este tipo de delitos y los de contenido, dado que estos últimos son más difíciles de probar y perseguir.

3 LEGISLACIÓN ACTUAL EN ESPAÑA FRENTE A LOS DELITOS INFORMÁTICOS

En las siguientes líneas, se recoge la situación legislativa vigente actualmente en España, con el objetivo de clarificar lo que es considerado como delito informático y las consecuencias de los mismos para las personas que realicen estos actos.

3.1 Legislación actual en España

Se entiende por delito informático todo acto ilícito penal llevado a cabo a través de medios informáticos que esté íntimamente ligado a los bienes jurídicos relacionados con las tecnologías de la información o que tiene como fin estos bienes.

3.1.1 Delitos informáticos y el Código Penal

Aunque los delitos informáticos no están contemplados como un tipo especial de delito en la legislación española, existen varias normas relacionadas con este tipo de conductas:

- Ley Orgánica de Protección de Datos de Carácter Personal (LOPDCP).
- Ley de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI).
- Real Decreto 1720/2007
- Ley General de Telecomunicaciones.
- Ley de Propiedad Intelectual.
- Ley de Firma Electrónica.

Además de estas normas, en el Código Penal español se incluyen multitud de conductas ilícitas relacionadas con los delitos informáticos. Las que más se aproximan a la clasificación propuesta por el "Convenio sobre la Ciberdelincuencia" (clasificación mencionada en el apartado 2 de este mismo documento) se reflejan en los siguientes artículos:

- Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:

    - El Artículo 197 contempla las penas con las que se castigará:

        - A quien, con el fin de descubrir los secretos o vulnerar la intimidad de otro, se apodere de cualquier documentación o efecto personal, intercepte sus telecomunicaciones o utilice artificios de escucha, transmisión, grabación o reproducción de cualquier señal de comunicación.

        - A quien acceda por cualquier medio, utilice o modifique, en perjuicio de terceros, a datos reservados de carácter personal o familiar, registrados o almacenados en cualquier tipo de soporte.

        - Si se difunden, revelan o ceden a terceros los datos o hechos descubiertos.

          En el artículo 278.1 se exponen las penas con las que se castigará a quien lleve a cabo las mismas acciones expuestas anteriormente, pero con el fin de descubrir secretos de empresa.

    - El Artículo 264.2 trata de las penas que se impondrán al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

- Delitos informáticos:

    - Los artículos 248 y 249 tratan las estafas. En concreto el artículo 248.2 considera las estafas llevadas a cabo mediante manipulación informática o

artificios semejantes.

- Los artículos 255 y 256 mencionan las penas que se impondrán a quienes cometan defraudaciones utilizando, entre otros medios, las telecomunicaciones.

- Delitos relacionados con el contenido:

  - El artículo 186 cita las penas que se impondrán a aquellos, que por cualquier medio directo, vendan, difundan o exhiban material pornográfico entre menores de edad o incapaces.

  - El artículo 189 trata las medidas que se impondrán a quien utilice a menores de edad o a incapaces con fines exhibicionistas o pornográficos, y quien produzca, venda, distribuya, exhiba o facilite la producción, venta, distribución o exhibición de material pornográfico, en cuya elaboración se hayan utilizado menores de edad o incapaces.

- Delitos relacionados con infracciones de la propiedad intelectual y derechos afines:

  - El Artículo 270 recopila las penas con las que se castigará a quienes reproduzcan, distribuyan o comuniquen públicamente, una parte o la totalidad, de una obra literaria, artística o científica, con ánimo de lucro y en perjuicio de terceros.

  - El artículo 273 trata las penas que se impondrán a quienes sin consentimiento del titular de una patente, fabrique, importe, posea, utilice, ofrezca o introduzca en el comercio, objetos amparados por tales derechos, con fines comerciales o industriales.

A día de hoy, las leyes se van adaptando poco a poco a las nuevas situaciones y escenarios que se presentan en el ámbito tecnológico, de tal forma que su cometido es ir poniendo límites y acotando las

nuevas amenazas que pueden irse presentando día a día al usuario de cualquier tipo de tecnología informática. Evidentemente, la ley siempre irá un paso por detrás de los infractores que utilicen las nuevas tecnologías para perjudicar a los usuarios, pero el esfuerzo de los cuerpos legislativos del Estado se centra en mantener un estrecho cerco a estos infractores, así como perseguir y denunciar los nuevos métodos que éstos vayan implementando para cometer los fraudes y estafas.

Así, algunas conductas como el spam (envío de publicidad no deseada, normalmente a través del correo electrónico) no estaban contempladas entre los delitos tipificados en el Código penal español, pero esta actividad ya ha sido incorporada en la LSSI de tal forma que actualmente ya es imputable este tipo de actividades. Como vemos, la legislación va avanzando y amoldándose a todas estas nuevas tecnologías, pero como siempre, el problema reside en que primero han de ocurrir reiteradamente estos "nuevos delitos" para que posteriormente sean reflejados en la legislación española.

3.1.2 Legislación adicional

Existen numerosas leyes adicionales que versan sobre la regulación de la Sociedad de la Información, centrándose en aspectos tales como la privacidad y la protección de la intimidad de los usuarios. A continuación se exponen las principales leyes, para poder dar una mayor completitud al ámbito legislativo que engloba todos los comportamientos registrados como delitos en el Código Penal español, con el fin de poder adoptar comportamientos útiles legalmente en caso de delito.

3.1.2.1 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)

Supone una modificación importante del régimen sobre protección de datos de personas físicas contenido hasta entonces en la extinta LORTAD.

Tiene como objetivo "garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de

su honor e intimidad personal y familiar."

Ámbito de aplicación:

1. La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal:

a. Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.
b. Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público.
c. Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

2. El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación:

a. A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
b. A los ficheros sometidos a la normativa sobre protección de materias clasificadas.
c. A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia Española de Protección de Datos.

3. Se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales:

a. Los ficheros regulados por la legislación de régimen electoral.

b. Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública.
c. Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del régimen del personal de las Fuerzas Armadas.
d. Los derivados del Registro Civil y del Registro Central de penados y rebeldes.
e. Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.

3.1.2.2 Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSICE)

La LSSICE supone la primera regulación legal que con carácter general se dicta en España para el entorno de Internet. Sus principales objetivos consisten en:

1. Es objeto de la presente Ley la regulación del régimen jurídico de los servicios de la sociedad de la información y de la contratación por vía electrónica, en lo referente a las obligaciones de los prestadores de servicios incluidos los que actúen como intermediarios en la transmisión de contenidos por las redes de telecomunicaciones, las comunicaciones comerciales por vía electrónica, la información previa y posterior a la celebración de contratos electrónicos, las condiciones relativas a su validez y eficacia y el régimen sancionador aplicable a los prestadores de servicios de la sociedad de la información.

2. Las disposiciones contenidas en esta Ley se entenderán sin perjuicio de lo dispuesto en otras normas estatales o autonómicas ajenas al ámbito normativo coordinado, o que tengan como finalidad la protección de la salud y seguridad pública, incluida la salvaguarda de la defensa nacional, los intereses del consumidor, el régimen tributario aplicable a los servicios de la sociedad de la información, la protección de datos personales y la normativa reguladora de defensa de la

competencia.

3.1.2.3 Real Decreto Legislativo 1/1996, de 12 de abril (BOE 22-4-1996), por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual.

Esta Ley regula, aclara y armoniza las disposiciones legales vigentes sobre este tema. Constituye la referencia principal relativa a la regulación de la propiedad intelectual en España.

3.1.2.4 Real Decreto Legislativo 14/1999, de 17 de septiembre, sobre Firma Electrónica.

1. Este Real Decreto-Ley regula el uso de la firma electrónica, el reconocimiento de su eficacia jurídica y la prestación al público de servicios de certificación. Las normas sobre esta actividad son de aplicación a los prestadores de servicios establecidos en España.

2. Las disposiciones contenidas en este Real Decreto-Ley no alteran las normas relativas a la celebración, la formalización, la validez y la eficacia de los contratos y otros actos jurídicos ni al régimen jurídico aplicable a las obligaciones.

   Las normas sobre la prestación de servicios de certificación de firma electrónica que recoge este Real Decreto-Ley no sustituyen ni modifican las que regulan las funciones que corresponde realizar a las personas facultadas, con arreglo a derecho, para dar fe de la firma en documentos o para intervenir en su elevación a públicos.

3.1.3 Organismos Especiales

Dado el carácter de este documento, en donde se busca informar a los usuarios que hayan sido objeto de cualquier tipo de fraude o delito informático acerca de las vías de acción y los cauces que han de seguir para poder denunciar y evitar que esas situaciones se reproduzcan en sucesivas ocasiones, se expone la información acerca de los dos organismos oficiales de las Fuerzas de Seguridad del Estado, que persiguen este tipo de delitos

informáticos de forma específica. Son los siguientes:

- Brigada de Investigación Tecnológica (Cuerpo Nacional de Policía)
- Grupo de Delitos Telemáticos (Guardia Civil)

Con objeto de dar máxima difusión a estos organismos y dar a conocer a los mismos al lector de este documento, se pasan a describir cada uno de estos organismos con la información recogida en sus respectivas páginas web.

3.1.3.1 Brigada de Investigación Tecnológica (Cuerpo Nacional de Policía)

La Brigada de Investigación Tecnológica es la unidad policial destinada a desmantelar las nuevas formas de delincuencia que han ido surgiendo con el uso de las nuevas tecnologías, tales como pornografía infantil, estafas y fraudes por Internet, fraudes en el uso de las comunicaciones, ataques cibernéticos, piratería...

Su principal misión es perseguir a delincuentes y obtener las suficientes pruebas, para poder poner a éstos a disposición judicial.

Como herramientas principales en la lucha contra los delitos informáticos, se encuentran "la formación progresiva de los investigadores, la colaboración de las más punteras instituciones públicas y privadas, la participación activa en los foros internacionales de cooperación policial y la colaboración ciudadana".

Las principales funciones de este organismo del Estado, tal y como se recogen en su página web, son:

- La realización directa de las investigaciones especialmente complejas.
- La coordinación de las operaciones que involucren a diversas Jefaturas Superiores.
- La formación del personal del Cuerpo Nacional de Policía y otros cuerpos de Policía extranjeros.

- La representación internacional y la ejecución y/o coordinación de las investigaciones que tengan su origen en otros países.

En su página web (http://www.policia.es/org_central/judicial/udef/bit_alertas.html) se puede encontrar información de todo tipo acerca de sus intervenciones, acciones, etc., así como interponer denuncias si se ha sido objeto de algún delito informático. De esta forma, los usuarios que hayan sido víctimas de cualquier delito o fraude informático podrán acudir a esta organización y poner en conocimiento de la misma cualquier estafa a la que hayan sido sometidos.

3.1.3.2 Grupo de delitos Telemáticos (Guardia Civil)

El Grupo de Delitos Telemáticos fue creado en 1996 para investigar cualquier actividad ilícita que se cometa a través de la red.

En sus inicios se creó para atender a las pocas denuncias que había entonces por los llamados delitos informáticos, pero el crecimiento exponencial de usuarios de la red hace indispensable la presencia de este organismo hoy en día, siendo su alcance todas aquellas conductas delictivas realizadas a través de los sistemas de información o contra éstos.

El esfuerzo principal del GDT ha sido la investigación de la delincuencia realizada a través de las redes y sistemas de información. También cabe destacar los esfuerzos que realizan para fomentar un uso seguro de las nuevas tecnologías.

En su página web (https://www.gdt.guardiacivil.es/webgdt/home_alerta.php) se puede consultar la legislación actual, denunciar delitos informáticos o consultar consejos prácticos para la seguridad de usuarios particulares mientras navegan por internet.

3.1.4 Necesidades y deficiencias

En la lucha contra este tipo de delincuencia, existe un

problema que a priori va a sucederse recurrentemente, y es que se ha de ser consciente de la velocidad con que se desarrollan las nuevas tecnologías, lo cual, unido a la posibilidad de actuar desde cualquier lugar y en cualquier momento del día. A continuación, se muestran una serie de aspectos que dificultan la tarea de las personas que luchan contra este tipo de delitos:

- Determinar la jurisdicción competente: las actividades provenientes de un país en el que no exista regulación alguna acerca de los delitos informáticos tiende a ser una problemática importante ante la imposibilidad de imputar delito alguno.

- Recabar las pruebas suficientes para inculpar a un infractor suele ser una tarea muy costosa.

- Identificar el autor de un delito informático es mucho más complejo que el de uno convencional, ya que existen técnicas de ocultación de dirección IP[12] por parte de un intruso (spoofing[13]) que pueden complicar sobremanera la localización e identificación del infractor.

- El continuo cambio y evolución en las técnicas de ataques informáticos y de los procesos para cometer delitos o fraudes a través de la red, hace que la legislación tenga que estar amoldándose constantemente e ir recogiendo cada uno de los nuevos procesos ilícitos como actividades no permitidas, para poder tener un soporte legal que no se quede anticuado, de tal forma que se puedan imputar cargos a los infractores por muy modernas que sean sus técnicas, con la ley como principal respaldo.

- La necesidad de un mayor apoyo y colaboración entre los distintos países en la búsqueda y detención de este tipo de infractores.

3.1.5 Conclusiones

Una de las principales conclusiones que se puede extraer sería

que España aún debe mejorar su legislación en relación a las nuevas tecnologías, para poder ser equiparable a otros países del planeta en donde la actualización de las leyes es mucho más dinámica.

Otra conclusión recalcable sería la falta de medios con los que cuenta el personal destinado a investigar los delitos relacionados con las tecnologías de la información, por lo que sería deseable una mayor aportación tanto en capital humano como en recursos económicos para paliar estas deficiencias.

Una de las principales apuestas para poder avanzar en esta materia es la mejora en cuanto a coordinación y cooperación entre los distintos países para la creación de leyes conjuntas y que sean vigentes en todos los países que formen el acuerdo, con el objetivo de facilitar el rastreo, persecución y detección de los infractores, con independencia de su situación geográfica, para tratar de evitar la impunidad de la que gozan ciertos delincuentes informáticos a la hora de operar desde diferentes países.

4 TIPOS DE FRAUDE

En este apartado vamos a tratar cada uno de los diferentes tipos de fraude que nos podemos encontrar en el ámbito de la informática, clasificando cada uno de ellos y describiéndolos detalladamente, para poder entender qué técnicas utilizan y cómo actúan los estafadores en cada ocasión y a partir de ahí establecer las acciones a realizar por los usuarios para poder prevenir este tipo de peligros y ataques, a los que absolutamente todos los usuarios estamos irremediablemente expuestos.

4.1 Virus y programas maliciosos

Los virus (también código o software malicioso, software malintencionado o malware) son programas maliciosos que se crean para modificar la conducta habitual de un programa, con el fin de entorpecer o bloquear sus funciones, generalmente sin que el usuario víctima sea consciente de ello.

Hoy en día, el término virus se ha extrapolado para referirse a todos los programas que infectan un ordenador, aunque el término original sólo se refiere a una pequeña parte de todo el software malicioso existente, la cual será objeto de estudio en este punto.

Los virus pueden modificar tanto los mecanismos y funcionamiento de un programa como la información que se almacena en el mismo, pudiendo variar estas acciones maliciosas desde el robo de información sensible del sistema infectado, borrado de datos, o el uso deliberado del sistema infectado para realizar a partir de este equipo otro tipo de actividades ilegales, pudiendo llegar a tener consecuencias legales para la persona cuyo sistema ha sido infectado y que involuntariamente pueda estar sirviendo de plataforma para que una tercera persona esté cometiendo a través del mismo.

En sus orígenes, los virus fueron diseñados persiguiendo un afán de protagonismo por parte del creador. Por ello, este malware se diseñaba de tal forma que el creador pudiera obtener un

reconocimiento público por sus habilidades para modificar programas o por entorpecer su correcto funcionamiento, de tal forma que los virus se caracterizaban por ser de fácil visibilidad para la víctima y generalmente los daños causados en el equipo infectado eran visibles dado que era justo lo que buscaban los infractores: un reconocimiento público de sus acciones maliciosas por parte del resto de usuarios. Algunas acciones que desarrollaban en sus inicios era la eliminación de ficheros importantes, borrado de datos, modificación de caracteres de escritura, etc.

Con el paso del tiempo, la constatación de Internet como un elemento central en las relaciones tanto personales como profesionales entre las personas, y como espacio para todo tipo de intercambios comerciales y transacciones financieras, ha supuesto que los ciberdelincuentes pasen a ver esta herramienta como una fuente de ingresos muy importante. Así, la motivación de la creación de virus ha ido cambiando desde entonces, pues la creación de los primeros virus se debía a simple afán de protagonismo por parte de algún delincuente informático, pero esta motivación se ha ido dejando de lado tras ver las importantes cantidades de dinero que se comenzaban a mover a través de la red, por lo que actualmente la motivación principal de los delincuentes es la económica. Esto se refleja en la evolución del perfil medio de un delincuente informático desde sus inicios hasta la actualidad.

En los comienzos de Internet, el delincuente informático era una persona inteligente e inquieta, que simplemente trataba de obtener un reconocimiento público por sus habilidades informáticas, pero actualmente, la mayor parte de los delincuentes informáticos actúan en grupos extraordinariamente organizados que desarrollan los códigos maliciosos con la intención de que pasen lo más desapercibidos posibles, pues cuanto más tarde detecte la víctima que ha sido objeto de algún tipo de fraude, más tiempo van a disponer para seguir perpetrándolo.

Cualquier dispositivo cuyo sistema operativo sea capaz de entender y manejar algún tipo de malware, podrá ser víctima del mismo. Así, actualmente los equipos informáticos más comunes como los ordenadores personales, los dispositivos móviles, los servidores, las

tablets[14], o las videoconsolas son dispositivos que están en el punto de mira de todo desarrollador de malware, por lo que para poder utilizarlos de manera segura es aconsejable disponer de herramientas software que lo mantengan protegido de estas amenazas y a ser posible, cerciorarse de que el dispositivo no está infectado incluso cada vez que lo vaya a usar cualquier usuario, especialmente si va a realizar actividades críticas como puede ser una transferencia bancaria a través de su ordenador personal.

4.1.1 Tipos de virus

Podemos clasificar los distintos tipos de virus hallados hasta el momento atendiendo a varios factores:

- Por su capacidad de propagación
- Por las acciones que realizan en el equipo infectado.
- Otras clasificaciones

4.1.2 Según su capacidad de propagación

Existen tres tipos de malware según la propagación que realizan: virus, gusanos y troyanos.

4.1.2.1 Virus

Infectan otros archivos, por lo que sólo pueden existir en un equipo si se hallan dentro de otro fichero. Los ficheros infectados generalmente son ejecutables, pero también pueden infectar otros archivos que se hallen en el propio equipo infectado.

Los virus pueden ejecutarse cuando el usuario ejecute un fichero que se halle infectado, o si están programados para ello, cuando se realice una determinada acción o se cumpla una determinada condición (por ejemplo una fecha concreta, una cuenta atrás, etc.). El mecanismo de los virus básicamente es el infectar a otros ficheros con las mismas características que él mismo, así, las posibilidades de propagación son infinitas si no se intercepta a tiempo, y puede pasar a infectar a otros equipos si el fichero infectado se halla en un dispositivo extraíble o en una unidad de red, dado que cada vez que un nuevo usuario ejecute el fichero

dañado, se estará poniendo en peligro el equipo con el que se maneja el fichero malicioso.

Los virus fueron los primeros ejemplos de malware pero hoy en día no resultan atractivos para los infractores ya que se han ido creando nuevos tipos de malware más desarrollados, por lo que su uso hoy día es casi anecdótico.

Algunos ejemplos de este tipo de malware son:

- Viernes 13 o Jerusalem: Creado en Israel en 1988. Cada viernes 13 todos los programas que intentaban ejecutarse en el ordenador se borraban. Se cree que conmemoraba el cuarenta aniversario del Estado Judío en la ciudad de Jerusalén.

- Barrotes: Es el primer virus español con relevancia internacional. Surgió en 1993 y su funcionamiento hacía que el virus permaneciera hasta el 5 de enero en el equipo infectado, y era entonces cuando aparecían unas barras en el monitor simulando una cárcel.

Ilustración 5: Captura de pantalla del malware conocido como "Barrotes"

En este ejemplo se aprecia claramente como la finalidad de este tipo de malware era principalmente crear problemas visibles al usuario, intentando obtener relevancia y reconocimiento público

el atacante (prueba de ello es la firma del virus con un pseudónimo).

4.1.2.2 Gusanos:

Son programas maliciosos que basan su funcionamiento en realizar el máximo número de copias de sí mismos, con el objetivo de crear una propagación masiva. La principal diferencia respecto a los virus es que no infectan otros ficheros que se alojen en el equipo víctima. Los principales métodos de propagación de este tipo de malware son los correos electrónicos, las redes P2P[15], la mensajería instantánea y los canales de chat.

Generalmente los creadores de este tipo de malware utilizan la ingeniería social[16] para alentar al usuario receptor a usar el fichero infectado con el gusano. Así, los infractores generalmente intentan poner un título atractivo para la mayor cantidad de usuarios posibles a los archivos que contienen un gusano. Si se trata de las redes P2P, pueden nombrar al archivo con títulos de discos de música de actualidad, o si se trata de un correo electrónico, con ofertas sugerentes o temas que atraigan la atención del usuario medio.

Para eliminar este tipo de malware del equipo, simplemente bastará con eliminar el archivo que sea el foco de infección, así como todas las copias que haya generado en el tiempo que estuviera activo, aunque dependiendo de la sofisticación del gusano, puede resultar más difícil su eliminación, ya que en ocasiones éstos modifican ciertos parámetros del sistema de tal forma que, por ejemplo, siempre que se arranque el equipo, se ejecute el gusano con el resto de programas que por defecto se han de arrancar al encender el dispositivo infectado. De esta forma el gusano se protege y se asegura una copia de sí mismo cada vez que se inicie el sistema.

Algunos ejemplos de gusanos informáticos famosos son:

- **ILoveYou (o VBS/LoveLetter):** Es un gusano informático escrito en VBScript. En mayo del 2000 infectó aproximadamente 50 millones de computadores (entre otros, equipos informáticos del Parlamento Británico) provocando pérdidas de más de 5.500 millones de dólares.

VBS/LoveLetter llega al usuario en un e-mail que tiene por Asunto: 'ILOVEYOU' e incluye un fichero llamado 'LOVE-LETTER-FOR-YOU. TXT.vbs'.

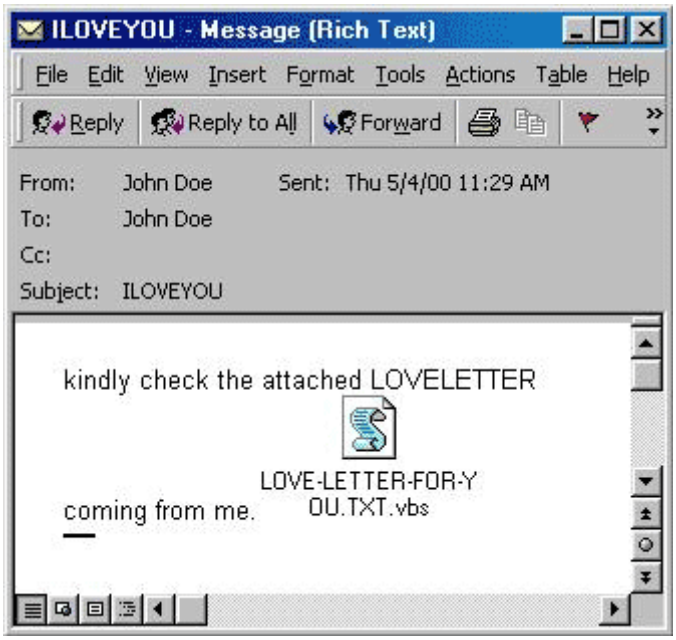


Ilustración 6: Correo electrónico enviado con el gusano "I love you"

Como curiosidad, cabe apuntar que el creador del programa malicioso fue un informático filipino (Onel de Guzmán) que tras haber propagado el código por todo el mundo, primero declaró haberlo transmitido "accidentalmente" y días después confesó haberlo realizado y propagado deliberadamente. La justicia filipina no pudo imputarle ningún delito ya que en ese año dicho país carecía de leyes contra los delitos informáticos y no se consideraba delito la intrusión en las computadoras, por lo que le fueron retirados todos los cargos, y pocos meses después, Filipinas emitió una ley regulatoria de las actividades en Internet, que hoy día sigue vigente.

4.1.2.3 Troyanos:

Software malicioso caracterizado con aspecto de programa legítimo, pero que al ejecutarse crea una puerta trasera que permite la administración remota del equipo a un usuario no autorizado. Carecen de rutina propia de propagación, pueden llegar al sistema de diferentes formas, las más comunes son:

- Descargado por otro programa malicioso.

- Descargado sin el conocimiento del usuario al visitar una página web maliciosa.
- Dentro de otro programa que simula ser inofensivo.

En sus orígenes, la aparición de troyanos iba encauzada a realizar el máximo daño posible en el equipo infectado. Una vez que se había ejecutado el troyano, el infractor podía manejar el equipo infectado de forma remota, pudiendo realizar todo tipo de acciones tales como borrar información de los discos duros, ocupar los discos duros con archivos superfluos, realizar capturas de pantalla, monitorizar pulsaciones del teclado, instalación de otros programas en el equipo infectado, etc.

El funcionamiento de los troyanos se basa en tres programas: un cliente, que es el que dirige al equipo infectado y va ordenando cada uno de los movimientos a realizar, un servidor situado en la computadora infectada, que recibe y ejecuta las órdenes que le va suministrando el cliente, y en función de los resultados obtenidos, devuelve un resultado al programa cliente, y por último un editor del servidor, que tiene como principales funciones la modificación del servidor, la protección del mismo (por ejemplo, a través de contraseñas) y el desarrollo de otras actividades como la unión del servidor a otros programas para que al abrirlos se ejecute, configurar en el puerto donde se instalará, etc.

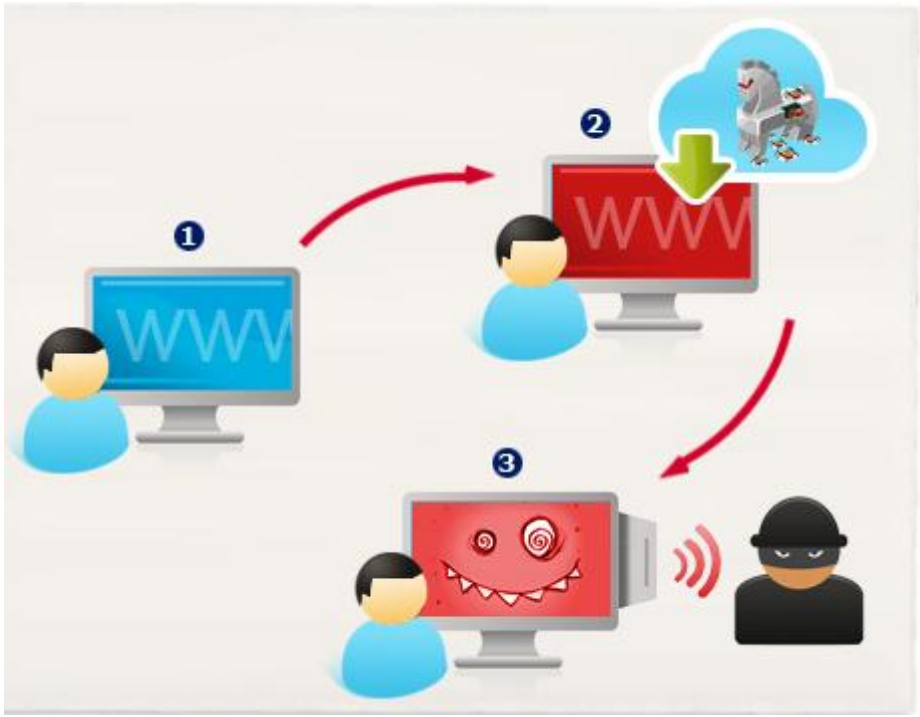


Ilustración 7: Esquema sobre cómo actúan los troyanos

Existen Dos tipos de conexión entre el cliente y el servidor:

- Conexión directa (el cliente se conecta al servidor).
- Conexión inversa (el servidor se conecta al cliente).

La conexión inversa posee ciertas ventajas respecto a la conexión directa; ésta traspasa algunos firewalls[17], pueden ser usados en redes situadas detrás de un router sin problemas (no es necesario redirigir los puertos) y no es necesario conocer la dirección IP del servidor.

Existen otro tipo de conexiones diferentes a las mencionadas, basadas en la comunicación con un servidor intermedio que realiza el proceso de control. Se suele utilizar para este propósito el protocolo IRC[18] o incluso FTP[19], HTTP[20] u otros.

Lo cierto es que lo realmente difícil para poder eliminar un virus troyano de un equipo informático para un usuario medio es darse cuenta de que su equipo está infectado. Esto puede parecer trivial, pero, para empezar, puede ser que un troyano haya infectado su equipo durante meses mientras el usuario legítimo del mismo no se cerciore de actividades anómalas, ya que puede que el troyano no esté desarrollando aún actividades maliciosas. Es cuando el usuario legítimo detecta actividades anómalas (archivos que se borran sin previo aviso, programas que se ejecutan automáticamente al iniciar

el equipo, el equipo se reinicia sin previo aviso, etc.) cuando el usuario se da cuenta de que su ordenador está infectado. En este momento, ha de proceder a remover el virus troyano de su equipo.

Eliminar un troyano puede ser una tarea fácil si se van siguiendo una serie de pasos sencillos indicados en cualquier web especializada (por ejemplo: http://www.informatica-hoy.com.ar/software-seguridad-virus-antivirus/Como-eliminar-un-virus-troyano.php). Si se siguen correctamente los pasos indicados en los manuales web, el usuario no debe tener ningún problema en hacer desaparecer este programa malicioso de su equipo.

- **Troyanos famosos: Sabotaje de oleoductos siberianos**

El sabotaje de los oleoductos siberianos es referido a la sospecha por parte de la URSS en 1982, de un ataque llevado a cabo por la CIA (Agencia Central de Inteligencia de USA) por medio de un troyano al gaseoducto Urengoy–Surgut–Chelyabinsk como parte de una política americana para contrarrestar el robo de tecnología canadiense por parte de la URSS.

En plena guerra fría, la KGB había robado a una empresa canadiense un software muy sofisticado que permitía gestionar el sistema de control de gaseoductos. La reacción de la CIA no se hizo esperar, y sabiendo que la KGB estaba robando este tipo de información, comenzó a manipularla con la compañía canadiense en cuestión, de forma que comenzaron a introducir errores deliberadamente en el código, e introdujeron un troyano en el mismo. Cuando la KGB comenzó a usar estos códigos el troyano comenzó a ejecutarse, y así fue como la CIA pudo acceder al sistema de control de los oleoductos soviéticos de forma remota. Las consecuencias que tuvo esta acción fue un sabotaje por parte de la CIA, que modificó una serie de condiciones en el sistema de control de los oleoductos que finalmente desencadenó una explosión gravísima en terreno de la URSS, hasta tal punto que fue la explosión no nuclear más fuerte jamás vista hasta ese momento.

4.1.2.4 Troyanos bancarios:

En las líneas anteriores, hemos descrito los códigos maliciosos conocidos como "troyanos" y sus actividades, pero hoy en día, debido al alto volumen de transacciones bancarias y movimientos comerciales a través de los equipos informáticos, existe una tendencia a elaborar estos troyanos especialmente enfocados a usarlos para acceder a equipos ajenos con el objetivo de robar datos bancarios o información personal relacionada con cualquier movimiento financiero que el usuario atacado realice en su equipo. Estos son los denominados "troyanos bancarios", una especie de evolución natural de los códigos maliciosos que ha ido ascendiendo conforme han ido aumentando las transacciones bancarias y las actividades comerciales a través de la red, y que, aunque su presencia se ha ido estabilizando, representan un porcentaje muy importante del total de troyanos encontrados, como se puede observar en el siguiente gráfico:

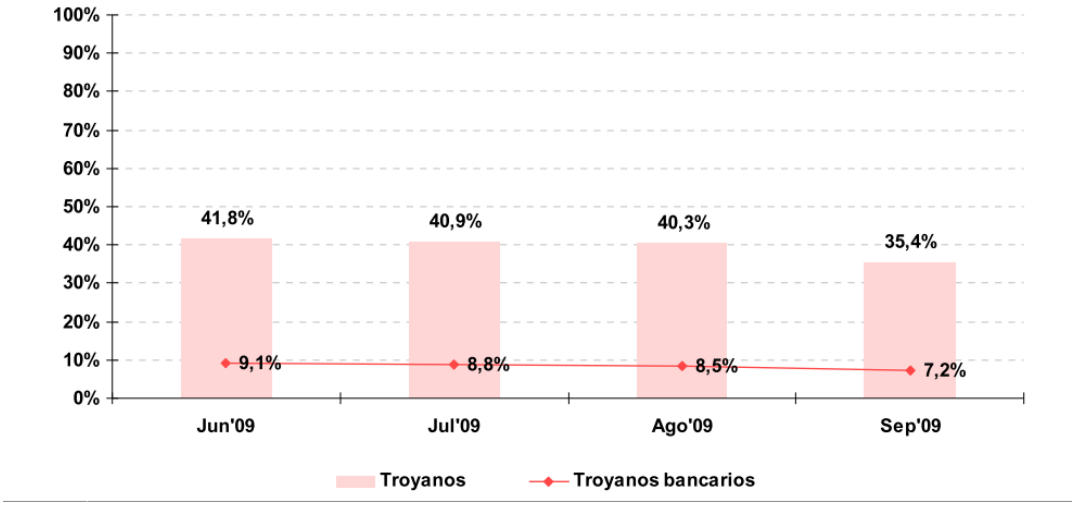


Ilustración 8: Evolución de sistemas infectados con troyanos bancarios en el año 2009

Los troyanos que se diseñaron específicamente para capturar información bancaria comenzaron a aparecer en 2004, y desde entonces técnicas como la captura de credenciales o la monitorización de entidades visitadas se han depurado tanto que las normas y consejos de seguridad seguidos hasta el momento se han quedado obsoletos y han demostrado ser insuficientes. Existe el problema de que normalmente los infractores son los que van desarrollando nuevas tecnologías para poder realizar estas

actividades ilícitas, por lo que los grupos encargados de la seguridad informática en entidades bancarias, entidades públicas, etc., siempre actúan tras haberse cometido el delito, siendo muy difícil el adelantarse y evitarlos, ya que generalmente primero se comete un delito con una nueva tecnología y posteriormente se analiza el método usado para el delito y se deciden las nuevas medidas de seguridad a llevar a cabo.

Los troyanos bancarios generalmente se centran en obtener y actualizar grandes listados de entidades bancarias a través de sitios web relacionados con éstas, y a los que accede el usuario que posee el equipo infectado, siendo su único objetivo recopilar toda esa información únicamente de las páginas visitadas por el usuario, ya que de ahí podrán extraer información personal que les permitirá el acceso ilícito a las cuentas bancarias personales del usuario.

Así, en el trascurso del estudio de este tipo de malware, se ha podido observar ciertas características ligadas a los orígenes de los desarrolladores de este tipo de malware, pudiendo diferenciarse dos tipos de elaboración de malware o dos tipos de "escuelas" según la procedencia de los infractores: la rusa (caracterizada por ser un tipo de malware silencioso sofisticado y sobre todo muy discreto y por lo tanto, más difícil de detectar) y la brasileña (mucho más anárquica y ruidosa, menos sofisticada).

Se ha de tener en cuenta que el hecho del robo de información a través de estos troyanos puede que no acabe siempre en fraude, ya que para que éste se produzca, se han de dar tres circunstancias:

- El infractor ha de infectar el equipo informático del usuario víctima.
- El infractor que logró situar el troyano bancario en el equipo informático de la víctima ha de atacar a la entidad bancaria con la que ésta opera.
- La víctima ha de entrar a su cuenta personal bancaria con el equipo infectado y rellenar los datos adicionales que se le soliciten.

Una vez obtenidos los datos del usuario afectado, los infractores generalmente realizan una labor de filtrado, en donde desechan los datos obtenidos que no tienen relevancia alguna, y recopilan los datos sensibles que puedan reportarles un beneficio. Este tipo de filtrado se lleva a cabo mediante listas de entidades bancarias a monitorizar. Dichas listas contienen cadenas de texto, como pueden ser la propia URL del banco objeto de suplantación (http://www.mibanco.com), subcadenas de la URL del banco (*mibanco.com), cadenas particulares del cuerpo de la página de banca en línea (© MiBanco 2011. Todos los derechos reservados.), etc. En la siguiente imagen se puede observar un programa de filtrado de datos:

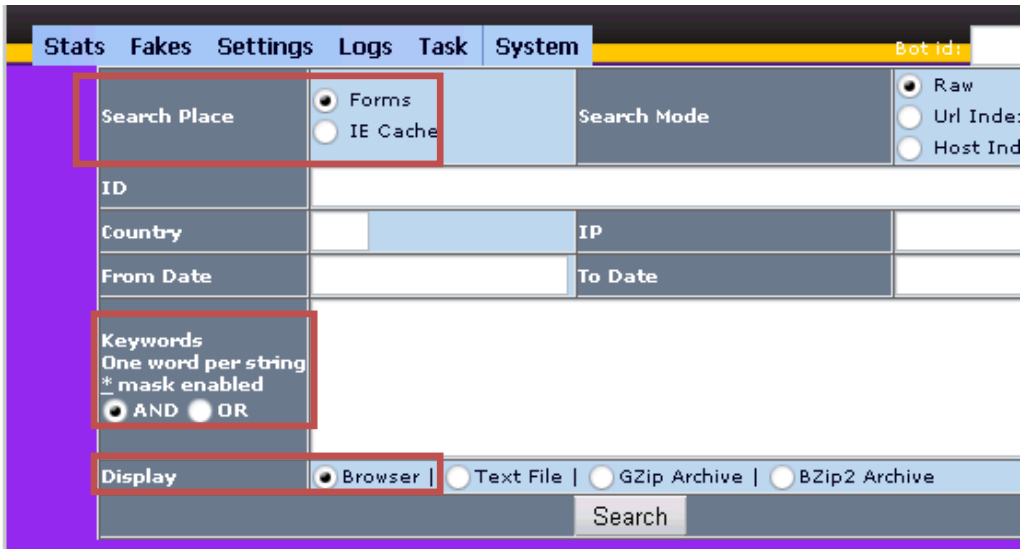


Ilustración 9: Programa para filtrado de datos robados

Toda vez que se han recopilado estos datos, se procede a compararlos con distintos parámetros como puede ser el nombre, número de identificación, etc., de las páginas visitadas. Ha de existir un mecanismo que permita interactuar con el contexto de la página visitada (inspección de ventanas abiertas, instalación de controladores en el sistema, etc.), y de esta forma, se pueden obtener los datos bancarios o la información personal del usuario que ha introducido esta información sensible y confidencial desde el equipo infectado. Así, vemos el resultado que provocó el filtrado de datos mostrado en la anterior imagen:

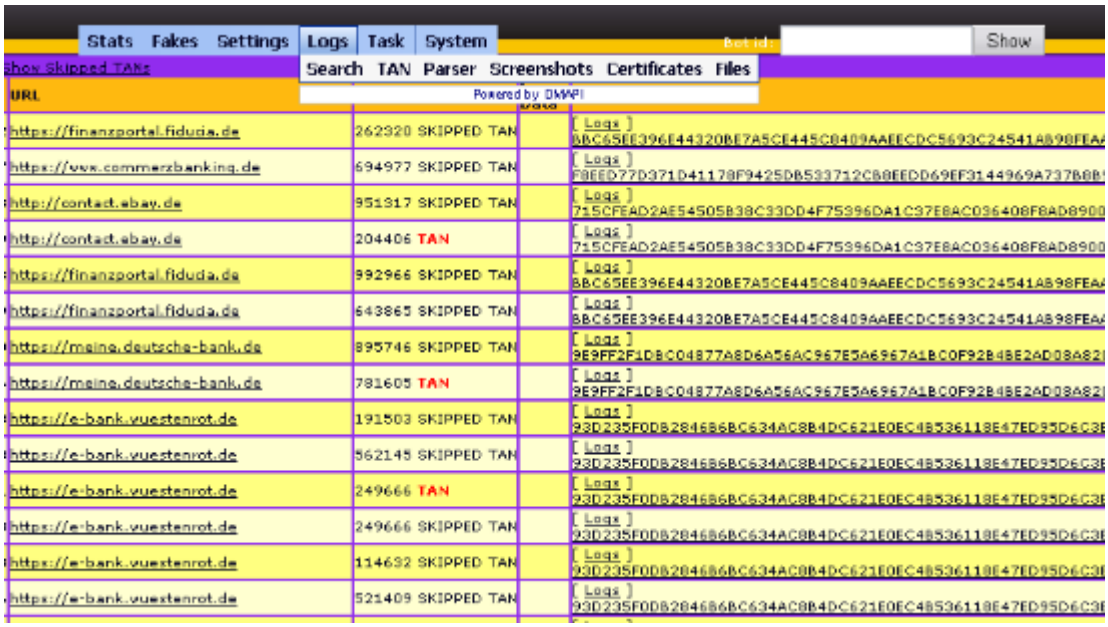


Ilustración 10: Datos recogidos por los infractores tras el filtrado de datos

Las técnicas más comunes empleadas para capturar los datos de los usuarios son:

1. Registro de teclas pulsadas
2. Captura de formularios
3. Capturas de pantalla y grabación de video
4. Inyección de campos de formulario fraudulentos
5. Inyección de páginas fraudulentas
6. Redirección de páginas bancarias
7. Hombre-en-el-medio (man-in-the-middle)

Dado el amplio uso de estas técnicas hoy en día, pasamos a describir el funcionamiento de cada una de ellas para una mejor comprensión de los riesgos que provocan y las medidas que toman las instituciones financieras para evitar que sus clientes sean víctimas de estas técnicas:

4.1.2.5 Registro de teclas pulsadas

Su objetivo es obtener la información de acceso a las cuentas bancarias del usuario víctima, por lo que monitoriza cada una de las teclas que se pulsan en el ordenador infectado, con el fin de extraer a partir de esa información las credenciales necesarias para acceder

a la página bancaria personal de la víctima. También es ampliamente usado para extraer otro tipo de información como cualquier mensaje escrito en el equipo infectado, conversaciones privadas, etc.

Los troyanos bancarios a menudo combinan estas técnicas con métodos de monitorización de entidades, con el objetivo de filtrar toda la información superflua y eliminarla y capturar únicamente las pulsaciones en páginas bancarias concretas. Este método tiene sus limitaciones, ya que si los bancos tienen algún tipo de prueba de acceso que no se pueda introducir por teclado, mediante este sistema los infractores no podrán conseguir la información necesaria para saltarse esa credencial. Además, siempre se han de tener en cuenta excepciones como por ejemplo si un usuario se equivoca y borra, y rescribe de nuevo su contraseña, o si directamente el usuario introduce de forma errónea su propia contraseña, casos que pueden dificultar la extracción de la credencial correcta por parte del infractor.

Este tipo de programas también se utilizan como control parental para vigilar por dónde navegan los usuarios menores de edad de forma oculta, por lo que es muy sencillo adquirir de forma gratuita herramientas de keylogger. En la siguiente página web:

http://www.freedownloadmanager.org/es/downloads/Keylogger_Free_Download_66343_p/

Se puede descargar un programa basado en la técnica de keylogger de forma gratuita.

Una vez adquirido, el usuario puede usarlo para vigilar a menores de edad que estén a su cargo (funcionalidad original del programa) o como una herramienta más para realizar actividades fraudulentas como los citados troyanos bancarios.

Aquí podemos ver un ejemplo de programa que registra las teclas pulsadas en un equipo:

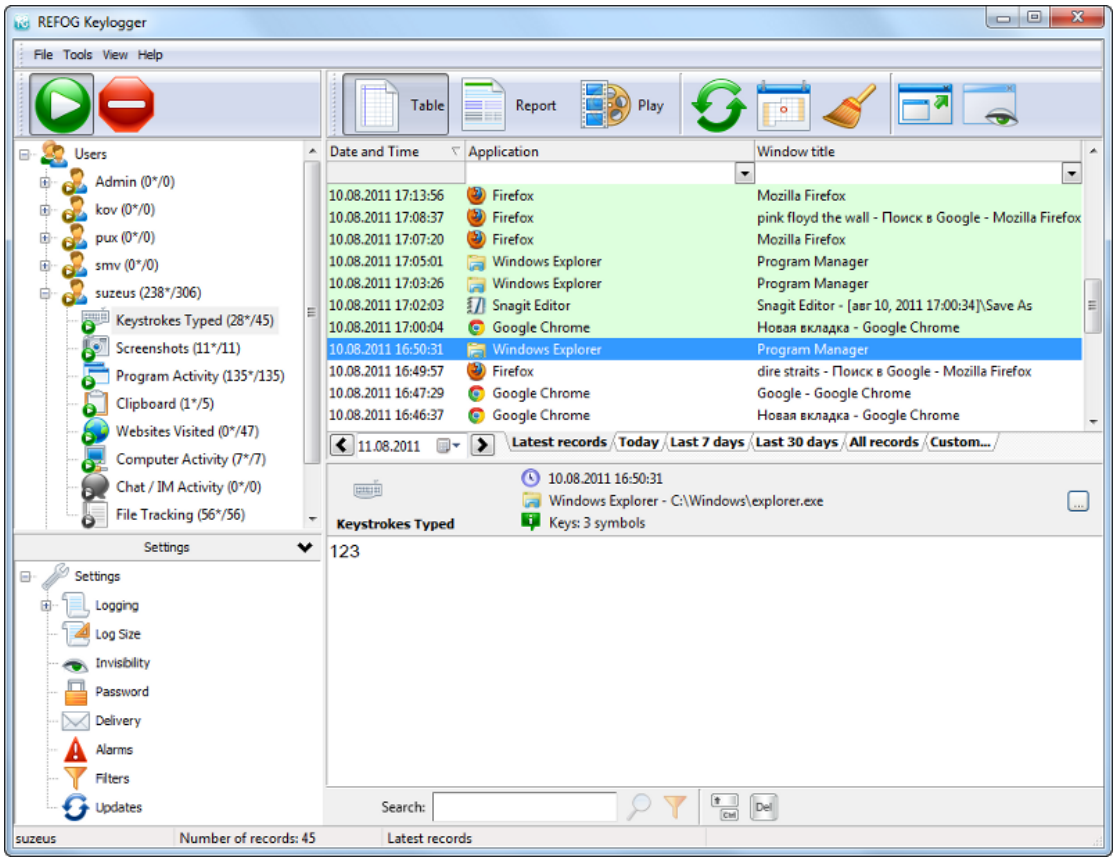


Ilustración 11: Software de registro de teclas pulsadas

4.1.2.6 Captura de formularios

Este proceso es un nuevo avance respecto al anteriormente comentado, y se basa en la captura de los campos requeridos para el acceso a un sitio web bancario. Esta técnica recoge todos los datos proporcionados por el usuario víctima y los almacena en un fichero de texto plano, como se puede observar en la imagen:

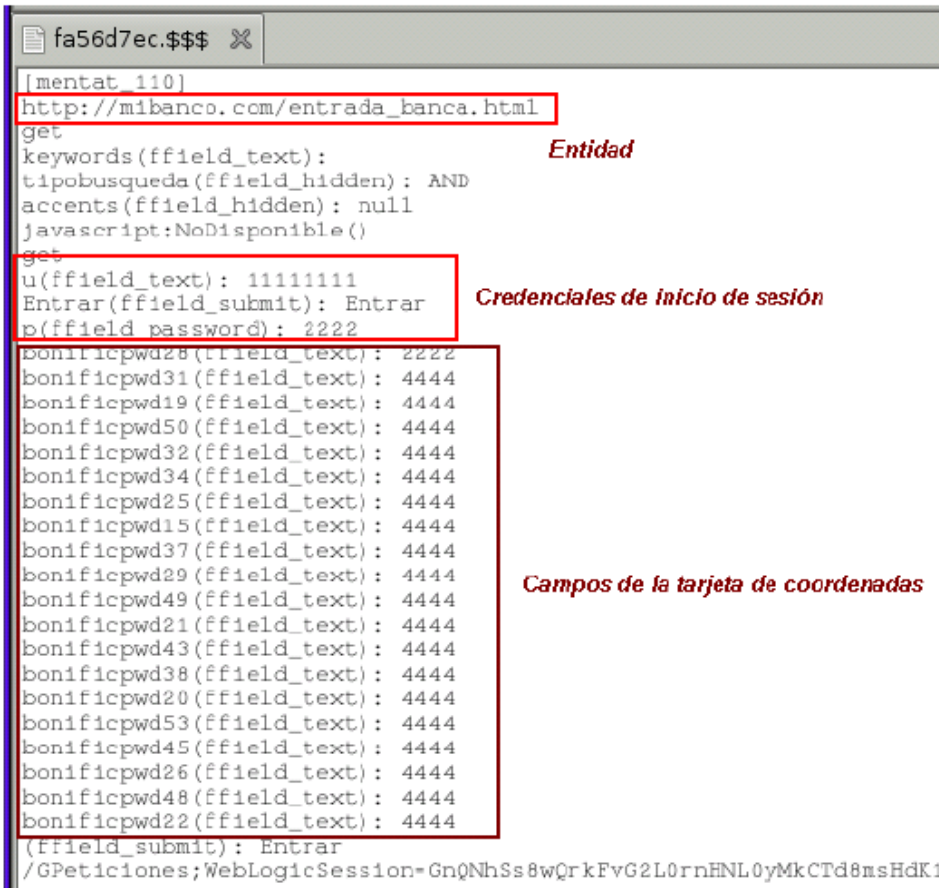


Ilustración 12: Captura de datos robados almacenados en un fichero de texto

Por otro parte, el robo de información sigue siendo previa al cifrado (anterior al envío de datos), por lo que sigue siendo posible recoger los datos de forma inteligible.

4.1.2.7 Capturas de pantalla y grabación de video

Para contrarrestar la técnica de registro de teclas pulsadas y las capturas de credenciales en formularios (técnicas explicadas anteriormente en este mismo apartado), las bancas electrónicas decidieron incluir teclados virtuales en las páginas web de inicio de sesión de los usuarios. Esta herramienta se basa en un teclado que se muestra por pantalla, donde el usuario puede introducir su contraseña para acceder a sus cuentas bancarias simplemente pulsando con el ratón sobre las teclas virtuales, y sin necesidad de tener que pulsar las teclas físicas de su teclado, como podemos observar en la siguiente imagen:

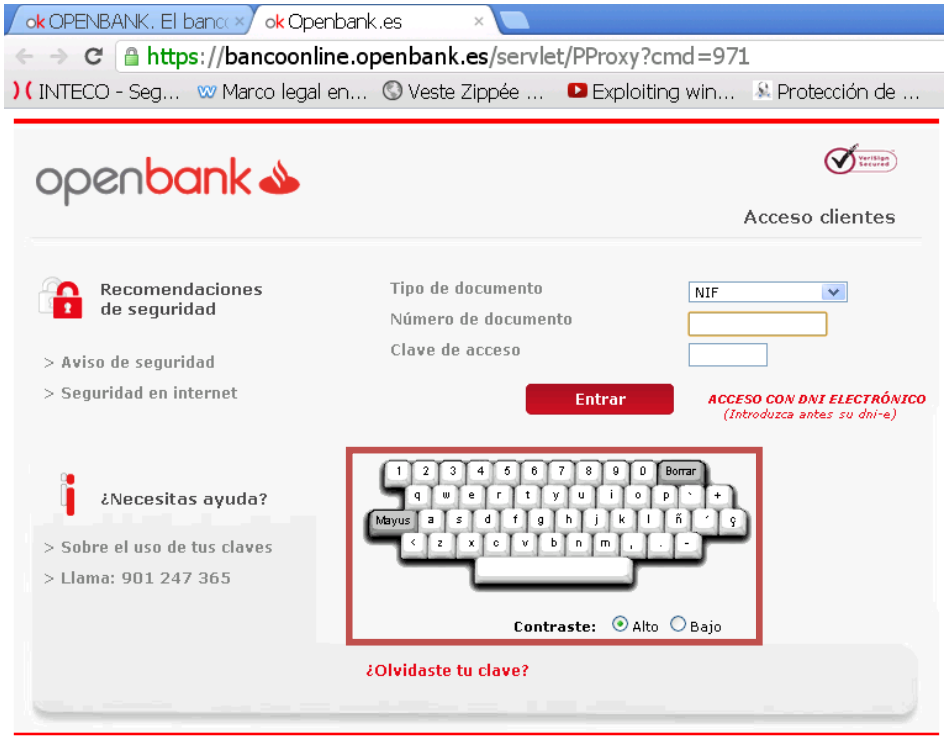


Ilustración 13: Teclado virtual para usuarios que quieran consultar sus datos bancarios

De esta forma, los creadores de troyanos bancarios, tras ver como se quedaban obsoletas sus anteriores técnicas, decidieron valerse de técnicas relacionadas con las capturas de pantalla.

Así, cada vez que se percibe una pulsación de ratón en una página de banca electrónica, se captura la imagen que sale por pantalla en el ordenador infectado, de tal forma que pueden recopilar mediante estas capturas la navegación completa a través de la web de la banca electrónica que el usuario ha hecho en el equipo infectado.

Además, se sabe que normalmente este tipo de malware envía sólo la región próxima al lugar donde se produjo la pulsación de ratón de forma automática, ya que el envío de la captura completa supondría una gran cantidad de megabytes a enviar. Algunos ejemplos de este tipo de capturas reducidas son los siguientes (la cruz roja indica el número que se pulsó con el ratón, recuadrado en marco rojo):

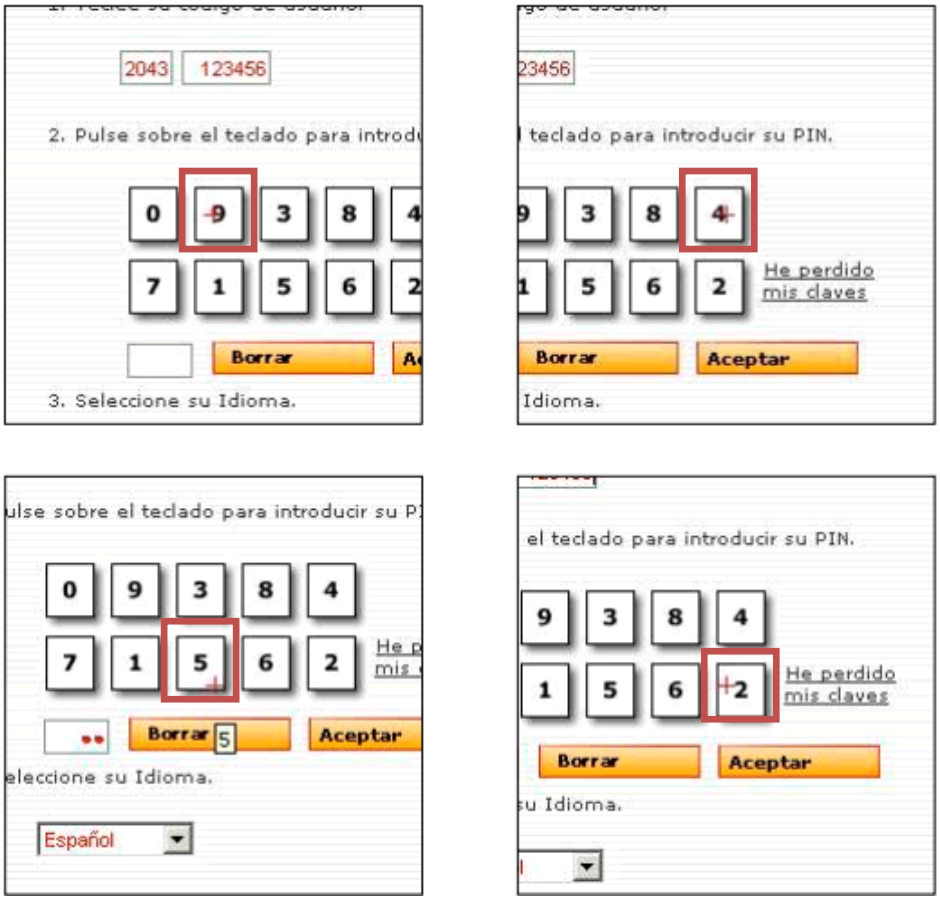


Ilustración 14: Captura que demuestra el radio de acción (recuadrado) de algunos capturadores

Para intentar protegerse de esta nueva amenaza, muchas entidades bancarias han implementado métodos alternativos para cambiar la apariencia de los números que aparecen por pantalla.

Por ejemplo, algunos bancos, a la hora de realizar el click de ratón para introducir el número secreto, muestran por pantalla asteriscos en el teclado, de tal forma que el usuario ve el teclado virtual de forma normal, y justo cuando pincha en la letra o el número, éste pasa a ser un asterisco. Otros bancos tienen otro sistema, en donde justo en el momento en el que el usuario pincha una tecla del teclado virtual, el teclado se desplaza ligeramente hacia otro lado de la pantalla. Esta es la opción que actualmente posee el banco electrónico Openbank:

Ilustración 15: Comparativa entre el antes y el después al pulsar una tecla del teclado virtual

Como se puede apreciar en las anteriores imágenes, el teclado se desplaza ligeramente, en este caso se desplaza hacia arriba y a la derecha. Esto resulta muy útil, pues si se realiza una captura de pantalla, el atacante va a obtener una región diferente de teclas a la que realmente ha pinchado el usuario.

Ante esta situación, los desarrolladores de códigos maliciosos decidieron atacar a través de grabaciones de vídeo.
Podemos ver un ejemplo de ello en la siguiente dirección web:

http://www.hispasec.com/laboratorio/troyano_video.htm

Como vemos, esto supone otro reto para las bancas electrónicas, las cuales han desarrollado otro tipo de protección específica para este tipo de ataques, basada en dar ciertos números de la clave ya rellenados (con salida por pantalla en forma de asteriscos), de tal manera que sólo piden cierta parte de la clave del usuario. Si, por ejemplo, la clave de un usuario es de 8 caracteres, pueden pedir al usuario, por ejemplo, 4 de ellos, y el resto venir ya rellenados, como muestra la siguiente imagen:

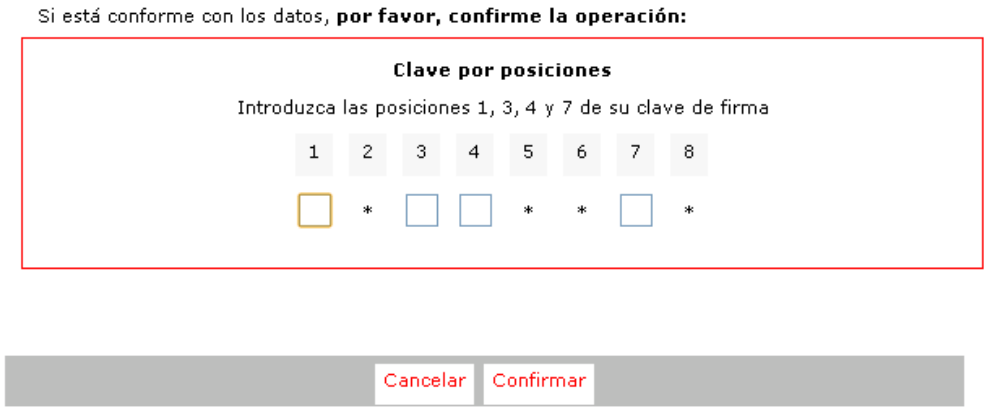


Ilustración 16: Captura de pantalla donde se requieren parte de los caracteres de la contraseña personal del usuario

Este método permite que, aun habiendo grabación de vídeo en un equipo infectado, este vídeo no va a poder sustraer la clave completa del usuario, ya que nunca se va a introducir entera. La única posibilidad para el atacante es esperar a que el usuario se conecte muchas veces desde el equipo infectado hasta rellenar en varias tandas todos los caracteres que conforman su clave. Por lo tanto, esta técnica dificulta en gran medida la posibilidad de robo de datos bancarios a los usuarios infectados.

4.1.2.8 Inyección de campos de formulario fraudulentos

Hoy en día, la mayor parte de las bancas electrónicas, aparte de requerir una contraseña para acceder a la cuenta de usuario y por tanto, a la información del dinero disponible en las cuentas, requieren una contraseña adicional para realizar cualquier tipo de transacción bancaria. Las más usadas son las denominadas tarjetas de coordenadas, que consisten en una tabla con una serie de números (normalmente más de 50), a los cuales se les asocia un código con una serie de dígitos. Un ejemplo de tarjeta de coordenadas sería el empleado por ING Direct actualmente:

Ilustración 17: Ejemplo de tarjeta de coordenadas de ING Direct

Como vemos, cada una de las posiciones tiene asociado un código. En el momento de realizar una transferencia o algún tipo de movimiento económico en una cuenta del banco, el usuario, que ya ha introducido anteriormente su clave personal para acceder a su cuenta, tendrá que introducir uno de los códigos asociados a un número. Es decir, en el ejemplo, si le piden el código 11, tendrá que introducir la secuencia "416":

Ilustración 18: Ejemplo de petición de una sola coordenada de la tarjeta anterior

Por lo tanto, a lo máximo que puede llegar un atacante sin poseer los datos de la tarjeta de coordenadas es a entrar a la cuenta bancaria pero sin poder realizar ningún tipo de movimiento o transacción. Por otro lado, para poder obtener los datos de la tarjeta de coordenadas, el troyano tendrá que espiar 50 transferencias diferentes para poder obtener los 50 códigos que conforman la tarjeta, lo que supone un tiempo muy elevado para

las bandas de crimen electrónico.

Ante esta situación, los atacantes optan por implementar páginas web falsas, que simulan el aspecto de la página inicial de una banca electrónica, pero donde requieren este tipo de información sensible del usuario, que no les es posible sustraer mediante los troyanos u otros códigos maliciosos, pretendiendo hacer creer al usuario que su banco es realmente el que está solicitándole esa información. Un ejemplo de esta práctica lo encontramos al comparar el acceso a una web de banca electrónica, con su copia por parte de los atacantes pidiendo un campo adicional "firma" cuyo contenido permite realizar transferencias desde la cuenta del usuario atacado:

Ilustración 19: Comparativa entre dos páginas web. La de la izquierda es legítima, pero la de la derecha no lo es, pidiendo además datos adicionales

4.1.2.9 Inyección de páginas fraudulentas

Es un método exactamente igual que el anterior, con la salvedad de que este tipo de métodos se basa en falsificar sitios web completos, incluyendo los certificados de seguridad de la entidad. La única diferencia con la web oficial es que en este caso, se van a pedir muchos más datos, como por ejemplo campos de tarjetas de coordenadas, o claves secundarias que restringen las transferencias.

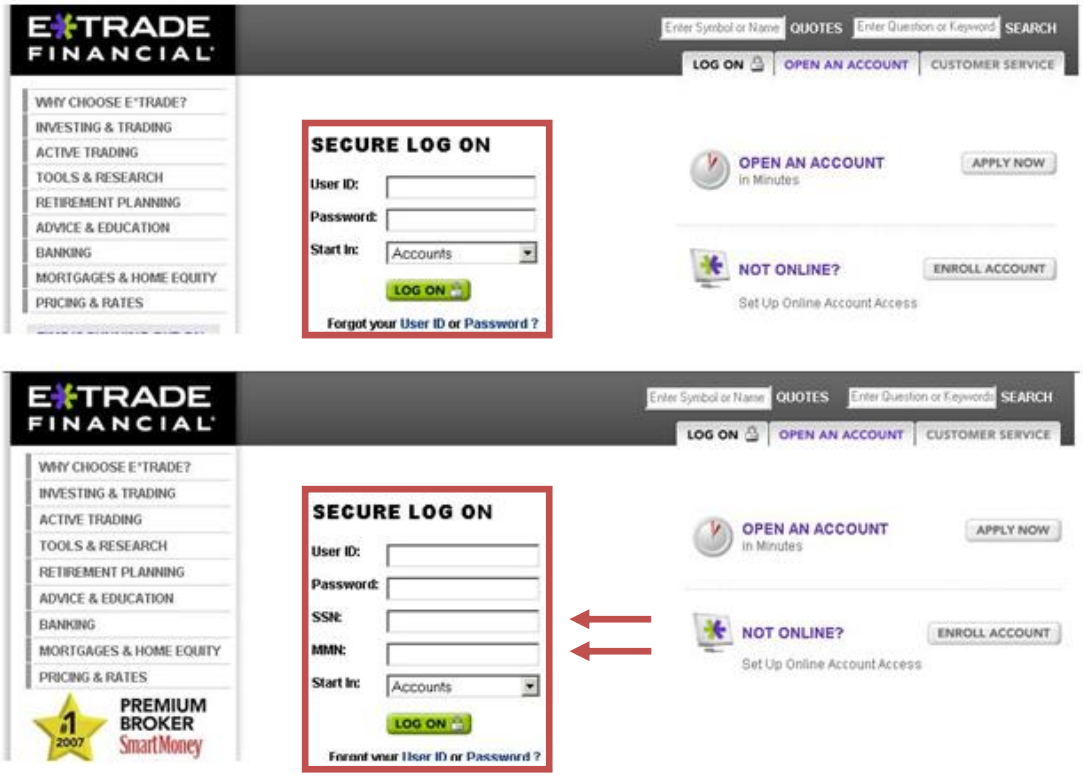


Ilustración 20: Comparativa entre dos páginas web, la primera lícita, y la segunda fraudulenta. En esta última se solicitan datos personales para el acceso del usuario.

4.1.2.10 Redirección de páginas bancarias (pharming)

Esta técnica se basa en falsear la resolución del DNS de algunas páginas, con el fin de redirigir a la víctima a una página idéntica a la que se esperaba encontrar en la web de su banco, pero que resulta ser fraudulenta.

Básicamente, cada vez que se introduce una dirección web en nuestro navegador (por ejemplo: http://www.ingdirect.es/), éste lo traduce a una dirección IP, de forma numérica (por ejemplo: 192.168.0.0). De ello se encargan los servidores DNS, en los cuales se almacenan tablas con las direcciones IP asociadas a cada nombre de dominio. Por lo tanto, el DNS transcribe nuestra petición en forma de texto a forma numérica (a una IP), que está asociada a una determinada dirección web. Por lo tanto, si introducimos http://www.ingdirect.es/ en el navegador, el DNS lo pasa a forma numérica, lo compara en una tabla, y nos envía a la página web asociada a esa IP numérica.

El pharming modifica las tablas numéricas que almacena el DNS, de tal forma que modifica la dirección IP a la que se ha de redirigir al usuario al introducir un determinado texto. Si el atacante modifica la dirección IP del DNS de un usuario, para que cuando éste introduzca en el navegador http://www.ingdirect.es/ le redirija a una página web fraudulenta, el usuario va a entrar a una página web fraudulenta introduciendo la dirección web oficial de su banco electrónico, de forma que el fraude que se comete es totalmente transparente al usuario atacado. La única posibilidad de darse cuenta del fraude es que, generalmente, en estas páginas falsas, el certificado de seguridad no es el legítimo de la entidad bancaria.

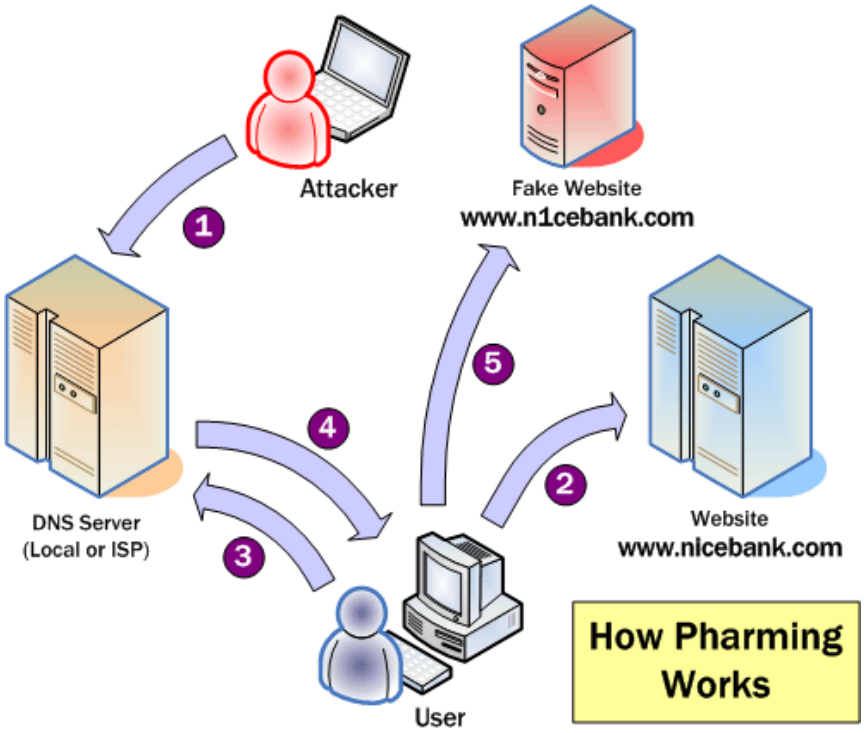


Ilustración 21: Esquema representativo del proceso conocido como "Pharming"

Para esta técnica no es necesario atacar directamente al DNS, sino a un fichero que es creado por defecto en cada ordenador, donde se almacena una pequeña tabla con nombres de servidores y direcciones IP, de manera que no haga falta acceder a los DNS para determinados nombres de servidor, o incluso para evitarlo. Los troyanos menos sofisticados simplemente modifican dicho archivo local para perpetrar el pharming. En adición, existen otros métodos más avanzados como atacar al propio enrutador de la víctima o redirigir todo su tráfico web hacia un servidor proxy que realice una

redirección hacia un servidor fraudulento al solicitar ciertas páginas bancarias legítimas.

- **Pasos para realizar pharming en un ordenador:**

1) Dirigirnos al fichero "hosts" del PC:

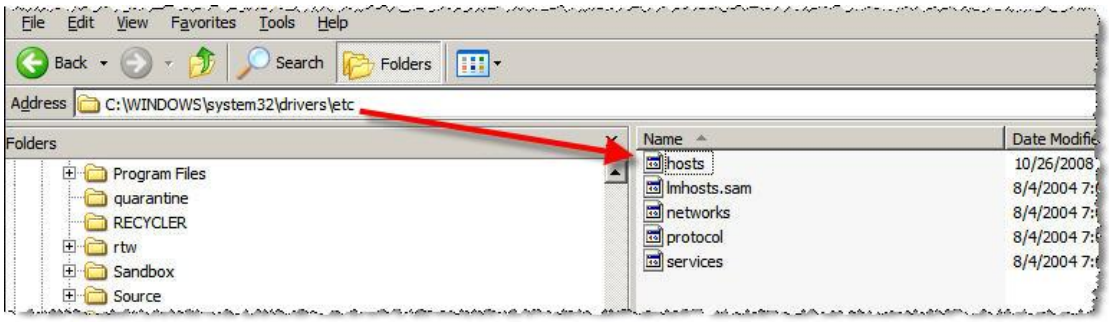


Ilustración 22: Paso 1 del proceso de pharming

2) Abrimos el fichero y vemos las direcciones alfanuméricas y sus IP asociadas:

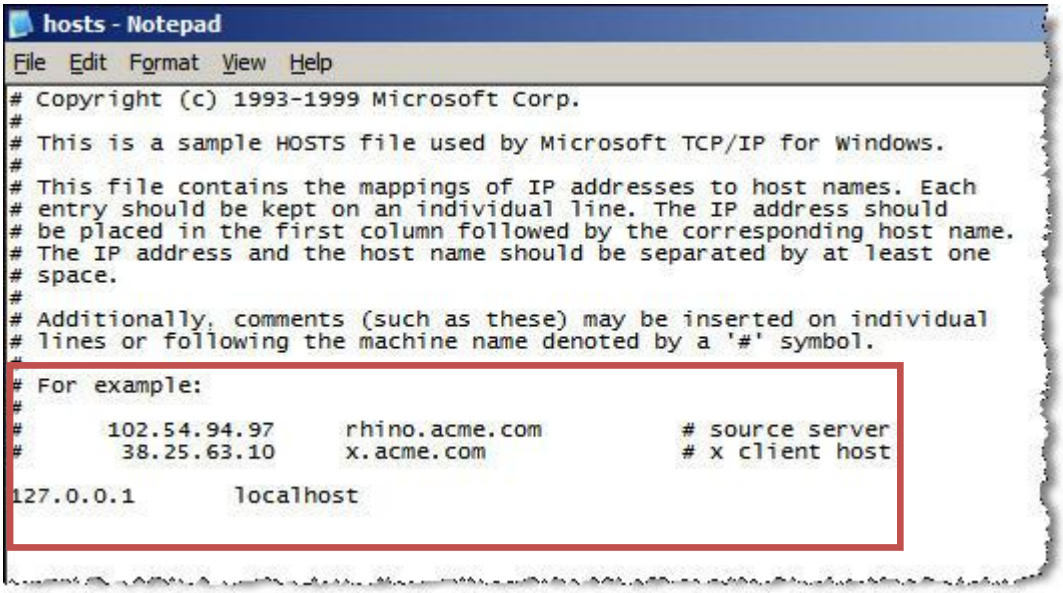


Ilustración 23: Paso 2 del proceso de pharming

3) Modificamos las direcciones IP para redirigirnos a otra página web diferente a la requerida por el usuario:

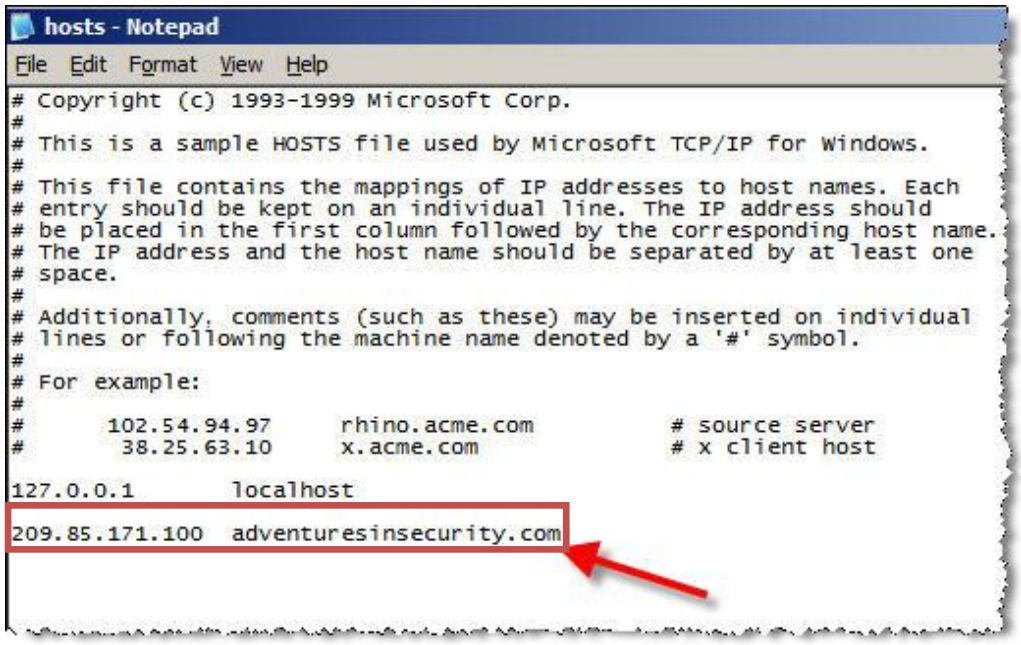


Ilustración 24: Paso 3 del proceso de Pharming

4) En este caso se ha modificado la dirección IP de la página http://wwww.adventuresinsecurity.com para redirigir al usuario a la página inicial de Google:

Ilustración 25: Paso 4 del proceso de pharming

Otro ejemplo, modificando el mismo fichero para que cuando el usuario introduzca la dirección web http://inteco.es/ se le redirija a la página web del ministerio de educación y ciencia:

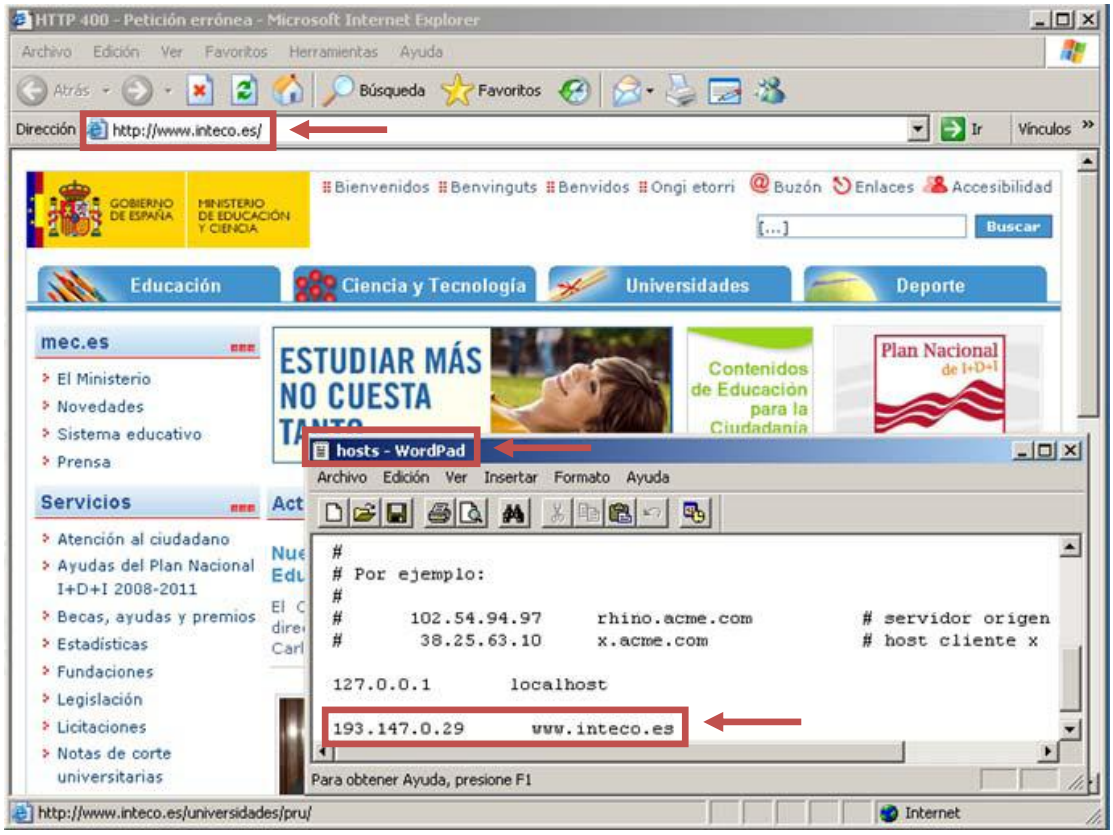


Ilustración 26: Ejemplo de página manipulada para ser re direccionada

4.1.3 Según las acciones que realizan

Siguiendo con la clasificación de los tipos de códigos maliciosos, pasaremos a enumerar aquellos clasificados por las acciones que realizan.

Existen varios tipos, por lo que es posible que exista malware que pertenezca a varios de ellos o conjunte varias acciones por su naturaleza, pudiendo pertenecer a varias de estas categorías a la vez. A continuación veremos los más relevantes:

4.1.3.1 Adware:

Software malicioso que al ejecutarse muestra publicidad de productos o servicios. Generalmente, la publicidad que se muestre no es aleatoria, sino que es enfocada expresamente a los gustos que se creen que tiene el usuario. Por ello, este software es relacionado frecuentemente con los espías, ya que para saber qué gustos, preferencias o hábitos de consumo posee un determinado usuario, previamente ha sido vigilado y se han recopilado datos sobre los sitios web que frecuenta, sus preferencias, etc. Toda esta información se envía a un servidor externo y en función de la

misma, el servidor envía una determinada publicidad personalizada y que se piensa que puede atraer con mayor facilidad al usuario. Generalmente este tipo de malware tiene funcionalidades que permiten mostrar la publicidad en ventanas emergentes, siendo especialmente molesto su visionado:

Ilustración 27: Captura de pantalla con multitud de adware

Estas aplicaciones también pueden instalar iconos gráficos en las barras de herramientas de los navegadores o en los clientes de correo, teniendo éstas una estructura que alberga palabras clave predefinidas, de forma que cuando el usuario realiza una búsqueda usando este tipo de aplicaciones, independientemente de la búsqueda que se realice el usuario será redirigido a páginas concretas y sitios web con publicidad.

Generalmente, estas aplicaciones son introducidas en los ordenadores estando ocultos en programas gratuitos, los cuales al aceptar sus condiciones de uso (casi siempre en inglés y que por norma general el usuario medio no se detiene a leerlas detenidamente) el usuario también está consintiendo que se muestre publicidad durante su uso. Algunos ejemplos de programas que incluyen adware pueden ser: Alexa, MyWebSearch, FlashGet, Cydoors, etc.

4.1.3.2 Spyware

Los spyware o "software espía" son programas que trabajan en la sombra recopilando datos sobre costumbres, gustos, preferencias y hábitos de consumo del usuario que utiliza el equipo infectado. Así, este tipo de software es la semilla inicial del anteriormente explicado "adware" ya que el spyware es la fuente que le proporciona los conocimientos necesarios acerca del usuario al adware, para poder realizar un envío masivo de publicidad personalizada al equipo infectado. En ocasiones, también esta recopilación de hábitos, gustos, costumbres, etc. se vende a empresas interesadas en saber los hábitos de consumo de las personas, ya sea para crear perfiles estadísticos de los hábitos de los internautas o para lanzar ataques personalizados al sujeto pasivo.

Así, en la siguiente imagen podemos ver dos ejemplos de envío de correos SPAM a una dirección de correo electrónico:

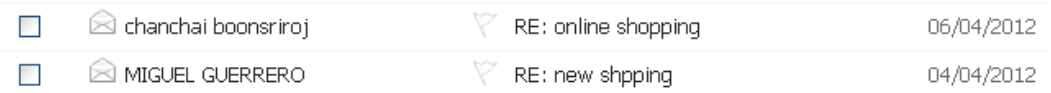


Ilustración 28: Entrada de correo electrónico desconocido a un usuario

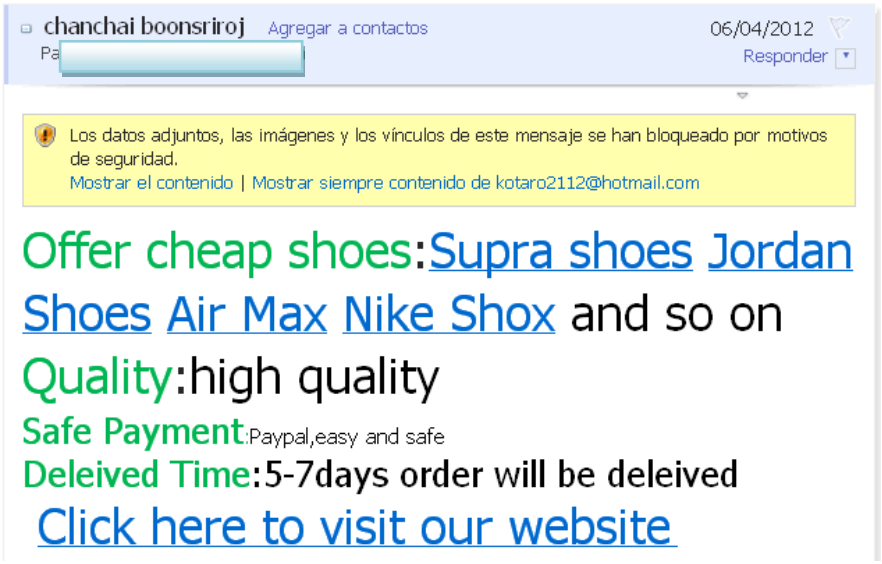


Ilustración 29: Al abrir el correo, sólo se obtiene el conocido SPAM

En el caso de la imagen anterior, el usuario que ha recibido el correo, nunca se ha puesto en contacto con las personas que le

envían el correo, ni siquiera ha visitado sus tiendas on-line, pero si ha navegado por otras de características parecidas, por lo que probablemente los atacantes tengan datos de sus hábitos de navegación y le manden información con actividades relacionadas a las que el usuario realiza habitualmente en la red.

4.1.3.3 Bloqueador

Impide la ejecución de determinados programas o aplicaciones, también puede bloquear el acceso a determinadas direcciones de Internet.

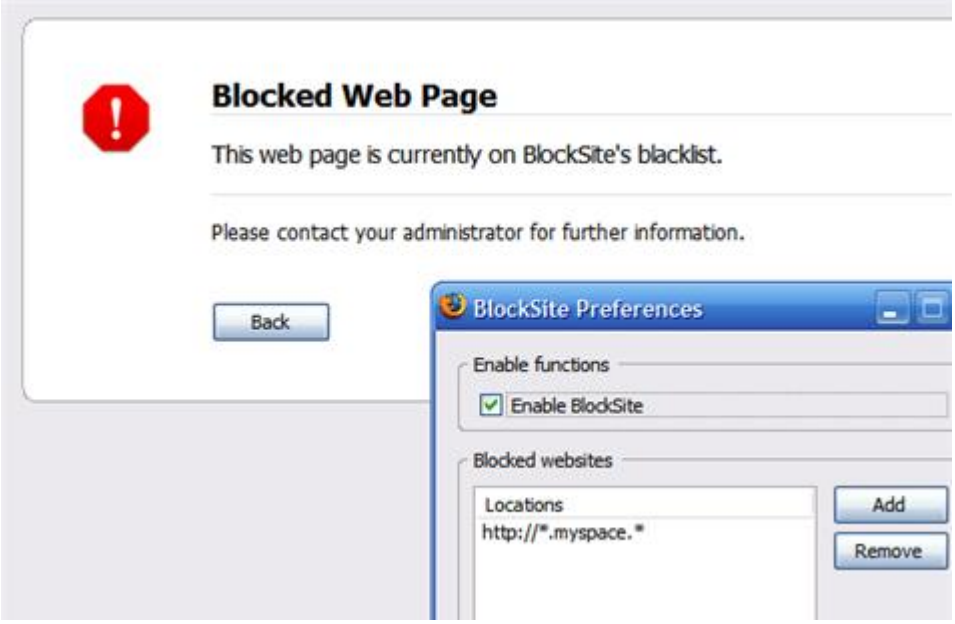


Ilustración 30: Captura de pantalla de un bloqueador en ejecución

Básicamente, este tipo de malware no permite la ejecución de determinados programas (frecuentemente antivirus y otros programas relacionados con la seguridad del sistema) para que resulte más difícil diagnosticar que el equipo ha sido infectado por algún tipo de malware. También puede bloquear cualquier tipo de acceso a información, como por ejemplo algunas direcciones web, para así evitar que el usuario infectado por ejemplo pueda consultar determinadas páginas web que expliquen cómo deshacerse del propio malware que infectó su sistema, o pueda descargar actualizaciones de antivirus que permitan eliminar este malware del sistema.

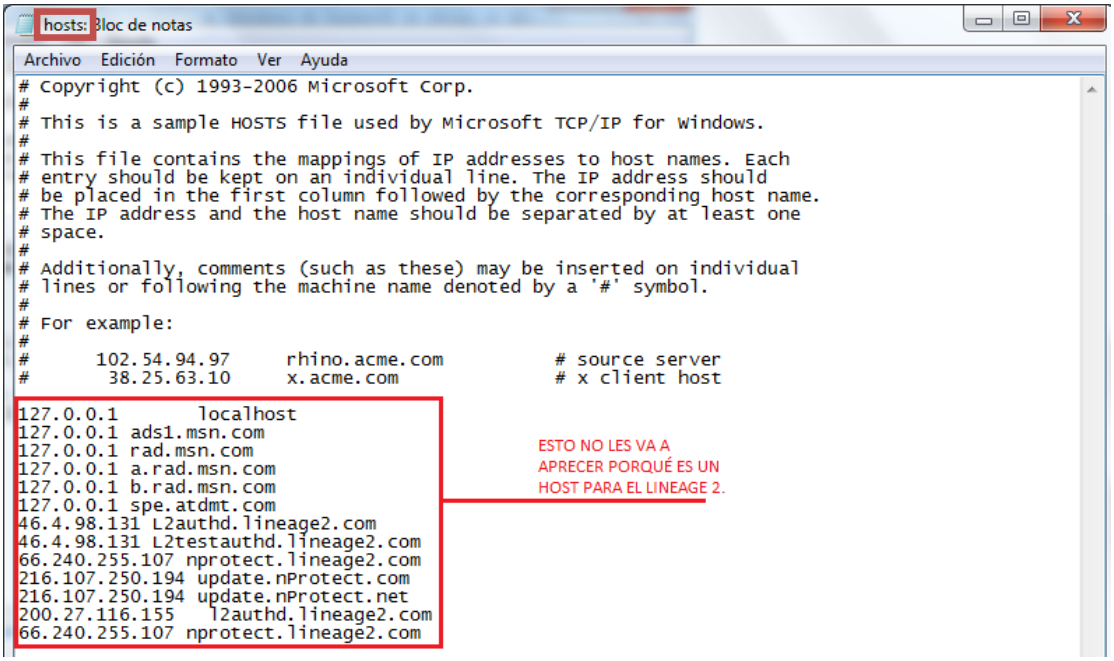


Ilustración 31: Modificación del fichero "host" para bloquear una dirección web

Para poder bloquear las páginas web de un usuario que use un sistema operativo “Windows”, a los atacantes les basta con lograr modificar un solo fichero (denominado “hosts”, como se puede ver en la imagen anterior).

Aparte de esta opción, existen multitud de programas que te permiten ir bloqueando el acceso a cada uno de los sitios web que vaya introduciendo el usuario, por lo que si el atacante tiene acceso a un equipo de un usuario, y puede modificar ficheros en el equipo infectado, le será muy fácil poder bloquear el contenido web que no le interese que el usuario acceda.

Ilustración 32: Captura de pantalla de software que bloquea automáticamente direcciones web

4.1.3.4 Bomba lógica

Es un tipo de malware que tiene como característica principal que el comienzo de sus actividades maliciosas viene dado por una determinada fecha u hora, por lo que no actúa inmediatamente después de haberse infiltrado en el sistema, sino que lo hará tiempo después, lo cual hace que sea mucho más difícil su detección por parte del usuario.

Ilustración 33: Bomba lógica con una "cuenta atrás" para el comienzo de su ejecución

Su uso más reconocido son los ataques de denegación de servicio. El funcionamiento de la bomba lógica tiene un primer estado en el que se introduce de manera silenciosa en un sistema informático y permanece en él sin realizar ningún tipo de actividad. Las bombas lógicas comenzarán sus actividades maliciosas cuando venza la condición impuesta para que comience a actuar (generalmente una fecha determinada o una acción concreta del sistema infectado) y es entonces cuando el usuario sufre las consecuencias de un malware que puede haber residido durante meses inoperativo en su sistema sin que el éste sospechara nada.

Como el resto de malware, el objetivo final siempre es dañar al sistema o datos, aunque este tipo de malware también se puede emplear para actividades totalmente legales y comunes como ordenar pagos, realizar transferencias de fondos, etc.

Este tipo de malware es sumamente fácil de realizar, por lo que se erige como uno de los malware más comunes. De hecho, cualquier usuario puede crear uno, simplemente se ha de crear un pequeño programa como el que se ve a continuación:

```
00 @echo off
01 msg * Mi primera Bomba
02 echo.
03 taskkill /F /IM explorer.exe
04 echo.
05 start www.coecys.com
06 echo.
07 exit
```

Ilustración 34: Ejemplo de código para crear una bomba lógica

Al ejecutar el programa, se mostrará en pantalla el mensaje "Mi primera bomba", luego se cerrará el proceso de Explorer y se abrirá la página www.coecys.com

Así, el autor, una vez ha creado el fichero, tratará de difundirlo por la red, o introducirlo en determinados equipos informáticos si lo que busca es un ataque específico contra datos concretos.

En este ejemplo, se ha expuesto un fichero que no es dañino para el equipo, pero normalmente las bombas lógicas borran ficheros, o

sustraen información sensible del equipo infectado, etc. como podemos ver en los siguientes ejemplos:

- **Caso Real: Un empleado descontento coloca una bomba lógica SiliconValley (19 diciembre 2002)**

Un ex-empleado de la compañía "UBS PaineWebber", descontento tras su cese, introdujo una bomba lógica en el sistema informático de la empresa, causando unas pérdidas a la misma valoradas en 3 millones de dólares.

La bomba lógica afectó a cerca de 1.000 ordenadores -de los 1.500 que integran la red de sucursales de UBS PaineWebber en Estados Unidos-, eliminando y dañando archivos.

El objetivo del empleado era provocar con esta acción una considerable caída de las acciones de la empresa, para poder beneficiarse económicamente de ello, pero finalmente esto no ocurrió y el ex-empleado fue descubierto y puesto a disposición judicial.

Tras las investigaciones realizadas, se descubrió que el empleado había dejado de prestar sus servicios a la empresa tan sólo 10 días antes, y mientras estuvo en ella se había quejado múltiples veces sobre el salario y las primas que percibía. Finalmente, fue acusado federalmente por fraude de la seguridad y en la conexión con los ordenadores, pidiéndole la justicia hasta 10 años en prisión por cada uno de los cargos imputados, y una sanción económica que podía alcanzar hasta 1 millón de dólares por fraude a la seguridad y de 250.000 dólares por fraude informático.

Como se observa en esta noticia, es común que los ex empleados perpetren ataques a los sistemas informáticos que hasta hace pocos días gestionaban, y suponen una amenaza muy importante para la seguridad de las compañías ya que nadie mejor que ellos mismos puede saber dónde y cómo se puede atacar un sistema de forma efectiva, ya que son ellos mismos los que los dirigían. También se puede sacar otra conclusión, y son las fuertes multas y castigos que establecen legislaciones como la estadounidense, muy avanzadas en leyes para el tratamiento de las nuevas tecnologías.

- **Caso Real: Una bomba lógica en FannieMae deja a la empresa parada una semana (17 febrero 2009)**

Un ex ingeniero de la empresa "Fannie Mae", despedido en Octubre de 2008, atacó mediante una bomba lógica el sistema informático de la empresa, centrando el ataque en los 4000 servidores de la empresa y teniendo unas terribles consecuencias para la empresa, que se vio obligada a cerrar durante una semana para poder subsanar el problema.

El infractor creó un script[21] en el servidor central de la compañía (para ello, el ex empleado separó el código mediante una serie de saltos de línea para poder ocultarlo entre el software legítimo), y lo mantuvo en espera durante un tiempo para que no se le pudiera relacionar su despido con el malware de una forma clara y directa.

Finalmente, la investigación del FBI otorgó la autoría del malware al ex empleado, ya que pudieron seguir varias pistas como que éste mantuvo sus privilegios en el sistema hasta un día después de ser despedido y se demostró que en ese tiempo fue cuando logró introducir el malware en el sistema. Aparentemente por "razones burocráticas" pudo haber mantenido esos permisos en la Intranet de la empresa.

En la investigación, se descubrió el enorme daño que se había generado en los servidores de la empresa por el script creado por el infractor, el cual deshabilitaba el login a los servidores en producción para toda la empresa, modificaba el password de root, rescribía información (incluidos los backups[22]) y generaba una denegación de servicio en un software de alta criticidad. Además, se replicaba automáticamente en el resto de los servidores.

Este tipo de hechos, demuestran una vez más la criticidad de los ataques perpetrados por personal interno de la organización, más específicamente por personal con acceso administrativo a los servidores y conocimientos informáticos.

4.1.3.5 Broma (Joke)

Es un tipo de malware que a priori resulta inofensivo, ya que en su naturaleza no está el realizar acciones perversas o en contra de cualquier equipo o sistema informático, sino que simplemente se intenta hacer creer a la víctima que ha sido objeto de algún tipo de malware o que si equipo está infectado. En general, se intentan transmitir a través de la ingeniería social y suelen ser bromas que realizan los usuarios entre sí, pero en ocasiones la víctima puede acabar realizando acciones que no son necesarias (por ejemplo formateo del ordenador personal) simplemente por prevención porque realmente cree que su equipo está infectado, cuando en realidad su equipo no ha estado amenazado en ningún momento.

- **Caso real: Virus que apaga el equipo informático del usuario**

1) Se crea un nuevo acceso directo en el escritorio del equipo a infectar.

2) En la ventana que aparece para crear un nuevo acceso directo, se escribe lo siguiente:

shutdown -s -t 60 -c "Virus detectado, la computadora se apagará automáticamente"

Ilustración 35: Proceso de creación de malware para apagar un sistema informático

3) Se nombra a este acceso directo como Internet Explorer.

4) Se crea un icono nuevo en el escritorio del usuario, adoptando la misma imagen que el de "Internet Explorer" y se elimina el original.

5) Ahora, cada vez que el usuario intente ejecutar Internet Explorer le aparecerá el siguiente mensaje:

Ilustración 36: Mensaje final de apagado del sistema

Como se observa, resulta muy fácil realizar este tipo de acciones inofensivas, pero un malware de este tipo puede requerir al usuario que elimine ficheros importantes de su equipo informático, de tal forma que, lo que en principio resultaba una broma inofensiva para un usuario, puede acabar perjudicando al normal funcionamiento del equipo.

4.1.3.6 Bulo (Hoax)

Los hoaxes o bulos, es un tipo de malware basado en la generación de noticias falsas con la intención de hacer creer a los usuarios algo que es falso. Generalmente se distribuyen a través del envío de correos electrónico que se distribuyen en cadena. Cabe destacar el aumento de este tipo de malware en redes sociales como Facebook o Tuenti (a través de la creación de eventos), en detrimento de los servidores de correo usuales.

El contenido de estos mensajes engañosos suele tener temáticas populares como noticias inventadas, alertas inexistentes, etc. con el objetivo de llamar la atención del usuario. Posteriormente se suele solicitar que ese propio correo recibido se reenvíe a un determinado

número de usuarios. En general, no representan ningún problema o amenaza real más allá de la generación de una alarma innecesaria, y del tiempo que les usuarios desperdician con este tipo de correos, aunque dependiendo de las acciones que se soliciten en el mismo, estos correos pueden tornarse en una seria amenaza para el usuario si decide hacer caso de los mismos.

Los ejemplos más conocidos de este tipo de malware tratan sobre la posibilidad de hacerte millonario con sólo reenviar el mensaje o que apelan a la sensibilidad invocando supuestos niños enfermos. También es común el envío de mensajes pidiendo que se cree una cadena de mensajes entre los usuarios que reciben el correo electrónico, asegurando que si el usuario no realiza esa acción le pasará cualquier tipo de desgracia.

A priori, no existe ningún objetivo claro en quienes crean este tipo de malware, pero se han detectado casos donde las personas que crean este tipo de correos desean alguno de los siguientes objetivos:

- Captar direcciones de correo (para mandar spam, virus, mensajes con phishing o más bulo a gran escala)

- Intentar engañar al destinatario para que revele su contraseña o acepte un archivo de malware.

- Confundir a la opinión pública de la sociedad

Algunos detalles sobre los hoaxes

Características	Objetivos	Consecuencias
■ No tienen **firma.** ■ Algunos invocan los nombres de **grandes compañías.** ■ Piden al receptor que lo **envíe a todos sus contactos.** ■ Te amenazan con **grandes desgracias** si no lo reenviás.	■ **Conseguir direcciones** de mail. ■ Congestionar los **servidores.** ■ Alimentar el **ego del autor.**	■ Hacen **perder tiempo y dinero** al receptor. ■ Congestionan los **servidores.** ■ Nos llenan de **publicidad y basura.** ■ Hacen **perder valor** a cadenas creadas por gente que realmente lo necesita.

Ilustración 37: Tabla-resumen de las características de los hoax

- **Ejemplo de Hoax:**

Ilustración 38: Ejemplo de hoax

- **La realidad sobre los Hoax:**

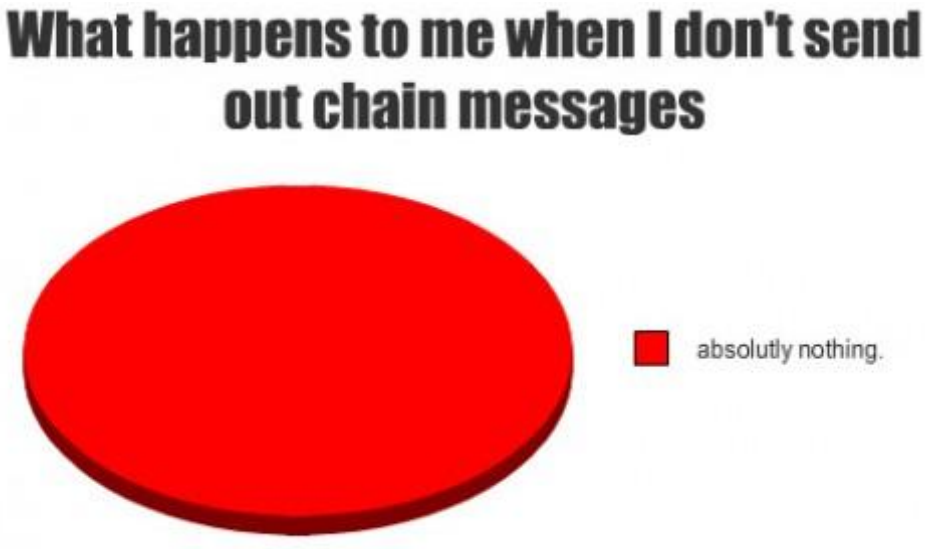


Ilustración 39: Gráfico sobre las consecuencias de no enviar mensajes en cadena y demás bulos

4.1.3.7 Clicker

Malware basado en re direccionar las páginas web a las que quiere acceder un usuario desde su sistema, de tal forma que se le encamine hacia páginas web diferentes, con objetivos tan variados como realizar ataques de Denegación de Servicio a una página víctima o engañar al usuario sobre la página que está visitando, por ejemplo, creyendo que está accediendo a una página legítima de un banco cuando en realidad está accediendo a una dirección falsa.

- **Ejemplo de Clicker Troyano: Trojan-Clicker.Win32.VB.b**

I. Detalles Técnicos

Programa troyano cuyo funcionamiento se basa en abrir páginas web a través del navegador Internet Explorer sin que el usuario se cerciore de ello.

II. Instalación

Al ejecutarse, el troyano copia su cuerpo al siguiente directorio bajo el nombre "EXEC.exe”:

%System%\VMM32\AUTOEXEC\EXEC.exe

Para poder realizar un inicio de forma automática cada vez que se arranque el sistema informático, el malware añade un enlace a un

fichero ejecutable de tal forma que siempre se inicie el malware toda vez que se arranque el sistema operativo:

[HKLM\Software\Microsoft\Windows\CurrentVersion\Run]

"AUTOEXEC" = "%System%\VMM32\AUTOEXEC\EXEC.exe

III. Daños

El troyano envía una solicitud al sitio:

*http://www.angelfire.com/geek/bestjavascripts/v/***.rld*

A través de esta página web el malware comenzará a abrir determinadas ventanas emergentes sin que el usuario del sistema infectado lo haya requerido o sea consciente de ello.

IV. Instrucciones de eliminación

1) Eliminar el archivo original del troyano (la ubicación del mismo puede depender de la forma en que se ha infectado el sistema informático, por lo que el usuario deberá ser el responsable de encontrarlo dentro de su propio sistema de archivos.)
2) Eliminar los ficheros creados por el troyano:

%System%\VMM32\AUTOEXEC\EXEC.exe

3) Eliminar el siguiente parámetro de la llave del registro:

[HKLM\Software\Microsoft\Windows\CurrentVersion\Run]

"AUTOEXEC" = "%System%\VMM32\AUTOEXEC\EXEC.exe hidden"

4) Realizar un exhaustivo análisis del sistema informático infectado por medio de un antivirus.

4.1.3.8 Criptovirus (ransomware)

Los criptovirus son un tipo de malware cuya técnica se basa en introducirse en un equipo informático y hacer que determinados ficheros (normalmente ficheros importantes para el funcionamiento

del sistema, o ficheros con los que el usuario trabaje normalmente) sean inaccesibles para el usuario atacado, generalmente cifrando estos ficheros, de forma que siguen existiendo éstos en el equipo infectado, sin estar corruptos, pero que sólo se podrán volver a usar si se descifran correctamente.

Tras esto, el atacante coacciona al usuario a pagar un "rescate" para poder acceder a la información cifrada.

Generalmente el pago se indica a través de un depósito bancario, y tras haber pagado la cantidad indicada el usuario víctima, el atacante le proporciona la contraseña que libera la información del disco duro.

En las primeras ocasiones que se usó este tipo de malware, los métodos de cifrado no eran demasiado sofisticados, por lo que el propio usuario podía descifrar el contenido bloqueado y recuperarlo sin necesidad alguna de pagar ningún tipo de rescate al infractor, pero a medida que los infractores han ido refinando y perfeccionando sus técnicas, los usuarios se han visto incapaces de poder recuperar la información bloqueada, de forma que este tipo de malware ha ido creciendo conforme han ido evolucionando las técnicas de cifrado, y actualmente representa una seria amenaza a los usuarios de cualquier sistema informático.

Los orígenes de este tipo de malware se remontan al año 1989, cuando fueron enviados unos diskettes a empresas farmacéuticas, los cuales supuestamente contenían información respecto al VIH, pero que al ejecutar los archivos que contenían se producían los efectos del ataque: ciertos archivos de cada uno de los ordenadores en donde fue introducido alguno de los diskettes repartidos fueron cifrados, y la víctima podía observar una serie de instrucciones y requerimientos para recuperar sus datos, que incluían la entrega de dinero al atacante.

El principal método, no para evitar ser víctima de este tipo de malware, pero si para minimizar sus daños, es la realización de backups de forma periódica con los datos más importantes para el usuario que contenga el ordenador.

Otra opción es alojar los datos más importantes en espacios de almacenamiento en la red, como puede ser en la famosa plataforma "Dropbox"[23], o la utilización de discos RAID[24] para poder replicar cualquier tipo de información que se almacene en el equipo, de forma que se pueda recuperar posteriormente por medio de un disco duro replicante, en caso de que se haya "secuestrado" la información en alguno de los discos de almacenamiento.

- **Ejemplo de Criptovirus:**

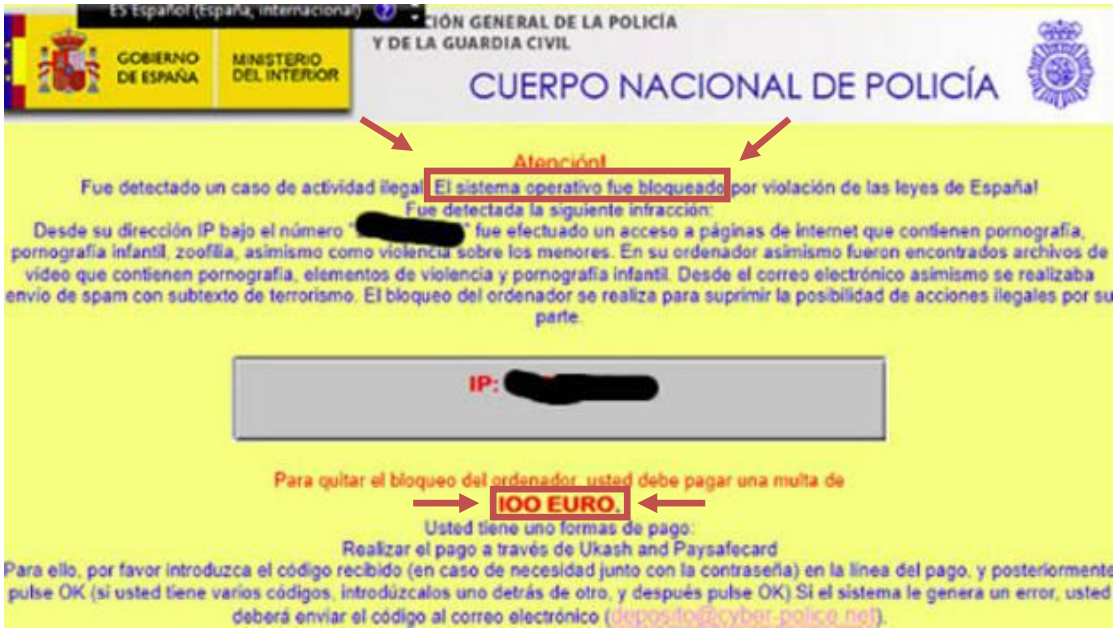


Ilustración 40: Criptovirus famoso conocido popularmente como "Virus de la policía"

Como se puede observar en la ilustración anterior, el mensaje indica que el sistema operativo (en este caso al completo y no sólo unos ficheros) ha sido bloqueado, y se deberán abonar 100 euros para poder desbloquearlo.

Este es uno más de los múltiples ejemplos de criptovirus hallados en la red, aunque este en concreto, ha llegado a tener tal nivel de propagación en los primeros meses de 2012, que la propia policía ha denunciado a través de su página web oficial este tipo de ataque y ha publicado una serie de instrucciones para poder eliminarlo, dada la gran difusión del mismo.

4.1.3.9 Descargador (Downloader)

Tipo de código malicioso que tiene como misión principal descargar otros programas (generalmente también maliciosos) en el ordenador infectado.

Normalmente, los descargadores son los primeros programas que se infiltran en los sistemas informáticos, para, a través de ellos, poder introducir otros más dañinos posteriormente.

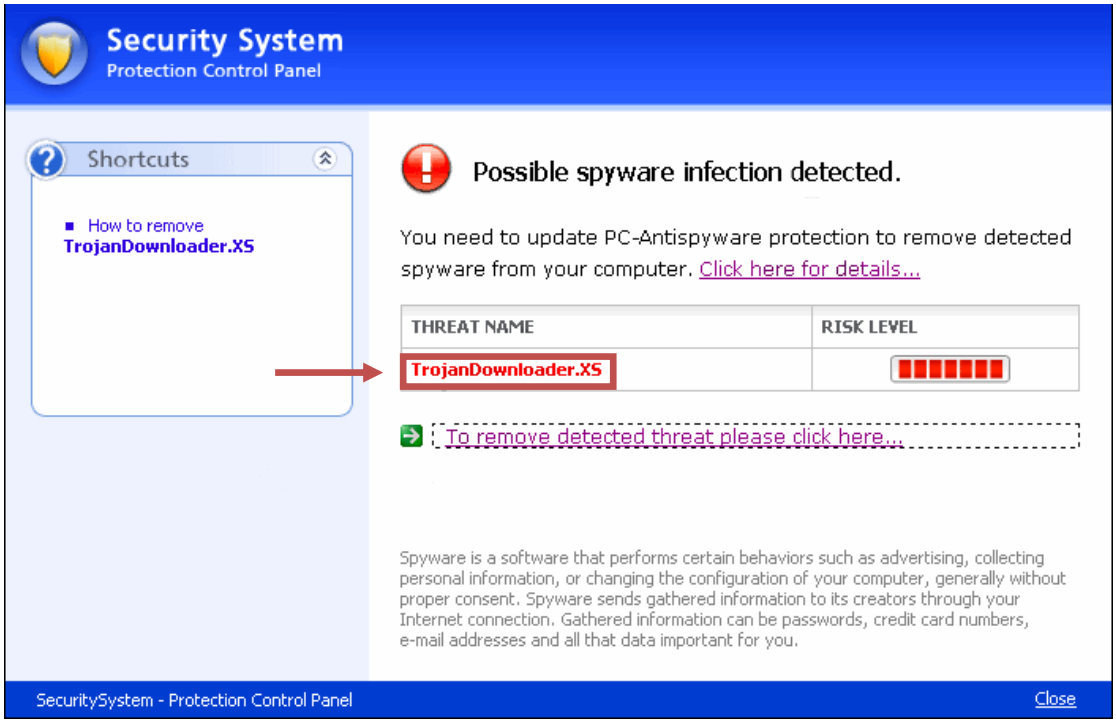


Ilustración 41: Pantalla de aviso alertando de la presencia de malware, en este caso de un Downloader

Este tipo de malware ha sido originado debido a las nuevas estrategias que emplean los infractores para poder adentrarse con más facilidad en los sistemas informáticos. Antes, los atacantes creaban un solo malware que se introducía en el sistema y él mismo generaba las acciones dañinas. Actualmente, los infractores están siguiendo técnicas más sofisticadas donde en lugar de crear un solo programa malicioso, crean varias tipos de malware, cada uno con una función determinada, para poder ir perpetrando sus acciones de una manera más cómoda. Así, los descargadores son el primer paso, ya que simplemente se cuelan en el sistema para poder permitir la posterior entrada en el mismo de otros programas más dañinos, es decir, este malware sería el primer elemento de un proceso que acabaría permitiendo insertar un malware en el sistema mucho más peligroso que el propio descargador en sí. Una de las mayores ventajas para el infractor al usar este tipo de malware, es

que es reutilizable, y una vez dentro del sistema infectado, el atacante puede introducir todo el malware que desee en el sistema de la víctima con mucha más facilidad.

Las características principales de los downloaders son:

- Tamaño reducido, código sencillo.
- Suelen estar cifrado para intentar eludir a los antivirus.
- Se aprovechan de ciertas vulnerabilidades de los sistemas informáticos para poder adentrarse en ellos.
- Instalan otras amenazas usando técnicas de rootkits (definido más adelante en este mismo capítulo del documento).

4.1.3.10 Exploit

Código que utiliza una vulnerabilidad del sistema o de algún punto en concreto de éste para aprovechar esta deficiencia e introducirse en un sistema sin estar autorizado.

El programa que explota la vulnerabilidad no es un código malicioso en sí mismo, pero, como en el caso anterior, es la puerta de inicio al envío de códigos maliciosos posteriores que representen amenazas reales para el sistema. También son utilizados para simplemente obtener un acceso a un equipo no autorizado, aún sin tener como finalidad el infectarlo con algún malware posteriormente.

Se conoce como "Zero Day" a los exploits que describen vulnerabilidades de la seguridad que no son conocidas por los propios profesionales del campo, o por los propios desarrolladores de los programas, y que aún no ha sido solventado por un parche del vendedor que comercializa el producto.

- **Caso real: Descubiertos dos casos de uso de debilidades en programas informáticos para campañas de envío de malware por todo el mundo.**

En febrero de 2012 se han descubierto dos nuevos casos de clientes que se aprovechan de las debilidades en diferentes programas informáticos, las cuales han sido empleadas para lanzar ataques masivos de malware. Lo peculiar de estos ataques, es que las primeras investigaciones han concluido que provienen de la misma persona.

Actualmente, el número de equipos infectados asciende a más de 20.000 alrededor de todo el mundo. Podemos verlo en el siguiente cuadro resumen:

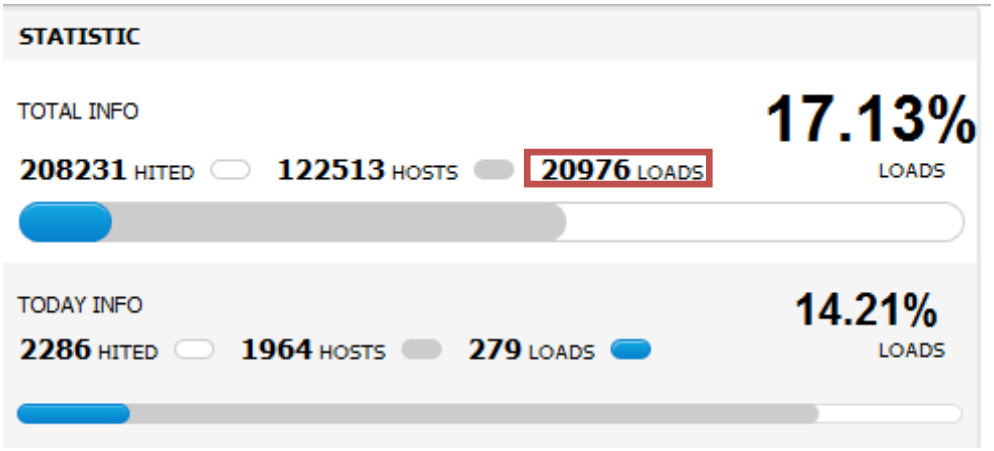


Ilustración 42: Número de cargas de malware conocido como "exploit"

Los programas donde se han encontrado debilidades han sido los siguientes:

EXPLOITS	LOADS	% ↑
Java Rhino	17530	82.63
Windows 7	10331	58.66
Windows XP	4195	23.82
Windows Vista	2994	17.00
Windows 2003	74	0.42
Windows 2000	12	0.07
Windows NT	5	0.03
Linux	1	0.01
PDF LIBTIFF	3163	14.91
Windows Vista	1775	56.03
Windows 7	742	23.42
Windows XP	637	20.11
Windows 2003	14	0.44
PDF ALL	375	1.77
Windows XP	322	85.87
Windows Vista	45	12.00
Windows 7	7	1.87
Windows 2003	1	0.27
FLASH	70	0.33
Windows XP	67	95.71
Windows 2003	2	2.86
Windows 2000	1	1.43
HCP	29	0.14
Windows XP	28	96.55
Windows Vista	1	3.45

Ilustración 43: Lista de programas con debilidades detectadas

Y la clasificación según el sistema operativo infectado es:

OS	HITS	HOSTS	LOADS ↑	%
Windows 7	122354	73373	11052	15.06
Windows XP	44958	26489	5197	19.64
Windows Vista	39916	23830	4739	19.89
Windows 2003	688	318	91	28.71
Windows 2000	220	119	14	11.86
Windows NT	52	31	5	16.13
Linux	20	15	1	7.14
Windows 98	21	8	0	0.00
Mac OS	2	2	0	0.00

Ilustración 44: Clasificación de exploits según el sistema operativo

Los datos de equipos infectados según su navegador son:

BROWSERS ↓	HITS	HOSTS	LOADS	%
Chrome ›	76	38	2	5.26
Firefox ›	72824	45692	9259	20.27
MSIE ›	133375	77131	11648	15.10
Mozilla ›	388	183	20	10.99
Opera ›	1566	760	131	17.24
Safari ›	2	2	0	0.00

Ilustración 45: Clasificación de sistemas infectados, según el navegador usado

Los datos por número de equipos infectados por país son:

COUNTRIES	HITS	HOSTS ↑	LOADS	%
United States	205420	121814	20815	17.09
Canada	323	183	48	26.23
United Kingdom	91	72	16	22.54
Germany	196	62	11	17.74
Anonymous Proxy	75	47	9	19.15
Russian Federation	120	37	14	37.84
Poland	37	29	8	28.57
Other country	40	22	4	18.18
Croatia	19	18	6	33.33
France	51	15	3	21.43

Ilustración 46: Clasificación de los equipos infectados según el país

Siendo pertenecientes todos los datos mostrados anteriormente para uno sólo de los dos clientes que lanzan malware aprovechando los diferentes exploits encontrados.

Por lo tanto, se ha de ser consciente de la amenaza que supone este tipo de debilidades en los programas y códigos que se emplean habitualmente en los sistemas informáticos, y su no reparación o solución mediante actualizaciones o parches.

4.1.3.11 Herramienta de fraude

Malware que simula un comportamiento extraño o inusual en el sistema, con el objetivo de crear confusión en el usuario y hacerle pensar que su equipo está infectado por algún malware potencialmente peligroso. En ese momento es cuando estas herramientas de fraude sugieren la compra de algún programa de pago para solucionar el problema, cuando el problema real se trata de la propia herramienta que está sugiriendo las compras de productos informáticos.

- **Caso Real: Microsoft Security Essentials Alert**

Microsoft Security Essentials Alert es un código malicioso, denominado como "falso antivirus". Este malware intenta hacerse

pasar por un antivirus legítimo para intentar confundir a los usuarios y hacerle creer que su equipo está infectado, sugiriendo una serie de programas al mismo, y asegurando que al adquirir esos programas los supuestos problemas que está sufriendo el equipo en esos momentos se verán resueltos de inmediato.

Para dar una mayor credibilidad a la alerta generada, generalmente este tipo de antivirus ilegítimos utilizan técnicas de ingeniería social para tratar de convencer al usuario de que realmente su equipo se encuentra ante un gran peligro, creando falsas alarmas generando ventanas emergentes o publicidad aleatoria que tendrán como objetivo mostrar comportamientos anómalos en el sistema para que el usuario se apresure a adquirir las soluciones informáticas que el propio antivirus falso le sugiere.

Para poder permanecer en el sistema sin ser detectado como malware por un antivirus legítimo, el antivirus falso anula toda la seguridad del equipo infectado y restringe el uso de varias aplicaciones del sistema, tras esto comienza a emitir pantallas acerca de la detección de supuestas amenazas para el sistema:

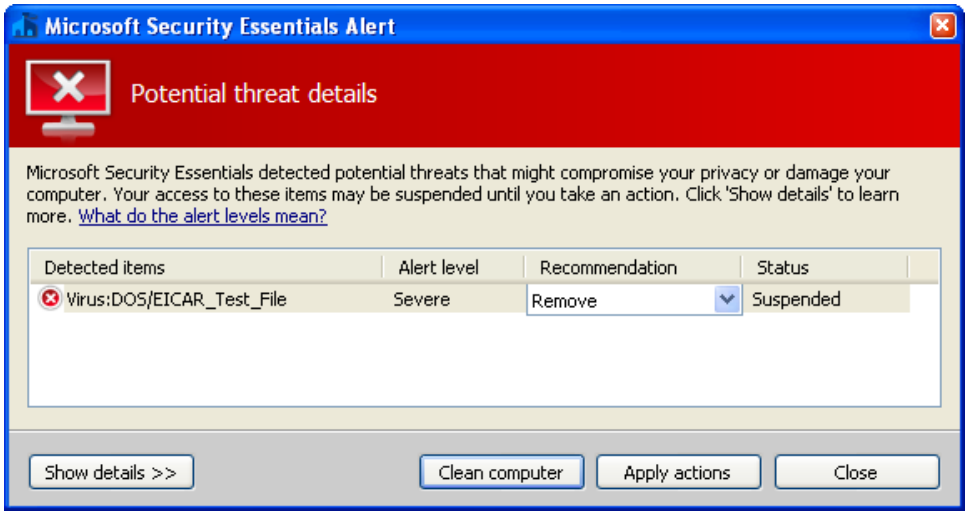


Ilustración 47: Falsa detección de amenaza en el sistema

Adjuntado a su vez una pantalla con una serie de software que sugiere descargar para poder eliminar todas las amenazas que supuestamente asolan al sistema:

Ilustración 48: Conjunto de soluciones recomendadas por el falso antivirus a raíz de la falsa alarma

Si el usuario no detecta que todas las amenazas creadas son irreales (ya que en realidad la única amenaza sería el falso antivirus) y finalmente decide adquirir los programas sugeridos, se le pedirá una cantidad de dinero por la descargar de cada uno de los supuestos programas que arreglarán su computadora. Si accede a ello y paga, el propio malware mostrará una pantalla en donde se simulará la descarga de los mismos (aunque en realidad no se esté descargando nada) y finalmente le comunicará al usuario que todas las incidencias y amenazas han sido subsanadas de forma exitosa. Así, el usuario quedará contento pues ha evitado el supuesto peligro que se cernía sobre su sistema informático, aunque en realidad sólo habrá sido objeto de un fraude donde el infractor habrá recibido dinero por simular una amenaza en el sistema infectado. Generalmente, si el usuario cae en la trampa y paga alguna vez, a los pocos días el antivirus falso vuelve a simular amenazas para que el usuario vuelva a pagar por la supuesta eliminación de las amenazas.

4.1.3.12 Instalador (Dropper)

Bajo una apariencia de programa legítimo, los droppers instalan y ejecutan otros programas y archivos maliciosos en el equipo del usuario atacado. La diferencia de los droppers con los troyanos comunes es que éstos están destinados para alojar información, o un paquete de datos concretos en el equipo infectado, y no suponen un fin en sí mismos, sino que son una herramienta más para conseguir un fin.

Al ejecutarse un dropper, su código se carga en la memoria y posteriormente se extrae el fragmento de código malicioso que se desee almacenar de forma ilegítima en el sistema infectado y se graba en el sistema de archivos. Se puede ejecutar durante cualquier proceso de instalación, por lo que un solo dropper podrá descargar numerosos códigos maliciosos.

Los droppers son utilizados por los creadores de malware para ocultar algún tipo de malware, buscando crear confusión entre los usuarios y que estos piensen que son programas inofensivos.

- **Casos reales: Ejemplos de Droppers por el mundo:**

Algunos ejemplos de este tipo de malware son:

1. México: El dropper más popular en México es explorer.exe (Windows Explorer).

2. EE.UU.: El dropper más popular es winlogon.exe

3. Brasil: El dropper más común es explorer.exe.

4.1.3.13 Ladrón de contraseñas

Malware cuyo objetivo es el obtener nombres de usuario y contraseñas de forma ilegítima. Para obtener este tipo de información, este malware se introduce en el sistema informático del usuario al que se le quiere sustraer la información personal y es entonces cuando accede a determinados ficheros del sistema que almacenan este tipo de información. Para comprender mejor cuál es el funcionamiento de este tipo de software, su campo de acción dentro de un sistema y el tremendo daño que puede infringir a los

equipos donde se ejecute, veremos el siguiente ejemplo de este tipo de software.

- **Caso real: Software "PMS Stealer 0.1"**

Navegando a través de la red, se pueden encontrar multitud de ofertas de software diseñado para robar contraseñas en sistemas informáticos ajenos. Uno de estos casos es el del programa PMS Stealer 0.1, que se oferta como una herramienta capaz de extraer cualquier tipo de contraseñas, por su interés, se pasa a citar las características técnicas:

- Envío de la información por FTP en un archivo de texto
- MELT (hace que el stealer al ser ejecutado desaparezca)
- XP FWB (traspasa el firewall de windows para enviar la información sin problema al FTP)
- Propagación LAN (hace que el stealer se propague por LAN/Red, En un cibercafé por ejemplo con ejecutar el stealer en un PC obtendrían las claves de todo el local.
- UPX 3.03 (comprime el stealer y reduce su tamaño)
- Cambiar Icono (cambia el icono final que tendrá el stealer)
- ReAlign PE Header (Reorganiza la cabecera PE)
- Windows Vista UAC ByPass (salta la protección de windows vista que evita que se instale la mayoría del malware)

Ilustración 49: Captura de pantalla del malware "PMS Stealer 1.0"

4.1.3.14 Marcador (Dialer)

Es un tipo de malware muy difícil de detectar. Generalmente infectan a los equipos a través de descargas de software libre, y una vez dentro del sistema, este tipo de malware comienza a realizar llamadas no solicitadas por el usuario, normalmente, a números de teléfono de pago.

Este malware sólo puede entrar en acción cuando el usuario accede a Internet, y es entonces cuando comienza a ejecutarse. Su funcionamiento es sencillo, este malware se dedica a hacer llamadas a Números de Tarificación Adicional (NTA) de forma reiterada, lo que desemboca en un considerable incremento de la factura telefónica.

Ilustración 50: Las facturas de teléfono pueden revelar que el usuario ha sido víctima de un fraude

Actualmente este tipo de malware no es muy usado dado que la mayor parte de las conexiones a Internet que se realizan hoy día son a través de ADSL[25] o WiFi[26], por lo que su uso ha quedado anticuado.

Este malware, pese a estar desfasado por las tecnologías que empleaba (módems) en un pasado reciente resultó ser extraordinariamente dañino ya que muchas veces el usuario se daba cuenta de la estafa cuando le llegaban facturas extraordinariamente altas, lo que desembocaba en problemas

legales para demostrar que el propio usuario era víctima de un delito, o en otros muchos casos, el tener que pagar estas facturas astronómicas.

4.1.3.15 Puerta trasera (Backdoor)

Malware cuyo objetivo es permitir el acceso a un sistema o página web, evitando toda restricción o método de autenticación que pueda existir, permitiendo al usuario adentrarse en los sistemas infectados y poder realizar acciones de forma deliberada sin ningún tipo de control.

Este tipo de herramientas tiene (como muchos otros tipos de malware) un origen en actividades totalmente lícitas, pues este malware es usado por administradores de sistemas informáticos o webmasters[27], pero se ha comenzado a usar por infractores que desean atacar un determinado equipo. Entre las acciones que pueden perpetrar mediante este tipo de herramientas se encuentran:

- Manejar ficheros (en ocasiones confidenciales o con contenido de carácter privado) sin permiso alguno, pudiendo leerlos, copiarlos, eliminarlos, publicarlos, etc.
- Reiniciar el sistema informático al que ha tenido acceso.
- Obtener información confidencial acerca de la máquina infectada, como IP, dirección MAC[28], etc.

La finalidad de este tipo de malware es la infección masiva de cualquier tipo de sistema informático, con el objetivo de crear redes de botnets (o redes zombies) para poder perpetrar desde esas máquinas infectadas todo tipo de actos ilícitos.

- **Caso real: El BackDoor.Flashback.39 fue la mayor amenaza de malware para Mac OS X**

Este malware denominado como "Flashback", basado en la técnica de puerta trasera anteriormente explicada, consiguió infectar a más de 600.000 ordenadores Mac en todo el mundo (lo que supone por ejemplo un 12% de ordenadores con Mac OS vendidos en el cuarto

trimestre de 2011), siendo considerado por las empresas expertas en seguridad informática como la mayor amenaza de malware que jamás se ha visto en el Mac.

El malware BackDoor.Flashback.39 explota una vulnerabilidad del programa Java de Mac OS X. La compañía Oracle diseñó un parche para este fallo en cuanto tuvo constancia de ello, emitiéndolo en un espacio de tiempo aceptable y reaccionando ante este error para que no se vieran más equipos afectados, pero Apple tardó más tiempo y emitió el parche un mes y medio después, lo que supuso un alto número de equipos infectados, pues en todo ese tiempo cualquier ordenador Mac estaba desprotegido ante esta amenaza, que se ha demostrado devastadora.

Como se observa en este ejemplo, este tipo de ataques vienen dados por el descubrimiento de un exploit que permite posteriormente que los atacantes puedan realizar la técnica de puerta atrás y poder realizar acciones en los equipos infectados de forma remota.

Sorprende que esto haya ocurrido en ordenadores Macintosh, pues se creía que éstos no eran vulnerables ante los ataques informáticos a sus equipos, pero como vemos, todos los sistemas informáticos están expuestos a sufrir ataques mediante cualquier tipo de malware. Simplemente, éstos van en aumento en función de las posibilidades de lucrarse que tenga el atacante, por lo que antes los ordenadores Macintosh no eran un mercado atractivo puesto que tenían una cuota de mercado bastante reducida, pero en estos años se están empezando a convertir en un blanco más para los propagadores de malware debido a su auge en el mercado. Más adelante, en este mismo documento, se volverá a abordar este tema por su importancia para entender por qué surgen determinado tipo de malware y cuáles son los comportamientos, acciones y reacciones en los infractores a medida que evoluciona el mercado de la informática.

4.1.3.16 Rootkit

Malware cuyo objetivo principal es adquirir el control de un sistema de forma ilícita y poder conseguir privilegios equiparables al

de administrador del mismo, procurando en todo momento pasar desapercibido y ocultar la presencia en el sistema atacado.

Entre otras actividades, este tipo de malware puede esconder ficheros, procesos o conexiones creadas de forma ilícita, normalmente ocasionando alteraciones en el normal funcionamiento de los sistemas atacados.

Como otros muchos tipos de software, en ocasiones este tipo de programas no persigue realizar acciones maliciosas, sino que puede servir para realizar actividades completamente legales.

Los rootkit generalmente son la herramienta utilizada por los infractores inmediatamente posterior al uso de los exploit, por lo que en el proceso de ataque a un sistema informático, primero se encontraría la debilidad del mismo y se atacaría mediante un exploit, y tras conseguir con éxito adentrarse en el sistema, se comenzaría a ejecutar la herramienta rootkit con la que se podría causar el daño interno en el sistema siendo prácticamente invisible a los ojos del usuario infectado. A la hora de analizar un ataque, un rootkit puede transmitir mucha información acerca de las motivaciones que han llevado al atacante a realizar la infracción, así como sus objetivos finales y el nivel de sofisticación que se le puede presuponer al infractor.

Actualmente, son ampliamente utilizados para controlar componentes del sistema y permitir (o denegar) su utilización sin la autorización expresa del usuario.

El siguiente gráfico muestra un estudio acerca del número de rootkit almacenados en los diferentes sistemas operativos que tiene Microsoft en el mercado:

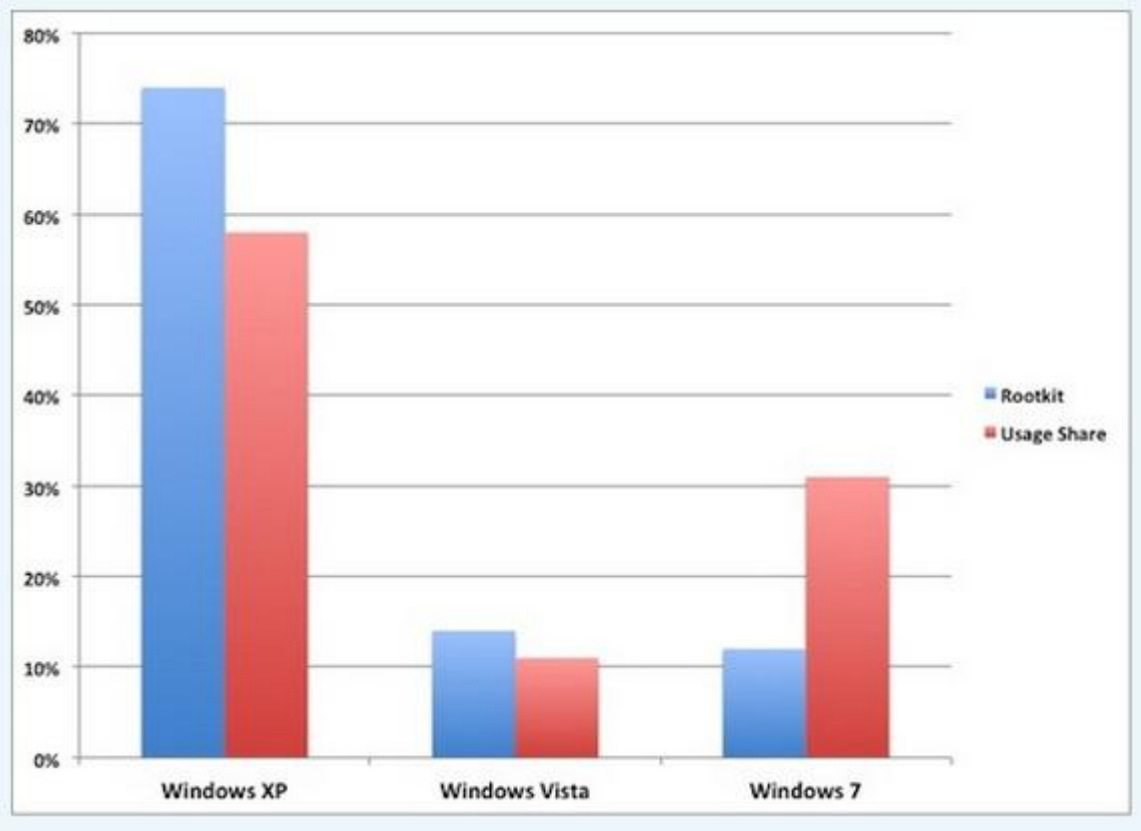


Ilustración 51: Según un estudio realizado por Avast en 2011, el sistema operativo Windows XP es el que almacena más rootkits

Del anterior gráfico se puede extraer que Windows XP es el sistema operativo que más rootkits alberga. Los expertos inciden en que es debido al uso generalizado de copias "pirata" de este sistema operativo con la actualización del mismo, el llamado "Service Pack 2". Esta actualización no evita que se introduzca este tipo de malware en los sistemas, y desde la propia compañía se recomienda el uso de la siguiente actualización "Service Pack 3" como único método de defensa para este tipo de ataques. Así, se observa como los infractores de nuevo se aprovechan de brechas de seguridad para poder penetrar en los sistemas mediante este tipo de malware. En la parte derecha del gráfico se puede observar como el resto de rootkits operativos aparecen en mucha menor medida en los sistemas "Windows Vista" y "Windows 7", los cuales sí poseen herramientas específicas para la detección de este tipo de malware.

- **Caso real: Sony utiliza un rootkit que pone en riesgo la seguridad de sus clientes.**

En el año 2005 saltó la noticia de que la empresa Sony utilizaba rootkits en algunos de sus sistemas anti copia.

Uno de esos rootkits fue usado por esta compañía para la consola Play Station 3, lo cual creó un gran revuelo entre la comunidad de usuarios y en los medios especializados en seguridad informática.

Este rootkit, conocido como Extended Copy Protection (XCP) y que también usan algunas otras compañías, se instalaba conjuntamente con el reproductor multimedia del CD/DVD al que acompañan. El rootkit trataba de evitar la copia o manipulación de los datos del soporte multimedia y ocultar por defecto todas las entradas del registro, carpetas y archivos cuyo nombre comenzase por la cadena de caracteres "sys".

Esto supone poner en un grave compromiso de seguridad a cada uno de los equipos en el que es instalado el rootkit, ya que al estar almacenando un rootkit que el propio administrador del sistema (el usuario final) no es capaz de eliminar (ya que Sony se encargó de instalarlo y no permitir su eliminación) éste puede ser un escondite perfecto para albergar toda clase de malware, ya que sabiendo que todas las carpetas que comiencen por la cadena de caracteres "sys" no van a ser visualizadas, cualquier creador de malware intentará alojar su código malicioso en esta carpeta y poder operar desde ahí para desarrollar sus actividades maliciosas, exactamente igual que opera el rootkit de Sony para evitar las copias de CD´s.

Como consecuencia, Sony se vio obligada a hacer pública una aplicación para eliminar este rootkit. Con esta noticia se prueba una vez más, tal y como se ha señalado anteriormente al describir los rootkits, cómo queda de manifiesto el uso de este tipo de software por algunas compañías para controlar componentes del sistema y permitir o denegar su utilización.

4.1.3.17 Secuestrador del navegador (browser hijacker)

Es un tipo de programa malicioso que altera la configuración del equipo navegador de manera que se le redirige a sitios web que no tenía intención de visitar en un principio. La mayoría de los secuestradores de navegador por defecto modifican páginas de

inicio y las páginas de búsqueda redirigiéndolas a las de sus clientes, que pagan por este servicio debido al tráfico que genera.

Las versiones más virulentas a menudo añaden marcadores para sitios web únicamente diseñados para la recolección de usuarios y por lo tanto obtener un gran incremento de visitantes. También generan ventanas emergentes en la pantalla del sistema, que incluso en ocasiones son tan rápidas que cualquier usuario medio es incapaz de hacer clic y cerrar estas ventanas, y por último también suelen redirigir a los usuarios a sitios web maliciosos, cuando, sin darse cuenta, escriben mal una dirección URL o introducen una dirección URL sin las "www" iniciales.

4.1.3.18 ¿Cómo puedo saber si el explorador ha sido asaltado?

- Existe un cambio de configuración de algunas páginas en el equipo informático sin previo aviso.
- Imposibilidad de acceder a determinadas páginas web, en especial a páginas con contenido relacionado con la seguridad informática, actualizaciones de antivirus, anti spyware, o descargas de software de seguridad.
- Aparición de forma reiterada de ventanas emergentes, nuevas pestañas, etc. con numerosos anuncios.
- Instalación sin previo aviso de nuevas barras de herramientas, aparición de nuevos íconos, vínculos a páginas web desconocidas, nuevos buscadores predeterminados, etc.
- Funcionamiento del sistema informático de forma más lenta de la habitual.

4.1.3.19 Otras clasificaciones

Dado el enorme catálogo de códigos maliciosos y malware en general que están ligados a los sistemas informáticos de hoy en día, se pueden realizar clasificaciones alternativas a la realizada en este documento, dependiendo del conjunto de características en el que nos centremos para definir cada grupo de malware. Así, se citará a continuación una clasificación más, donde se encuadrarán los diferentes códigos maliciosos según el tipo de actividad que desempeñan éstos:

- Ladrones de información (Infostealers): Este término engloba básicamente a todo el malware que se introducen a través de internet en los ordenadores de los usuarios legítimos, con propósito de conseguir información confidencial del propietario de forma ilícita. Entre los objetivos de este tipo de ataques está la obtención de información personal del usuario que posee el sistema infectado, como su nombre de acceso a páginas web, o sus contraseñas de acceso a su sistema bancario online, etc. Este tipo de malware ya ha sido citado en anteriores apartados del documento al enumerar diferentes clasificaciones del malware. En este caso, se podrían enmarcar en esta clasificación algunos ejemplos de malware tales como capturadores de pulsaciones, espías y ladrones de contraseñas.

  Por nombrar algunos de los stealers más famosos y dañinos de los últimos tiempos, se expone a continuación una gráfica con los stealers que más equipos informáticos infectaron en el año 2007:

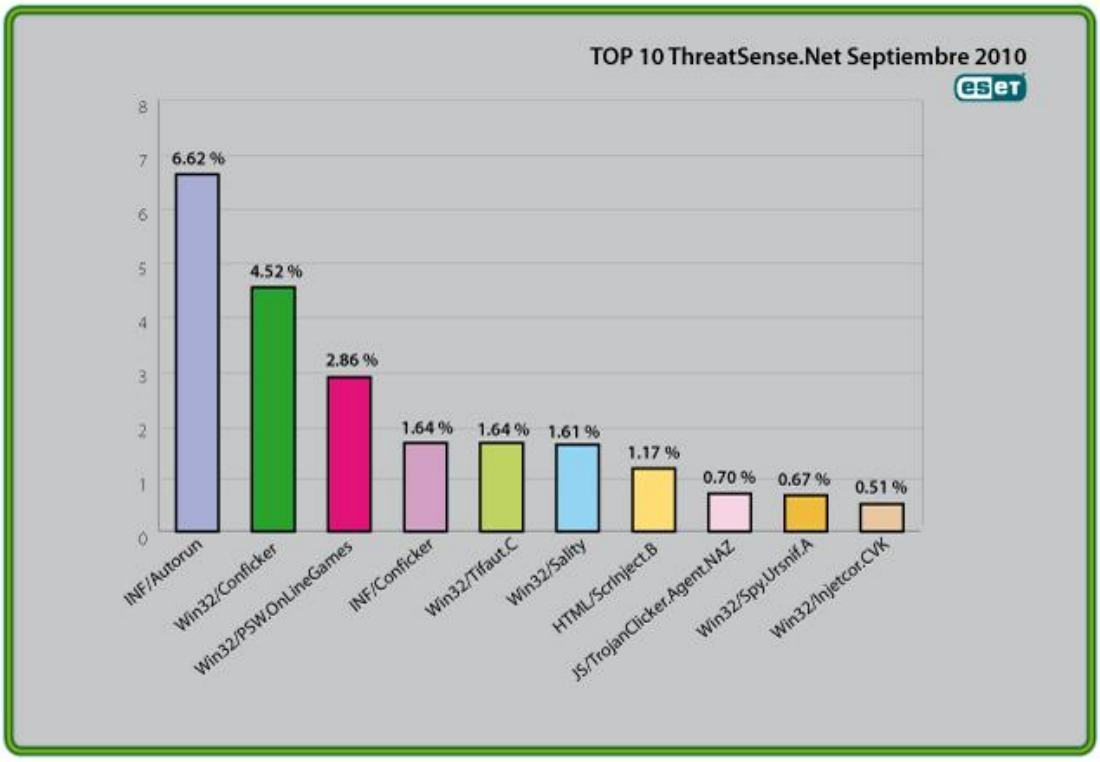


Ilustración 52: Gráfico elaborado por la compañía ESET acerca de los 10 infostealers más dañinos durante septiembre de 2010

- Código delictivo (crimeware): Se engloba en esta clasificación a cualquier tipo de malware que ha sido diseñado y desarrollado para perpetrar un delito del tipo financiero o económico. Algunos ejemplos de este tipo de infracciones serían las perpetradas mediante malware como mensajes de phishing, herramientas de fraude, marcadores, criptovirus o clickers que re direccionan al sujeto pasivo a falsas páginas bancarias o de seguridad.

  En el siguiente gráfico se muestra la evolución del número de crimeware no detectado desde el año 2003 hasta el 2010:

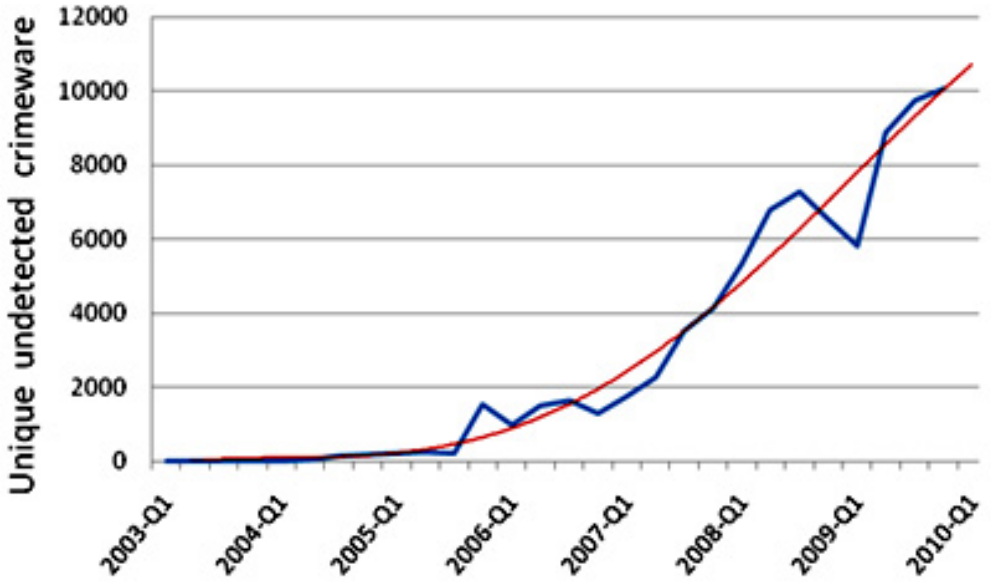


Ilustración 53: Gráfico que recoge la empresa de seguridad informática Karspersky Labs sobre el crimeware no detectado entre 2003 y 2011

  Como se observa, resulta bastante ilustrativa la gráfica acerca del crecimiento exponencial del crimeware sin detectar en estos últimos años, lo que da una idea de la sofisticación de esta técnica en los últimos tiempos.

- Grayware: A diferencia del resto de grupos, se caracteriza por no causar daños al equipo o a la red. Sin embargo ocasiona inconvenientes como ralentización del ordenador, despliegue de publicidad molesta, rastreo de la actividad del usuario con fines de marketing, modificación de la página de inicio del navegador, redireccionamiento de las búsquedas, etc.
  Agrupa algunos tipos de malware anteriormente comentados como el adware, espías que sólo roben información de

costumbres del usuario (que no reporten beneficio económico alguno), bromas, bulos, etc.

En la siguiente imagen, se muestra el número de malware clasificado como Grayware o Spyware detectado durante abril del 2010, con una proporción de 68 detecciones sobre un total de 288, lo que representa el 23,6% del total de programas maliciosos detectados:

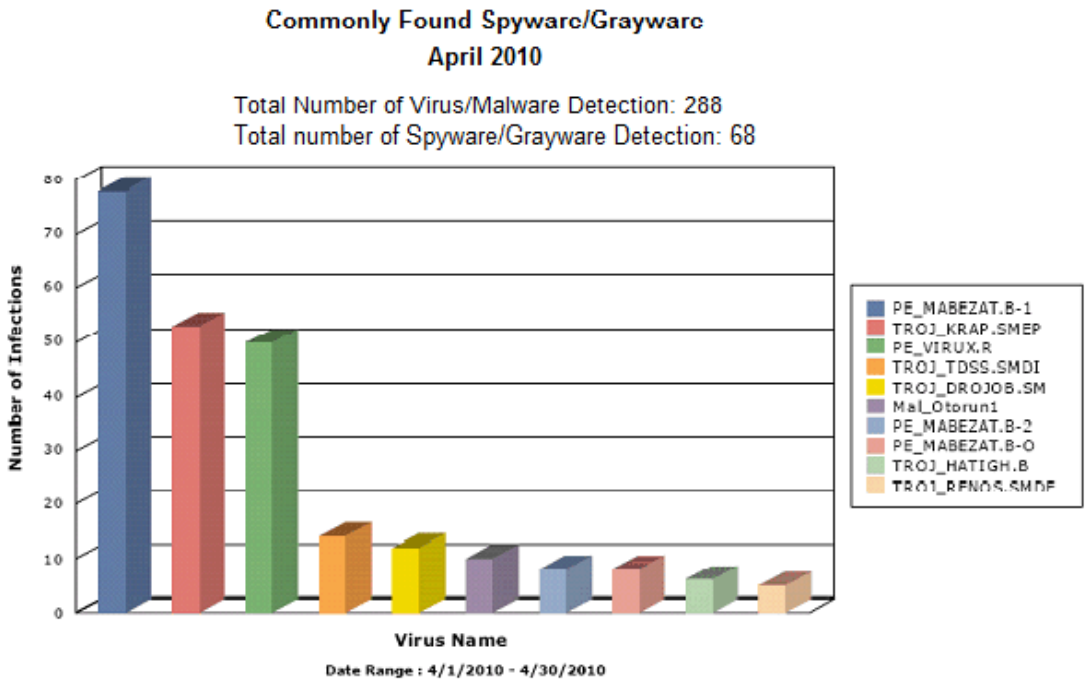


Ilustración 54: Spyware y Grayware detectado durante abril de 2010

4.1.4 Programas no recomendables

Existen algunos programas que, sin ser ellos mismos los originarios de acciones dañinas hacia el equipo en el que está operando, generalmente se consideran maliciosos por tener una serie de características o modos de funcionamiento que preceden a acciones ilegales o ilícitas, son los siguientes:

- Generador de claves (keygen): Son programas que generan claves para permitir el uso y disfrute de programas de pago de forma gratuita.

- Crack: Crean parches informáticos para permitir al usuario saltarse las restricciones de uso de determinados programas de pago, por lo que la finalidad es la misma que un generador de claves, aunque el proceso sea distinto.

- Herramienta de creación de malware: No realiza ninguna acción maliciosa en el ordenador. Es empleado por programadores maliciosos para crear programas dañinos personalizados. Se basa en el diseño anterior a la ejecución de la acción maliciosa.

Este conjunto de programas no son dañinos en sí, pero son empleados para propagar malware, por lo que su uso y pertenencia están tipificados como delito por la legislación española.

4.1.5 Cookies maliciosas

Las cookies son pequeños archivos que se almacenan en nuestro ordenador cuando visitamos páginas web y que guardan información que será utilizada la próxima vez que accedamos a esa página. Algunos de estos datos pueden ser nuestro nombre de usuario y contraseña, de forma que no tengamos que volver a introducirlos, etc. Esto resulta una herramienta muy cómoda ya que con un simple fichero de texto podemos almacenar cierta información que usamos para nuestra vida diaria cuando navegamos a través de la red, pero existen otro tipo de cookies, las denominadas "cookies maliciosas" cuya finalidad es monitorizar las actividades del usuario en Internet, pudiendo capturar datos confidenciales o de carácter privado durante la navegación del usuario, así como vender los hábitos de navegación de éstos a empresas de publicidad que se abastecerán de este tipo de infracciones para poder conocer de primera mano los gustos o las tendencias de cada uno de los consumidores para poder ofrecer productos que le puedan vender con una mayor facilidad dependiendo de sus hábitos.

Existe la posibilidad de desactivar las cookies de nuestro navegador, pero eso provocaría que muchas páginas no funcionasen de forma correcta, por ello lo más recomendable es eliminarlas cada poco tiempo.

También existen programas específicos que advierten o detectan cookies potencialmente peligrosas para el sistema y las eliminan:

Ilustración 55: Software que detecta y avisa sobre el riesgo de almacenar ciertas cookies

Aunque normalmente no es necesario utilizar este tipo de programas ya que en los propios navegadores ampliamente usados por toda la comunidad de usuarios (como por ejemplo Internet Explorer) ponen a disposición de éstos opciones de configuración donde se puede establecer un nivel predeterminado de seguridad respecto a las cookies que se almacenarán en el equipo personal, por lo que si se establece un nivel alto de seguridad se pueden tener alejadas a todas las cookies maliciosas y no almacenarlas en ningún momento:

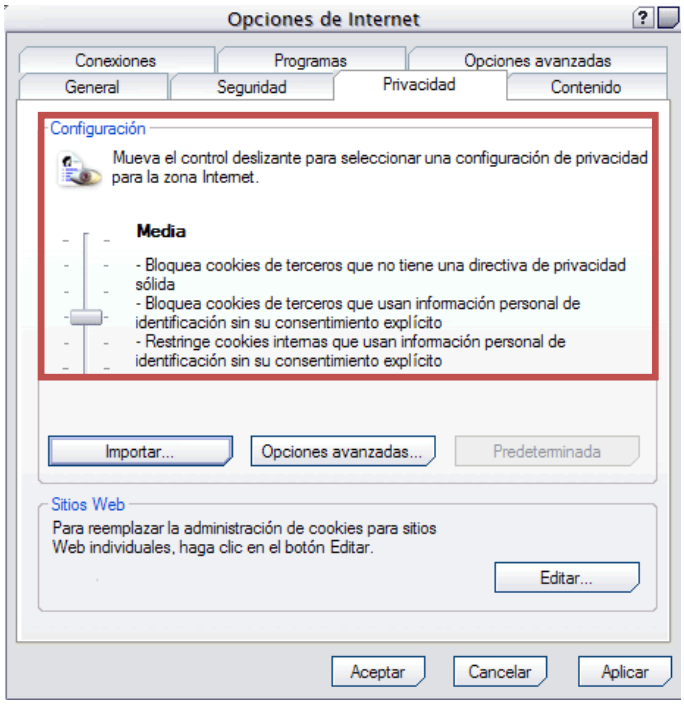


Ilustración 56: Captura de pantalla que indica el nivel de seguridad al navegar por Internet

4.2 Malware: Cómo llega al sistema informático y cómo prevenirlo

Existen multitud de formas por las que los virus, gusanos, troyanos y malware en general, llegan a un equipo informático. En muchas ocasiones, la infección de los equipos viene producida por una falta de protección de los mismos, ya sea configurando las opciones de navegación por internet, no tener cuidado a la hora de abrir los correos electrónicos sospechosos, no utilizar antivirus, etc.

Las principales vías de acceso de un virus a un equipo informático son las siguientes:

- Explotando una vulnerabilidad: todo programa informático es susceptible de tener ciertas vulnerabilidades o fallos en el sistema, y consecuentemente para cada uno de estos fallos o brechas de seguridad existe el peligro de que suponga una vía de entrada en el sistema para cualquier tipo de amenaza. Esto es un riesgo que es imposible de evitar, pues siempre podrán existir ese tipo de fallos, pero si es posible vigilar por parte del usuario, y para ello la única solución para poder mantener cierta seguridad en el equipo y poder prevenir una infección

en el mismo, es mantener siempre actualizado el software que habitualmente se emplee en el mismo.

De esta forma, si aparecieran vulnerabilidades en los códigos de los programas usados, con descargarse la actualización de la empresa que lo comercializa se podría solucionar esa vulnerabilidad, aunque se ha de tener en cuenta que durante el tiempo que transcurre desde que se descubre la vulnerabilidad hasta que se crea el parche para subsanarla por parte de la compañía propietaria del software y el usuario se la descarga para actualizar su programa inevitablemente se está corriendo un peligro que será subsanado en el momento que el usuario se descargue la actualización del programa en cuestión.

Como conclusión, se puede afirmar que aun teniendo el equipo completamente actualizado nunca se puede estar completamente seguro de la invulnerabilidad del sistema informático frente a posibles nuevos ataques a partir de nuevas vulnerabilidades descubiertas antes por los infractores y delincuentes informáticos que por los empleados de seguridad del software que use el usuario.

- Ingeniería social: La ingeniería social es principalmente utilizada en correos que emplean la técnica de phishing (comentada en anteriores apartados de este mismo documento), pero también puede ser usada para crear conmoción o llamar la atención, como por ejemplo informando de una falsa noticia de gran impacto. Su objetivo siempre será atraer la atención del usuario y a través de ello sugerirle realizar una serie de acciones que previamente el usuario no haría. Las medidas más apropiadas para evitar este tipo de ataques a los usuarios son la omisión de correos recibidos de remitentes desconocidos y la constatación de que nunca se le van a requerir los datos bancarios a los usuarios de un banco a través de un correo electrónico. La ingeniería social persigue que, por medio de mensajes que le pueden despertar la curiosidad al usuario, por ejemplo, acceda a páginas web con contenido malicioso.

A priori algunas técnicas de ingeniería social empleadas que se han llevado a cabo a través de la red parecerían simplemente una estafa muy poco lograda o incluso podría parecer imposible que nadie pudiera ser estafado mediante este mecanismo, pero es sorprendente el gran volumen de usuarios estafados que ha habido a lo largo de estos últimos años a través de técnicas como la conocida "estafa nigeriana".

Esta estafa se basa en mandar correos de forma indiscriminada a un número indeterminado de personas (cuantas más, más posibilidades de estafa) haciéndose pasar por un banco, el cual comunica al destinatario del correo la existencia de una fortuna (realmente inexistente) y le persuade por diferentes medios para que pague una suma de dinero por adelantado, como condición para acceder a la supuesta fortuna. Las sumas solicitadas son bastante elevadas, pero insignificantes comparadas con la fortuna que las víctimas esperan recibir.

En dichos mails generalmente suelen tener un aspecto formal y oficial, llegando incluso a incorporar notas legales o logotipos de bancos contrastados y firmas de funcionarios reales, para dar mayor credibilidad a la estafa. Estos mails muchas veces suelen estar personalizados con información del destinatario obtenida de la guía telefónica, sitios web donde el usuario haya dejado sus datos, o sustraídos al propio usuario mediante algún tipo de malware.

CENTRAL BANK OF NIGERIA

PRESS STATEMENT ON ADVANCE FEE FRAUD/SCAM

DON'T BE FOOLED! MANY HAVE LOST MONEY!!

IF IT SOUNDS TOO GOOD TO BE TRUE THEN IT IS NOT TRUE!!!

1 The publicity campaigns by the Central Bank of Nigeria (CBN) and the Government of the Federal Republic of Nigeria have proved successful in sensitising the public about the menace of advance fee fraud and the falsehood of claims that easy money could be made in Nigeria. Consequently, the reported incidence of advance fee fraud (A.K.A. '419'), has declined significantly. Nevertheless, there are still some people who have continued to fall victim to the solicitations of advance fee fraudsters. This warning is, therefore, specifically intended for the benefit of those misguided people who, in the quest to make easy money at the expense of Nigeria, are defrauded by international fraudsters.

2 The advance fee fraud is perpetrated by enticing the victim with a bogus 'business' proposal which promises millions of US dollars as a reward. The scam letter usually promises to transfer huge amounts of money, usually in US dollars, purported to be part proceeds of certain contracts, to the addressee's bank account, to be shared in some proportion between the parties. A favourable response to the letter is followed by excuses why the funds cannot be remitted readily and subsequently by demands for proportionate sharing of payments for various 'taxes' and 'fees' supposedly to facilitate the processing and remittance of the alleged funds. The use of 'fake' Government, Central Bank of Nigeria, Nigerian National Petroleum Corporation, etc. documents is a common practice.

3 The fraudsters usually request that the transaction be done under the cover of confidentiality. Sometimes, the 'victims' are invited to Nigeria where they are given red-carpet reception and attended to by the fraudsters, posing as Nigerian Government officials. Quite often the fraudsters invent bogus Government committees purported to have cleared the payments. Also, it is not unusual for them to contrive fake publications in the newspapers evidencing purported approvals to transfer non-existent funds.

4 To consummate the transaction, the 'victim' would be required to pay 'advance fees' for various purposes: e.g. processing fees, unforeseen taxes, licence fees, registration fees, signing/legal fees, fees for National Economic Recovery Fund, VAT, audit fees, insurance coverage fees, etc. The collection of these 'advance fees' is actually the real objective of the scam!

5 A recent variant of the scam directed primarily at charitable organisations and religious bodies overseas involves bogus inheritance under a will. Again the sole aim is to collect the 'advance fees' already described above. A new strategy that has also been used to defraud the 'victims' is an offer to use chemicals to transform ordinary paper into United States dollar bills, which would be subsequently shared by the parties.

6 You are again warned in your own interest not to become yet another dupe to these fraudulent solicitations or schemes. Genuine and prospective investors in Nigeria are advised to consult their home Chambers' of Commerce and Industry, or Nigeria's Chambers' of Commerce and Industry, Manufacturers' Associations of Nigeria, Federal Ministries of Commerce and Industry, Nigerian Missions in their countries of origin, their embassies or High Commissions in Nigeria for proper briefing and advice.

7 The Central Bank and indeed, the Federal Government of Nigeria cannot and should not be held responsible for bogus and shady deals transacted with criminal intentions. As a responsible corporate body, the Central Bank of Nigeria is once again warning all recipients of fraudulent letters on bogus deals, that there are no contract payments trapped in the bank's vaults. They are once again put on notice that all documents appertaining to the payment, claims, or transfers purportedly issued by the bank, its senior executives or the Government of the Federal Republic of Nigeria for the various purposes described above are all forgeries, bogus and fraudulent.

8 Please join the Central Bank and the Federal Government of Nigeria to fight the criminal syndicates who play on the gullibility and greed of their victims by reporting any solicitation to your local law enforcement agencies or the local International Police Organisation (Interpol).

9 You have been warned several times before! You have been warned again!!

CENTRAL BANK OF NIGERIA
Samuel Ladoke Akintola Way, P.M.B. 0187, Garki, Abuja, NIGERIA

Ilustración 57: Ejemplo del conocido "Timo nigeriano"

Otro ejemplo de email enviado que versa sobre el mismo tema:

MR RAMOND SALIM
AUDITING AND ACCOUNTING UNIT,
BANK OF AFRICA.(BOA)
OUAGADOUGOU -BURKINA FASO,

Dear Friend,

This message might meet you in utmost surprise, however,it's just my urgent need for foreign partner that made me to contact you for this transaction, I choose to reach you through it because it still remains the fastest medium of communication. However, this correspondence is private. I got your contact from the chambers of commerce here in my country ouagadougou,burkina faso.

I am a banker by profession from Burkina faso in west Africa and currently working in the Auditing and Accounting unit of the bank. I have the opportunity of transfering the left over funds ($25 million) of one of my bank clients late Mr.Andrea schranner who died along with his entire family on 31 july 2000 in a plane crash.The fund for transfer is of clean origin.You can confirm the genuiness of the deceased death by clicking on this web site

http://news.bbc.co.uk/1/hi/world/europe/859479.stm

Hence,i am inviting you for a business deal where this money can be shared between us in the ratio of 50/40 while 10% will be mapped out for expenses after the fund has been transfer into your bank account.If you agree to my business proposal i require you to send me your personal informations such as your full name,your telephone number,your occupation,your full home address, and your scanned photograph,immediately i receive those datas,i will forward the details of the transfer and the application of claim to you which you will fill and send to the bank for the claim .have a great day.

Your Faithfully
Mr .Ramond Salim

NB, MAKE SURE YOU KEEP THIS TRANSACTION AS YOUR TOP SECRECT AND MAKE IT CONFIDENTIAL TILL WE RECEIVES THE FUND INTO THE ACCOUNT.

Ilustración 58: Otra versión del conocido "Timo nigeriano"

Este sería un claro ejemplo de estafa a través de la ingeniería social, y en principio la mayor parte de los usuarios no caerían en esta trampa y no enviarían dinero a los remitentes de estos correos, pero sorprende que según se recoge en diversos medios, se estima que este tipo de estafa llegó a representar una parte importante del PIB de Nigeria (país de origen de esta estafa, de ahí su nombre) y en el año 2001 alrededor de 2,600 ciudadanos americanos fueron víctimas de esta estafa, con un pérdida de más de $300,000 dólares.

- Por un archivo malicioso: es la forma de infección más común en los casos de troyanos. La infección de este tipo de malware puede proceder de cualquier archivo descargado, email abierto, cualquier carpeta compartida, etc. Por ello, es aconsejable realizar un chequeo previo a la descarga de cualquier tipo de archivo, así como descargar contenido únicamente de sitios web de confianza. Medidas complementarias serían el uso exclusivamente de software legal y la posterior descarga de las actualizaciones del mismo desde los canales oficiales y no cualquier otro.

  En el siguiente ejemplo se puede observar cómo se envía un correo electrónico a un usuario diciéndole que se le ha procedido al cambio de contraseña en la red social "Facebook" por lo que se ha de descargar un archivo para conocer su nueva contraseña:

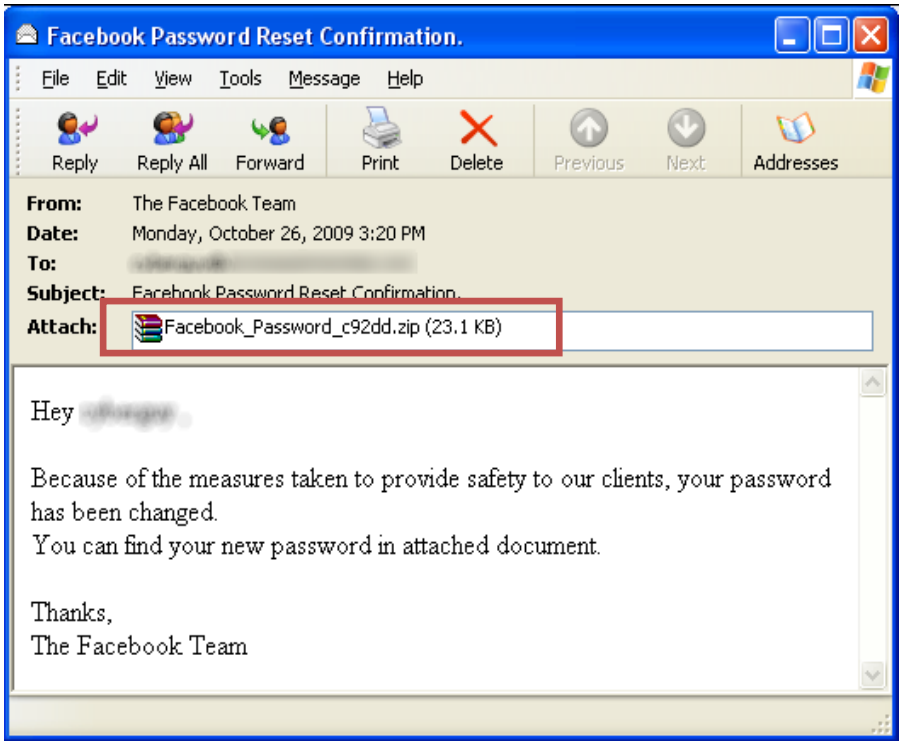


Ilustración 59: Email con contenido sospechoso acerca del cambio de contraseña en Facebook

En este caso, se observa lo fácil que puede resultar un equipo infectado si no se tiene especial cuidado a la hora de abrir los correos electrónicos, ya que sería tan sencillo como proceder a la descarga de este archivo para ser presos de cualquier tipo de malware que se encuentre en el fichero descargado.

- Dispositivos extraíbles: Como se ha comentado anteriormente, los gusanos basan su actividad en la realización de sucesivas copias de sí mismos dentro de un equipo informático, por lo que su nivel de propagación en caso de que se realice una copia en un dispositivo extraíble pasa a ser extraordinariamente alto. De hecho, si se produce esta situación, cuando el dispositivo extraíble se conecte a otro soporte informático, automáticamente se ejecutará de nuevo el gusano, infectando al nuevo equipo.

  Así, se pueden encontrar gusanos diseñados específicamente para infectar a los dispositivos extraíbles, como es el caso del denominado "IRCbot.k". Este programa está codificado para ejecutarse automáticamente cada 30 segundos en busca de nuevos dispositivos extraíbles que se hayan conectado al equipo infectado. Una vez dentro, el virus crea copias de sí mismo imitando los nombres de las carpetas que ya están

guardadas en el dispositivo en cuestión, además de un acceso directo que apunta al archivo malicioso.

Ilustración 60: Los dispositivos físicos externos son una fuente importante en la entrada de malware

Para evitar este tipo de situaciones, se recomienda a los usuarios deshabilitar el autoarranque de los dispositivos que se conecten al ordenador así como el uso de cortafuegos.

Aunque, como se ha visto, existen gran cantidad de códigos maliciosos, es muy fácil prevenir quedarse infectado por la mayoría de ellos y así poder utilizar el ordenador de forma segura.

4.3 ¿Qué sucede con los datos robados?

Toda vez que se ha perpetrado el robo de datos por parte del infractor, éstos han de llegar al verdadero atacante que perpetre el fraude o robo. En sí, el robo de información personal o de carácter privado constituye un delito, aunque a partir de este robo se puede, o bien venderlos a terceras personas para que puedan cometer éstas actos ilícitos, o simplemente (si se trata de compañías o empresas privadas) vendérselos como información sobre los hábitos de consumo de un determinado conjunto de usuarios, o, si el infractor desea cometer otra serie de infracciones a partir de este robo, comenzar a diseñar y perpetrar acciones más dañinas para la víctima.

Dependiendo del método que se haya empleado para la obtención de los datos robados, el infractor podrá recabarlos de unas formas u otras. Así, si el método empleado es el pharming o el phising, el propio servidor fraudulento es el que le irá proporcionando toda la información al infractor enviándola desde el propio equipo infectado, pero, si no se emplean estas técnicas, se pueden utilizar algunas otras para hacer llegar la información que se quiere extraer del sujeto pasivo. Las más recurrentes son:

- Envío mediante peticiones HTTP POST[29] y GET[30].
- Conexión a un servidor SMTP[31] a través del cual se elabora un correo electrónico con los datos robados que es enviado a una dirección de confianza del infractor.
- Mediante el envío de archivos con los datos sustraídos a un servidor FTP que disponga el infractor.
- También se emplean conexiones, para depositar los datos robados en un canal de chat.

Dependiendo del nivel de sofisticación del atacante, éste puede incluso llegar a cifrar esos datos antes de enviarlos y así evitar la detección de los mismos, de tal forma que si algún otro usuario estuviera monitorizando el tráfico y detectara esa serie de comunicaciones extrañas, éste no sería capaz de obtener la información robada. Un ejemplo de este tipo de prácticas es el empleado para el envío del mensaje cifrado de la siguiente ilustración:

```
POST /BAD1D22270B42485/AVJn4mNkVVDRpmTCFULrc4RnJmLHcRFxEzMxFxEXfCYGVWDiAqTUUHHWV
PLEMevTdCNHMicR0CHVY5EDxFarFlEyl3ZjxDW0VWMBJ0HnfxK0RnNT57GhIdUToLdRJ9oW0VKXNtJQE
XE0U3FnoTcbJpF2Aw HTTP/1.0
Host: hda8pra.biz
Content-Length: 228
Connection: close
Content-Type: multipart/form-data; boundary=utorfktsgdretdg

--utorfktsgdretdg
Content-Disposition: form-data; name=datafile; filename="data.str"
Content-Type: application/octet-stream

4kPno6JkdHShtrdy9FK6IUdVkMSgF8Z302S3YJInGzfh06JnAnSktMJ2hFKwYD2VpjWAM
+eg1GRxdtSyx3L+U8ClQZEBMJGg0WYEcqSyzXOEJ8YEcQbHZtNk1nHHQCzxJuFnMkaRoNRhdgSitMF
+8yTDUOWwpnamlyNAl6DSbnME18LEAvRUsCM1VuCScw/DReEnYjexYWFkQxEnIEdbdhHSF0LXQSEgEfS
```

Ilustración 61: Datos robados y enviados de manera cifrada empleando el protocolo HTTP

Hoy en día es ya un hábito entre los sujetos activos más avezados el empleo de portales web para la recogida de datos robados. En ellos, se almacena una base de datos y un conjunto de scripts, los

cuales pueden llegar a organizar al conjunto de los equipos infectados, de forma que se le asigne a cada uno de ellos una determinada tarea, como por ejemplo, el apagado sistemático del equipo, alojar phising, o realizar ataques de denegación de servicio a un segundo objetivo, siendo éste un encubridor de la persona que realmente está cometiendo la infracción.

Cabe destacar los casos de phising en donde el infractor se intenta ocultar mediante el equipo infectado, generalmente haciendo uso de botnets por lo que los equipos infectados actuarían como proxies encubiertos, por lo que resultaría mucho más difícil encontrar quién es el verdadero artífice de la infracción que se está cometiendo, ya que escondería su identidad a través de un sistema de múltiples encadenamientos de IP´s. Para solucionar este tipo de casos habría que realizar un bloqueo del dominio involucrado (Fast Flux). A continuación se puede observar la resolución DNS de un dominio fraudulento utilizando esta técnica:

```
D:\>dig fill-moms.com

; <<>> DiG 9.3.2 <<>> fill-moms.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 136
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 5, ADDITIONAL: 0

;; QUESTION SECTION:
;fill-moms.com.                 IN      A

;; ANSWER SECTION:
fill-moms.com.          521     IN      A       123.111.168.224
fill-moms.com.          521     IN      A       66.176.11.228
fill-moms.com.          521     IN      A       75.83.137.165
fill-moms.com.          521     IN      A       116.81.70.10

;; AUTHORITY SECTION:
fill-moms.com.          135145  IN      NS      ns1.maillabsservice.com.
fill-moms.com.          135145  IN      NS      ns2.maillabsservice.com.
fill-moms.com.          135145  IN      NS      ns3.maillabsservice.com.
fill-moms.com.          135145  IN      NS      ns4.maillabsservice.com.
fill-moms.com.          135145  IN      NS      ns5.maillabsservice.com.

;; Query time: 70 msec
;; SERVER: [redacted]#53([redacted])
;; WHEN: Sat Apr 18 10:08:40 2009
;; MSG SIZE  rcvd: 201
```

Ilustración 62: Ejemplo de resolución DNS de un dominio fraudulento

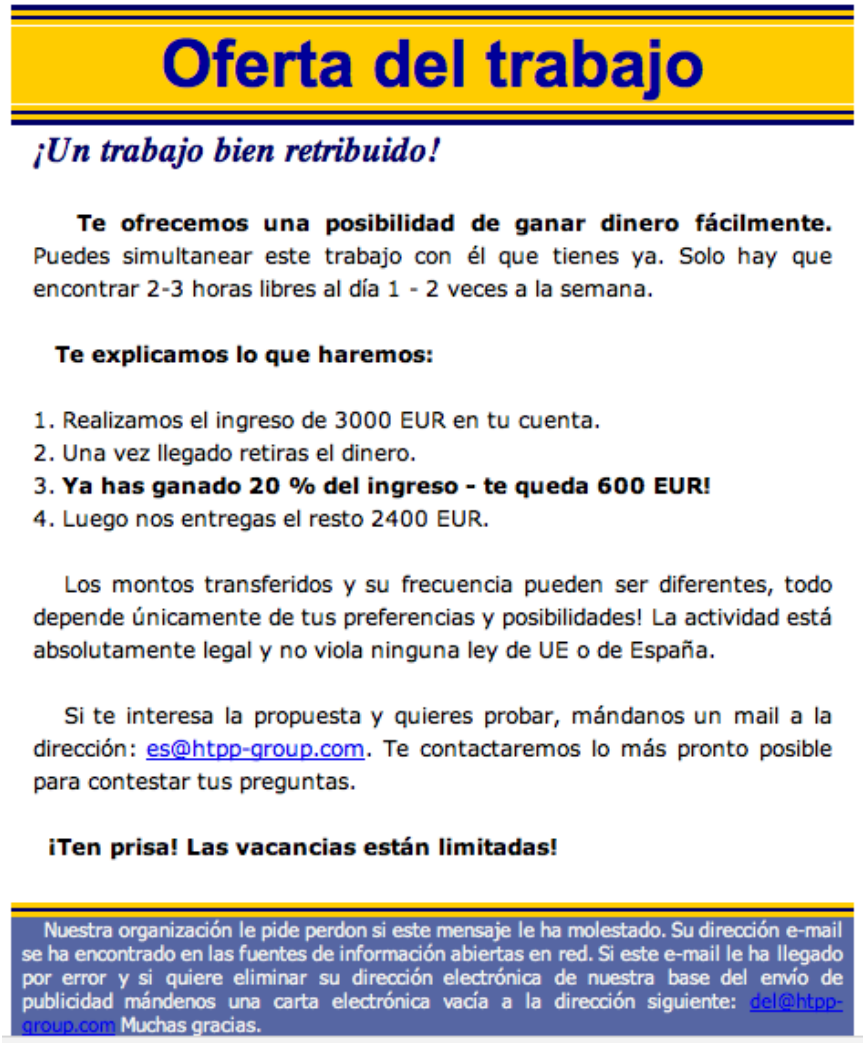
La facilidad de manejo de estos sistemas de gestión de datos robados permite que el propio creador del malware pueda alquilar la herramienta para que otras personas que no tengan la suficiente destreza como para crear una herramienta de esas características, pero sí tengan la voluntad de cometer la infracción, puedan

aprovecharse de ésta y utilizarla durante ciertos periodos de tiempo, permitiendo que el dueño del malware a efectos legales no sea siempre el responsable de la herramienta y aun así siga sacando beneficio de ella.

4.3.1 ¿Cómo se materializa finalmente el robo?

Toda vez que el atacante cuenta con las credenciales y datos de acceso a las cuentas bancarias, tiene que proceder al último paso: extraer el dinero de las cuentas.

Una de las preocupaciones de los infractores es, evidentemente, proteger su identidad en todo momento para no ser descubiertos con facilidad, y para ello se valen de innumerables técnicas, aunque la más utilizada es el recurrir a los llamados "muleros". Un mulero es una persona que, pensando que realizan un trabajo totalmente legal para una empresa, actúa como pantalla para el infractor y permite obtener el dinero a éste a partir de transacciones bancarias, siendo la persona que se expone a ser vinculada a la infracción. Generalmente a los muleros se les ofrece una alta remuneración económica por simplemente realizar movimientos bancarios a través de un sistema de cuentas, aunque lo que realmente hacen (sin ellos saberlo) es actuar de pantalla del delincuente frente a las posibles consecuencias que pueden tener esos movimientos financieros, procedentes de los fraudes llevados a cabo previamente. Normalmente estos muleros son captados para realizar estas operaciones mediante ofertas de trabajo falsas por Internet, como la que muestra la siguiente ilustración:



Oferta del trabajo

¡Un trabajo bien retribuido!

Te ofrecemos una posibilidad de ganar dinero fácilmente. Puedes simultanear este trabajo con él que tienes ya. Solo hay que encontrar 2-3 horas libres al día 1 - 2 veces a la semana.

Te explicamos lo que haremos:

1. Realizamos el ingreso de 3000 EUR en tu cuenta.
2. Una vez llegado retiras el dinero.
3. **Ya has ganado 20 % del ingreso - te queda 600 EUR!**
4. Luego nos entregas el resto 2400 EUR.

Los montos transferidos y su frecuencia pueden ser diferentes, todo depende únicamente de tus preferencias y posibilidades! La actividad está absolutamente legal y no viola ninguna ley de UE o de España.

Si te interesa la propuesta y quieres probar, mándanos un mail a la dirección: es@htpp-group.com. Te contactaremos lo más pronto posible para contestar tus preguntas.

¡Ten prisa! Las vacancias están limitadas!

Nuestra organización le pide perdon si este mensaje le ha molestado. Su dirección e-mail se ha encontrado en las fuentes de información abiertas en red. Si este e-mail le ha llegado por error y si quiere eliminar su dirección electrónica de nuestra base del envío de publicidad mándenos una carta electrónica vacía a la dirección siguiente: del@htpp-group.com Muchas gracias.

Ilustración 63: Ejemplo de oferta de trabajo que esconde el blanqueo de dinero de delincuentes informáticos

El sistema de transferencias para que el dinero obtenido de la infracción llegue finalmente al infractor funciona del siguiente modo: los atacantes se introducen en la cuenta del usuario del que tienen los datos, y se hacen pasar por el usuario. En ese momento, aprovechan para realizar una transacción a una cuenta bancaria a nombre del mulero (es el titular de la cuenta). Posteriormente, los infractores le piden al mulero que extraiga el dinero en efectivo de esa cuenta, a cambio de que éste se quede un pequeño porcentaje de la operación. De esta forma, no se registra dato alguno acerca del auténtico infractor a lo largo de toda la operación, y no puede ser relacionado con la misma en ningún momento.

Otro sistema sería el de cobro en cajero. En este caso el mulero envía una cantidad de dinero que le solicite el infractor para poder recogerla en un cajero determinado. A esa operación el banco le asigna un código que el mulero pasa al infractor de tal forma que

éste pueda recogerlo en el cajero concretado. Así, el infractor ni siquiera ha de conocer personalmente al mulero, sino que simplemente ha de tener a una persona, sin ni siquiera ser necesario que habiten en la misma ciudad, que le vaya proporcionando los códigos para ir recogiendo el dinero producto del fraude en los cajeros.

El tercer método más usado es montar un casino en línea. La idea puede resultar a priori mucho más compleja que las anteriores, pero debido a las fuertes investigaciones de los cuerpos de seguridad del Estado, los infractores han visto como las dos primeras técnicas, ya sobradamente conocidas por la policía, se han quedado anticuadas y han tenido que ir ingeniando otros métodos más complejos como éste.

El proceso es el siguiente: el infractor crea un casino en línea donde con las tarjetas de crédito o cuentas bancarias robadas a las víctimas apuestan en su propio casino con la finalidad de perder todo el dinero que haya en las cuentas. De tal forma que simplemente juegan en su propio casino con los datos robados de los sujetos pasivos, y pierden todo el dinero posible. Algunas variaciones en este tipo de métodos son la creación de casas de apuestas falsas en línea o la simulación de otros servicios parecidos que ofrece Internet.

Ilustración 64: Ejemplo de casino online fraudulento

5 CÓMO ACTUAR TRAS SER OBJETO DE UN FRAUDE INFORMÁTICO

En este apartado se van a abordar los procedimientos a realizar por parte de un usuario que ha sido objeto de un delito informático o cualquier fraude informático.

Normalmente, suelen pasar horas, días, o incluso meses hasta que un usuario se da cuenta de que ha sido objeto de un fraude o un delito informático. Esto es debido, por ejemplo, a que si el atacante está realizando llamadas no permitidas a números de alta tarificación desde el equipo del usuario infectado, éste sólo se dará cuenta cuando reciba una factura telefónica desorbitada al mes siguiente.

Tras confirmar que se ha sido objeto de un fraude o delito informático (consultar clasificación de delitos informáticos de la Brigada de Investigación Tecnológica de la Policía Nacional Española, en el punto 2 de este documento) hay una serie de pasos que se han de seguir para actuar y subsanar los perjuicios ocasionados. Dependiendo de qué tipo de ataque se haya sufrido, se puede disponer de una serie de medidas u otras. Veamos las medidas a tomar si se ha perpetrado un ataque software al sistema informático, o si se ha sufrido un fraude online con un perjuicio económico.

5.1 Software de actividades ilegales

Si el usuario es consciente de que pueden estar ejecutándose actividades ilegales en su sistema, o de que se ha instalado algún software en su equipo que el propio usuario no ha permitido o del que no es consciente, o si simplemente, éste sospecha que su ordenador puede estar infectado o está teniendo un comportamiento anómalo, la primera medida que se ha de tomar es la desconexión inmediata de la red. Deshabilitar la conexión a la red permite que se corten de inmediato el flujo de datos hacia el infractor en caso de que se esté perpetrando en ese momento el ataque, pudiendo evitar de forma inmediata que los daños ocasionados aumenten.

En caso de que se el sistema infectado sea el equipo habitual de trabajo, y esté conectado a la red de la empresa, el usuario debe de ponerse en contacto de forma inmediata con el Departamento de Seguridad Informática (si lo hubiera) para que éstos puedan subsanar el problema con la mayor brevedad posible. Evidentemente, en estos casos cuanto antes se actúe menores serán los daños ocasionados y, teniendo en cuenta que en un lugar de trabajo se pueden manejar no ya sólo datos personales del propio usuario que usa el equipo, sino dependiendo del tipo de trabajo, datos sensibles de la propia empresa o incluso de personas ajenas a la misma, resulta de especial importancia detectar las anomalías a tiempo y prevenir cualquier tipo de ataque que pueda poner en riesgo los datos que se manejan.

Por otro lado, si el equipo infectado es de uso doméstico, el usuario se ha de poner en contacto con su proveedor de servicios de Internet (ISP), para que éste le pueda resolver los posibles problemas que se hallen en el equipo.

Es importante el análisis del equipo infectado con un programa antivirus actualizado, pudiendo a través de esta herramienta localizar cualquier tipo de malware o amenazas que se hallen en el sistema y que podrían seguir poniendo en peligro la seguridad del mismo si no se realizara el pertinente chequeo. En ocasiones, el antivirus sólo es capaz de detectar la amenaza pero no eliminarla, por lo que en estos casos el usuario debe informarse acerca de qué herramientas informáticas o qué utilidades pueden servirle para poder eliminar de su equipo dicha amenaza.

En los sistemas informáticos los usuarios normalmente guardan cantidad de información y datos que pueden ser de carácter personal o laboral, y la eliminación de éstos podría suponer un gran trastorno a un usuario o incluso a una empresa. Una buena forma de evitar estos problemas cuando los equipos se ven amenazados es realizar de forma periódica copias de seguridad (o backups) de los archivos y datos más importantes que alberga el equipo. De esta forma, el daño se puede reducir considerablemente, ya que como máximo ante un ataque devastador el usuario perdería los datos que no ha almacenado desde la última copia de seguridad,

reduciendo significativamente los daños potenciales. Así, dependiendo de la criticidad de los datos los usuarios podrán realizar copias de seguridad cada mes, cada semana, cada día, cada hora, o en datos cruciales como el registro de movimientos bancarios, prácticamente cada vez que se realice algún movimiento será automáticamente guardada una copia de seguridad del mismo.

Estas copias de seguridad generalmente podrán realizarse en dispositivos físicos como CD´s o DVD´s, servidores RAID, etc., o almacenar los datos en la red (en plataformas como Dropbox, DiscoWeb, o plataformas similares de almacenamiento de información) o en dispositivos extraíbles como los pendrive. Dependiendo de la criticidad de los datos y el presupuesto disponible para su almacenamiento y aseguramiento, se emplearán unos métodos u otros.

Por último, en ocasiones el daño producido es tan grande que hay que sopesar la posibilidad de comenzar desde cero y cargar en el equipo infectado una copia de seguridad para poder volver a trabajar a partir del momento en el que se guardó dicha copia. Dependiendo del tiempo transcurrido desde la última copia de seguridad, del tipo de malware que ha afectado al equipo, etc. se podrá tomar esta decisión, que aunque drástica, en ocasiones resulta mucho más favorable en tiempo y forma para el usuario, ya que existen precedentes de malware que por su extraordinaria criticidad resulta imposible la recuperación de los datos perdidos.
Por último, cuando se desconoce cuándo se ha infectado el equipo y la criticidad de los datos es considerable, se puede ejecutar un "formateo" del equipo, consistente en guardar en un soporte ajeno al equipo los datos más relevantes que se encuentren en él y volver a reinstalar el sistema operativo para comenzar de nuevo y eliminar todo tipo de amenaza que se hallará en el sistema.

5.2 Fraude online

Si cualquier usuario es objeto de un fraude online lo primero que ha de hacer es dirigirse a las autoridades policiales para denunciar el caso, si fuera posible, en la zona en la que se ha cometido el delito. Es probable que en ese momento el usuario no pueda describir de forma completa y exacta qué es exactamente lo

que le ha ocurrido o cómo se ha perpetrado el fraude, pero el simple hecho de interponer la denuncia le puede servir como prueba ante los posibles acreedores que le puedan reclamar algún dinero relacionado con el fraude del que ha sido víctima.

Se pueden presentar denuncias al grupo especializado en delitos informáticos de la Policía Nacional ("Brigada de Investigación Tecnológica") a través del siguiente número de teléfono: 902 102 112, en su página web (http://www.policia.es/org_central/judicial/udef/bit_alertas.html) o en cualquier comisaría del Estado.

También se pueden presentar denuncias (o simplemente informar de un acto delictivo relacionado con los delitos informáticos) en el grupo de delitos telemáticos de la Guardia Civil (especializado en este tipo de casos), a través de su página web (https://www.gdt.guardiacivil.es/webgdt/home_alerta.php).

El siguiente paso a realizar por parte del usuario sería el cierre inmediato de las cuentas bancarias afectadas. Si el objeto del fraude han sido las tarjetas de crédito o bancarias, o cualquier otra cuenta de servicios online, se han de eliminar o cancelar dichas cuentas para evitar que el atacante se aproveche de ellas.

Para denunciar este hecho se ha de poner en contacto con la institución financiera, e informarse de los daños y repercusiones sufridos en su cuenta y los pasos que debe realizar en caso de que la cuenta haya resultado afectada durante un ataque. La institución financiera ha de indicarle cómo puede recuperar los cargos fraudulentos y los fondos perdidos en las cuentas afectadas. Dependiendo de cada institución financiera, éstas tendrán una serie de políticas y métodos de actuación para cada caso.

De forma adicional, el usuario ha de comunicar una alerta de fraude a las tres agencias nacionales de verificación de crédito para consumidores (Equifax, Experian y TransUnion). Realmente, es suficiente con comunicar el fraude a una de ellas, ya que ésta se la comunicará a las dos restantes. Esta alerta sirve para informar a los acreedores que soliciten el pago de alguna deuda relacionada con el fraude perpetrado, de que se han de poner en contacto

primeramente con el usuario para posteriormente si éste lo confirma poder pasar al cobro de la deuda, o si éste identifica ese cobro como un elemento relacionado con el fraude del que ha sido objeto, poder inmediatamente cancelarlo. Este paso es fundamental para poder tomar control de los movimientos bancarios que se realicen mientras pueda haber riesgo de fraude, además de servir como termómetro para comprobar el verdadero alcance del mismo.

Así, también es aconsejable que el usuario solicite sus informes de crédito a las tres agencias citadas, y examinar los mismos en búsqueda de anomalías. Es muy importante realizar este control exhaustivo, realizando comparaciones entre las cuentas de las tres agencias, para poder contrastar toda la información y comprobar que en todas ellas se reflejan los mismos movimientos y la misma información, comprobando que no existe diferencia alguna en los movimientos reflejados en los tres informes. Si se sospecha que los movimientos ilícitos pueden ser los últimos realizados, el usuario ha de ser consciente que éstos tardarán en reflejarse en los informes de cuentas, por lo que deberá estar atento a las actualizaciones de estos informes para comprobar la evolución de sus cuentas durante los últimos días.

Para finalizar, se ha de tener muy en cuenta la posibilidad de haber sufrido el llamado robo de identidad. Para verificar si ha sido así, el usuario ha de estar atento a posibles envíos postales inesperados o extraños, con productos que el usuario no ha solicitado, como pueden ser tarjetas de crédito o demás productos financieros o industriales. En adición, el usuario debe revisar todas las facturas que se le envíen para comprobar si son correctas o existe algún tipo de anomalía. Puede ocurrir que existan facturas de las que no se tiene conocimiento alguno, o aparecer proveedores que le soliciten el pago de cuentas de las que el usuario no tiene conocimiento alguno. Este tipo de situaciones están estrechamente relacionadas con el robo de identidad.

5.3 Delitos en la legislación complementaria

Existe un tercer grupo de delitos, que no están comprendidos como delitos informáticos en la clasificación de la Policía Nacional, pero están estrechamente ligados con estas tecnologías: ¿qué

sucede con actividades como el spam, el scaneo de puertos, comercio electrónico, etc. que no tienen cabida en el Código Penal?

En los casos en los que el infractor no puede ser perseguido por la vía penal, hay que acudir a la legislación propia que regula la sociedad de la información donde sí se encuentran tipificadas estas infracciones.

Así, en materia de protección de datos personales se ha de acudir a la "Ley Orgánica de Protección de Datos Personales" (LOPD), en cuestiones de la sociedad de la información y envío de correos electrónicos a la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico.

Con respecto a la presentación de denuncias cuando no se encuentra recogido el delito o falta dentro del Código Penal, se ha de recurrir a la legislación específica. En materia de protección de datos y comunicaciones comerciales la denuncia (totalmente gratuita) podrá ser instada de oficio o por parte del afectado o su representante legal ante la Agencia Española de Protección de Datos.

Con respecto a aquellos actos que infrinjan las obligaciones así reguladas por la Ley de Servicios de la Sociedad de la Información, a excepción del envío de correos comerciales, el órgano al que se deben presentar las denuncias oportunas es la Secretaría de Estado de Telecomunicaciones y Sociedad de la Información, adscrita al Ministerio de Industria, Turismo y Comercio.

6 CÓMO PREVENIR LOS FRAUDES INFORMÁTICOS

En este apartado se van a abordar todos los consejos y medidas de seguridad necesarias para prevenir, o al menos evitar en la medida de lo posible, el ser objeto de un fraude a través de la red.

6.1 Medidas de seguridad recomendadas

En las siguientes líneas se expondrán los consejos y medidas de seguridad que recomiendan las principales autoridades del Estado en la lucha contra los ciberdelitos.

Para comenzar, haremos una clasificación de los mismos en dos apartados: consejos acerca de su sistema, y costumbres y metodologías que ha de adoptar como usuario de internet para evitar ser víctima de estafas o fraudes informáticos.

6.1.1 Consejos relacionados con su sistema:

I. Tenga su sistema al día

- Se recomienda al usuario actualizar de forma periódica tanto el sistema operativo como todo el software instalado en el equipo, prestando especial atención a los navegadores web que se dispongan. Asimismo, se recomienda activar la función de actualización automática disponible tanto para los sistemas operativos como para la mayoría de los programas utilizados por el usuario.

- Se recomienda la realización de copias de seguridad del sistema de forma periódica, así como la creación de puntos de restauración para poder evitar la pérdida de información por incidentes de seguridad.

II. Reduzca el riesgo de infecciones de malware

- Se recomienda el uso tanto de software antivirus como de cortafuegos o firewall. Todas estas aplicaciones se pueden encontrar en la red (algunas de ellas de forma gratuita) y han demostrado ser un potente sistema de defensa y sobre todo protección de los sistemas informáticos.

- Si el usuario posee cualquier sistema operativo Windows, se recomienda que éste trabaje desde una cuenta de usuario que no posea privilegios de administrador, con el fin de evitar la posibilidad de instalación de muchos programas maliciosos.

- Se recomienda tener especial cuidado en el uso de las redes P2P, ya que han demostrado ser una importante fuente de infección de malware. Es aconsejable analizar todos los ficheros descargados a través de este tipo de redes con el antivirus del que se disponga.

- Se aconseja no abrir correos electrónicos no solicitados, o cuya procedencia se desconozca. Lo más seguro es eliminar este tipo de correos sin previsualizarlos.

- Se ha de utilizar siempre software legal. No es aconsejable realizar descargas de software de lugares de Internet cuya seguridad sea desconocida por el usuario, ya que muchas fuentes de malware provienen de la descarga gratuita de software.

- Por último, se recomienda al usuario la instalación en el equipo informático de algún tipo de software anti-spyware, de forma que se puedan evitar y detectar a tiempo posibles intrusiones en el equipo mediante programas espías destinados a sustraer información del equipo del que se está haciendo uso.

6.1.2 Consejos relacionados con la navegación en Internet: Métodos y procedimientos a realizar para una mayor seguridad como usuario.

I. Proteja su identidad

- Se aconseja utilizar contraseñas fuertes, es decir, que consten de más de 8 caracteres, y exista una combinación de letras números, mayúsculas, minúsculas y caracteres especiales.
- En el caso de recibir mensajes que pidan el reenvío del mismo a sus conocidos, se recomienda no seguir esta cadena de mensajes ya que el envío de este tipo de correos puede llevar acciones ocultas por parte del emisor original del correo en cuestión, tales como la captación de nuevas direcciones de correo electrónico para propósitos comerciales, o la búsqueda de algún tipo de engaño a los usuarios que reciben este tipo de información, con noticias falsas o bulos (hoax).

II. Evite que le estafen en la red

- Para evitar ser estafado en la red, se recomienda al usuario visitar páginas de confianza y con una reputación contrastada. Es aconsejable hacer caso omiso a vendedores que ofrecen súper ofertas, así como otros que ofrecen productos a precios fuera de mercado. Se aconseja buscar en la red referencias de cualquier vendedor del que estemos interesados en adquirir sus productos, antes de realizar cualquier tipo de compra. El usuario ha de ser precavido en las compras, especialmente con vendedores que digan residir en el extranjero y se aconseja el pago contra rembolso para evitar casos de compras en donde se envíe el dinero por adelantado y posteriormente no se reciba el artículo prometido a cambio. Los sistemas de envío de dinero por internet aportan al vendedor un alto grado de anonimato, de tal forma que será mucho más difícil la recuperación del mismo si se ha caído en una estafa.
- Se aconseja navegar por páginas web de confianza. Se pueden identificar ciertos sellos o certificados que garantizan la calidad y fiabilidad de la página en la que se está navegando (se abordará este tema en posteriores apartados

en este mismo documento). Se ha de extremar la precaución a la hora de realizar compras a través de la red o al facilitar datos personales a determinados sitios web u organizaciones. En estos casos reconocerá como páginas seguras aquellas que cumplan dos requisitos:

  - Deben empezar por https:// en lugar de http.
  - En la barra del navegador debe aparecer el icono del candado cerrado. A través de este icono se puede acceder a un certificado digital que confirma la autenticidad de la página.
  -

- Se ha de prestar especial atención en el uso de programas de acceso remoto. A través de internet y mediante estos programas, es posible acceder a un ordenador, desde cualquier otro. Por un lado, esto supone una gran ventaja, pero si se utiliza de forma ilícita esta herramienta, puede poner en peligro la seguridad del equipo informático.
- El usuario ha de ser consciente de que cualquier empresa relativamente grande, no manda correos con dominios de Gmail, Hotmail o Yahoo, ya que poseen su propio dominio, por lo que si el usuario recibe este tipo de correos de empresas grandes con ese tipo de dominios, ha de desconfiar de ellos y eliminarlos por la propia seguridad del sistema.
- No crea en las herencias, loterías o inversiones millonarias que, casualmente, le han correspondido, ni en los negocios piramidales.

III. Detecte el riesgo en la banca electrónica

- Se recomienda al usuario acceder al sitio web de su banco introduciendo el mismo la dirección web en la barra de direcciones del navegador, evitando acceder a este tipo de sitios web a través de enlaces externos o mensajes de correo, ya que le pueden re direccionar a páginas web aparentemente originales pero que son fraudulentas, y puede finalmente ser objeto de un fraude.
- El usuario se ha de cerciorar del tipo de comunicación que se está empleando a la hora de navegar a través del sitio web de

su banco: la comunicación con los bancos es siempre a través de protocolos seguros (https).

- Se recomienda cerrar la sesión personal al finalizar sus consultas en su sitio web bancario, ya que si cierra la ventana del navegador sin haber cerrado previamente la sesión, deja una puerta abierta a través de la cual los delincuentes informáticos pueden acceder a su cuenta bancaria, al no haberla cerrado correctamente.
- Se aconseja desconfiar de los mensajes de correo electrónico o SMS procedentes de supuestas entidades bancarias. El usuario ha de confirmar vía telefónica, en su sucursal bancaria, cualquier petición que reciba de datos de banca electrónica.

IV. Su privacidad en redes sociales

- En las redes sociales, se recomienda a los usuarios limitar el acceso de la información que compartan, a personas conocidas (amigos o personas de confianza). Cuanto más amplio sea el círculo de contactos (amigos de mis amigos y todos los usuarios), a mayores riesgos se expone el usuario y da una mayor facilidad para que terceras personas puedan disponer de la información privada que se refleje en su perfil.
- Se aconseja no colgar fotografías ni vídeos privados que no le gustaría que se difundieran. Una vez en la red, no pueden retirarse.
- Sea prudente a la hora de suscribirse a grupos o eventos. En muchos de ellos no se sabe con certeza a quién estamos permitiendo ver nuestros datos.
- Es importante habilitar la navegación segura (https) para dificultar el robo de contraseñas y escuchas en las comunicaciones.

En general, es fundamental estar al día de la aparición de nuevas técnicas que amenazan la seguridad de su equipo informático, para tratar de evitarlas o de aplicar la solución más efectiva posible.

6.2 ¿Cómo reconocer una página web fraudulenta?

En ocasiones, los usuarios no saben si están en un sitio web legítimo, o por el contrario se encuentran navegando por páginas que pueden suponerles una amenaza, por lo que para poder avisar al usuario de la legitimidad de la web por la que se está navegando, y comunicar la fiabilidad de la web visitada como un sitio totalmente confiable y seguro, existen una serie de elementos (como los certificados digitales, otorgados por organismos oficiales) que las páginas web legítimas obtienen y que hacen que el usuario se pueda sentir totalmente seguro mientras visita un determinado sitio web.

Para que este proceso sea sencillo de llevar a cabo, los usuarios pueden comprobar la legitimidad de las páginas web donde se hallan a través de una serie de códigos de colores que los navegadores asocian al nivel de seguridad y legitimidad que otorgan al sitio web por el que se está navegando, como veremos en el siguiente apartado.

6.2.1 Página confiable si…

Si la barra de direcciones es de color verde, se puede estar seguro de que la página es de la entidad que dice ser.

Internet Explorer

- Fondo de la barra de direcciones en color verde
- Aparece el nombre de la entidad al lado del candado, también en fondo verde.

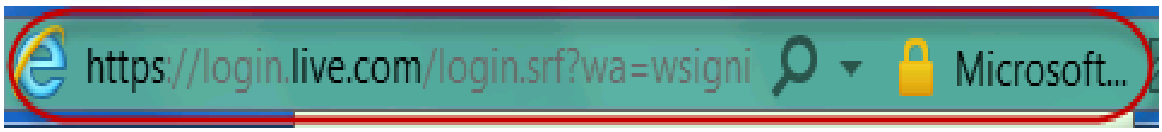


Ilustración 65: Barra de navegación Internet Explorer en sitio web confiable

Mozilla Firefox

- En el icono de la página aparece el nombre de la entidad y todo ello con fondo verde.

Ilustración 66: Barra de navegación de Mozilla Firefox en sitio web confiable

Google Chrome

- En el icono de la página aparece el nombre de la entidad con un candado y si se está usando el protocolo https, se encuentra señalado en verde.

Ilustración 67: Barra de navegación de Google Chrome en sitio web confiable

Opera

- En el icono de la página aparece el nombre de la entidad con un candado y el fondo en verde.

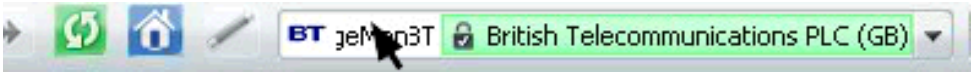


Ilustración 68: Barra de navegación de Opera en sitio web confiable

Safari

- Aparece el nombre de la entidad, con fondo verde cuando se pasa el cursor por encima.

Ilustración 69: Barra de navegación de Safari en sitio web confiable

6.2.2 Página confiable (con restricciones) si…

Si la página visitada muestra el protocolo "https" pero la barra de direcciones no aparece de color verde, puede ser debido a que el certificado de la página en cuestión no se ha verificado que pertenezca realmente a la entidad que asegura representar, en ese

caso, se ha de tener en cuenta una serie de elementos adicionales para poder confiar plenamente en la seguridad de la página visitada:

- La dirección de la página visitada pertenece a la entidad.
- El usuario debe comprobar si ha escrito correctamente todos los caracteres en la barra de navegación, ya que en ocasiones, algunos infractores compran dominios que se diferencian en apenas un carácter de otras entidades legítimas, y crean sitios web idénticos, con la esperanza de que cualquier usuario teclee mal el nombre de la entidad en la barra de direcciones y finalmente acabe en su página web fraudulenta.

En cualquier caso, si el usuario está completamente seguro de que la página en la que se encuentra es de confianza, puede utilizarla.

Internet Explorer

- Aparece un candado con fondo azul, que al pulsarlo nos muestra el certificado que garantiza la conexión segura y el nivel de legitimidad.

Ilustración 70: Candado de Internet Explorer

Mozilla Firefox

- En el icono de la página que está a la izquierda de la barra de direcciones, aparece el nombre de la entidad y todo ello con fondo azul.

Ilustración 71: Barra de navegación de Mozilla Firefox con fondo azul

Safari

- Aparece un candado en el extremo derecho de la barra de direcciones, pero no aparece el fondo verde, ni el nombre de la entidad.

Ilustración 72: Barra de navegación de Safari con candado

6.3 Peritaje Informático

En ocasiones, las empresas o particulares pueden tener ciertas sospechas sobre la realización de actividades ilícitas de algunos de sus empleados, por lo que una opción muy común en el entorno empresarial es la contratación de peritos informáticos, cuya misión fundamental es la investigación a fondo de cualquier actividad sospechosa de ser fraudulenta por parte de cualquier empleado o entidad que guarde relación con la empresa contratante.

De esta forma, los pasos principales (a grandes rasgos) que ha de seguir un perito a lo largo de la investigación son la obtención de pruebas, la realización de un informe, y, si fuera necesario, la declaración ante un juez o un tribunal en los casos más graves.

6.3.1 Fases

Normalmente, el método seguido durante una investigación informática consta de tres periodos o fases: toma de contacto, desarrollo de la investigación y elaboración del informe, y por último, si fuese necesario, declaración en los tribunales. Este número de fases es el usado más habitualmente por todas las empresas del sector, aunque también puede variar dependiendo de los métodos propios que utilice cada empresa privada para elaborar el informe pericial. A continuación se describirá cada una de estas fases con mayor detalle.

El método seguido para llevar a cabo una investigación informática consta de tres fases:

1. **Toma de contacto:**

   La toma de contacto es la fase donde se comienzan a fijar los objetivos de la investigación y a trazar las líneas fundamentales a trabajar. Comprende, a su vez, tres etapas:

- Análisis de la situación inicial:

  El perito informático lleva a cabo un análisis de la situación inicial donde se cerciora de los principales problemas que ha de solventar y los aspectos fundamentales a tratar. Posteriormente, tras analizar la situación el perito informático se reúne con el cliente, en donde se discuten aspectos como:

  - se fijan los objetivos de la investigación
  - se realiza un estudio de viabilidad
  - se establece el procedimiento a seguir para la extracción de pruebas
  - se estiman los tiempos de ejecución, la fecha tope de la investigación y el dead-line[32].

- Presupuesto del servicio de peritaje informático:

  Tras discutir los aspectos antes mencionados, el perito informático elabora un presupuesto para recabar todas las pruebas posibles y en el que se incluye todas las acciones que se han de ejecutar para obtenerlas.

- Aceptación del presupuesto:

  Esta fase es una mera formalidad donde el cliente recibe el presupuesto y si finalmente acepta la oferta, se comenzará con las labores de peritaje informático.

2. Desarrollo de la investigación y elaboración del Informe:

Tras la primera fase, los peritos informáticos comienzan su "trabajo de campo", centrándose en la búsqueda y recopilación de cualquier tipo de pruebas que lleven a demostrar cualquier aspecto de la investigación. Se podría decir que el perito informático realiza una labor de investigación como si de un detective se tratase, donde su labor fundamental se centrará en poder recolectar pruebas que puedan demostrar al cliente (o incluso a un tribunal) lo ocurrido en cada momento en relación al caso objeto de estudio. Para ello, se procede a efectuar la recogida de los elementos que pueden intervenir en la investigación, como equipos informáticos, dispositivos de almacenamiento, etc.

El perito informático realiza un análisis exhaustivo de dichos elementos, y en base a las conclusiones que vaya recogiendo de los análisis realizados, comienza a redactar el informe pericial que presentará al propio cliente, y si fuera necesario, ante los Tribunales de Justicia.

3. **Declaración ante Tribunales:**

   En caso de que sea necesario, el perito informático que ha elaborado el informe, testificará ante los Tribunales de Justicia para aportar las conclusiones de la investigación.

6.3.2 Evidencias electrónicas

Las evidencias electrónicas son pruebas físicas aunque de carácter intangible, ya que suelen ser rastros o acciones que quedan registradas en un equipo informático y que sirven para probar la participación o realización de algún tipo de acción por parte de un usuario concreto a través de un sistema informático determinado. Se podría decir que son las "huellas digitales" de los ciberdelincuentes.

Hoy en día, todos los datos introducidos o manipulados en un ordenador quedan registrados, de tal forma que todas las actividades que el usuario realiza pueden ser seguidas o estudiadas tiempo después. Este hecho permite a los peritos informáticos poder realizar un seguimiento exhaustivo a cualquier usuario, siguiendo las pistas que van dejando estos logs[33], se puede determinar el tipo de actividades que ha estado desempeñando un determinado usuario en el equipo informático, y así poder verificar si se ha hecho un uso correcto de las herramientas puestas a su disposición o si por el contrario no ha hecho un buen uso, o incluso ha cometido algún delito a través de ese equipo.

A partir de esta última observación, podemos cerciorarnos de la importancia capital de dichos registros o logs en las investigaciones informáticas, siempre que se pueda comprobar que no han sido manipulados. Los servidores de correo, cortafuegos o el router también generan logs, por lo que pueden ser analizados de igual forma en la búsqueda de pruebas que determinen el autor de una determinada infracción o delito.

Existen herramientas especializadas en la investigación informática como por ejemplo:

- OSSIM: Sistema de monitorización de seguridad, de tecnología Open Source[34], que permite acceder a toda la información recogida y almacenada por el recolector, permitiendo al administrador analizar, a posteriori y de forma centralizada, los eventos de seguridad de todos los elementos críticos de la red. Básicamente resuelve el problema de dónde buscar la evidencia digital.

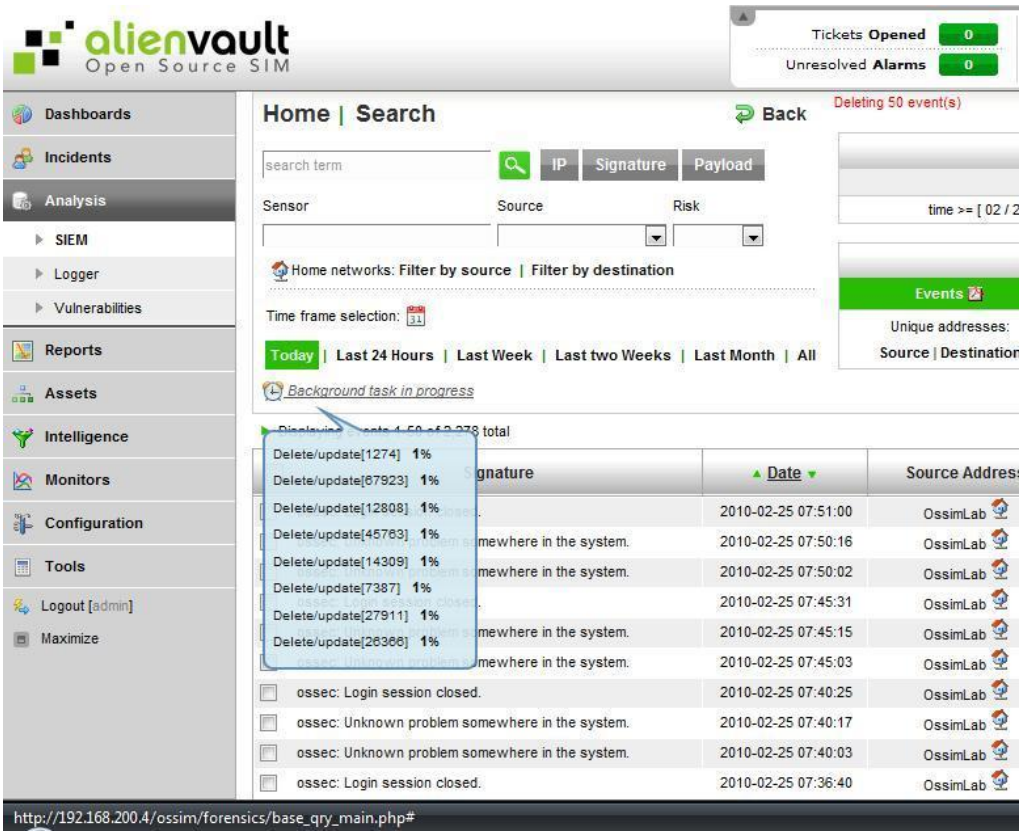


Ilustración 73: Captura de pantalla del software OSSIM

- The Forensic ToolKit: Se trata de una colección de herramientas forenses para plataformas Windows, creadas por el equipo de Foundstone.

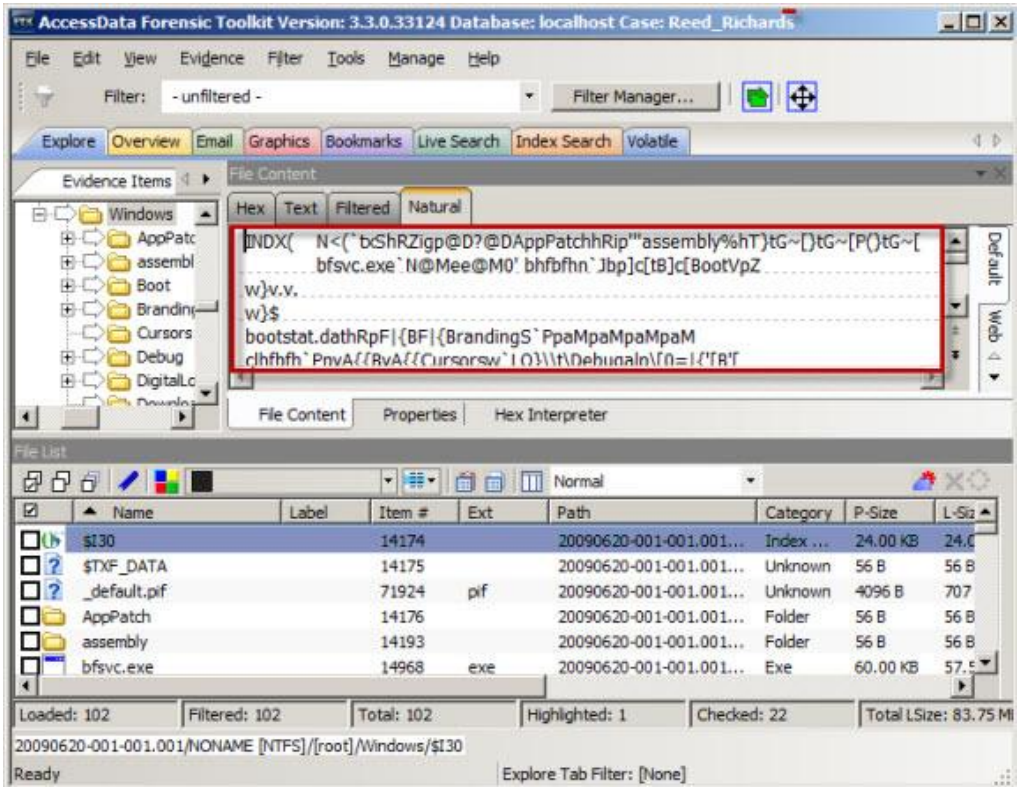


Ilustración 74: Captura de pantalla de The Forensic Toolkit

- The Sleuth Kit y Autopsy: Consistente en una colección de herramientas forenses para entornos UNIX/Linux. De libre distribución, incluye funciones como registro de casos separados e investigaciones múltiples, acceso a estructuras de archivos y directorios de bajo nivel y eliminados, genera la línea temporal de actividad de los archivos, permite buscar datos dentro de las imágenes por palabras clave, permite crear notas del investigador e incluso genera informes.
- HELIX CD: Se trata de un Live CD de respuesta ante incidentes, basado en una distribución Linux denominada Knoppix. Posee la mayoría de las herramientas necesarias para realizar un análisis forense tanto de equipos como de imágenes de disco.

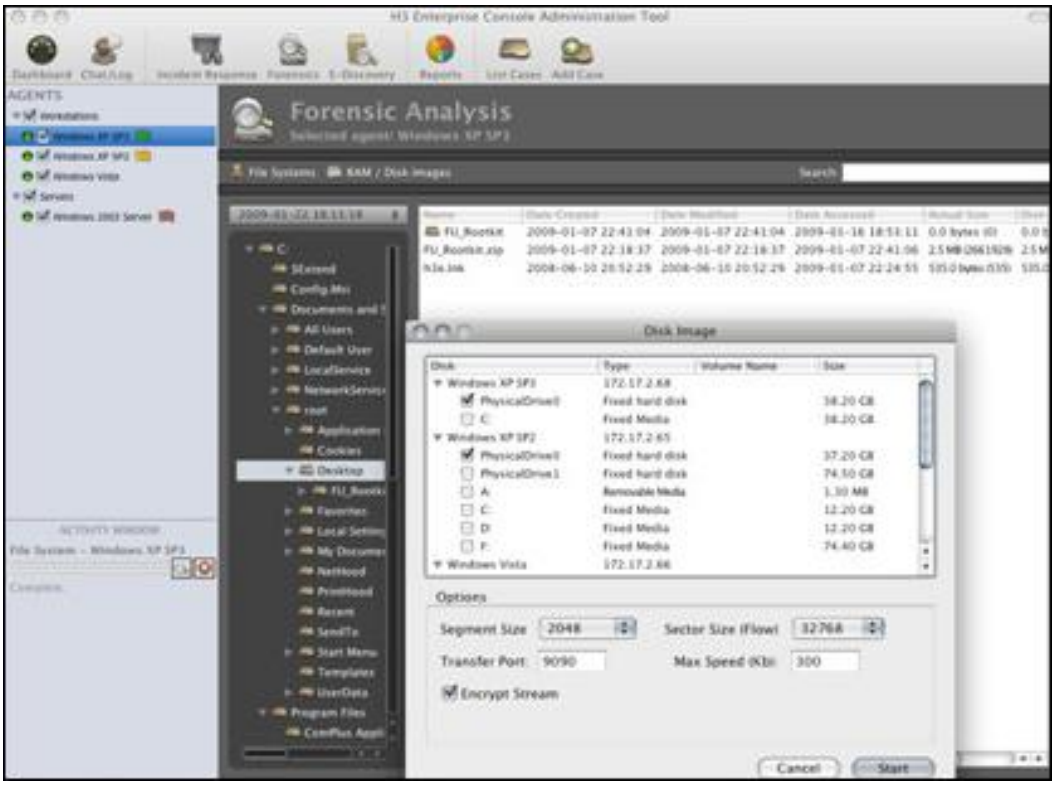


Ilustración 75: Captura de pantalla de Helix CD

Durante el proceso de investigación, suelen aparecer algún tipo de problemas para poder reconstruir las evidencias electrónicas, ya que por ejemplo, puede que éstas hayan sido modificadas adrede por los propios infractores, o encontrarse dañadas, o directamente haber sido eliminadas, por lo que es de suma importancia contar con herramientas tecnológicas que permitan la recuperación de los datos, elemento fundamental ya que normalmente son las pruebas principales que se pueden presentar en casos con estas características. Algunas herramientas software anteriormente mencionadas ayudan a realizar este tipo de procedimientos, facilitando la labor del perito a la hora de recuperar datos borrados o dañados.

Durante el proceso de adquisición y tratado de la evidencia electrónica, el perito informático debe seguir dos conceptos de manera escrupulosa:

- La no alteración de la prueba.
- El principio de imparcialidad.

Con el fin de garantizar la autenticidad y seguridad de la información que constituye la prueba, la IOCE (International Organization on Computer Evidence) propone cinco principios sobre la adquisición y el tratamiento de la evidencia electrónica, que se pasan a enumerar:

8 Las acciones llevadas a cabo para adquirir la evidencia electrónica no deben modificarla.
9 Las personas que accedan a la evidencia electrónica original deben estar formadas especialmente para ello.
10 Toda aquella actividad referente a la adquisición, acceso, almacenamiento o transferencia de la evidencia electrónica, debe ser totalmente documentada, almacenada y debe estar disponible para revisión.
11 Un individuo es responsable de todas las acciones llevadas a cabo con respecto a la evidencia electrónica mientras ésta está en su posesión.
12 Cualquier organismo que sea responsable de la adquisición, acceso, almacenamiento o transferencia de la evidencia electrónica debe cumplir estos principios.

6.3.3 Informe pericial

En este apartado vamos a describir la metodología que usan los peritos a la hora de realizar el informe final que va a llegar a manos de la empresa que los ha contratado. Las partes de que ha de constar y los procedimientos que siguen los peritos para su realización y la obtención de las conclusiones finales.

El Informe pericial debe incluir:

- Los datos del cliente.
- Los objetivos de la investigación.
- La declaración previa del perito informático, en la que se establecen los principios de profesionalidad, veracidad e independencia.
- Documentación sobre el proceso de adquisición de pruebas.
- Detalle de las acciones que el perito informático lleva a cabo durante la investigación.
- Resultados de la investigación informática y conclusiones.

La elaboración del informe consta a su vez de tres fases:

1. **Fase de adquisición de las pruebas:**

   En esta fase el perito procede a examinar todos los elementos del entorno que necesite y estén disponibles, recogiendo el máximo número de pruebas posibles, pero respetando escrupulosamente todas las garantías para las dos partes durante la intervención de los equipos informáticos.

   Todas las pruebas recogidas pasarán a formar parte de la información que se deba plasmar en el informe pericial.

2. **Fase de la investigación:**

   El perito informático revisa y analiza cada uno de los equipos informáticos que estime oportunos, en la búsqueda de elementos que supongan una evidencia electrónica y puedan llevar a detener a los infractores.

   En el informe el perito ha de describir con sumo detalle qué acciones ha llevado a cabo, qué herramientas usó para realizar dichas acciones, y qué evidencias electrónicas halló a partir de las mismas, para cada uno de los dispositivos estudiados.

3. **Fase de elaboración de la memoria.**

   En esta fase, el perito redacta el informe que se presentará a la empresa contratante (o ante los Tribunales en caso de que fuera necesario) con las conclusiones finales que ha obtenido a partir de la investigación realizada.

6.3.4 Casos reales

En este apartado vamos a exponer algunos casos reales de peritajes informáticos realizados por la empresa de seguridad informática "Recovery Labs" a empresas reales y exponer los métodos de investigación llevados a cabo y las soluciones dadas a cada uno de los casos expuestos, con el fin de poner en contraste la teoría expuesta en los anteriores apartados y ver cómo se lleva a la práctica por empresas profesionales del sector.

6.3.4.1 Caso de fuga de datos

En este caso, tras haber realizado previamente un exhaustivo análisis de la situación inicial, se determinó que el objetivo de la investigación informática que se iba a llevar a cabo era demostrar que el responsable de las Tecnologías de Información de una compañía estaba sacando información confidencial de la empresa, con el fin de tomar las medidas necesarias contra dicho empleado.

Para llevar a cabo la investigación, se realizó un análisis exhaustivo al equipo usado por el empleado en cuestión, mediante el cual se comprobó que por dicho ordenador habían pasado archivos que no tenían por qué estar ahí como: nóminas de empleados, actas del consejo de administración, etc. Además, al poner en común los resultados con el cliente, se descubrió que el acceso a los documentos confidenciales se había producido en períodos de tiempo en los que el empleado no se encontraba dentro de la empresa, lo que llevó a abrir otra vía de investigación.

Se solicitó a la compañía el acceso al router de la empresa por parte del perito informático y se analizaron los registros de alerta del sistema.

Examinando dichos registros se comprobó que el empleado había iniciado sesiones remotas desde su domicilio fuera del horario de oficina, a través de las cuales había sacado información confidencial de la empresa.

Los registros de alerta del sistema supusieron la evidencia electrónica buscada por los peritos, por lo que el informe final elaborado por el perito informático sirvió para probar que el IT manager era el responsable de la fuga de datos confidenciales de esta compañía.

6.3.4.2 Caso de uso indebido de internet (Pornografía Infantil)

En este caso la empresa contratante sospechaba que un trabajador estaba utilizando el ordenador portátil de la compañía para conectarse a páginas de descarga ilegal de música.

El objetivo de la investigación informática era probar que desde el equipo y con el usuario del empleado en cuestión se estaba realizando un uso indebido de las herramientas que la empresa ponía a su disposición, en este caso internet.

Tras examinar varios registros que no dieron ninguna pista concluyente, se decidió investigar los archivos temporales de internet. Al proceder a la inspección de los elementos temporales, el hallazgo fue mucho más desagradable de lo que cabía esperar. Se descubrieron más de 20.000 imágenes de contenido pornográfico, de las que gran parte eran pornografía infantil.

Con este descubrimiento se tuvo, por un lado, la evidencia electrónica necesaria para probar que se estaba utilizando ese equipo con fines extra laborales y, además, se tenía la obligación de poner en conocimiento de las autoridades lo que se había descubierto. Por lo tanto, se decidió redactar el informe pericial que cerraba el caso de peritaje informático solicitado por el cliente y denunciar lo ocurrido a las autoridades competentes.

Como resultado de esta investigación, fue abierto un proceso penal en contra del usuario del equipo.

7 EVOLUCIÓN DE LOS CIBERDELITOS EN LOS PRÓXIMOS AÑOS

En anteriores secciones de este documento se han analizado los diferentes tipos de fraude que han existido y existen en la actualidad, pero ¿cuáles serán las nuevas amenazas informáticas que nos deparará el futuro?

Para saber responder esta pregunta, primero debemos analizar los últimos informes que recogen el estado actual de los ciberdelitos.

7.1 Principales delitos informáticos cometidos en el año 2011

Durante el pasado año (2011) las principales amenazas a los sistemas informáticos fueron las siguientes:

1. Aumento del "Hacktivismo"[35]. Una de las principales tendencias de 2011 que, sin duda continuará dando mucho que hablar en 2012 y años sucesivos.

2. Hackeo de HBGary Federal. O cómo las contraseñas débiles y los sistemas de software anticuados unidos al uso de cloud convierten la seguridad en una pesadilla.

3. Advanced Persistent Threats (APTs). Estos ataques confirman la consolidación del ciber-espionaje como práctica común entre altas esferas estatales.

4. La confianza en las autoridades certificadoras (CA) ha estado bajo amenaza (una prueba de ello son los ataques contra Comodo y DigiNotar). En el futuro, es muy probable que aparezca más malware de firma digital.

5. Duqu y Stuxnet. Estado del arte de la ciberguerra. ¿Veremos el nacimiento de la Ciber Guerra Fría?

6. Hackeo de la red Sony PlayStation. Los nuevos peligros escondidos tras la nube. Información personal accesible en un solo sitio, lista para ser robada en caso de desconfiguración o problemas de seguridad.

7. Desarticulación de botnets y la batalla contra el ciberdelito. Las bandas organizadas de ciberdelito han comprobado cómo sus timos conllevan riesgos. Cada batalla contra el ciberdelito evidencia las limitaciones de nuestro actual sistema legal en lo que se refiere a afrontar el ciberdelito con contundencia.

8. El aumento de malware para Android. Diversos factores convierten a Android en un objetivo vulnerable para el ciberdelito: crecimiento rápido, acceso gratuito a la documentación de la plataforma y escaneado débil en Google Market, facilitando la subida de programas maliciosos.

9. El incidente de CarrierIQ. ¿Sabes qué hay instalado en tu dispositivo móvil? Un solo incidente nos mostró los pocos datos que tenemos sobre quién controla nuestro hardware.

10. Malware para Mac OS. El salto de la amenazas de PC al sistema operativo de Mac ha sido una de las importantes tendencias del pasado 2011 y continuará en el año que comienza.

7.2 Previsiones sobre delitos que se perpetrarán durante el año 2012 y sucesivos

Podemos ver un par de gráficos muy representativos sobre las previsiones realizadas por las empresas de seguridad informática más prestigiosas, acerca de las amenazas que han copado (y que se espera que sigan copando) los primeros puestos durante el año 2012 y sucesivos:

Vendor	CISCO	FORTINET	KASPERSKY	McAfee	SOPHOS	TREND MICRO	websense
APT							
Attacks to Online Banking				Via Mobile Devices			
Attacks via SSL/TLS							
Adoption of DLP							
Adoption of DNSSEC							
Crime as a Service							
Cyber Weapons							
Clampdown on Money Laundering							
Cloud							
Consumerization						BYOD	
New ways to hide for Criminals							
Data Theft Trojans							
Diversification of Targets (OS)							
Embedded Hardware							
Fine Tuned attacks vs SMBs							
Hactivism							
High Profile Loss							
Malware moving beyond OS							
Mass Targeted Attack						Smaller Botnets	
Mobile		Ramsomware Worm Polymorphism	Vulnerability Morphing Geolocation			Vulnerability	
NFC							
Public-Private Relationship in Security							
Rogue Certificates							
SCADA							
Scareware							
SEO Poisoning							
Social Media							
SPAM Going "legitimate"							
Virtual Currency							
Web Exploits					Leveraging new technologies		

Ilustración 76: Comparativa entre las predicciones de diferentes empresas dedicadas a la seguridad informática para 2012

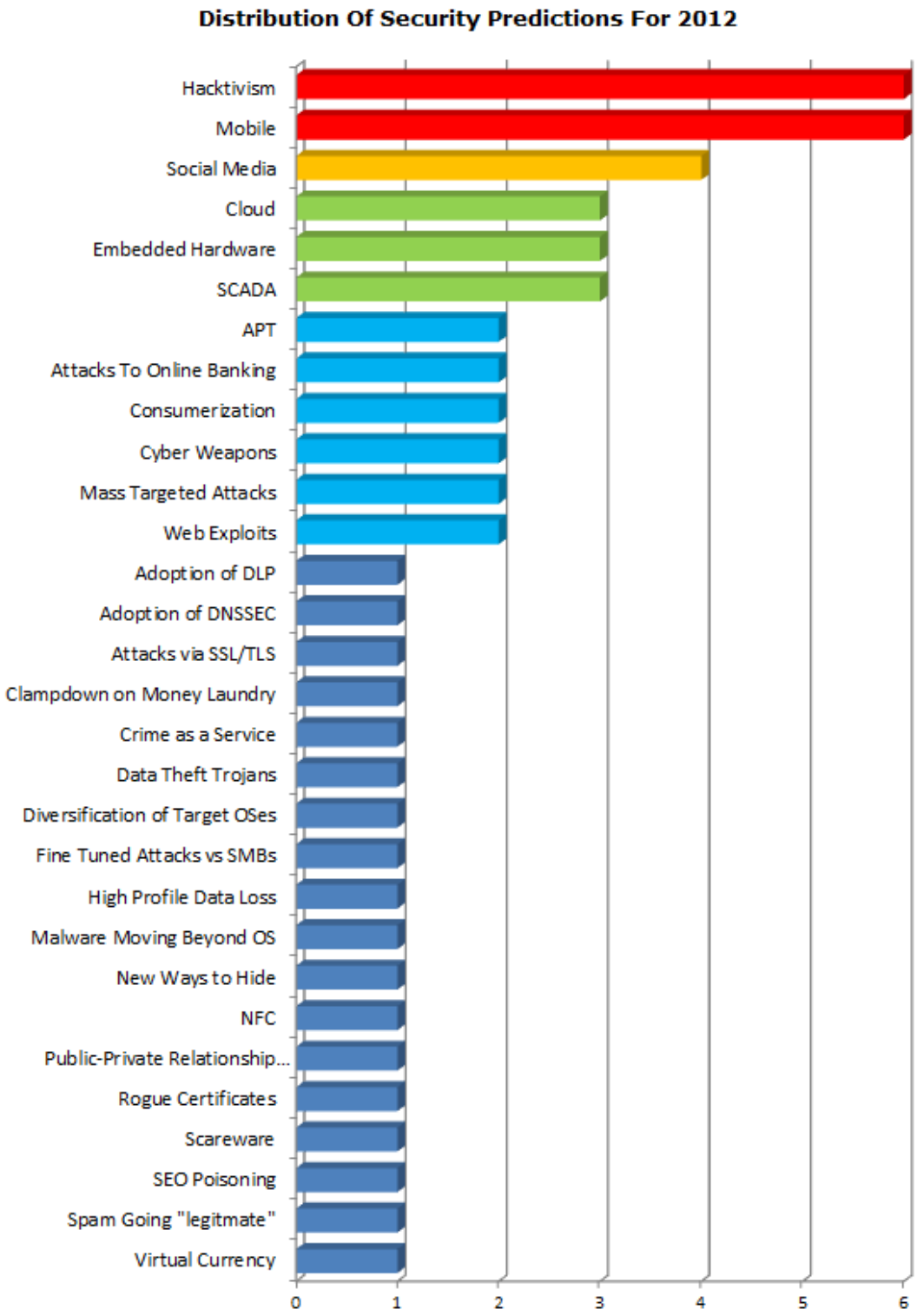


Ilustración 77: Predicciones de amenazas para la seguridad informática durante 2012, realizadas por la empresa Trend Micro

7.3 ¿Hacia dónde vamos?: Previsión sobre los principales delitos informáticos de la próxima década.

En las siguientes líneas se pretende realizar una recopilación de las principales amenazas que se presentarán en el ámbito informático durante la próxima década, prestando especial atención a la explicación de las mismas y su problemática, buscando una fácil comprensión de las nuevas amenazas y explicando las posibilidades de defensa que tienen los usuarios ante las mismas.

7.3.1 Hacktivismo: una amenaza latente y en expansión

7.3.1.1 ¿Qué es el hacktivismo?

Esta práctica consiste en el ataque organizado a través de la red a un objetivo concreto, con el fin de producirle una caída del sistema (ya sea el sitio web de la empresa o ente atacado, su correo electrónico, etc.) y como consecuencia la no operatividad de estos recursos.

Son muchos los analistas que indican que el hacktivismo se ha posicionado como una de las mayores amenazas en internet en estos últimos años, siendo de especial singularidad estos ataques, dadas las características de los mismos. Generalmente vienen promovidos por organizaciones ilícitas como los ya mundialmente conocidos "Anonymous"[36] y motivados por un trasfondo social o político, que nada tiene que ver con las motivaciones de los hackers comunes, que hasta hace muy poco tiempo eran principalmente económicas.

Los hacktivistas se sirven de la red para poder organizar y tratar de atacar de forma coordinada los sitios web de entidades bancarias, organizaciones gubernamentales, partidos políticos, etc. fundamentalmente por medio de ataques de denegación de servicio (DDoS), en respuesta a lo que estas nuevas organizaciones creen ataques injustos o desmedidos hacia entidades que consideran

legítimas (famoso es el caso de MegaUpload y el posterior ataque al sitio web del FBI), o situaciones políticas que los atacantes creen injustas y en donde deciden actuar atacando a través de la red a entidades por motivos políticos (estas organizaciones han realizado recientemente ataques a los sitios web de los gobiernos de Siria, Egipto o Túnez, entre otros, como medida de protesta por la situación social y política vivida en estos países).
Como podemos ver en el siguiente gráfico (extraído del informe anual de la empresa norteamericana "Arbor Network", dedicado a analizar las amenazas informáticas producidas durante el año 2011) el protagonismo de este tipo de actividad ha tomado una relevancia notable (teniendo en cuenta que esta práctica no existía hace pocos años):

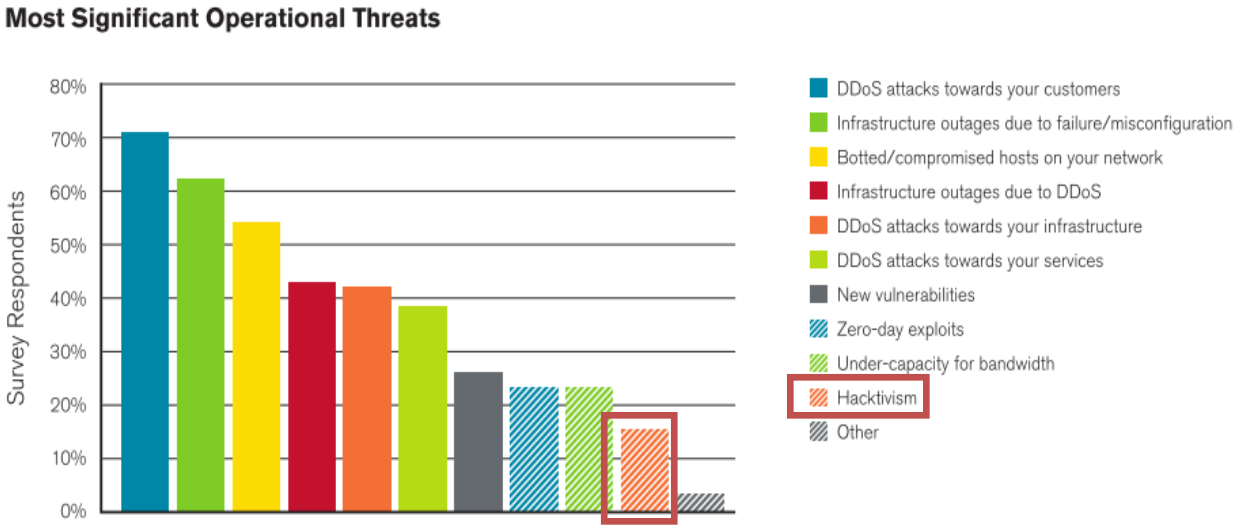


Ilustración 78: Resumen de las amenazas más significativas durante el año 2011, elaborado por Arbor Networks

Así, en el informe también se recoge una encuesta entre las empresas que sufrieron algún tipo de ataque informático, donde se puede ver la incipiente preocupación por la proliferación del hacktivismo y sus recientes ataques:

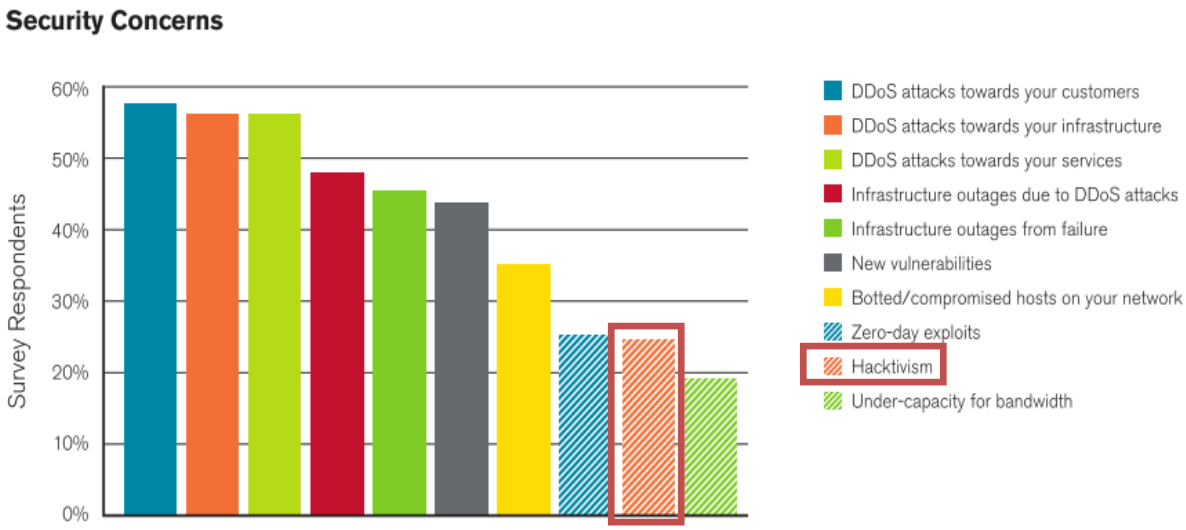


Ilustración 79: Principales amenazas según las empresas encuestadas por Arbor Networks

En los anteriores gráficos se observa como la preocupación principal de los encuestados son los ataques DDoS, y sabiendo que ese es el sistema de ataque usado por los hacktivistas, podríamos interpretar que este tipo de ataques DDoS recogidos en el gráfico anterior podrían ser producidos por los mismos hacktivistas, a los cuales se encuadra en otra clasificación en el gráfico. De hecho, en el mismo informe que ha servido de referente para estas líneas, se propusieron realizar una encuesta a los miembros de las empresas escogidos para ser entrevistados, preguntando los motivos por los cuales creían que se realizaban estos ataques de denegación de servicio, obteniendo los siguientes resultados:

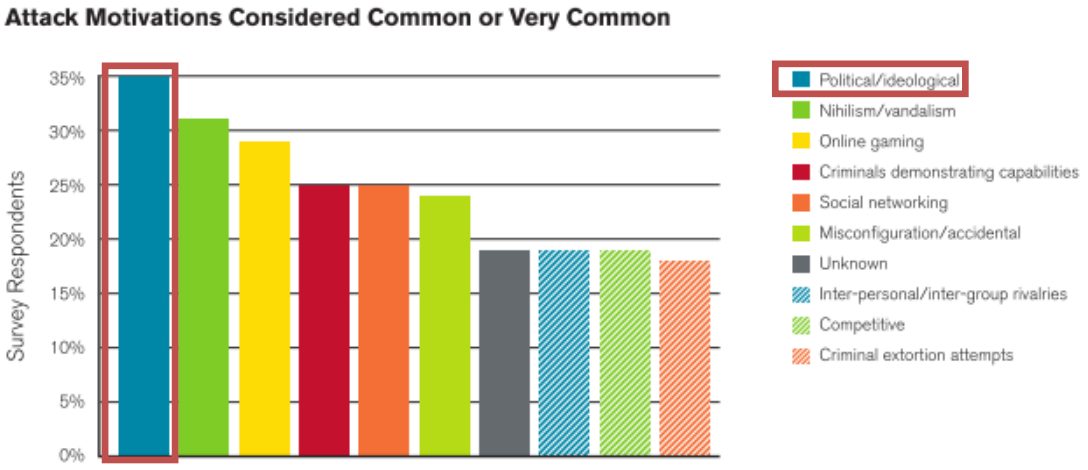
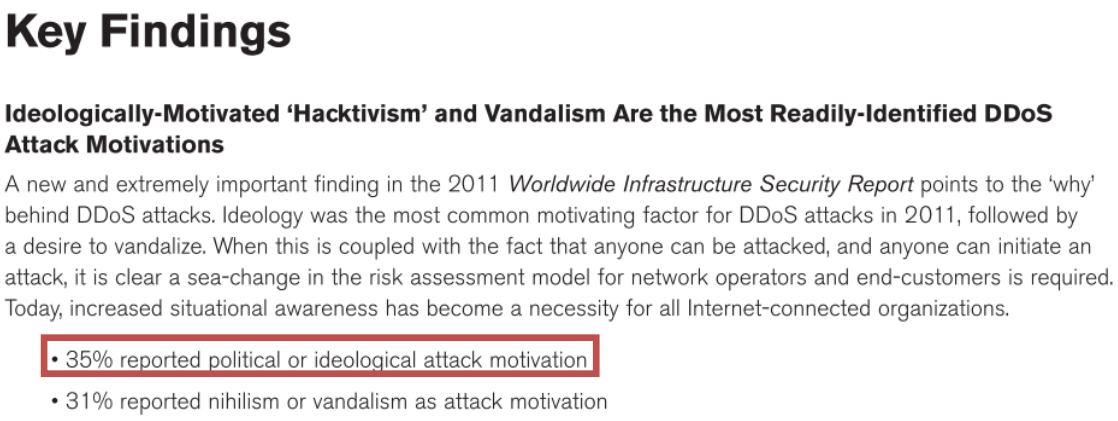


Ilustración 80: Gráfica sobre los motivos de ataque de los ciberdelincuentes

Por lo tanto, podemos pensar que aparte del porcentaje de amenazas de seguridad asignado al Hacktivismo en sí, podríamos sumar el porcentaje de ataques de denegación de servicio que se

han perpetrado por motivos ideológicos o políticos, concluyendo que si a priori el hacktivismo parece una amenaza que ha penetrado con fuerza en estos últimos tiempos, lo es aún más cuando le sumamos estos porcentajes de ataques DDoS directamente relacionados con el hacktivismo. En el propio informe de Arbor Networks, finalizan la encuesta con esta serie de conclusiones:



Key Findings

Ideologically-Motivated 'Hacktivism' and Vandalism Are the Most Readily-Identified DDoS Attack Motivations

A new and extremely important finding in the 2011 *Worldwide Infrastructure Security Report* points to the 'why' behind DDoS attacks. Ideology was the most common motivating factor for DDoS attacks in 2011, followed by a desire to vandalize. When this is coupled with the fact that anyone can be attacked, and anyone can initiate an attack, it is clear a sea-change in the risk assessment model for network operators and end-customers is required. Today, increased situational awareness has become a necessity for all Internet-connected organizations.

- 35% reported political or ideological attack motivation
- 31% reported nihilism or vandalism as attack motivation

Ilustración 81: Resumen acerca de las motivaciones de los ciberdelincuentes a la hora de perpetrar un ataque

De esta forma, cabe destacar que como conclusión principal, en un primer momento podemos esperar que los directivos de las grandes empresas tiendan a evitar decir que atacan a sus entidades por motivos políticos e ideológicos, atribuyendo estos ataques al vandalismo informático o a usuarios que persiguen un objetivo económico, pero como se puede apreciar, sorprendentemente los entrevistados han afirmado que atribuyen la mayoría de los ataques DDoS al hacktivismo, de tal forma que a los resultados del primer gráfico, donde el 16% de los encuestados consideraba al hacktivismo como una amenaza capital, le hemos de sumar el 35% de los ataques DDoS (que representa un 55% en la primera encuesta), ya que en la segunda encuesta los consideran motivados por el hacktivismo. En total, sumando estos dos parámetros, obtenemos que el hacktivismo es considerado como una gran amenaza para el 36% de las grandes empresas confirmando que en pocos años ha pasado de ser una amenaza inexistente a ser uno de los mayores problemas de seguridad de las mayores empresas mundiales.

7.3.1.2 ¿Cómo se realizan estos ataques? Metodología y software empleado por los hacktivistas

Hasta el momento parece clara la idea de la aparición de un nuevo grupo de usuarios dispuestos a realizar ataques a grandes entidades o corporaciones internacionales de forma coordinada, obteniendo hasta el momento resultados bastante exitosos, siendo eficaces atacantes y, como se refleja en los informes internacionales, ganándose el temor de las grandes corporaciones, pero, ¿cómo han conseguido una serie de usuarios poner en jaque a autoridades como el FBI o diferentes gobiernos del mundo? ¿Qué estrategias y herramientas usan estas organizaciones en sus ataques?

7.3.1.3 Ataques Distribuidos de Denegación de Servicio (DDoS)

Gran parte del éxito en las acciones que llevan a cabo los hacktivistas en la red se debe a su filosofía como grupo anónimo y su forma de interrelacionarse entre ellos.

Una de las peculiaridades de los hacktivistas es el método de ataque que emplean: los conocidos como ataques DDoS o ataques distribuidos de denegación de servicio, los cuales tienen como cometido principal entorpecer el acceso de los usuarios al servidor.

Esta técnica se basa en atacar a un sistema de computadores o red para provocar la pérdida de conectividad por el consumo del ancho de banda que producen los hacktivistas durante el tiempo que perdure el ataque, sobrecargando los recursos computacionales del sistema víctima. La idea de los hacktivistas es sobrecargar el servidor mediante la saturación de los puertos con flujo de información y así impedir que éste siga prestando servicios a los clientes que lo soliciten, es decir, si un servidor puede dar conexión a un número determinado de clientes, los hacktivistas tratarían de realizar muchas más peticiones de servicio de las que el servidor pudiera gestionar, provocando que se produjesen las denominadas "denegaciones de servicio" que simplemente serían producto de la imposibilidad técnica por parte del servidor de dar cobertura a más clientes de los que realmente puede procesar. Por lo tanto, los hacktivistas serían "falsos usuarios" que colapsarían de forma intencionada estos servidores, e imposibilitarían su normal uso a los usuarios legítimos, ya que estarían ocupando toda la capacidad del servidor. Generalmente, los hacktivistas realizan este tipo de

ataques de forma distribuida, es decir, generan un gran flujo de información desde varios puntos de conexión, por lo tanto, la clave para que estos ataques tengan éxito será el número de usuarios dispuestos a atacar simultáneamente a un determinado sistema. Si por ejemplo, los hacktivistas realizan un ataque a un determinado servidor, cuantos más usuarios realicen este ataque, más peticiones de servicio va a tener que procesar el servidor atacado, por lo que en algún momento los hacktivistas pueden llegar a conseguir que el servidor "caiga" y no pueda ofrecer sus servicios al resto de usuarios.

Cabe destacar que en este tipo de ataques la denegación del servicio continuará mientras los atacantes sigan realizando peticiones de servicio contra el servidor, cuando estas peticiones vayan disminuyendo, llegará un momento en el que el servidor podrá dar servicio de nuevo a todos sus clientes.

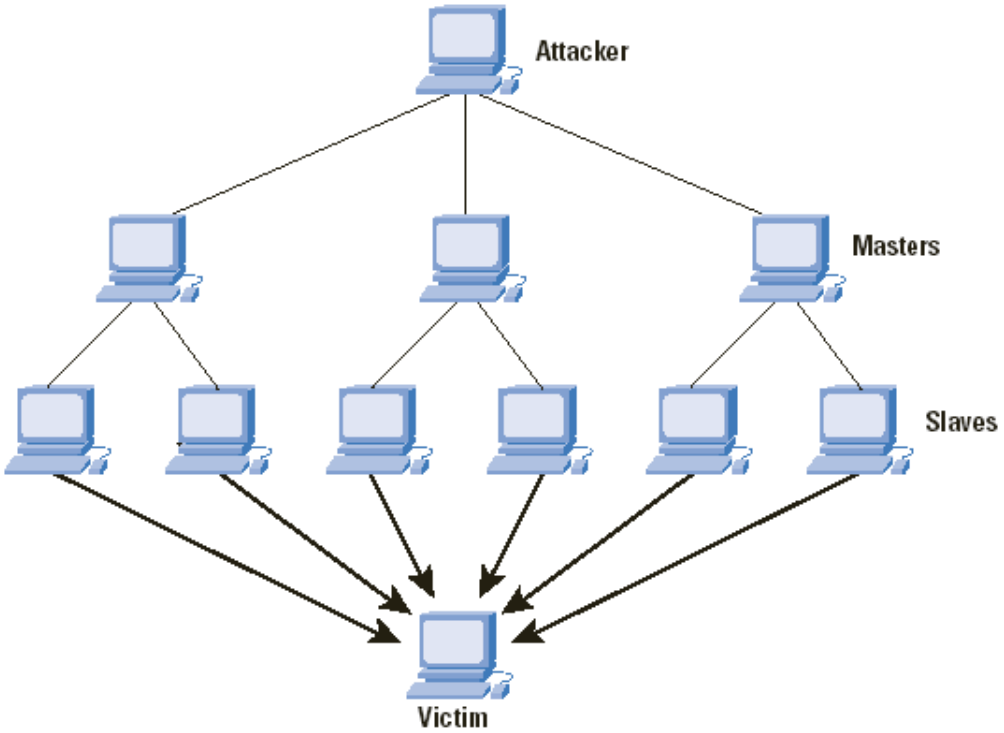


Ilustración 82: Esquema de un ataque DDOS

La peculiar manera de organizarse y relacionarse por parte de los hacktivistas hace que sea muy difícil identificar quienes forman parte de estas organizaciones, y más aún demostrar su implicación en los ataques que ejecutan.

Un ataque se comienza a labrar cuando una serie de hacktivistas lo proponen en diferentes medios a través de la red (foros, chats, etc. normalmente, organizaciones como Anonymous frecuentan determinados chats como "http://www.4chan.org/", afines a sus ideas). Generalmente cuando ya se ha pensado un determinado ataque a una empresa u organización (como se ha mencionado antes, basados o inspirados en motivos políticos e ideológicos) pasan al siguiente paso del proceso, donde intentan dar la mayor publicidad posible a este ataque, buscando sitios de difusión masiva (normalmente en portales como http://www.youtube.com/ y canales similares de difusión de vídeos, además de multitud de blogs personales, páginas web que difunden la noticia, etc.) donde los usuarios comunes de internet puedan encontrarla fácilmente, en busca de posibles aliados que compartan o defiendan las causas ideológicas o hechos concretos por los que los hacktivistas desean protestar.

Una vez que se ha conseguido la mayor difusión posible, sólo queda esperar el día y hora anunciados para realizar el ataque al sitio web señalado. Evidentemente, el éxito de un ataque DDoS de los hacktivistas residirá en el número de usuarios dispuestos a realizarlo y que tecnológicamente tengan las herramientas suficientes para ser capaces de perpetrarlo, por lo que ¿cómo pueden solventar este problema los hacktivistas?

7.3.1.4 ¿Qué hacer para poder realizar un ataque DDoS?: De usuario común a amenaza latente para un sitio web.

Evidentemente, cuando realizan los hacktivistas un ataque a un determinado sistema, no realizan una sola petición de servicio por cada uno de los hacktivistas involucrados, ya que resultarían ser una amenaza muy pobre, debiéndose juntar muchísimos miles de usuarios dispuestos a realizar el ataque a la vez para poder ser una amenaza real, y además tener que ir renovando esa petición de servicio constantemente para suponer un peligro durante un tiempo más o menos prolongado. Para que cada uno de los hacktivistas que realizan el ataque sea una amenaza seria para un sistema, éstos usan determinados software con los que realizan miles de peticiones por segundo de forma automática.

Existen varios software que organizaciones como Anonymous recomiendan a los usuarios y ponen a su disposición para que éstos puedan descargarlos libremente y puedan contar con ellos para poder realizar los ataques. Los más conocidos son:

LOIC: Low Orbit Ion Cannon (Cañón de Iones de Órbita Baja) originalmente es un software utilizado para pruebas de estrés en red. De código abierto y escrito en C#, sirve para ejecutar ataques distribuidos de denegación de servicio sobre un sitio web objetivo, inundando al servidor objetivo mediante paquetes TCP, UDP o realizando múltiples peticiones HTTP. Estos tipos de ataques son muy similares, abriendo múltiples conexiones con el servidor objetivo para enviar cadenas predeterminadas.

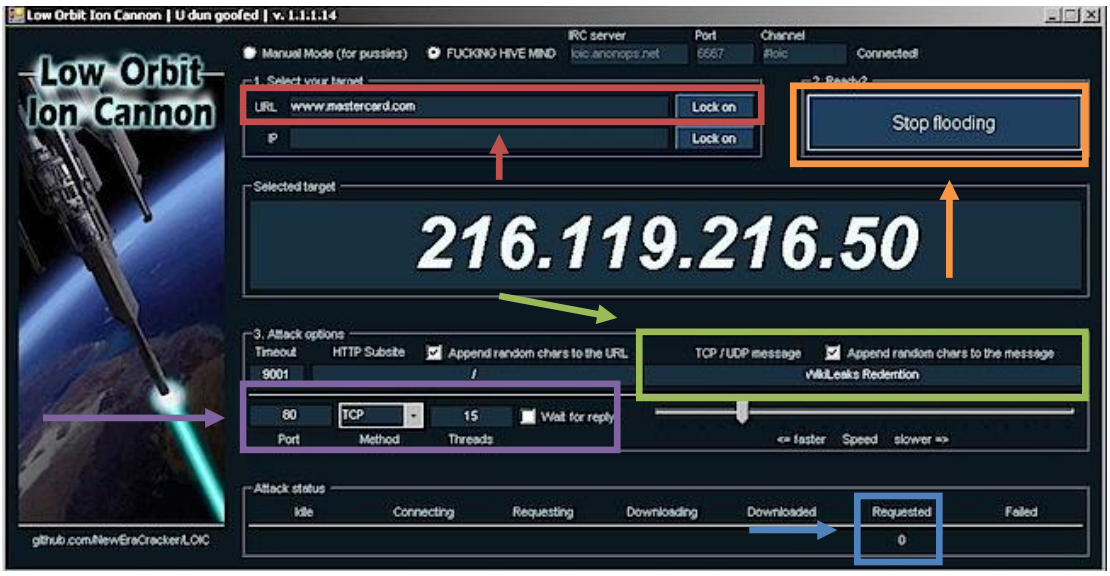


Ilustración 83: Captura de pantalla del software LOIC utilizado por Anonymous

En la imagen anterior vemos la interfaz de este software. Se puede observar que cualquier usuario con conocimientos mínimos sobre redes e internet puede utilizar este programa casi intuitivamente.

En el cuadro señalado en rojo vemos como se pide la URL del sitio web objetivo. Simplemente habría que introducir una dirección válida, y automáticamente el programa descifra su dirección numérica, como vemos en el centro de la imagen. El recuadro naranja señala el botón que acciona el usuario para comenzar a enviar mensajes o para detener los mismos.

El recuadro morado indica que podemos configurar el protocolo que usaremos para el envío de mensajes, en este caso se elige TCP y el recuadro verde señala al campo en el que el usuario introduce el mensaje que desea que se envíe en cada uno de los mensajes al servidor objetivo.

Por último, el recuadro azul señala el número de peticiones que hemos realizado desde que comenzó el ataque.

REFREF: Escrito en Perl, a diferencia de LOIC que inundaba el servidor objetivo con paquetes UDP y TCP, la herramienta REFREF se basa en la petición de consultas SQL, más dañinas ya que le suponen un procesamiento más costoso al servidor objetivo, y por lo tanto puede colapsarse con menos esfuerzo por parte de los atacantes. Como particularidad, los expertos que ya han probado la herramienta afirman que sólo consta de 51 líneas de código que aseguran ser suficientes para constituir esta herramienta como una amenaza poderosísima. A continuación podemos ver un extracto del código empleado:

```
sub now {
print "\n[+] Target : ".$_[0]."\n";
print "\n[+] Starting the attack\n[+] Info : control+c for stop attack\n\n";
while(true) {
$SIG{INT} = \&adios;
$code = toma($_[0]." and (select+benchmark(99999999999,0x70726f62616e646f70726f62616e646f70726f62616e646f))");
unless($code->is_success) {
print "[+] Web Off\n";
copyright();
}}}
```

Ilustración 84: Código empleado para la elaboración de RefRef

La clave de este código es la consulta SQL llevada a cabo en la siguiente línea:

```
select benchmark(99999999999,0x70726f62616e646f70726f62616e646f70726f62616e646f)
```

Ilustración 85: Consulta SQL en el código de Ref Ref

Donde se pide evaluar la expresión:

```
0x70726f62616e646f70726f62616e646f70726f62616e646f)
```

Ilustración 86: Extracto de código hexadecimal de RefRef

100 trillones de veces (primer argumento de la función anterior). Esta expresión está codificada en hexadecimal, pero pasándola a código ascii[37] podemos comprobar que la expresión a evaluar es "probandoprobandoprobando". Esta técnica generalmente sirve como benchmark[38] para realizar pruebas de estrés a determinadas aplicaciones de un sistema, pero en este caso se puede utilizar para provocar la caída de un sistema al completo.

Hasta el momento, dado que REFREF aún es una herramienta casi experimental, se han realizado muy pocas pruebas. Algunos expertos han realizado pruebas en su propio ordenador sin atacar sitios web públicos por temor a ser denunciados, y por ahora se han obtenido pruebas en donde tras ejecutar REFREF en la consola de comandos de Windows de un ordenador personal:

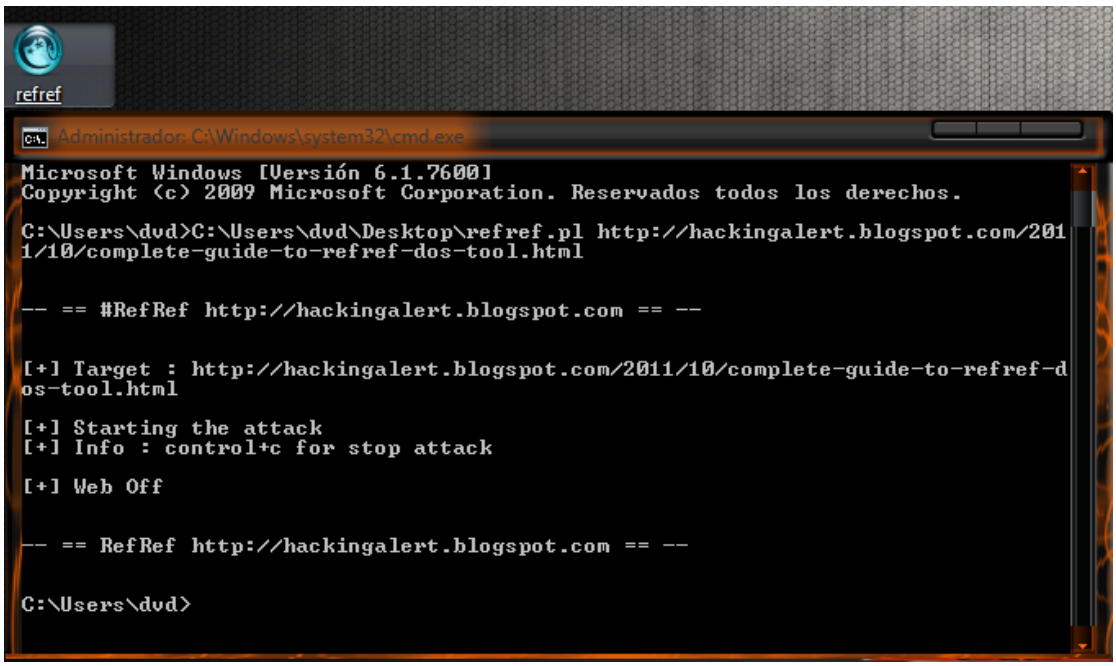


Ilustración 87: Ejecución del software RefRef

Se ha tardado solamente 25 segundos en colapsar de consultas SQL la base de datos.

Hasta el momento, los expertos que han analizado esta herramienta han realizado una serie de estudios donde recomiendan que para evitar ser víctima de este tipo de ataques, los servidores deben de estar protegidos y adaptados para no permitir inserciones SQL o consultas a la base de datos del servidor, para evitar si quiera que éste intente procesar las peticiones del cliente atacante.

```
RewriteEngine on
RewriteCond %{QUERY_STRING} .*(/\*|union|select|insert|cast|set|declare|drop|update|md5|benchmark) [NC]
RewriteRule .* - [R=406,L]
```

Ilustración 88: Ejemplo de código para proteger la base de datos de un servidor

También recomiendan bloquear las consultas SQL que se realicen a través del protocolo HTTP usando para ello una clave de acceso que pueda filtrar las peticiones no deseadas:

```
* 1:19870 <-> ENABLED <-> DOS Anonymous Perl RefRef DoS tool (dos.rules)
* 1:19869 <-> ENABLED <-> DOS Anonymous PHP RefRef DoS tool (dos.rules)
```

Ilustración 89: Código de ejemplo para protegerse de RefRef

Así, podríamos proteger nuestros servidores con filtros sencillos de implementar y poder evitar ataques a través de estos protocolos. Esto resulta de vital importancia, ya que como se ha plasmado en recientes estudios realizados podemos observar el número de peticiones de "falsos usuarios" realizadas a través de los diferentes protocolos de red:

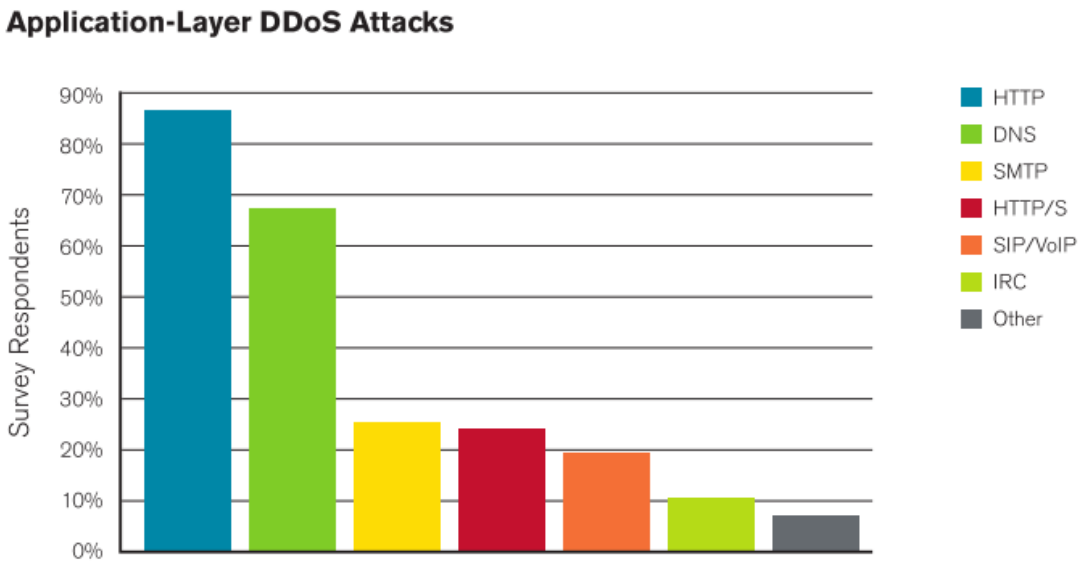


Ilustración 90: Gráfica que muestra los tipos de ataque DDoS más utilizados

Fuente: Arbor Networks

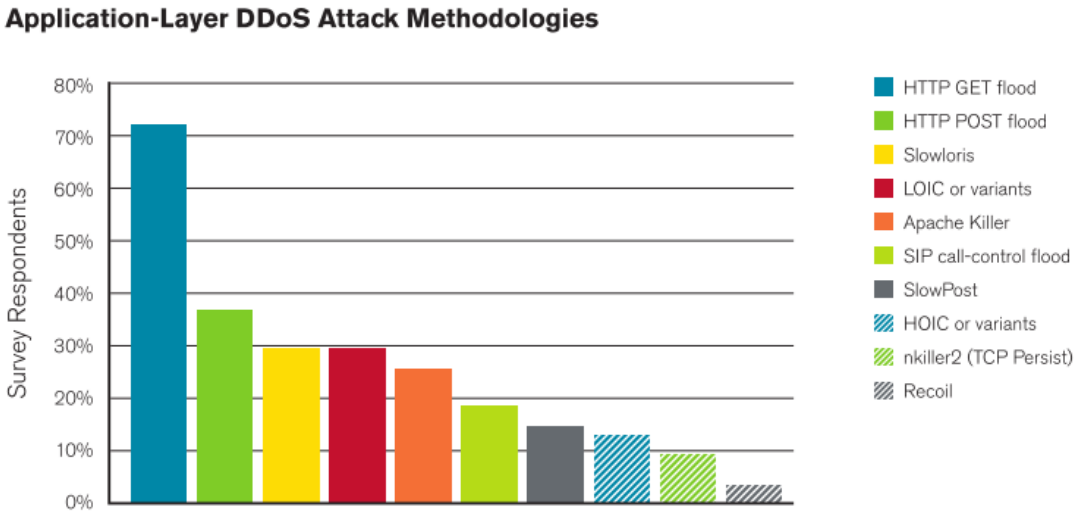


Ilustración 91: Gráfica con las metodologías más empleadas en los ataques DDoS

Fuente: Arbor Networks

Donde vemos que el protocolo más usado para perpetrar los ataques es el HTTP.

7.3.1.5 Software complementario

Como se ha visto, para un usuario es sencillo obtener y usar algún tipo de software para poder realizar ataques, pero estos programas no tienen ninguna función para ocultar la dirección IP del atacante, por lo que el hacktivista generalmente utiliza procesos adicionales para poder ocultar su dirección IP y evitar ser detectado de manera sencilla. Generalmente, le basta con obtener algún software que proteja su IP al navegar por Internet, como por ejemplo CyberGhost, o software similares. Aunque lo más frecuente es el uso de redes virtuales privadas o VPN para poder ocultar su IP, asegurándose cierto grado de anonimato en la red. También es común el uso de la denominada red Tor, basada en el encadenamiento de proxies en cascada para la transmisión de los mensajes de los usuarios de esta red, de forma que se guarde el anonimato de éstos, y que sea muy difícil rastrear un mensaje hasta llegar a la IP que emitió determinado mensaje. Aunque todas estas técnicas de ocultación de IP no son 100% seguras, la mayoría de los hacktivistas las usan como protección y en diferentes organizaciones como Anonymous recomiendan su uso para todos aquellos usuarios que deseen colaborar con ellos. Sólo cuando el

hacktivista ha logrado ese anonimato a través de estos procesos, comienza a realizar los ataques DDoS.

Esto ha llevado a que cualquier usuario con unos conocimientos medios de Internet y realmente interesado en colaborar con organizaciones como Anonymous, pueda de una manera realmente sencilla descargarse el software que estas organizaciones ponen a su disposición de forma gratuita y comenzar a realizar ataques contra sistemas objetivo, haciendo de la unión y la coordinación sus puntos fuertes para poder dirigir ataques realizados por usuarios anónimos, y su creciente popularidad las convierten en amenazas potenciales para las grandes empresas en un futuro muy próximo.

7.3.1.6 Conclusiones sobre el hacktivismo

Así, vemos como se está produciendo una evolución en las motivaciones que llevan a las personas a realizar actos ilícitos en internet; si bien al comienzo de la era informática estábamos hablando de personas que se entrometían en las redes de empresas o entidades simplemente como satisfacción personal y para alertar a las propias empresas de las vulnerabilidades de sus sistemas y deficiencias en la seguridad de los mismos, pudimos comprobar como con el paso de los años y el aumento de las transacciones comerciales a través de la red se cambiaron las motivaciones de los atacantes, los cuales pasaron a perseguir un beneficio económico, modificando también los tipos de herramientas usadas, los métodos de actuación, etc., buscando siempre ser lo más silenciosos y transparentes posibles.

Hoy en día, en el año 2012, la tendencia está cambiando paulatinamente, y si bien aún sigue habiendo multitud de atacantes que tienen como principal objetivo el afán de lucro, empiezan a existir grandes "ejércitos" de usuarios que mediante un software sofisticado pero de fácil uso comienzan a cambiar el perfil del atacante, y sobre todo sus motivaciones, que pasan a tener un carácter social, de protesta y de rechazo hacia ciertas organizaciones, empresas o gobiernos, alejándose de los incentivos económicos como motivación principal.

7.3.2 HBGary Federal: Más allá de la denegación de servicio

Como se ha comentado en el anterior apartado, los motivos ideológicos están siendo la motivación más importante de los atacantes en los últimos tiempos. Ya se ha puesto en escena la problemática del hacktivismo y sus cada vez más temidos ataques de denegación de servicio, pero no es la única técnica que utilizan estas organizaciones como forma de protesta. Prueba de ello fue el caso del hackeo a las oficinas HBGary Federal llevado a cabo en el año 2011, donde Anonymous burló la web oficial de esta empresa y la remplazó por un texto donde explicaban sus motivos para hackearla, además de manipular los datos de la empresa de seguridad acerca del malware, productos, finanzas, telefonía y sobre todo, el sistema de correo electrónico:

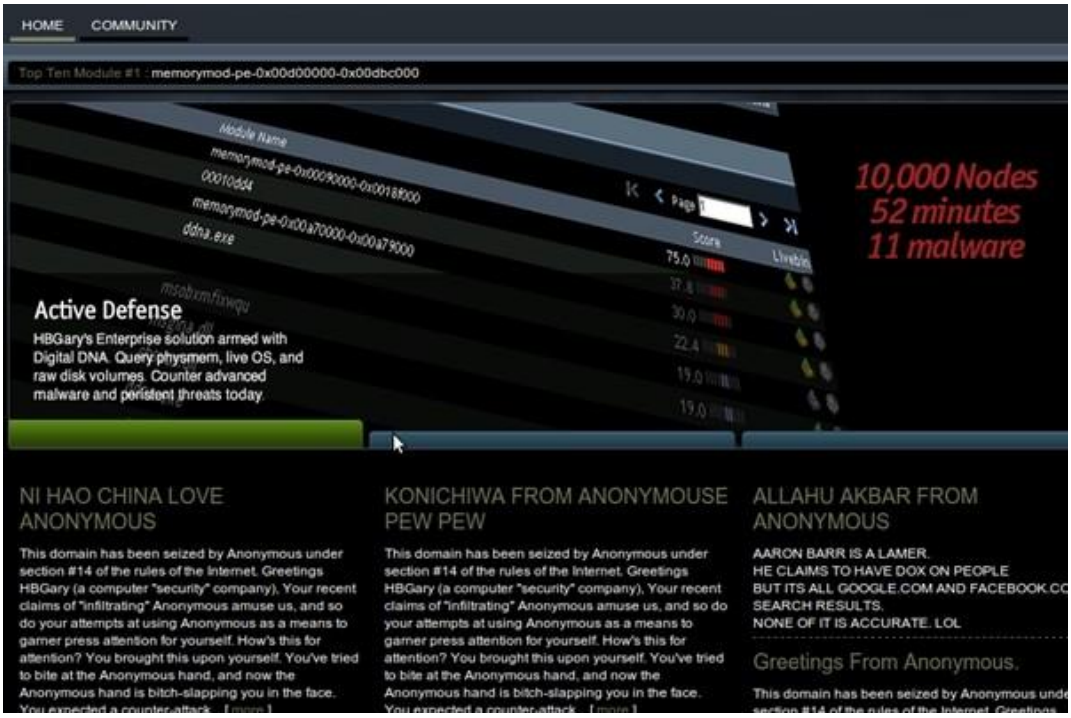


Ilustración 92: Página de inicio de HBGaryfederal.com después del hackeo

This domain has been seized by Anonymous under section #14 of the rules of the Internet.

Greetings HBGary (a computer "security" company),

Your recent claims of "infiltrating" Anonymous amuse us, and so do your attempts at using Anonymous as a means to garner press attention for yourself. How's this for attention?

You brought this upon yourself. You've tried to bite at the Anonymous hand, and now the Anonymous hand is bitch-slapping you in the face. You expected a counter-attack in the form of a verbal braul (as you so eloquently put it in one of your private emails), but now you've received the full fury of Anonymous. We award you no points.

What you seem to have failed to realize is that, just because you have the title and general appearence of a "security" company, you're nothing compared to Anonymous. You have little to no security knowledge. Your business thrives off charging ridiclous prices for simple things like NMAPs, and you don't deserve praise or even recognition as security experts. And now you turn to Anonymous for fame and attention? You're a pathetic gathering of media-whoring money-grabbing sycophants who want to reel in business for your equally pathetic company.

Let us teach you a lesson you'll never forget: you don't mess with Anonymous. You especially don't mess with Anonymous simply because you want to jump on a trend for public attention, which Aaron Barr admitted to in the following email:

"But its not about them...its about our audience having the right impression of our capability and the competency of our research. Anonymous will do what every they can to discredit that. and they have the mic so to speak because they are on Al Jazeeera, ABC, CNN, etc. I am going to keep up the debate because I think it is good business but I will be smart about my public responses."

You've clearly overlooked something very obvious here: we are everyone and we are no one. If you swing a sword of malice into Anonymous' innards, we will simply engulf it. You cannot break us, you cannot harm us, even though you have clearly tried...

You think you've gathered full names and home addresses of the "higher-ups" of Anonymous? You haven't. You think Anonymous has a founder and various co-founders? False. You believe that you can sell the information you've found to the FBI? False. Now, why is this one false? We've seen your internal documents, all of them, and do you know what we did? We laughed. Most of the information you've "extracted" is publicly available via our IRC networks. The personal details of Anonymous "members" you think you've acquired are, quite simply, nonsense.

So why can't you sell this information to the FBI like you intended? Because we're going to give it to them for free. Your gloriously fallacious work can be a wonder for all to scour, as will all of your private emails (more than 66,000 beauties for the public to enjoy). Now as you're probably aware, Anonymous is quite serious when it comes to things like this, and usually we can elaborate gratuitously on our reasoning behind operations, but we will give you a simple explanation, because you seem like primitive people:

You have blindly charged into the Anonymous hive, a hive from which you've tried to steal honey. Did you think the bees would not defend it? Well here we are. You've angered the hive, and now you are being stung.

It would appear that security experts are not expertly secured.

```
We are Anonymous.
We are legion.
We do not forgive.
We do not forget.
Expect us - always.
```

Download HBGary email leaks

Ilustración 93: Comunicado de Anonymous tras el hackeo a HBGary

Se puede ver como este tipo de organizaciones están llevando a cabo acciones más sofisticadas que las hasta ahora vistas, poniendo en peligro información confidencial de la compañía atacada, como fue en este caso, donde cerca de 60.000 e-mails de empleados de la compañía fueron descargados y publicados en el portal "The Pirate Bay". Como se puede ver en la imagen anterior, estos emails estuvieron en descarga directa mediante un enlace mientras duró el hackeo a la página principal de la compañía, un ejemplo de los múltiples correos a los que se tuvo acceso es el siguiente:

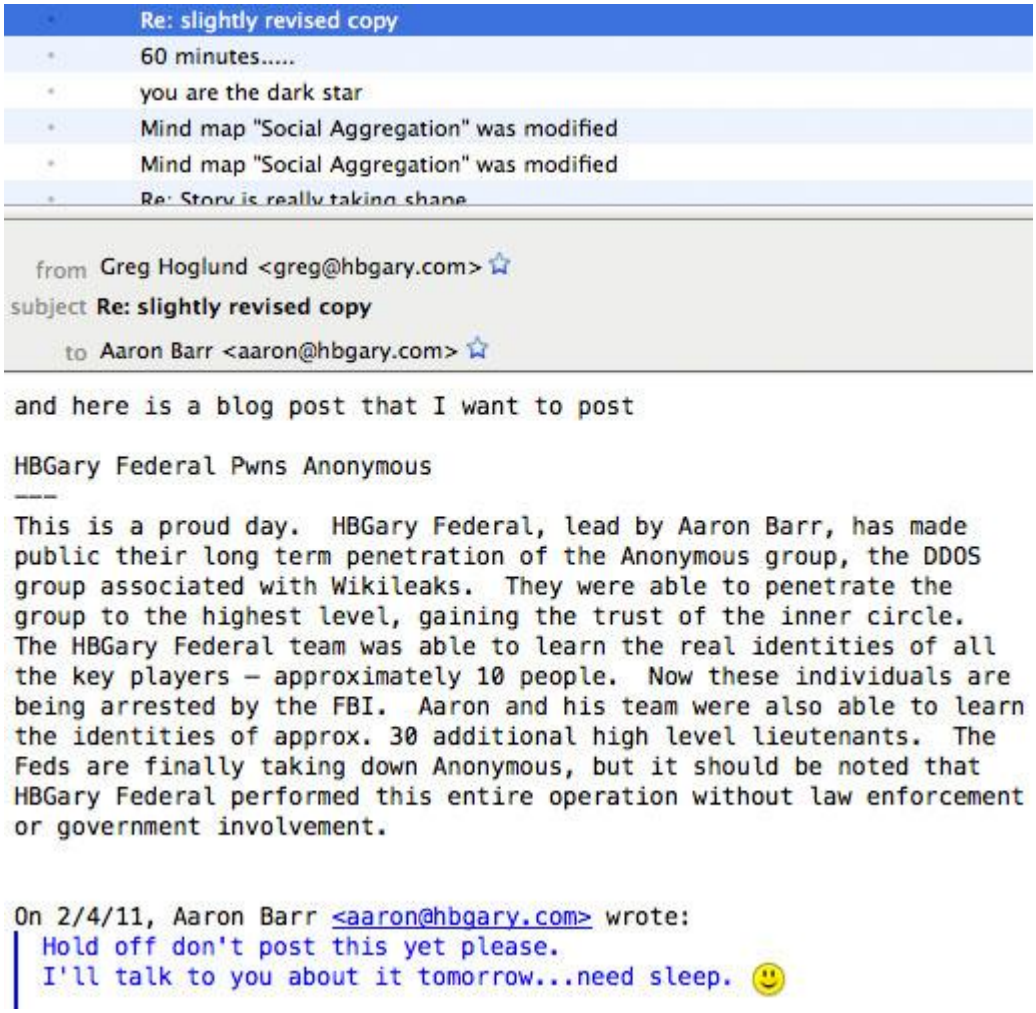


Ilustración 94: Ejemplo de correo filtrado de HBGary

Fuente: http://serpentsembrace.wordpress.com

Además de ser comprometida la cuenta CEO de HBGary en Twitter:

Ilustración 95: Mensaje en Twitter desde la cuenta del dirigente de HBGary, claramente saboteada

En adición, una de las empresas asociadas al propietario de HBGary, Greg Hoglund, fue atacada, quedando sin servicio durante un tiempo, y además fueron robados y publicados en la red los datos del registro de usuarios de la empresa, quedando en entredicho la seguridad de la misma, más aún si la propia compañía se postula como una empresa "experta en seguridad informática".

En este caso, el motivo del ataque fue la colaboración y trabajo conjunto entre esta empresa y el FBI para investigar los ataques a las compañías que cortaron la financiación de Wikileaks (entre las que se encuentran MasterCard o Visa por ejemplo).

El robo de información a HBGary se perpetró a partir de inserciones SQL que permitían modificar y obtener datos operando sobre el CMS que soportaba y gestionaba la página de la compañía. La inserción de dos parámetros de este enlace:

```
http://www.hbgaryfederal.com/pages.php?pageNav=2&page=27.
```

Ilustración 96: Inserción SQL que permitió modificar la web de HBGary

Donde alguno de los dos parámetros (PageNav o Page) o ambos, fueron manejados incorrectamente por el CMS que gestiona la página de HBGary, permitiendo a los hackers acceder a información privilegiada de la base de datos, lo que evidentemente, no debería

de haber ocurrido si la tecnología CMS que maneja esta web fuera lo suficientemente robusta y segura.

A partir de esa puerta de entrada, los hacktivistas pudieron comenzar a alterar los sistemas informáticos de la empresa objetivo y lo más importante: constituyó un nuevo avance en el ataque a las empresas objetivo, ya que como se ha visto, no se conformaron con derribar el servicio del servidor durante un tiempo, sino que hackearon la web oficial de la empresa, lo que lleva a pensar que los hacktivistas no sólo son usuarios que protestan de forma coordinada con ataques DDoS, sino que poseen una gran destreza y conocimientos suficientes como para poner en jaque a cualquier compañía, por muy fuerte que sea.

7.3.3 Advanced Persistent Threat (APT)

Este nuevo tipo de malware está afianzándose como una novedosa práctica entre los atacantes a redes y sistemas informáticos. Su objetivo suele ser el ataque a entornos empresariales u objetivos políticos, y su mayor baza para lograr perpetrar esos ataques es la capacidad de ocultamiento que posee este malware.

Una vez introducido en el sistema objetivo, dicho malware tiene como principal meta perdurar en el sistema durante el mayor tiempo posible, intentando pasar lo más desapercibido posible, caracterizándose por ser muy sigiloso para no ser detectado.

Este tipo de amenazas se diferencian del resto porque cuentan con varios métodos de ataque, propagación dentro del sistema y ocultamiento en el mismo. Generalmente la construcción de este tipo de malware no responde a los métodos de generación de malware convencionales, sino que cada uno de estos APT´s es considerado una pieza única y totalmente diferente al resto, ya que comienzan a construirse desde cero, generalmente por grupos de profesionales con capacidades técnicas muy avanzadas y que disponen del tiempo y la paciencia suficientes como para crear una amenaza prácticamente de la nada, por lo que cabe pensar que detrás de este tipo de malware existen motivaciones lo

suficientemente fuertes para dedicarle tanto tiempo a este tipo de software. Tal es el grado de originalidad en la construcción y, por así decirlo, "fabricación manual" que en algunos de estos tipos de malware se han detectado hasta 20 tipos de codificación distinta, generalmente destinados a evitar que se pueda definir un perfil del programador que implementó el malware.

Las personas que implementan un APT no buscan obtener un beneficio del mismo de forma inmediata, sino que sus métodos de actuación se basan en introducirse en su objetivo por medio de diferentes sistemas de infección (mediante medios físicos, provenientes de Internet o por exploit externos) como podemos ver en la siguiente imagen:

Infección de malware proveniente de Internet	Infección de malware por medios "físicos"	Infección por exploit externo
• Downloaders • Archivos adjuntos en correos electrónicos • Archivos compartidos o redes P2P • Software pirata o uso de Keygens • Phishing • Envenenamiento de DNS, etc.	• Pendrives o Sticks USB • CDs o DVDs • Tarjetas de memoria • Appliances • Equipos de tecnología con backdoors	• Hackers profesionales • Vulnerabilidades • Ingreso por Wifi • Ataque a la nube

Ilustración 97: Tipos de infección utilizados para introducirse en el sistema objetivo

Y esperar pacientemente, monitoreando las actividades del sistema objetivo de forma sigilosa y con un perfil bajo, moviéndose entre un host y otro llegando a darse casos en donde se detectan este tipo de amenazas tras llevar dentro del sistema más de un año.

No obstante, pese a que estas amenazas permanecen ocultas a nivel de host, necesitan comunicarse con su servidor de Command & Control, siendo este tipo de tráfico de red el único síntoma para poder detectar su presencia. Su ciclo de vida se representa en la

siguiente figura:

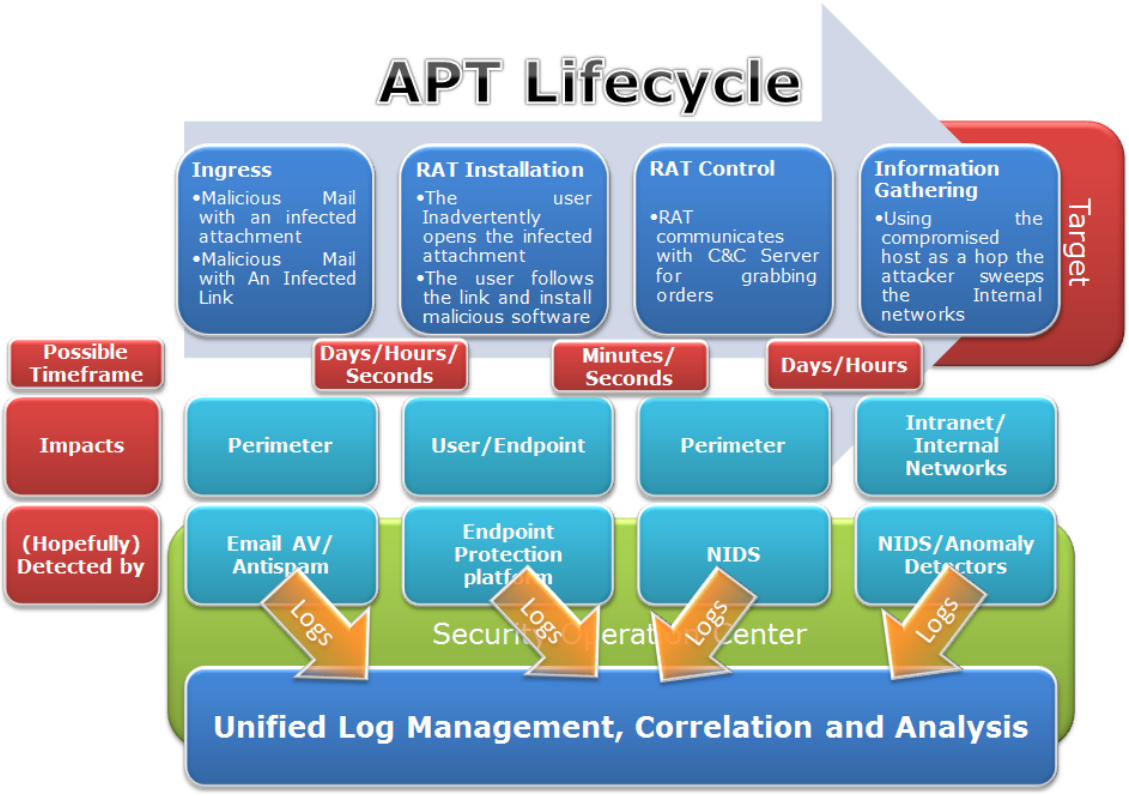


Ilustración 98: Esquema del ciclo de vida de un APT

Fuente: http://hackmageddon.com

Este tipo de ataques tienen la particularidad de estar en ocasiones perpetrados por países que buscan compañías que les puedan suponer un objetivo interesante (ya sea por motivos políticos o económicos) y agencias estatales que custodien información sensible o confidencial. En vez de destruir o dañar esta información sensible, los atacantes facilitan el ciber-espionaje a través de este tipo de software. En la mayoría de los casos los atacantes están trabajando para un objetivo muy determinado y definido, no son simples atacantes que peinan el sistema en busca de información que les pueda ser útil, sino que buscan una información que ya saben que existe en un determinado sistema, y crean una nueva amenaza exclusivamente para poder romper las barreras de seguridad del mismo y perpetrar el ataque.

Este malware está considerado como un sistema avanzado, ya que los criminales que se encuentran detrás de esta amenaza hacen uso de una amplia gama de tecnologías y técnicas de intrusión, combinando múltiples metodologías y herramientas de ataque para llegar a un objetivo concreto.

Algunas características de los APT´s son:

- Pequeño tamaño del ejecutable inicial.
- Medios para ocultar su código y su presencia activa.
- Código para despertar y activar la activación.
- Mecanismo de alerta atacante de la implementación exitosa / penetración.
- Mecanismo para comunicar información recopilada.
- Mecanismo de actualización para recibir los cambios de código y add-ons.
- Algunos pueden ofrecer acceso de puerta trasera, escaneo de vulnerabilidades y capacidades de propagación.
- Las actividades y la comunicación tienden a ser bajas y lentas, tratando de hacer el menor ruido posible, y que figuran como las comunicaciones de red normal o de fondo.

Se calcula que menos del 25% de los APT´s son detectados, debido a su gran sigilo y su forma de trabajo. El tiempo medio de estadía de este tipo de malware en un sistema es de 416 días, lo que da una idea de la paciencia y el sigilo que demuestran tener los atacantes en este tipo de casos.

Así, se comprueba cómo se ha pasado de una tendencia a crear malware donde se premiaba la celeridad de los ataques y el conseguir algún beneficio de forma rápida e instantánea, con unos objetivos amplios y nada concretos ni sofisticados, a la creación de este nuevo tipo de malware donde la filosofía es el sigilo, la cautela, la espera y en definitiva el permanecer en la sombra de forma paciente hasta que se pudiera obtener el objetivo determinado en un inicio, que sin duda es un objetivo claro y conciso, muy específico y estudiado.

7.3.4 Ataques a autoridades certificadoras: Malware en firmas digitales

En los últimos meses se ha detectado una nueva técnica para crear malware basada en la falsificación de los certificados digitales que proporcionan determinadas autoridades certificadoras.

Normalmente, cuando un usuario va a proceder a la descarga e instalación de un nuevo software, éste suele venir acompañado por un certificado digital, es decir, un certificado proveniente de una entidad de confianza que asegura que el producto a descargar ha sido revisado previamente y no es ningún tipo de malware o programa que pueda causar algún prejuicio en el equipo donde se va a instalar.

Ilustración 99: Ejemplo de certificado digital

Evidentemente, estas autoridades certificadoras han de tener medidas de seguridad especialmente fuertes para poder transmitir la seguridad necesaria a los usuarios, los cuales depositan toda su

confianza en estas entidades cuando descargan algún elemento que haya sido inspeccionado por éstas.

La problemática ha surgido en los últimos años (2011 en adelante) cuando se ha comprobado que ha habido ataques a estas autoridades certificadoras, lo que ha derivado en la obtención de certificados digitales por parte de usuarios ilegítimos, las cuales han sido utilizadas para dotar de una certificación falsa a determinado malware, por lo que muchos usuarios han estado descargándose ese malware pensando que había sido revisado y era totalmente seguro. Obviamente esto ha supuesto un fuerte perjuicio a las autoridades certificadoras que se han visto involucradas en estos ataques, dando una mala imagen a los usuarios afectados y al mercado informático en general.

La forma más común de obtener estos certificados es engañando a las propias compañías certificadoras para que emitan el certificado. De hecho, ha habido numerosos casos que para obtener un certificado por parte de una de las compañías emisoras, ha sido suficiente la obtención de un certificado SSL válido para un servidor.

Este fue el caso de la autoridad certificadora "Comodo SSL", la cual fue atacada en marzo de 2011. El fallo fue debido a la falta de comprobaciones a la hora de tramitar las certificaciones a sus clientes, y afectó a los certificados de nueve sitios web (entre ellos addons.mozilla.org, la página de plugins de mozilla, donde, una vez que el usuario se conectaba a dicho sitio web para descargarse un plugin de este navegador, era redirigido a páginas web falsas donde se descargaba plugins infectados).

Para poder subsanar este tipo de incidencias, las autoridades de certificación ofrecieron a sus usuarios una lista de revocación de certificados y un servicio de comprobación online (mediante el protocolo OCSP), donde podían comprobar si el certificado ofrecido por un determinado sitio web se encontraba comprometido.

En algunos casos, el problema fue aún mayor dado que estas peticiones de validación de los certificados pueden ser revocadas sin que se cerciore el navegador, por lo que si el malware tiene esa función, puede evitar que el usuario compruebe su validez mediante

los canales antes mencionados, por lo que las empresas emisoras de los certificados tuvieron que redoblar sus esfuerzos y realizar una "lista negra" con los números de serie de los certificados que se encontraran comprometidos, introduciéndose esta lista en las actualizaciones de los principales navegadores como Chrome o Mozilla, para facilitar al usuario la detección de este tipo de certificados ilegítimos.

Más grave fue el caso de la compañía "Diginotar", que emitió certificados falsos y comprometió la seguridad de compañías como Yahoo, GMail o Mozilla. Los usuarios de Google Chrome y Mozilla Firefox estaban protegidos desde un primer momento dado que Google no autoriza a esta compañía a emitir certificados suyos, por lo que Google Chrome avisaba al usuario de que los certificados eran falsos, pero otros usuarios sí se vieron afectados y fueron objeto de ataques para el robo de contraseñas y otros datos personales. Desde este incidente Diginotar dejó de emitir certificados y finalmente se ha declarado en bancarrota.

También ha sido frecuente el robo de certificados o claves privadas para posteriormente firmar determinado malware, o incluso utilizar plataformas como "Digital River" o similares, que simplemente se dedican a dar certificados a todo el software de sus clientes.

Otra técnica más sofisticada ha sido la de introducir un troyano en el ordenador de un desarrollador de software, y a la hora de ser firmado éste software legítimo del desarrollador, haya sido también firmado digitalmente el troyano introducido. Otra técnica detectada es el auto certificado de los propios desarrolladores en sus productos de ejemplo.

Por ahora este tipo de prácticas no ha sido muy extendida, pero se estima que en un futuro muy próximo será una gran amenaza, en gran parte por la gran expansión que está teniendo Windows 7, el cual requiere controles Authenticode mucho más estrictos que en versiones anteriores.

7.3.5 Ataques informáticos: ¿las guerras del futuro?

Hoy en día existe el debate acerca de la posibilidad de que en

un futuro no muy lejano las guerras entre países comiencen a entenderse como una batalla informática, en la lucha por tener el control de los recursos enemigos, tales como los sistemas informáticos de los reactores nucleares enemigos, los sistemas de alimentación energética, etc.

Lo que en un principio se consideró como algo inalcanzable y casi ciencia-ficción, está viéndose cada día como una opción que cada vez va tomando más forma entre los países. Numerosos son ya los ejemplos de ataques informáticos e infecciones perpetrados por gobiernos con el objetivo de, no ya sólo no dejar operativos, sino destruir los recursos más valiosos o peligrosos de una nación que consideren enemiga.

Así, recientemente se ha podido comprobar con el gusano "Stuxnet". Dada su sofisticación, no se puede saber a ciencia cierta quién está detrás de este tipo de ataques, pero en lo que todos los expertos se ponen de acuerdo es que este código malicioso es tan sofisticado que sólo puede estar detrás de él un gobierno. Lo novedoso de este malware no fue solo el hecho de que consiguiera introducirse en los sistemas de recursos sensibles de un gobierno, sino que además tenía la capacidad de modificarlos y/o destruirlos.

Stuxnet logró, por el año 2010, afectar a más de 30.000 computadoras y a un reactor nuclear en Irán, según reconocieron posteriormente fuentes de dicho país. Tras las investigaciones realizadas, se hallaron numerosas tarjetas de memoria en un baño de una base militar estadounidense en Medio Oriente, donde se realizaban labores de apoyo en la guerra de Irak.

Según se supo, alguna persona insertó este malware deliberadamente, lo que supuso su propagación por toda la red y todos los equipos informáticos militares iraníes, en un intento por inhabilitar el programa nuclear iraní desde dentro, sin necesidad de usar armamento bélico convencional.

Tal fue el nivel de sofisticación del arma usada, que se cree que se utilizaron agentes de inteligencia para guiar al malware hasta el objetivo indicado, un sistema de control fabricado por la empresa Siemens y ampliamente utilizado por las fuerzas de seguridad

iraníes en sus centrales nucleares. El resultado fue una infección a gran escala que obligó al retraso por parte del gobierno iraní en la finalización del reactor nuclear de Bushehr.

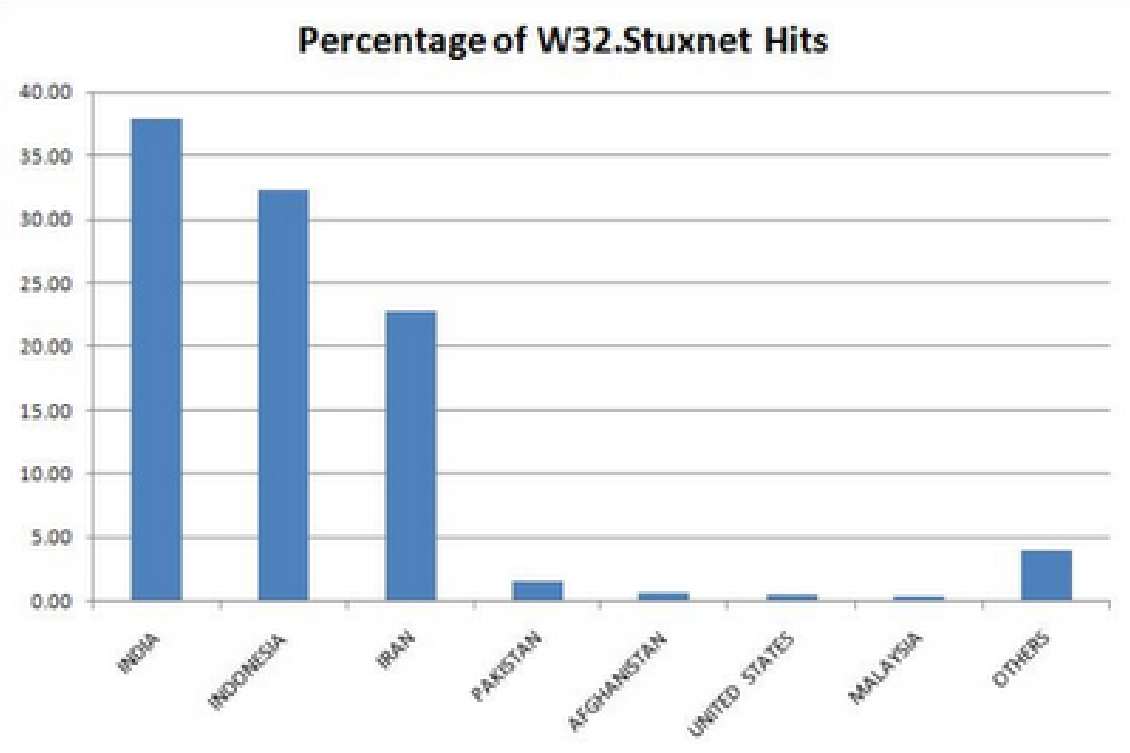


Ilustración 100: Porcentajes de equipos infectados con Stuxnet por países

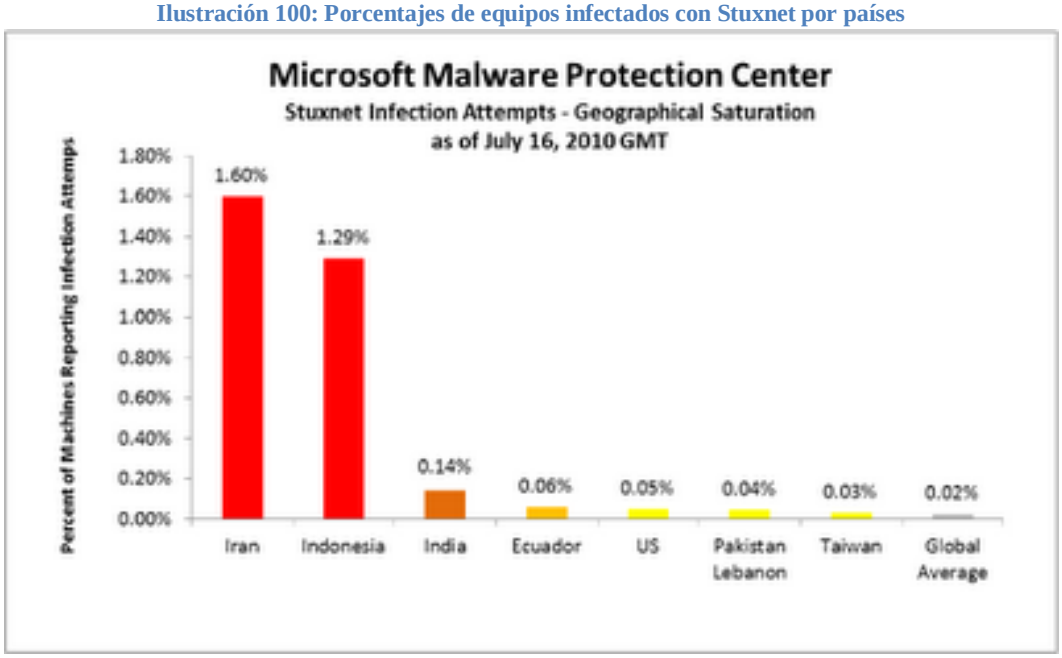


Ilustración 101: Gráfica con los intentos de ataque con la herramienta Stuxnet por países

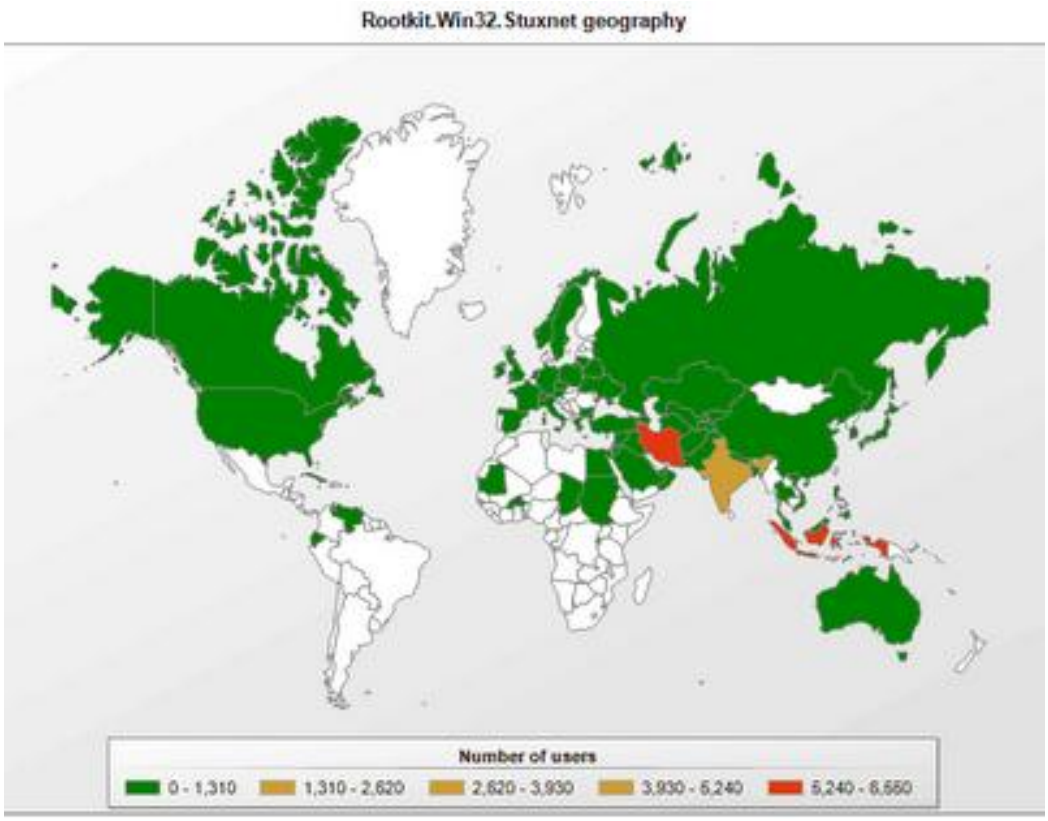


Ilustración 102: Ataques con la herramienta Stuxnet en todo el mundo

Este ataque da una idea del poder actual que pueden ejercer las nuevas tecnologías, por encima incluso de las propias armas y material bélico, y de cómo pueden comenzar a enfocarse los ataques entre países en un futuro.

De hecho, este ataque supuso que Estados Unidos comenzara a realizar pruebas dentro de su sistema de defensa, para comprobar cuán preparados estaban sus sistemas para resistir un ataque de características similares. La operación se llamó "Cyber Storm III" y tuvo como objetivos más de 1.500 blancos distintos. Hoy día no se puede saber cómo de preparados estaban en ese momento dado que nunca se llegaron a publicar los resultados de ese simulacro, por lo que se puede intuir que se encontraron deficiencias importantes.

Ya se han vivido muchos capítulos de las llamadas ciberguerras, pero este ataque supuso un punto de inflexión dada la extrema exactitud y habilidad a la hora de dañar los sistemas objetivo, y la facilidad inherente a estos ataques para poder ocultar el rostro de quien los perpetra. En la siguiente gráfica, se puede ver una encuesta realizada por una empresa de seguridad donde preguntan

a expertos acerca de quién consideran que podía estar detrás de este malware:

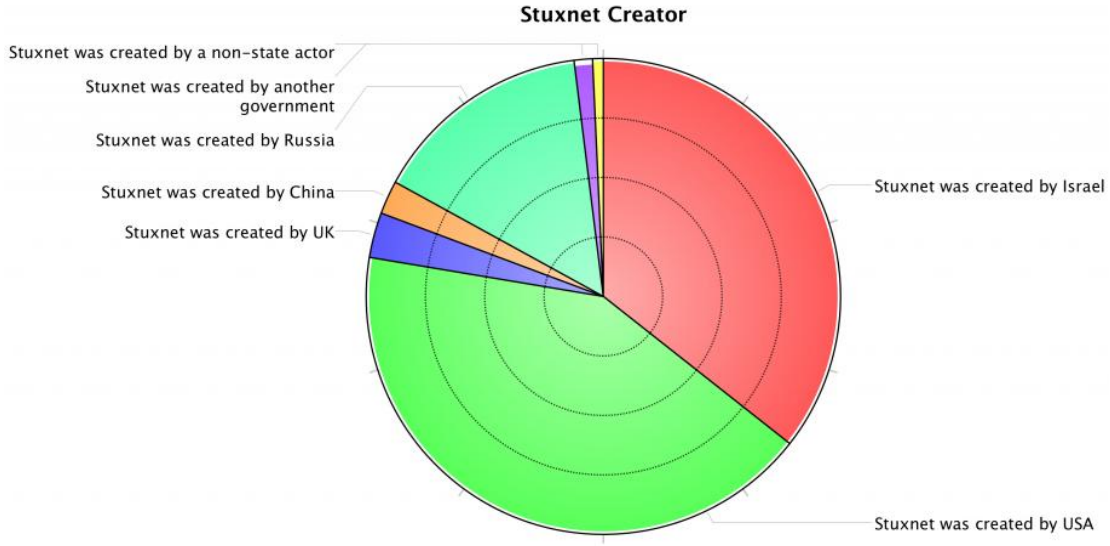


Ilustración 103: Encuesta sobre el posible creador de Stuxnet

7.3.5.1 Duqu, la evolución de Stuxnet

Sobre el año 2011, la empresa de seguridad informática Symantec descubrió un nuevo malware considerado como la evolución del ya comentado Stuxnet (ya que poseía trozos de código idénticos) pero con claras diferencias en el objetivo final. El objetivo de Duqu es la recopilación de información de inteligencia y de los activos de entidades como fábricas de sistemas de control industrial para ejecutar de una manera más sencilla ataques contra terceras partes en un futuro. Por lo tanto, Duqu sólo se centraría en recopilar la información y no se trataría de una amenaza por sí mismo, sino que simplemente ayuda a organizar ataques posteriores a determinados objetivos. Al igual que Stuxnet, se trata de un código realmente complejo y se ha hallado en un número ilimitado de instalaciones industriales y fábricas de sistemas de control industrial.

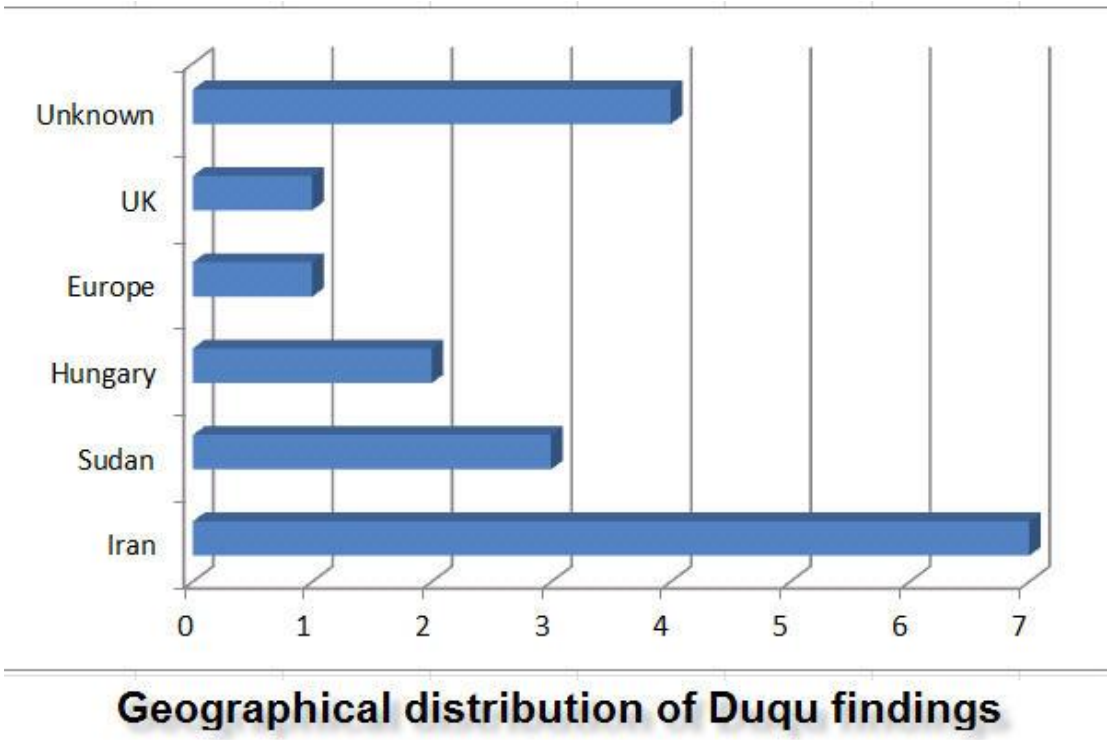


Ilustración 104: Distribución geográfica de ataques detectados con la herramienta Duqu

Duqu permanece durante 36 horas en el interior del sistema recopilando información y posteriormente se autodestruye. Está compuesto por una serie de códigos ”rompecabezas” que incluyen certificados digitales como el proporcionado por Symantec, que posteriormente se ha comprobado que ha sido robado a un cliente de Symantec en Taiwan y posteriormente reutilizado para certificar este nuevo malware.

Las consecuencias de este tipo de malware están siendo mucho más importantes de lo esperado a priori por expertos en seguridad nacional, llegando a afirmar que no se ha evaluado correctamente el daño que puede suponer la infección de una máquina con acceso a información sensible. Como muestra, tras los ataques de Stuxnet y Duqu, algunos gobiernos de todo el mundo comenzaron a reforzar los sistemas de seguridad informáticos que controlan los suministros de agua y electricidad entre su población.

Actualmente, las primeras potencias mundiales cuentan con secciones militares en donde se invierten millones de dólares anuales con el objetivo de protegerse ante este tipo de ataques destructivos, que pueden poner en jaque a todo un país.

7.3.6 Los peligros tras la "nube"

Otro de los ataques y fraudes que se espera que golpeen con fuerza durante la próxima década es el robo de datos y cuentas bancarias alojados en la nube. Conforme se va avanzando en el campo de la informática, existe la tendencia de conectar todos los sistemas y plataformas mediante Internet, de tal forma que se están viendo incrementados de forma gradual el número de datos personales que los usuarios de Internet están depositando en la red. Este hecho conlleva un riesgo bastante importante, ya que cualquier transacción o compra que realice un usuario por Internet deja un rastro de datos asociados al mismo. Así, el ataque a estas plataformas donde se almacenan datos personales como nombres de usuarios, contraseñas, números de cuentas bancarias, etc. es un objetivo cada vez más apetitoso dado el gran volumen de ventas que se realiza a través de la red. Por lo tanto, pueden existir plataformas que tengan un sistema de seguridad robusto y protejan los datos de forma excepcional, pero cada vez va a haber más atacantes en busca de una forma para introducirse en ellos.

Esto último es lo que le ocurrió a la red de Play Station 3 en el año 2011, y se espera que se incrementen estos casos de forma paulatina.

Un grupo de hackers consiguió introducirse mediante la actualización de un firmware en la red de PS3, de tal forma que consiguieron colocar una puerta trasera ("backdoor") para poder tener acceso a través de múltiples botnets. El resultado final fue la inhabilitación del servicio de la red de PS3 durante una semana y la alarma generada a todos los usuarios, a los que se les aconsejó desde la propia plataforma de Sony que cambiaran todas las contraseñas de acceso y vigilaran sus números de cuenta bancarios por si se realizaban transacciones sospechosas.

Ilustración 105: Mensaje de Sony durante la inhabilitación de la red de PS3

Este caso ejemplifica perfectamente los peligros a los que se enfrentan los usuarios de Internet al entregar sus datos personales a través de la red.

7.3.7 Smartphones, el futuro del malware

La evolución astronómica que han ido desarrollando en estos últimos años los dispositivos móviles, y la importante revolución que han supuesto los smartphones en este mercado, han hecho que hoy en día prácticamente cualquier dispositivo móvil que se saque al mercado por cualquier compañía esté considerado como un pequeño ordenador, en donde la clásica llamada a cualquier otro terminal, para el que se usaban estos dispositivos anteriormente, se ha visto relegada a un segundo o tercer plano.

En este marco, son multitud las nuevas aplicaciones que salen cada día al mercado, ofreciendo al usuario de cualquier dispositivo móvil (principalmente de smartphones) nuevas funcionalidades para poder desarrollar todo el potencial de los actuales dispositivos móviles. El usuario simplemente ha de comprar o directamente descargar de forma gratuita las aplicaciones que se le ofertan en diversas plataformas (cada sistema operativo posee su plataforma de difusión para las aplicaciones compatibles con ese sistema operativo) e instalarlas en su terminal.

Así, se han creado multitud de aplicaciones móviles para los diferentes sistemas operativos que existen actualmente, teniendo

cada una de ellas miles (o incluso millones) de usuarios que las utilizan día a día, prácticamente minuto a minuto. Todas las redes sociales disponen de su propia aplicación personalizada para que los usuarios dispongan de ella de forma gratuita, así como muchos de los bancos más importantes del planeta, medios de comunicación, etc. lo que supone una cantidad ingente de nuevos usuarios listos para utilizar estas nuevas tecnologías para su vida diaria; consultas por internet, utilización de las redes sociales, movimientos bancarios a través de su teléfono móvil, etc.

Esto ha supuesto un nuevo avance tecnológico donde los usuarios disponen de más medios para poder comunicarse entre sí, realizar negocios, etc. pero también supone un nuevo campo por explotar para las personas que deseen realizar cualquier tipo de fraude, teniendo en cuenta la cantidad ingente de datos personales que puede albergar un Smartphone, así como la posibilidad de poder realizar transacciones bancarias ilegítimas o robar los datos de las mismas a los usuarios víctima. Ante esta amenaza, resultan alarmantes los datos acerca de la protección que usan los usuarios de estos dispositivos contra estos posibles ataques. Así, un estudio realizado por la compañía de seguridad informática "Kasperski Lab" en enero de 2011 reflejaba que sólo el 12% de los usuarios europeos de smartphones poseen un antivirus.

Este dato es muy preocupante si tenemos en cuenta la situación que muchos expertos predicen, donde se estima un aumento del protagonismo de malware en los smartphones, de hecho, en el siguiente gráfico se puede comprobar la evolución de este tipo de ataques en los últimos tiempos:

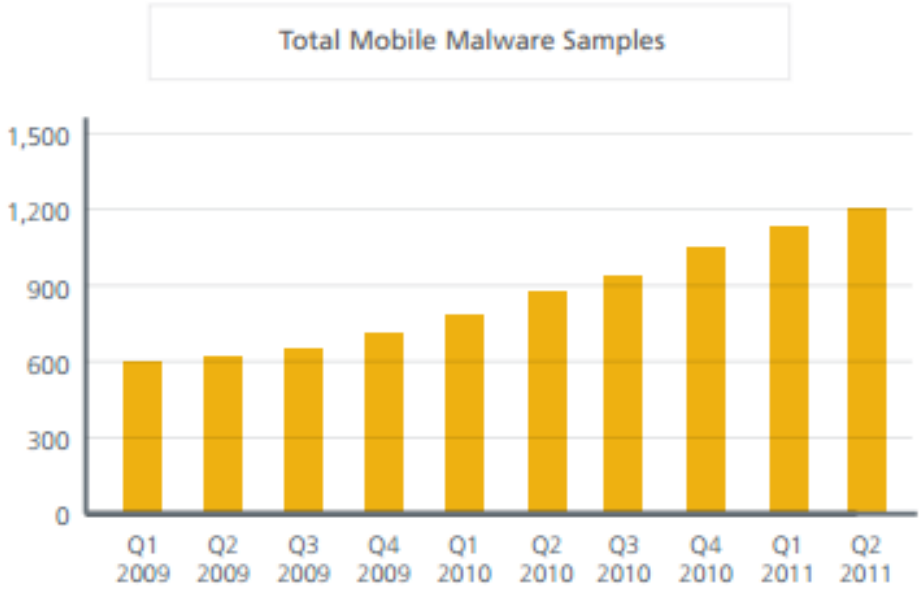


Ilustración 106: Gráfica sobre el número de ejemplos de malware encontrados para dispositivos móviles

Por lo que se antoja casi obligatorio para los usuarios el uso de algún sistema de seguridad efectivo que pueda detectar y mitigar las amenazas que intenten acceder al terminal. Más aún cuando se estima que la utilización de este tipo de dispositivos para actividades como pagar en las tiendas, guardar tickets y pases electrónicos o descargar información sobre servicios se convertirá en una realidad cotidiana. Nuestro confort, bienestar y nuestra capacidad para realizar actividades diarias indispensables dependerá cada vez más de estos dispositivos, que cada vez con mayor frecuencia se encuentran bajo amenaza.

Así, los casos más comunes de malware hasta el momento tratan del robo de datos personales, como por ejemplo es el caso de la aplicación de origen ruso "Find and Call", disponible en las plataformas oficiales de Android e iOs hasta que fue detectado, que se basaba en un buscador para la agenda de contactos, pero al mismo tiempo copiaba y enviaba a un servidor remoto los datos almacenados en la agenda del usuario para después poder enviar correo SPAM a estos contactos a través de mensajes de texto.

Ilustración 107: Captura de pantalla de la aplicación "Find and call"

Existen multitud de casos similares a éste, como el de la aplicación Loozfon, que sustraía direcciones de correo electrónico a usuarios en Japón ofreciendo como cebo la posibilidad de ganar grandes sumas de dinero simplemente enviando mensajes desde su terminal. Al entrar en estos anuncios se le redirigía al usuario a un sitio web donde se infectaba el terminal del mismo y se procedía a la sustracción de la información, según detectó Symantec.

Por último, recientemente se han descubierto aplicaciones que al descargarlas comienzan a modificar las preferencias de acceso a la tienda que el usuario tenía establecidas en el terminal, y lograba descargar aplicaciones de pago sin que el usuario fuera avisado previamente. En este caso, son más de 100.000 los terminales Android infectados en China

También existen casos donde la técnica utilizada se basa en elaborar una aplicación que atraiga al usuario, éste se la descargue, y una vez instaladas, estas aplicaciones se descargaban paquetes adicionales desde un servidor remoto que comenzaba a enviar SMS a números de tarificación adicional, propiedad de los atacantes, que así lograban obtener un beneficio directo del malware.

Pero los expertos aseguran que dentro de la problemática de la incipiente proliferación de malware entre los dispositivos móviles, el mayor problema se centra en los terminales que utilizan el sistema operativo Android. Esto es debido a las características que rodean a este sistema operativo.

- Actualmente, es el sistema operativo más utilizado en el mundo (un 59% de cuota de mercado en el primer cuarto de 2012), por lo que si un usuario crea algún tipo de malware, la primera opción será crearlo para Android, ya que existe un número de objetivos mucho mayor que si lo desarrolla para cualquier otra plataforma.

Top Six Smartphone Operating Systems, Shipments, and Market Share, 2012 Q1 (Units in Millions)

Mobile Operating System	1Q12 Unit Shipments	1Q12 Market Share	1Q11 Unit Shipments	1Q11 Market Share	Year-over-Year Change
Android	89.9	59.0%	36.7	36.1%	145.0%
iOS	35.1	23.0%	18.6	18.3%	88.7%
Symbian	10.4	6.8%	26.4	26.0%	-60.6%
BlackBerry OS	9.7	6.4%	13.8	13.6%	-29.7%
Linux	3.5	2.3%	3.2	3.1%	9.4%
Windows Phone 7/Windows Mobile	3.3	2.2%	2.6	2.6%	26.9%
Other	0.4	0.3%	0.3	0.3%	33.3%
Total	152.3	100.0%	101.6	100.0%	49.9%

Ilustración 108: Comparativa de ventas entre los sistemas operativos más importantes para smartphones

Fuente: IDC Worldwide Mobile Phone Tracker

En una muestra recogida a finales de 2011, se puede comprobar la gran cuota de mercado que posee Android en un país como EEUU, donde casi la mitad de los smartphones poseían el sistema operativo de Google:

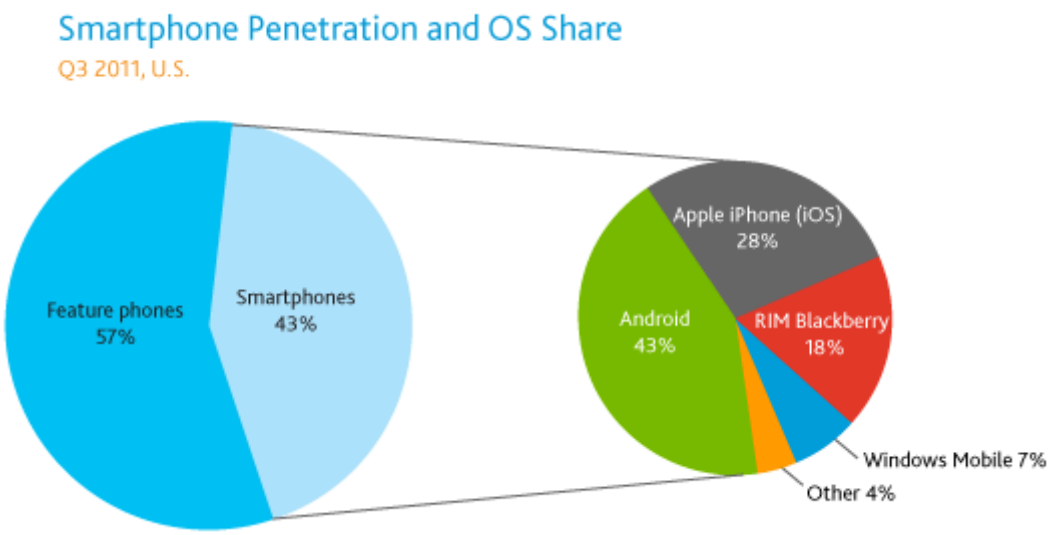


Ilustración 109: Cuota de mercado de los distintos sistemas operativos para smartphones

- El hecho de basarse en código abierto hace que cualquier desarrollador pueda elaborar una aplicación que aporte un beneficio a los usuarios, pero también los desarrolladores malintencionados tienen acceso libre a la creación de todo tipo de malware que pueden incorporar de manera muy sencilla al mercado de aplicaciones, como se ha podido comprobar en los ejemplos citados anteriormente.
- La existencia de tiendas de aplicaciones no controladas por Google hace que la seguridad en las mismas sea escasa. De hecho, la mayor parte de las veces el malware proviene de este tipo de tiendas no oficiales.
- La aparición de herramientas que directamente ayudan a los desarrolladores menos expertos, o a usuarios malintencionados, a crear su propio malware de forma automática y sencilla mediante una herramienta denominada "AFE".

Ilustración 110: Logotipo del malware AFE para Android

Esta herramienta, desarrollada por dos expertos en seguridad informática (los cuales aseguran que su propósito es ayudar a Google a mejorar sus vulnerabilidades), permite desarrollar hasta 20 acciones maliciosas, como grabar conversaciones, acceder al GPS, marcar números, acceder a los contactos y correos personales del infectado, etc., permitiendo además enmascarar fácilmente la aplicación creada como si fuera una aplicación "normal" para no levantar sospecha alguna.

Estos factores han acarreado un espectacular incremento de malware detectado para la plataforma Android, como se puede comprobar en el siguiente gráfico:

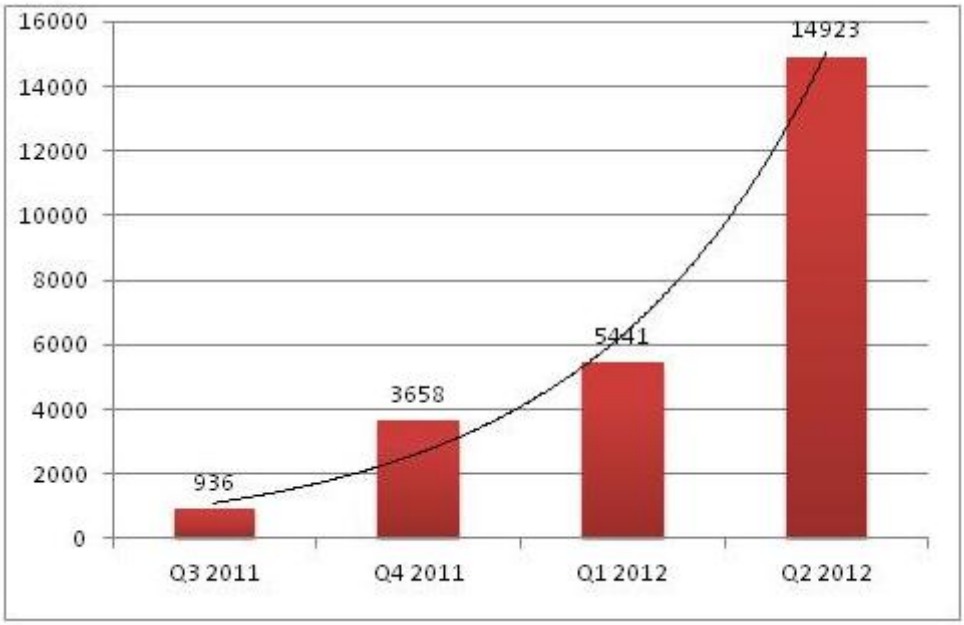


Ilustración 111: Gráfico sobre el aumento de malware en el sistema operativo Android

Fuente: Karspersky Labs

Donde se puede observar cómo se ha detectado un espectacular incremento desde el último trimestre de 2011 en adelante, llegándose a triplicar el número de amenazas durante el año 2012.

En una comparación realizada a mediados de 2011 con el resto de plataformas, el malware detectado en Android es muy superior al detectado en el resto:

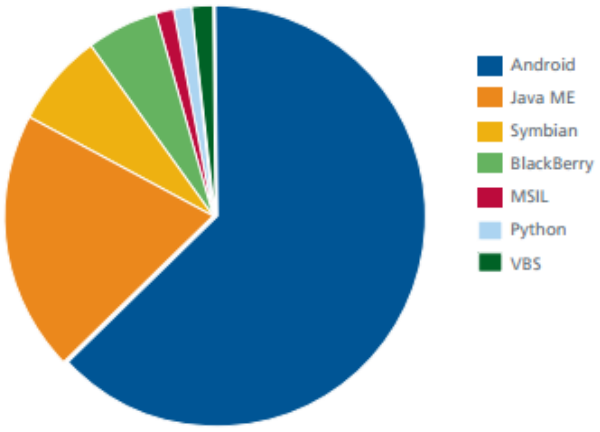


Ilustración 112: Malware detectado en cada uno de los sistemas operativos

Fuente: McAfee

Por otro lado, sabiendo las potenciales amenazas que pueden aparecer para este sistema operativo, Google toma ciertas medidas

de seguridad antes de autorizar el lanzamiento de cualquier aplicación en su tienda oficial, como por ejemplo la herramienta "Bouncer", que analiza cada aplicación antes de su incorporación desde la plataforma "Play Store" (la plataforma oficial de Google para la descarga de las aplicaciones Android) al dispositivo móvil del usuario, de tal forma que el usuario puede analizar el contenido que va a descargar y los desarrolladores no se ven obligados a pasar un proceso de aprobación de solicitudes.

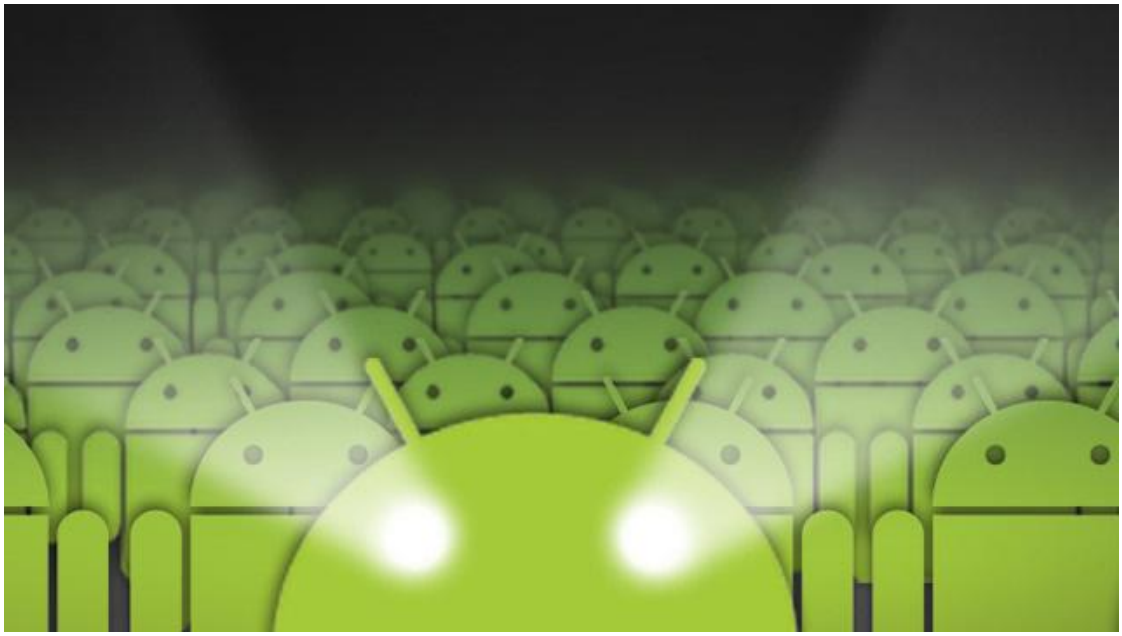


Ilustración 113: Bouncer se propone como herramienta para prevenir las masivas filtraciones de malware para Android

El funcionamiento es el siguiente: una vez que se carga la aplicación, Bouncer comienza a analizarla en busca de posibles troyanos, spyware, o cualquier malware conocido, así como cualquier tipo de comportamiento sospechoso que pueda dar indicios acerca de que la aplicación sea maliciosa, comparándola con aplicaciones anteriormente analizadas en la búsqueda de posibles señales de alerta. Básicamente, lo que se hace es simular el comportamiento de la aplicación en un entorno controlado en busca de un comportamiento malicioso u oculto. También se realizan chequeos sobre las cuentas de desarrolladores, intentando localizar a los desarrolladores de códigos maliciosos e impidiéndoles que se registren de nuevo.

Los primeros resultados indican que esta herramienta ha ayudado a reducir el malware en el sistema Android en torno a un 40% (según datos ofrecidos por Google).

Además, desde un primer momento Google ha puesto un especial empeño en la lucha contra el malware, y en intentar evitar las arquitecturas de los PC´s convencionales donde éste puede ser extremadamente dañino. La filosofía que han seguido desde la creación de Android ha sido que el malware siempre va a existir, por lo que se centrarían en que el malware para dispositivos móviles fuese lo menos perjudicial posible. Para ello han tomado ciertas medidas de seguridad, como las siguientes:

- Sandbox (Caja de arena): Delimita el acceso entre las aplicaciones y el resto de software del dispositivo, por lo tanto, una aplicación no podrá acceder a los datos de otras partes del terminal, limitando el daño potencial del malware.

- Permisos: Android gestiona una serie de permisos para las aplicaciones que cada usuario instala en su dispositivo móvil, pudiendo administrar éste sus propias preferencias y así asignar determinados permisos a cada una de las aplicaciones que instala en el terminal. De este modo, si por ejemplo un usuario se descarga un juego y posteriormente esa aplicación solicita el envío de SMS, el usuario se dará cuenta del potencial gasto de dinero que puede suponerle utilizar esa aplicación. Al no tener el permiso adecuado, la aplicación se ve forzada a solicitarlo cada vez que quiera realizar el envío de algún SMS, de tal forma que gracias a la restricción de los permisos el usuario puede ser alertado del peligro que conlleva la aplicación.

- Eliminación de malware: Android está diseñado para evitar que el malware se extienda por la plataforma o encuentre algún modo de esconderse del usuario, con el objetivo de facilitar la eliminación de todo malware que se vaya encontrando. El Android Market también dispone de capacidad para poder eliminar de forma remota malware de un dispositivo particular si fuese necesario.

Otra herramienta que sin duda ayuda a la protección contra el malware en Android son los antivirus para smartphones, que sin duda son un elemento más de protección ante posible intentos de

fraude o ataques, pero lo cierto es que aún no se han desarrollado antivirus lo suficientemente potentes como para parar todas las amenazas que intentan penetrar en los dispositivos móviles. Según un estudio llevado a cabo en 2012, sólo 7 de un total de 41 antivirus analizados detectaban más del 95% de las amenazas, y 24 de ellos mostraban un índice de detección por debajo del 65%. El muestrario de malware incluía troyanos de banca en línea, proveedores de servicios tarifados y spyware.

En líneas generales, uno de los principales problemas fue el hecho de que el software antivirus que fue probado detectaba principalmente el malware a través del uso de firma. Esto limita la protección contra malware conocido, dado que no pueden esperar proteger a los usuarios contra malware previamente desconocido, ya que para éstos aún no hay firmas. Actualmente Google está trabajando para poder anticiparse a malware no conocidos y poder detectarlos antes incluso de que comiencen a actuar.

Algunas recomendaciones de seguridad para este tipo de dispositivos móviles serían:

- Instalar aplicaciones solamente procedentes de tiendas oficiales o tiendas de los fabricantes de terminales.

- Prestar atención al número de veces que se ha descargado una aplicación y los comentarios sobre ésta antes de descargarla en el terminal personal.

- Comprobar las autorizaciones asociadas a cada aplicación prestando especial atención a los permisos acerca de la realización de llamadas y envío de SMS.

- Actualizar el sistema operativo de forma periódica.

- Comprobar la factura telefónica.

- Disponer de un antivirus que realice chequeos periódicamente al terminal.

Por lo tanto, se puede concluir que el malware para smartphones, y más en concreto el malware para los dispositivos Android, sufrirá un

crecimiento en los próximos años acorde al incremento de usuarios y las múltiples nuevas funcionalidades y opciones que se vayan desarrollando, por lo que, al ser una tecnología aún muy precoz, se ha de tener extrema precaución en el uso de estos terminales.

7.3.8 Malware para MAC OS

Por último, pasaremos a analizar la última amenaza que se espera que tenga un papel protagonista en los siguientes años: el malware para el sistema operativo MAC OS. Como otras muchas veces, el incremento de este malware va a venir asociado al incremento en el uso de esta tecnología, por lo que la razón de que anteriormente no haya tenido más relevancia este tipo de amenazas es el hecho de su escaso uso entre los usuarios de equipos informáticos.

En algunos entornos se ha pensado durante años que el sistema operativo MAC OS no estaba amenazado por ningún tipo de malware ya que se sostenía que simplemente no existía malware para este producto, o que el sistema operativo era inmune a los ataques de software malicioso. Este pensamiento es del todo erróneo, tal y como afirmó la propia compañía, la cual ya ha informado de varios tipos de malware que comienzan a crear problemas en este sistema operativo.

Ilustración 114: Cambio en la política de seguridad de MAC OS X

El malware de Mac no se diferencia en absoluto del malware que puede existir para Windows, que ya ha sido descrito ampliamente en este mismo documento. Así, existen algunos ejemplos conocidos, como el caso de "Mac Defender", un malware (concretamente un troyano) que se hacía pasar por un antivirus que arreglaba una supuesta infección en el equipo. A través de la ingeniería social se convence al usuario de que se instale en el equipo un software (de pago) para proteger al equipo de malware. Si el usuario accede a una primera revisión de prueba, el malware realiza una supuesta inspección al sistema, dando siempre resultados alarmantes (por supuesto, falsos) simulando comportamientos erróneos generalmente abriendo páginas aleatorias con el navegador web para demostrar la infección encontrada, todo con el objetivo final de que se materialice la compra. Una vez efectuada, aparte de concederle una cantidad económica al infractor, en el proceso de compra le cede los datos bancarios a éste, y a cambio se instala en su equipo un troyano.

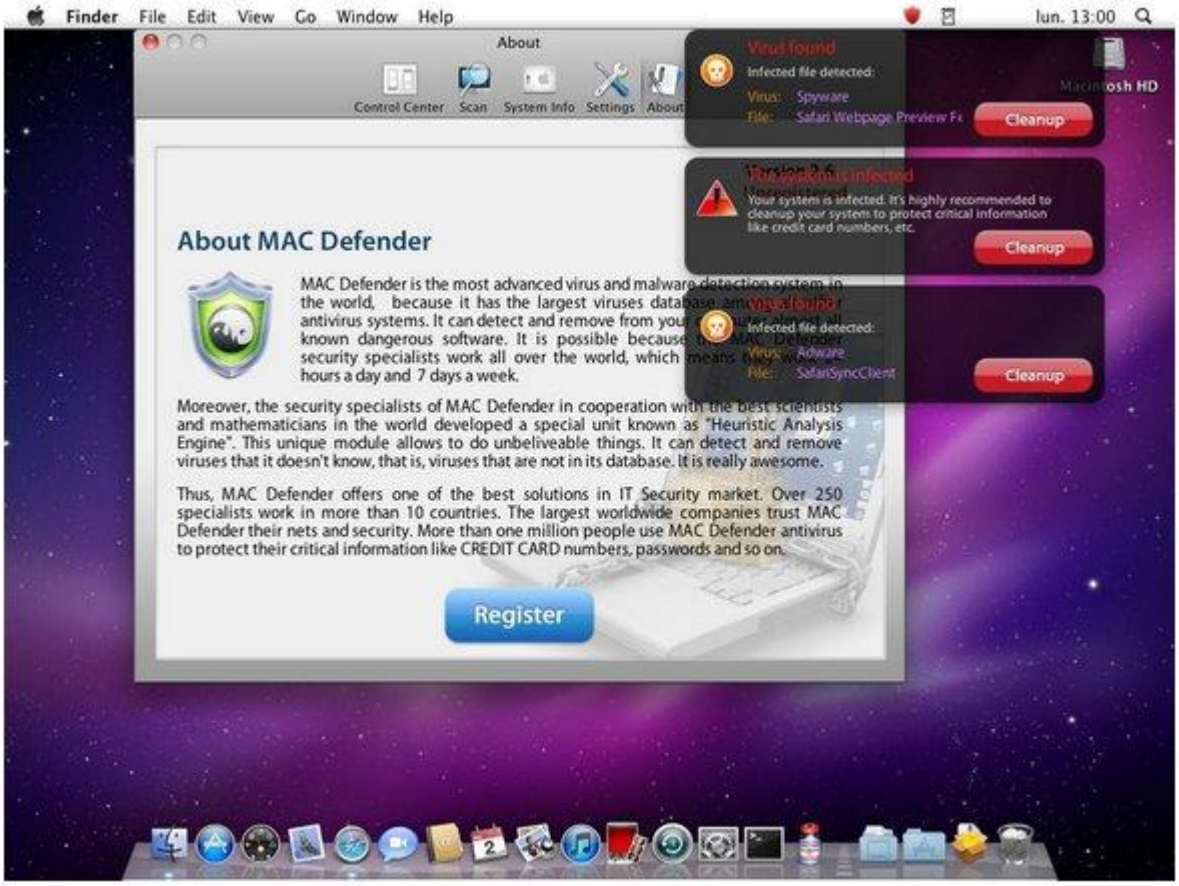


Ilustración 115: Captura de pantalla del malware Mac Defender

Se calcula que sólo en Estados Unidos, entre 60.000 y 150.000 equipos fueron afectados por este tipo de malware en 2011.

Otro malware que ha causado estragos en el entorno Mac es el conocido como "Flashback", que desactiva la protección anti-malware de MAC OS X bajo el aspecto de un falso instalador del software Flash Player.

Ilustración 116: Captura de pantalla del malware Flash back

Este malware desactiva las actualizaciones de seguridad, por lo que evita que los equipos que contengan este malware puedan ir dando solución a las amenazas que se detectan, y sigan estando desprotegidos. Según la empresa de seguridad informática "Kaspersky Labs", sólo en Estados Unidos más de 300.000 equipos han sido infectados por este malware, y más de medio millón en todo el mundo. A continuación se muestra la distribución por países de equipos afectados:

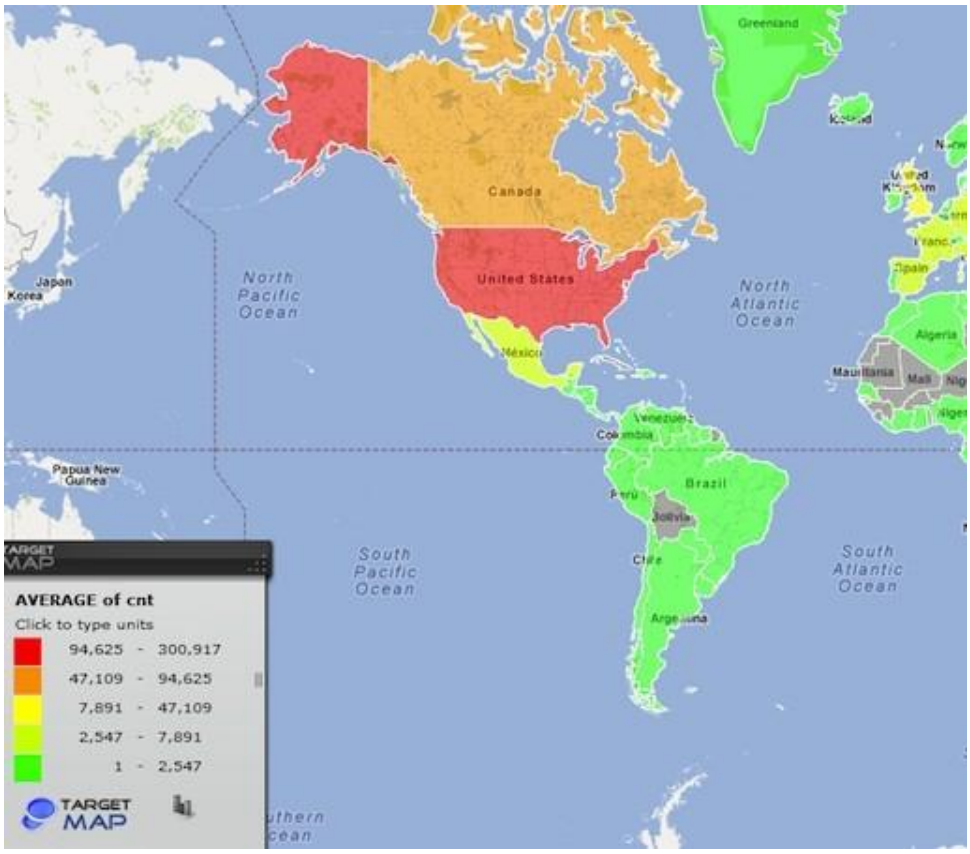


Ilustración 117: Distribución mundial de sistemas afectados por Flashback

Fuente: Kaspersky Labs

Afortunadamente, el malware "Flashback" ha sido controlado y actualmente experimenta un retroceso en el número de equipos infectados, como se puede observar en la siguiente ilustración:

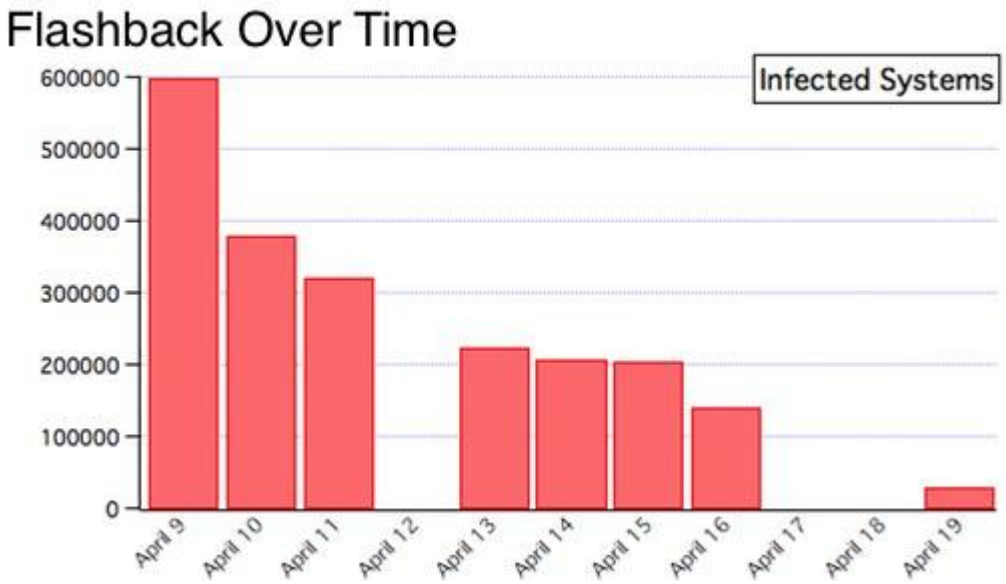


Ilustración 118: Decrecimiento del malware Flashbakc durante Abril de 2012

Como se observa, el sistema operativo MAC OS X ha pasado de pasar totalmente desapercibido para los desarrolladores de malware, a ser un importante objetivo, dada la subida de su cuota de mercado, por lo que Apple está tomando medidas para dotar a sus equipos de unas mayores medidas de seguridad frente a las nuevas amenazas. Actualmente Apple está desarrollando la última versión del sistema operativo (llamada Mountain Lion) cuyas principales novedades se centran en las medidas de seguridad tomadas para evitar ser un blanco fácil para el malware. Con la nueva versión se incorporan actualizaciones de seguridad que buscan diariamente nuevas actualizaciones en materias de seguridad de forma automática (o cada vez que se reinicie el equipo), tal y como lo pudiera hacer cualquier antivirus convencional, lo que supone un avance para la compañía Apple, que antes carecía de estas medidas de seguridad para su sistema operativo.

Otra herramienta que la compañía Apple pone al servicio de los usuarios de Mac es el software Gatekeeper, totalmente personalizable, permite configurar las opciones de seguridad en el equipo para poder restringir la descarga de software exclusivamente a la App Store (tienda oficial de Apple para Mac), o para instalar aplicaciones de desarrolladores que posean un identificador exclusivo emitido por Apple que garanticen la seguridad del software. Asimismo, Mac tiene una política de enjaulamiento de software para poder impedir que una aplicación maliciosa o cualquier tipo de malware pueda acceder al resto de partes del equipo infectado, e impedir que se ponga en peligro al sistema.

Ilustración 119: Opciones de seguridad y privacidad para MAC OS X

No obstante, pese a las medidas de seguridad implantadas por Apple en estos últimos años, lo cierto es que el malware para MAC OS X sigue aumentando de forma exponencial, como se puede ver en el siguiente gráfico:

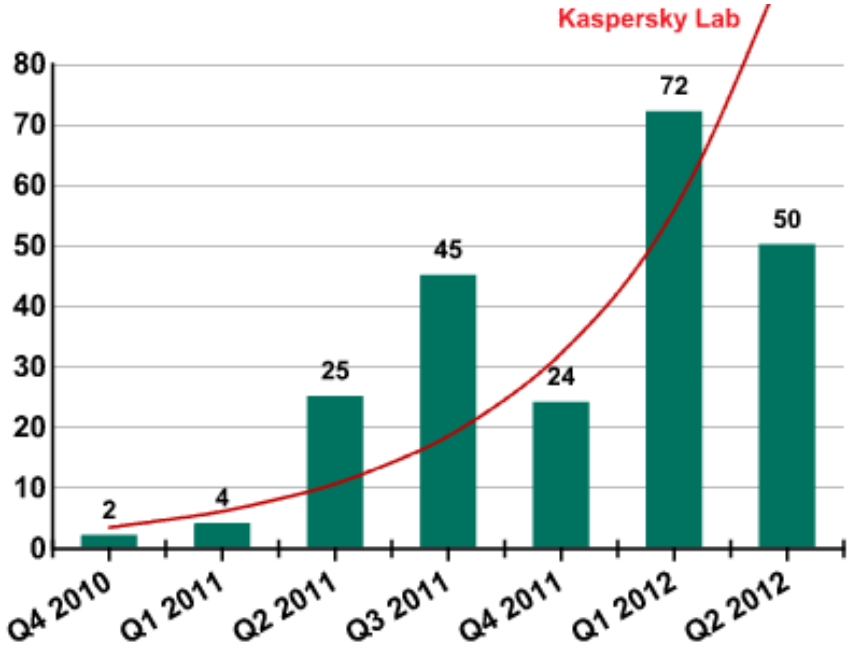


Ilustración 120: Previsión de malware para MAC OS X

Y se espera que sea así durante los próximos años, siendo una de las amenazas que mayor auge experimente.

8 GESTIÓN DEL PROYECTO

En este apartado se abordarán los aspectos más importantes que se han llevado a cabo para la consecución del proyecto, tales como la planificación realizada para la elaboración del documento, una valoración económica del mismo y las herramientas que se han empleado para poder elaborarlo.

8.1 Planificación del proyecto

En esta sección se van a resumir las diferentes fases que se han ido produciendo hasta poder concluir este proyecto.

- **Fase 1: Análisis**
  - **Objetivo del proyecto:** Determinar el objetivo principal del proyecto y los subobjetivos del mismo.
  - **Alcance del proyecto:** Determinar la profundización en los diversos temas tratados, así como el alcance de los mismos.
  - **Solución del proyecto**: Proponer y acordar una solución que aborde todos los objetivos a cumplir.

- **Fase 2: Planificación**
  - **Actividades necesarias:** Determinar todas las actividades que se han de realizar para ejecutar el proyecto.
  - **Recursos disponibles:** Esclarecer qué recursos tanto humanos como técnicos se van a disponer para poder desarrollar el proyecto.

- **Fase 3: Desarrollo**
  - **Recopilación de información:** Una vez fijados los objetivos a cubrir, se ha de buscar

todo tipo de documentación que pueda aportar información interesante y válida para el proyecto.

- **Selección de información:** De toda la información recogida, filtrar sólo la información más interesante y acorde a los objetivos del proyecto.
- **Elaboración de los contenidos:** Una vez acabado el proceso de documentación, se realiza la redacción de los contenidos del documento en base a los conocimientos adquiridos durante la documentación.
- **Revisión de los contenidos:** Toda vez que se ha confeccionado el documento, se pasa a revisar cada uno de los apartados para la aprobación final.

- **Fase 4: Entrega**

  - **Entrega del proyecto:** Una vez acabado y revisado, se procede a la entrega final del proyecto.

8.1.1 Estimación inicial

En el momento en el que se inició el proyecto, se realizaron una serie de estimaciones relativas al coste económico que podía suponer la realización del mismo, y el tiempo que podía llevar completarlo.

Se estimó el 1 de Febrero de 2012 como la fecha de inicio del proyecto, con un horario establecido para el alumno de 08:00 a 16:00 de lunes a viernes (40 horas semanales), y con un precio estimado por cada hora de trabajo del alumno de 4€.

Con estos parámetros, se calcularon los días que se iban a dedicar a cada una de las tareas, como se ve reflejado en el siguiente cuadro:

Nombre de tarea	Duración	Comienzo	Fin	Pre	Nombres de los recursos
Proyecto Fin de Carrera	**129 días**	**mié 01/02/12**	**lun 30/07/12**		
Fase 1: Análisis	**3 días**	**mié 01/02/12**	**vie 03/02/12**		
Objetivos del Proye	1 día	mié 01/02/12	mié 01/02/12		Alberto Gallego Yuste[40
Alcance del proyect	1 día	mié 01/02/12	mié 01/02/12		Alberto Gallego Yuste[30
Solución del proyec	1 día	jue 02/02/12	jue 02/02/12	6	Alberto Gallego Yuste[30
Fase 2: Planificación	**3 días**	**vie 03/02/12**	**mar 07/02/12**		
Actividades necesar	2 días	vie 03/02/12	lun 06/02/12	7	Alberto Gallego Yuste
Recursos disponible	1 día	mar 07/02/12	mar 07/02/12	9	Alberto Gallego Yuste[50
Fase 3: Desarrollo	**122 días**	**mié 08/02/12**	**jue 26/07/12**		
Recopilación de Inf	35 días	mié 08/02/12	mar 27/03/12	10	Alberto Gallego Yuste
Selección de Inform	20 días	mié 28/03/12	mar 24/04/12	12	Alberto Gallego Yuste
Elaboración de los c	60 días	mié 25/04/12	mar 17/07/12	13	Alberto Gallego Yuste
Revisión de los cont	7 días	mié 18/07/12	jue 26/07/12	14	Alberto Gallego Yuste
Fase 4: Entrega	**1 día**	**vie 27/07/12**	**vie 27/07/12**		
Entrega del proyect	1 día	vie 27/07/12	vie 27/07/12	15	Alberto Gallego Yuste

Ilustración 121: Distribución por fechas de las tareas a completar

El resultado final era un proyecto con una duración estimada de 129 días, finalizando así el 30 de Julio de 2012. La dedicación por parte del alumno iba a ser del 100% en cada una de las tareas excepto en 4 de ellas, recuadradas en rojo en la imagen anterior.

El diagrama de Gantt que se obtuvo fue el siguiente:

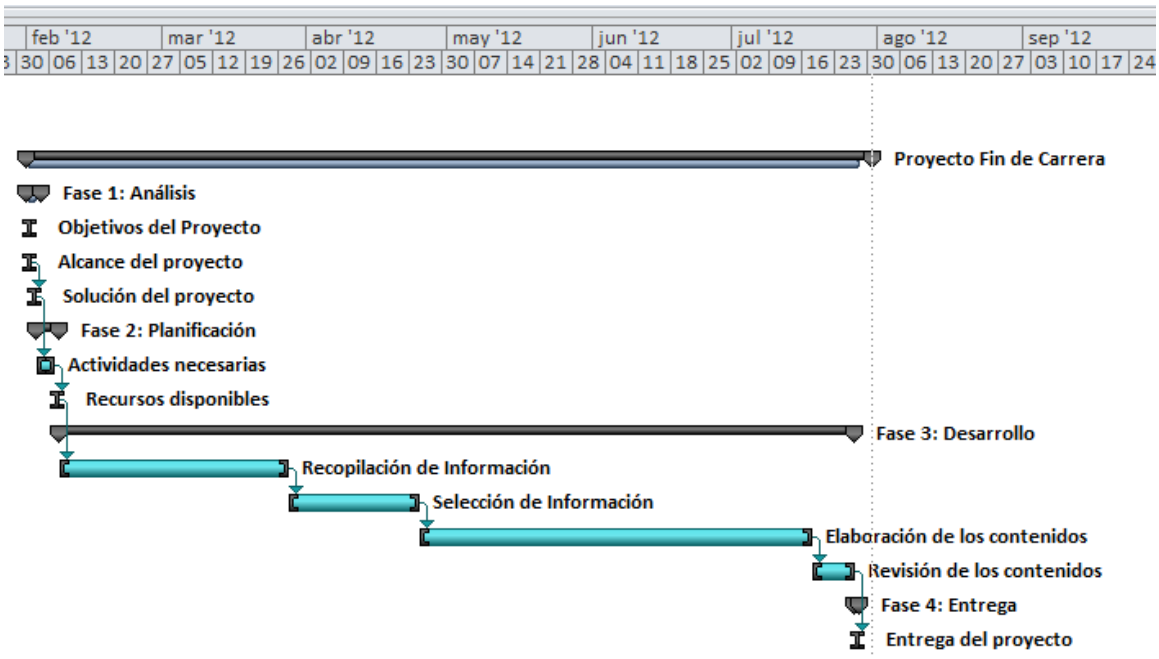


Ilustración 122: Diagrama de Gantt con planificación inicial

8.1.2 Planificación real

Como ocurre en la mayoría de los proyectos, las expectativas no fueron cumplidas y los plazos fueron superados ampliamente, por lo que en este apartado se procede a reflejar los plazos que se cumplieron en realidad durante el desarrollo del proyecto.

Así, veamos cuál fue la distribución de las tareas a lo largo del tiempo, y la duración final de las mismas:

Nombre de tarea	Duración	Comienzo	Fin	Pr	Nombres de los recursos	Comienzo de línea base	Duración de línea base	Variación de duración
Proyecto Fin de Carrera	**182 días**	**mié 01/02/12**	**jue 11/10/12**			**mié 01/02/12**	**129 días**	**53 días**
Fase 1: Análisis	**3 días**	**mié 01/02/12**	**vie 03/02/12**			**mié 01/02/12**	**3 días**	**0 días**
Objetivos del Proye	2 días	mié 01/02/12	jue 02/02/12		Alberto Galleg	mié 01/02/12	1 día	1 día
Alcance del proyect	2 días	mié 01/02/12	jue 02/02/12		Alberto Galleg	mié 01/02/12	1 día	1 día
Solución del proyecto	2 días	jue 02/02/12	vie 03/02/12		Alberto Gallego	jue 02/02/12	1 día	1 día
Fase 2: Planificación	**4 días**	**lun 06/02/12**	**jue 09/02/12**			**vie 03/02/12**	**3 días**	**1 día**
Actividades necesarias	3 días	lun 06/02/12	mié 08/02/12	7	Alberto Gallego Yuste	vie 03/02/12	2 días	1 día
Recursos disponible	1 día	jue 09/02/12	jue 09/02/12	9	Alberto Galleg	mar 07/02/12	1 día	0 días
Fase 3: Desarrollo	**174 días**	**vie 10/02/12**	**mié 10/10/12**			**mié 08/02/12**	**122 días**	**52 días**
Recopilación de Inf	55 días	vie 10/02/12	jue 26/04/12	10	Alberto Galleg	mié 08/02/12	35 días	20 días
Selección de Inform	35 días	vie 27/04/12	jue 14/06/12	12	Alberto Galleg	mié 28/03/12	20 días	15 días
Elaboración de los c	70 días	vie 15/06/12	jue 20/09/12	13	Alberto Galleg	mié 25/04/12	60 días	10 días
Revisión de los cont	14 días	vie 21/09/12	mié 10/10/12	14	Alberto Galleg	mié 18/07/12	7 días	7 días
Fase 4: Entrega	**1 día**	**jue 11/10/12**	**jue 11/10/12**			**vie 27/07/12**	**1 día**	**0 días**
Entrega del proyect	1 día	jue 11/10/12	jue 11/10/12	15	Alberto Galleg	vie 27/07/12	1 día	0 días

Ilustración 123: Planificación real del proyecto

Así, se observan una serie de variaciones e importantes cambios de plazo. Se observa una diferencia considerable en las estimaciones de las tareas de la fase 3, ya que, como es habitual, se tiende a pensar que una determinada actividad va a ser a priori sencilla, pero cuando se trata a fondo, se descubren multitud de problemas que hacen que la duración de la tarea sea mucho mayor de lo esperado, por lo que en las tareas más largas es donde más se ha notado esta diferencia entre la teoría y la práctica. Se pasa a mostrar el Gantt de seguimiento, que muestra el contraste entre la planificación real obtenida, con las tareas que sufrieron alguna variación (en rojo) y las tareas que se cumplieron como se planificó (en azul) con la planificación calculada inicialmente (en negro):

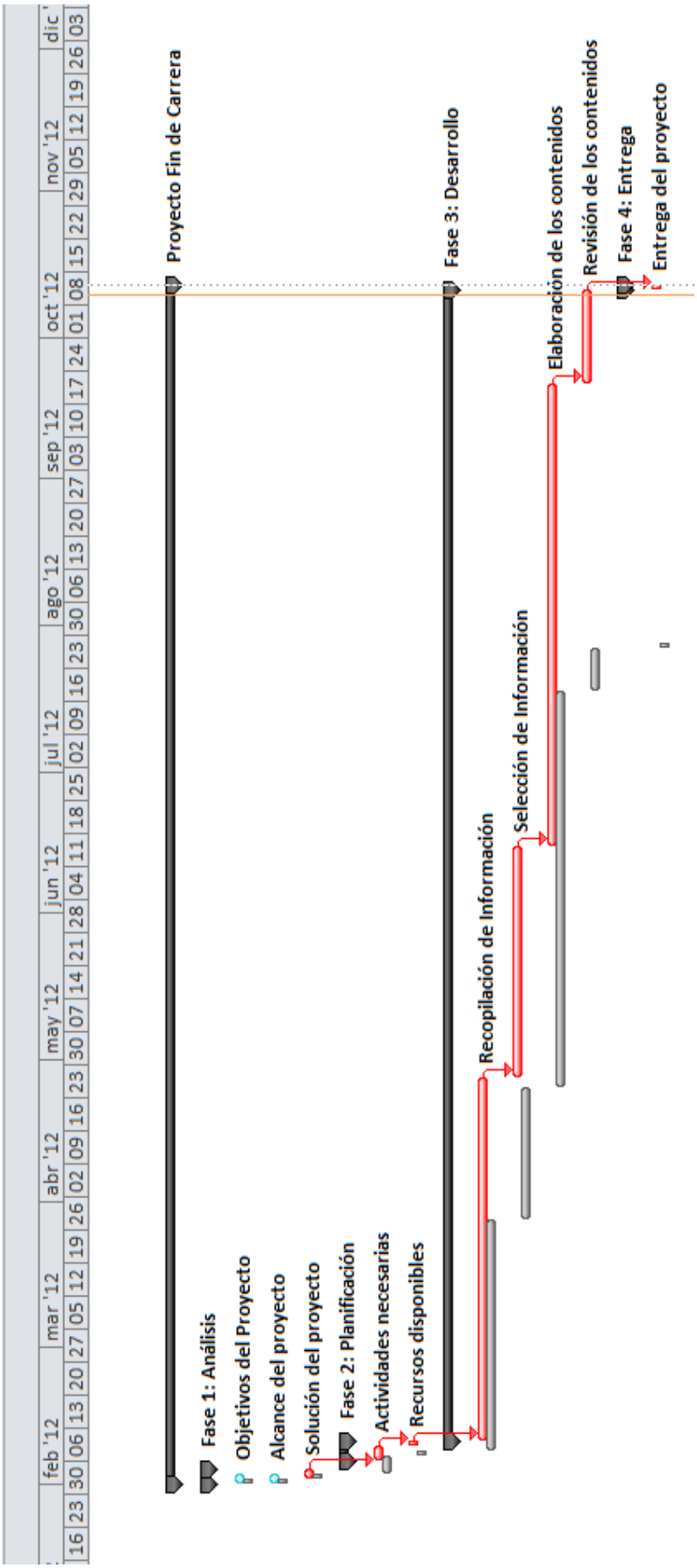


Ilustración 124: Gantt de seguimiento

8.1.3 Análisis de la planificación

Por último, se va a pasar a comentar un pequeño resumen de los planteamientos inicial y final recogidos por la herramienta Microsoft Office Project.

Cabe mencionar que los costes calculados corresponden sólo a costes humanos, por lo que más adelante se comentará con más detalle los costes totales de la elaboración del proyecto.

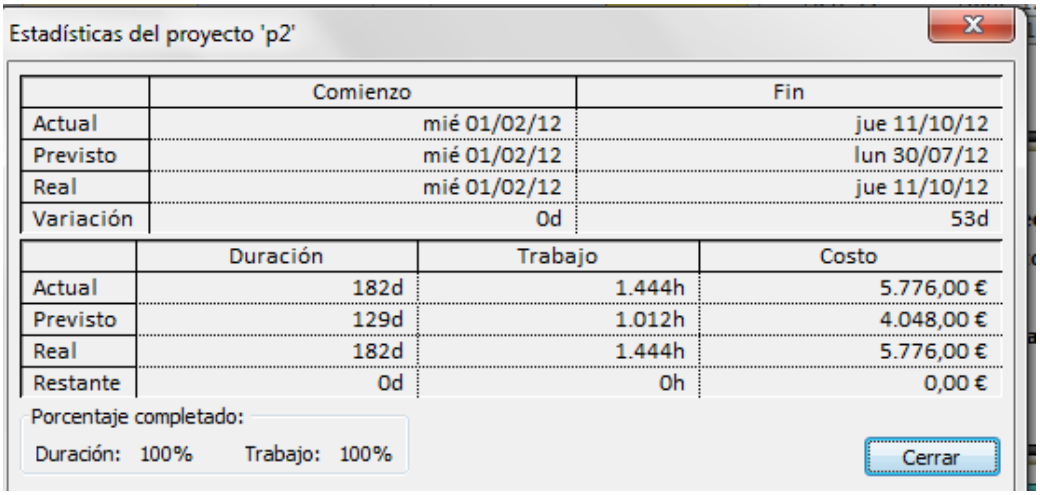


Ilustración 125: Estadísticas finales del proyecto

Como se observa, existe una diferencia considerable entre lo estimado y lo que ha ocurrido finalmente (53 días). Esto es debido a que el proyecto se realizó al mismo tiempo que el Curso de Adaptación al Grado de Informática, por lo que los horarios resultaron bastante difíciles de cumplir en algunas ocasiones, debido al alto volumen de trabajo en el curso mencionado. Así, hay que añadir el bajón que se produjo en el desarrollo del proyecto en los meses de julio y agosto, dado que se tuvo que compaginar la realización del proyecto con actividades laborales que ocupaban la mayor parte del día, por lo que los avances en ese tiempo fueron muy escasos.

En cuanto al costo se observa un incremento final en torno a los 1.700€, ya que pasamos de un presupuesto inicial de 4.048€ a un presupuesto final de 5.776€. Esto es debido a que la duración final del proyecto ha sido mayor de la esperada, por lo que se han ido aumentando los costes al utilizar mayor tiempo los recursos disponibles.

8.2 Recursos empleados

En este apartado se pasará a describir los recursos tanto materiales como humanos utilizados para el desarrollo del proyecto.

8.2.1 Recursos hardware

TIPO	NOMBRE
Ordenador portátil	Ordenador HP 630
Disco Duro Externo	Disco duro externo portátil Lacie 500GB
Impresora	Impresora HP Laser Jet

Tabla 1: Recursos Hardware disponibles

8.2.2 Recursos software

TIPO	NOMBRE
Sistema Operativo	Windows 7
Navegador	Google Chrome Web Browser
Editor de texto	Notepad++
Procesador de Texto	Microsoft Office Word 2010
Planificador y gestor de proyectos	Microsoft Office Project 2010
Elaboración de diapositivas	Microsoft Office Power Point 2010
Almacenamiento web	Discoweb y Dropbox

Tabla 2: Recursos software disponibles

8.3 Balance Económico

A continuación se procederá a analizar los aspectos económicos derivados de la realización del proyecto.
En este aspecto, se ha decidido clasificar los diferentes gastos dependiendo de su naturaleza, dividiéndolos en tres apartados:

- **Costes Humanos:** Derivados de las horas de dedicación de las personas que han participado en el desarrollo del proyecto.
- **Costes Materiales:** Derivados de todos los recursos materiales que se han usado para el desarrollo del proyecto.

- **Otros costes:** Cualquier otro gasto que no pudiera englobarse en ninguno de los dos apartados anteriores.

Primeramente, se verán los costes planificados para los recursos humanos:

Puesto	Coste/Hora	Total Horas	Coste total
Alberto Gallego Yuste (Ing. Técnico)	4 €	1.012	4.048 €

Tabla 3: Planificación inicial para costes humanos

Ahora, pasamos a ver los costes planificados para los recursos materiales:

Descripción	Coste (euro)	%Uso dedicado proyecto	Dedicación (Meses)	Periodo de depreciación	Coste Imputable
Ordenador Portátil Personal	396 €	100	6	48	49,50 €
Paquete Microsoft Office 2010	139 €	100	6	48	17,38 €
Disco duro externo 500GB	76,9€	100	6	48	9,61 €
				TOTAL	**76,49 €**

Tabla 4: Planificación inicial para costes materiales

Por último, vemos los costes planificados relativos a otros gastos:

Tipo	Empresa	Coste Imputable
Material de oficina		25 €
	TOTAL	**25 €**

Tabla 5: Planificación inicial para otros gastos

Se estiman unos costes indirectos de un 20% del total calculado, por lo que se han de añadir **829,9 €** a los costes ya realizados.

Pasaremos a resumir el conjunto de costes totales asociados al

proyecto, según la planificación inicial:

Presupuesto Total Planificación Inicial	
Costes humanos	4.048 €
Costes Materiales	76,49 €
Otros costes	25 €
Costes indirectos	829,9 €
TOTAL	**4.979,39 €**

Tabla 6: Planificación inicial del presupuesto total

Como se ha dicho anteriormente, se han sufrido algunas variaciones que hacen que el presupuesto haya sido modificado durante la realización del proyecto, por lo que se pasará a revisar la planificación real obtenida tras la finalización del mismo.

Primeramente veremos los costes asociados a los recursos humanos:

Puesto	Coste/Hora	Total Horas	Coste total
Alberto Gallego Yuste (Ing. Técnico)	4 €	1.444	5.776 €

Tabla 7: Planificación real para costes humanos

Ahora, los costes materiales:

Descripción	Coste (euro)	%Uso dedicado proyecto	Dedicación (Meses)	Periodo de depreciación	Coste Imputable
Ordenador Portátil Personal	396 €	100	9	48	74,25 €
Paquete Microsoft Office 2010	139 €	100	9	48	26,06 €
Disco duro externo 500 GB	76,9€	100	9	48	14,42 €
				TOTAL	**114,73 €**

Tabla 8: Planificación real para costes materiales

Los costes acarreados por otro tipo de gastos:

Tipo	Empresa	Coste Imputable
Material de oficina		40 €
	TOTAL	**40 €**

Tabla 9: Planificación real para otros gastos

Por último, se añaden a esos cálculos el 20% estimado como costes indirectos, lo que suponen **1186,14 €** más.

Finalmente, se procede a calcular la totalidad de costes acarreados durante el desarrollo del proyecto, según la planificación final:

Presupuesto Total Planificación Real	
Costes humanos	5.776 €
Costes Materiales	114,73 €
Otros costes	40 €
Costes indirectos	1.186,14 €
TOTAL	**7.116,87 €**

Tabla 10: Planificación real del presupuesto total

Por lo tanto, si se realiza una sencilla resta se podrá comprobar la diferencia de presupuestos planificados entre el momento de inicio del proyecto, y la planificación final del mismo, dando como resultado una cantidad de **2.137,48 €.**

9 CONCLUSIONES FINALES

Finalizado el documento, se puede concluir que la misión principal del mismo ha quedado resuelta, ya que este manual podrá servir a los usuarios para poder percatarse de los peligros que esconde Internet y las técnicas que pueden emplear los delincuentes informáticos para poder perpetrar sus acciones.

A través de este documento, el usuario podrá extraer la información suficiente para protegerse en todo momento de cualquier amenaza que pueda atacar a su sistema informático y poder mantener fuera del alcance de los infractores, tanto el funcionamiento de su equipo como los datos privados o confidenciales contenidos en él.

Además, el lector podrá informarse acerca del marco legal actual en este aspecto de la informática, los organismos a los que acudir para poder denunciar algún tipo de infracción, o simplemente obtener a título informativo un breve resumen de la forma de actuar de los ciberdelincuentes y su evolución a lo largo de la historia.

Este documento abre un abanico de posibilidades bastante amplio sobre posibles nuevos proyectos a realizar. Así, puede suponer un comienzo para un estudio más en profundidad acerca de las nuevas amenazas y medidas de seguridad a tomar en los smartphones, o estudios más amplios acerca de elementos como los conocidos "troyanos", el incipiente hacktivismo, o el malware para MAC OS X; temas que, habiendo sido comentados, podían haber sido extendidos aún con más detenimiento, ya que existe una gran cantidad de información acerca de los mismos y tienen un papel muy importante en la actualidad, pero que por restricciones en el tiempo de elaboración del proyecto han sido reducidos, aunque son temas tan amplios que pueden dar cabida a un estudio más detallado en un futuro.

Para finalizar, pienso que este proyecto es bastante útil dado que ningún usuario es ajeno a las amenazas informáticas. Por muy experto o muy precavido que pueda llegar a ser un usuario, siempre van a aparecer nuevos mecanismos, nuevas formas de actuar de

forma ilegal con posibles consecuencias nefastas para nuestros equipos informáticos, por lo que considero de gran utilidad el transmitir mediante este documento, no sólo las posibles amenazas detectadas, sino los derechos que el usuario posee y los lugares donde las víctimas pueden reclamar o denunciar actos delictivos de los que hayan sido objetos, habiendo puesto especial hincapié en la figura fundamental del denunciante, que considero que a partir de este documento podrán entender su importancia capital a la hora de detectar nuevas amenazas y podrán saber dónde pueden encontrar una respuesta a sus problemas.

Para finalizar, creo que este proyecto puede ser el punto de inicio para muchos otros en un futuro próximo. Así, se puede realizar una actualización periódica de las amenazas informáticas y el malware que sea frecuente en los próximos años, recopilando nuevas técnicas ilegítimas que puedan surgir, y sobre todo, nuevos métodos para poder prevenir estas amenazas.

También se podrían elaborar proyectos en torno a cualquier tipo de malware explicado en este documento, para pasarlo a documentar más a fondo y poder ahondar aún más en cada una de las técnicas empleadas, analizar cada uno de los malware empleados, descifrar y describir cada uno de los códigos empleados, etc. de forma más exhaustiva, cosa que ha resultado imposible en el presente documento dada la cantidad de temas que se querían abordar en el mismo.

Otro posible documento que podría elaborarse sería un manual específico sobre malware en dispositivos móviles, ya que considero que es una amenaza que aumenta exponencialmente y que no es tomada demasiado en cuenta hoy en día por los usuarios (observando por ejemplo el bajísimo número de antivirus instalados actualmente en smartphones operativos en España) por lo que en un futuro no muy lejano es presumible que para un usuario medio sea de igual o mayor relevancia saber cómo proteger su dispositivo móvil del malware y el fraude informático que su propio ordenador personal, por lo que un manual que aconsejara y ofreciera medidas de seguridad en este aspecto, y alertara de las posibles amenazas existentes para estos dispositivos, se antoja bastante interesante tanto para los usuarios de estos aparatos como para la persona que

tenga a bien elaborarlo.

Por último, se puede realizar un especial seguimiento al desarrollo de las nuevas tendencias sociales y comportamientos de los usuarios como el hacktivismo, que podrían tomar especial relevancia en los próximos años.

10 BIBLIOGRAFÍA

Título: Derecho informático
Autor: Téllez Valdés, Julio
ISBN: 968-36-0046-8

11 REFERENCIAS ELECTRÓNICAS

- Introducción y objetivos:

  http://www.zocalo.com.mx/seccion/articulo/aumentan-7-las-ventas-en-eeuu-gracias-al-viernes-negro

- Delitos informáticos en Internet: el inicio de una nueva amenaza para los consumidores

  http://delitosinformaticos.info/delitos_informaticos/definicion.html

- Características de los delitos informáticos

  http://delitosinformaticos.info/delitos_informaticos/definicion.html

- Clasificación de los delitos informáticos

- Clasificación según la ONU:

  https://sites.google.com/site/yirmaleandrohuepe/clasificacion delosdelitosinformaticos

- Clasificación según el "Convenio sobre la Ciberdelincuencia"

  http://delitosinformaticos.info/delitos_informaticos/tipos_delitos.html

- Clasificación según la Brigada de Investigación Tecnológica de la Policía Nacional Española

  http://delitosinformaticos.info/delitos_informaticos/tipos_delitos.html
  http://www.wikilearning.com/articulo/marco_legal_en_europa_y_espana_sobre_delitos_informaticos-legislacion_sobre_los_delitos_informaticos/8866-1

- Actores dentro de un delito informático
- Sujeto activo de los delitos informáticos
- Sujeto pasivo de los delitos informáticos:

  http://es.wikipedia.org/wiki/Delito_inform%C3%A1tico#Sujetos_activos_y_pasivos
  http://pegtrin332008.blogspot.com.es/2009/11/sujeto-activo-vs-sujeto-pasivo-de-los.html
  http://www.monografias.com/trabajos17/delitos-informaticos/delitos-informaticos.shtml#sujeto

- Hackers:

  http://www.informatica-juridica.com/trabajos/posibles_sujetos.asp

- Crackers:

  http://cerigrafiascreen.galeon.com/aficiones1892451.html

- Phreaker:

  http://es.wikipedia.org/wiki/Phreaking
  http://www.informatica-juridica.com/trabajos/posibles_sujetos.asp

- Lammers:

  http://es.wikipedia.org/wiki/Lamer_(inform%C3%A1tica)

- Gurús:

  http://hackers18.wordpress.com/tipos-de-hachers/

- Bucaneros:

  http://niknitro.blogspot.com.es/2010/08/tipos-de-informaticos.html

- Newbie:

  http://es.wikipedia.org/wiki/Newbie

- Trashing:

  http://xiomymck11.blogspot.com.es/2011/01/trashing_23.html

- Estadísticas de los delitos informáticos

  http://delitosinformaticos.info/peritaje_informatico/estadisticas.html

- Legislación actual en España frente a los delitos informáticos

- Legislación actual en España

  http://delitosinformaticos.com/delitos/codigopenal.shtml

- Delitos informáticos y el código penal

  http://delitosinformaticos.info/delitos_informaticos/legislacion.html

- Legislación adicional

  http://delitosinformaticos.com/delitos/codigopenal.shtml
  http://www.wikilearning.com/articulo/marco_legal_en_europa_y_espana_sobre_delitos_informaticos-legislacion_sobre_los_delitos_informaticos/8866-1

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)

  http://noticias.juridicas.com/base_datos/Admin/lo15-1999.html

- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSICE)

  http://noticias.juridicas.com/base_datos/Admin/l34-2002.t1.html#a1

- Real Decreto Legislativo 1/1996, de 12 de abril (BOE 22-4-1996), por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual.

  http://www.boe.es/buscar/doc.php?id=BOE-A-1996-8930

- Real Decreto Legislativo 14/1999, de 17 de septiembre, sobre Firma Electrónica.

  http://noticias.juridicas.com/base_datos/Derogadas/r0-rdl14-1999.t1.html#a1

- Organismos adicionales

- Brigada de Investigación Tecnológica (Cuerpo Nacional de Policía)

  http://www.policia.es/org_central/judicial/udef/bit_quienes_somos.html
  http://www.policia.es/org_central/judicial/udef/bit_funciones.html

- Grupo de Delitos Telemáticos (Guardia civil)

  http://www.guardiacivil.es/es/servicios/delitos_telematicos/index.html

- Necesidades y deficiencias

  http://www.wikilearning.com/articulo/marco_legal_en_europa_y_espana_sobre_delitos_informaticos-legislacion_sobre_los_delitos_informaticos/8866-1

- Conclusiones

  http://www.wikilearning.com/articulo/marco_legal_en_europa_y_espana_sobre_delitos_informaticos-legislacion_sobre_los_delitos_informaticos/8866-1

- Tipos de fraude

  http://cert.inteco.es/Formacion/Amenazas/Virus/

- Virus y programas maliciosos

  http://cert.inteco.es/Formacion/Amenazas/Virus/

- Según su capacidad de propagación

- Virus

  http://www.desarrolloweb.com/de_interes/virus-mas-famosos-historia-informatica-2328.html
  http://www.ionlitio.com/images/2006/11/virus_barrotes.gif

- Gusanos

  http://es.wikipedia.org/wiki/ILoveYou
  http://4.bp.blogspot.com/_iUmakzWkMDs/S4coWYHRoII/AAAAAAAAACc/BotLfIZCQ5Y/s320/virus_iloveyou.gif
  http://www.elmundo.es/navegante/2000/05/05/ailofiu_virus.html

  http://es.wikipedia.org/wiki/ILoveYou

- Troyanos

  http://es.wikipedia.org/wiki/Troyano_(inform%C3%A1tica)

  http://www.taringa.net/posts/info/13702839/lo-que-debes-saber-_-hackers-y-tipos-de-troyanos-_-famosos.html

  http://troyanosyvirus.com.ar/

  http://www.youtube.com/watch?v=Zz39iHrFGDY&feature=related

  http://www.informatica-hoy.com.ar/software-seguridad-virus-antivirus/Como-eliminar-un-virus-troyano.php

  http://en.wikipedia.org/wiki/Siberian_pipeline_sabotage

  http://www.teleobjetivo.org/blog/el-mayor-sabotaje-de-la-guerra-fria.html

  http://cybercrime.pandasecurity.com/bredolab/how_works.php?lang=es

- Troyanos bancarios

  http://www.inteco.es/Seguridad/Observatorio/Articulos//Que_son_y_como_funcionan_los_troyanos_bancarios

  http://www.infospyware.com/articulos/que-son-y-como-funcionan-los-troyanos-bancarios/

  http://blog.hispasec.com/laboratorio/267

  http://seguridad.internautas.org/html/4189.html

- Registro de teclas pulsadas

  http://es.wikipedia.org/wiki/Keylogger

  http://r-daddyparadise.blogspot.com.es/2008/07/instalar-un-ardamax-keylogger.html

  http://www.freedownloadmanager.org/es/downloads/Keylogg

er_Free_Download_66343_p/

- Capturas de pantalla y grabación de vídeo:

  https://bancoonline.openbank.es/servlet/PProxy?cmd=971
  http://www.hispasec.com/laboratorio/troyano_spain_latino.pdf
  http://blog.hispasec.com/laboratorio/153
  http://www.hispasec.com/laboratorio/troyano_video.htm
  http://www.hispasec.com/laboratorio/troyano_bancario_captura_video.pdf

- Inyección de campos fraudulentos en formularios:

  http://www.ingdirect.es/corporativo/por-que-elegirnos/seguridad6.html

- Pharming:

  http://identidadgeek.com/rodolfo-baz-spoofing-scamming-y-pharming-cpmexico/2010/08/
  http://www.techrepublic.com/blog/security/hosts-file-pharming-and-other-botnet-recruiting-methods/738

- Clasificación según las acciones que realizan

- Adware:

  http://www.infospyware.com/articulos/que-son-los-adware/
  http://es.wikipedia.org/wiki/Adware
  http://www.segu-info.com.ar/malware/spyware.htm
  http://www.eset-la.com/centro-amenazas/consejo/consejos-contra-malware-IV/1553

- Spyware:

  http://www.segu-info.com.ar/malware/spyware.htm

- Bloqueador:

  http://cert.inteco.es/Formacion/Amenazas/Virus/
  http://tecnolatino.com/como-bloquear-sitios-web-en-firefox/
  http://www.taringa.net/posts/hazlo-tu-mismo/10983745/Bloquear-paginas-web-con-el-HOST_-facil-y-rapido_-_XP-Y-7_.html
  http://lh3.ggpht.com/_HFWqTWZY0Nc/TQfIDi5lFqI/AAAAAAAAB3s/U5ROvYAPJt0/p1-v3.jpg

- Bomba lógica

  http://es.kioskea.net/contents/virus/bomblogi.php3
  http://www.dailymotion.com/video/xgd3k4_bacth-bomba-logica_creation
  http://2.bp.blogspot.com/_ZeeLp9OkVRA/S_hEq1scGSI/AAAAAAAAAPXk/uNOYY4fyUKA/s1600/reloj-despertador-bomba.jpg
  http://edwinnajera.wordpress.com/2009/04/30/bombas-logicas/
  http://delitosinformaticos.com/delitos/bombalogica.shtml
  http://www.dgamers.net/threads/54196-Una-bomba-l%C3%B3gica-en-Fannie-Mae-deja-a-la-empresa-parada-una-semana
  http://edwinnajera.wordpress.com/2009/04/30/bombas-logicas/

- Broma (Joke):

  http://ilmaistro.com/cmo-crear-un-virus-que-apague-la-pc/

- Bulo (Hoax):

  http://www.teraweb.net/articulos/informacion_falsa_en_internet_hoax_bulo.php
  http://www.rompecadenas.com.ar/hoaxes.htm

- Clicker:

  http://www.viruslist.com/sp/viruses/encyclopedia?virusid=38991

- Ransomware:

  http://www.eset-la.com/centro-amenazas/amenazas/Ransomware/2150
  http://www.infospyware.com/tag/ransomware/
  http://ateneo.unmsm.edu.pe/ateneo/bitstream/123456789/2740/1/William_Francisco_Pe%C3%B1a_Miranda_2010.pdf
  http://www.policia.es/prensa/20120130_4.html
  http://www.osi.es/es/actualidad/avisos/2012/01/virus-muestra-un-falso-mensaje-del-cuerpo-nacional-de-policia

- Downloader:

  http://virusattack.blogspot.com.es/2008/05/qu-es-un-downloader-leccin-18.html

- Exploit:

  http://www.segu-info.com.ar/malware/exploit.htm
  http://blog.webroot.com/2012/02/08/researchers-intercept-two-client-side-exploits-serving-malware-campaigns/

- Herramientas de fraude:

  http://www.infospyware.com/blog/falso-microsoft-security-essentials-alert/

- Dropper:

  http://www.symantec.com/security_response/writeup.jsp?docid=2002-082718-3007-99
  http://antivirus.interbusca.com/glosario/dropper.html

- Ladrón de contraseñas (PWStealer)

  http://descargashack.blogspot.com.es/2009/03/pms-stealer-01-by-drigin.html

- Marcador (dialer):

  http://thepcsecurity.com/dialer-malware-how-to-avoid-dialler-virus-infections/
  http://malware.wikia.com/wiki/Dialer
  http://www.worldstart.com/dialer-malware/

- Backdoor:

  http://cert.inteco.es/Formacion/Amenazas/Virus/
  http://www.segu-info.com.ar/malware/backdoor.htm
  http://news.softpedia.es/Un-troyano-Flashback-infecta-a-mas-de-600-000-ordenadores-Mac-262983.html

- Rootkit:

  http://www.segu-info.com.ar/malware/rootkit.htm
  http://www.muycomputer.com/2011/08/01/windows-xp-gran-almacen-rootkit-avast
  http://unaaldia.hispasec.com/2005/11/sony-utiliza-un-rootkit-que-pone-en.html

- Browser hijacker:

  http://www.microsoft.com/es-es/security/resources/hijacking-whatis.aspx
  http://www.pcstats.com/articleview.cfm?articleID=1579

- ¿Cómo puedo saber si el explorador ha sido asaltado?

  http://www.microsoft.com/es-es/security/resources/hijacking-whatis.aspx

- Otras clasificaciones

  http://cert.inteco.es/Formacion/Amenazas/Virus/
  http://es.wikipedia.org/wiki/Stealer_(inform%C3%A1tica)

- Programas no recomendables

  http://cert.inteco.es/Formacion/Amenazas/Virus/

- Cookies maliciosas

  http://cert.inteco.es/Formacion/Amenazas/Virus/

- Malware: Cómo llega al sistema informático y cómo prevenirlo

  http://cert.inteco.es/Formacion/Amenazas/Virus/
  http://www.enhacke.com/tag/windows/page/4/
  http://es.wikipedia.org/wiki/Estafa_nigeriana
  http://www.taringa.net/posts/info/1488825/El-timo-Nigeriano-es-la-tercera-fuente-de-ingresos-del-pais.html
  http://www.pandasecurity.com/spain/homeusers/security-info/42189/Bck%2FIRCbot.K/
  http://cert.inteco.es/virusDetail/Actualidad/Actualidad_Virus/Detalle_Virus/IRCbot_K
  http://www.elmundo.es/elmundo/2012/01/13/leon/1326456766.html

- ¿Qué sucede con los datos robados?

  http://www.inteco.es/Seguridad/Observatorio/Articulos//Que_son_y_como_funcionan_los_troyanos_bancarios

- ¿Cómo se materializa finalmente el robo?

  http://www.inteco.es/Seguridad/Observatorio/Articulos//Que_son_y_como_funcionan_los_troyanos_bancarios

- Cómo actuar tras ser objeto de un fraude en Internet

  http://es.norton.com/victim/article
  http://www.antifraude.org/2009/06/donde-denunciar-si-usted-es-victima-de-delitos-informaticos/
  http://www.microsoft.com/business/es-es/Content/Paginas/article.aspx?cbcid=123

- Cómo prevenir fraudes por Internet
- Medidas de seguridad recomendadas

  https://www.gdt.guardiacivil.es/webgdt/consejos.php
  http://delitosinformaticos.info/consejos/sobre_seguridad_informatica.html

- ¿Cómo reconocer una página web fraudulenta?

  http://cert.inteco.es/Formacion/Fraude_en_Internet/intecocert_fraude_cert_WebFraudulenta?orden=04

- Peritaje informático
- Fases

  http://www.delitosinformaticos.info/peritaje_informatico/servicios_peritaje.html

- Evidencias electrónica

  http://www.delitosinformaticos.info/peritaje_informatico/evidencia_electronica.html
  http://www.borrmart.es/articulo_redseguridad.php?id=1376
  http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

- Informe pericial

  http://www.delitosinformaticos.info/peritaje_informatico/informe_pericial.html

- Casos reales:

  http://www.delitosinformaticos.info/peritaje_informatico/case_studies.html

- Evolución de los ciberdelitos en los próximos años:
- Principales delitos informáticos cometidos en el año 2011

  http://www.kaspersky.com/sp/about/news/virus/2012/Amenazas_de_seguridad_mas_destacadas_de_2011_y_tendencias_2012

- Previsiones sobre delitos que se perpetrarán durante el año 2012 y sucesivos

  http://hackmageddon.com/2012/01/08/browsing-security-predictions-for-2012/

- ¿Hacia dónde vamos?: Previsión sobre los principales delitos informáticos de la próxima década

  http://www.nuevastecnologias.com/evolucion-del-cibercrimen-en-los-proximos-anos-14-03-2011/
  http://www.keegy.com/post/evolucion-del-cibercrimen-en-los-proximos-anos/
  http://www.pcactual.com/articulo/actualidad/noticias/8150/kaspersky_revela_sus_previsiones_sobre_evolucion_del_cibercrimen.html
  http://www.pcworld.com.mx/Articulos/12159.htm
  http://www.computing.es/seguridad/encuentros/1035597002501/cibercrimen-dirige-ahora-dispositivos.1.html
  http://conecti.ca/2012/02/24/segun-mcafee-dispositivos-moviles-son-el-mayor-blanco-de-malware/
  http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2011.pdf

- Hacktivismo: una amenaza latente y en expansión

  http://es.wikipedia.org/wiki/Ataque_de_denegaci%C3%B3n_de_servicio
  http://www.genbeta.com/web/son-los-ataques-ddos-efectivos-como-medio-de-protesta
  http://www.codigogeek.com/2008/02/08/que-hacer-ante-un-ataque-ddos/
  http://www.hackplayers.com/2010/12/loic-la-herramienta-

ddos-utilizada-por.html
http://www.taringa.net/posts/info/12061115/Loic-para-windows_-linux-y-mac-instalacion-y-uso.html
http://samkear.com/security/refref-latest-denial-service-tool-anonymous
http://www.itespresso.es/anonymous-anuncia-refref-su-nueva-arma-digital-52242.html
http://foro.elhacker.net/foro_libre/demostracion_de_la_arma_ddos_refref_de_anonymous-t335969.0.html
http://es.wikipedia.org/wiki/Tor

- HBGary Federal: Más allá de la denegación de servicio

http://www.pagina12.com.ar/diario/cdigital/31-161926-2011-02-08.html
http://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/
http://www.dailymail.co.uk/sciencetech/article-1354890/Cyber-warfare-breaks-security-firms-threat-expose-pro-WikiLeaks-hackers.html
http://arstechnica.com/tech-policy/2011/02/how-one-security-firm-tracked-anonymousand-paid-a-heavy-price/
http://www.thetechherald.com/articles/Report-HBGary-used-as-an-object-lesson-by-Anonymous/12723/
http://www.chw.net/2011/02/hbgary-intenta-averiguar-identidad-de-anonymous-salen-trasquilados/
http://nakedsecurity.sophos.com/2011/02/07/hbgary-federal-hacked-and-exposed-by-anonymous/

- Advanced Persistent Threat (ATP)

http://en.wikipedia.org/wiki/Advanced_persistent_threat
http://blog.segu-info.com.ar/2011/09/apt-advanced-persistent-threats.html#axzz24qzSNd5Y
http://hackmageddon.com/tag/mcafee/
https://www.bit9.com/advanced-persistent-threat/index.php
http://siforense.blogspot.com.es/2010/11/advanced-persistent-threat-apt.html

- Autoridades Certificadoras

  http://www.protegetuordenador.com/index.php/noticias/629-malware-con-certificado-de-confianza.html
  http://www.csirtcv.gva.es/es/noticias/descubren-malware-que-utiliza-un-certificado-digital-robado.html
  http://www.pcworld.com.mx/Articulos/19486.htm
  http://es.wikipedia.org/wiki/Autoridad_de_certificaci%C3%B3n
  http://certificadodigital-alejandro.blogspot.com.es/
  http://www.securitybydefault.com/2012/06/flame-y-los-certificados-digitales.html
  http://blog.nerion.es/2011/03/25/la-seguridad-de-los-certificados-de-comodo-puede-haber-sido-comprometida/
  http://www.redeszone.net/2011/08/30/la-seguridad-de-gmail-en-iran-en-entredicho-por-un-certificado-falso/

- Ataques informáticos: ¿las guerras del futuro?

  http://recursivefractal.blogspot.com.es/2012/06/on-stuxnet.html
  http://www.clarin.com/internet/virus-Stuxnet-fuerte-vienen-ciberguerras_0_344965751.html
  http://www.veriluma.com/2010/11/origins-of-stuxnet/
  http://securityaffairs.co/wordpress/3716/malware/duqu-cyber-weapons-factory-still-operating-its-just-the-beginning.html
  http://www.bbc.co.uk/mundo/noticias/2011/10/111020_tecnologia_duqu_sotware_malicioso_mr.shtml

- Los peligros tras la "nube"

  http://tecnomasciencia.com/red-de-playstation-hackeada/
  http://www.taringa.net/posts/info/10509883/La-verdad-sobre-el-Equot_hackeadoEquot_-de-Sony-y-ataques-a-.html
  http://diario.latercera.com/2011/04/28/01/contenido/tendencias/16-67265-9-expertos-dan-consejos-para-proteger-datos-tras-hackeo-a-red-de-playstation.shtml

- Smartphones, el futuro del malware

http://www.google.es/url?sa=t&rct=j&q=uso%20de%20antivirus%20en%20smartphones%20estadistica%20porcentaje&source=web&cd=2&ved=0CCsQFjAB&url=http%3A%2F%2Fwww.inteco.es%2Ffile%2FBbzXMkVkX8VG7-0ggHlozQ&ei=Yz4_UKvtNoLQ0QWf3YGYBw&usg=AFQjCNEA3ItH5U7zz98Uk1oRDAwIM8DouA
http://www.google.es/url?sa=t&rct=j&q=uso%20de%20antivirus%20en%20smartphones%20estadistica%20porcentaje&source=web&cd=4&ved=0CDUQFjAD&url=http%3A%2F%2Fmuyseguridad.net%2Fwp-content%2Fuploads%2F2011%2F02%2F20110215_INFORME-SEGURIDAD-Y-SMARTPHONES.doc&ei=Yz4_UKvtNoLQ0QWf3YGYBw&usg=AFQjCNFTua-upuM7MakLfwJFqfxufY6JLw
http://www.consumer.es/web/es/tecnologia/software/2012/08/01/211581.php
http://www.soyapps.com/apple-elimina-malware-virus-ruso-app-store-find-and-call-spam/
http://news.softpedia.es/El-malware-de-Android-Loozfon-roba-detalles-de-contactos-de-los-usuarios-femeninos-287963.html
http://www.elandroidelibre.com/2012/05/android-domina-el-59-del-mercado-mundial-de-smartphones.html
http://www.intomobile.com/2012/08/17/android-malware-threats-almost-15000-q2/
http://www.elmundo.es/elmundo/2012/07/11/navegante/1341988668.html
http://www.europapress.es/portaltic/software/seguridad-00646/noticia-malware-android-compra-aplicaciones-permiso-usuarios-20120730162405.html
http://news.softpedia.es/newsImage/Experts-Demonstrate-Security-Holes-in-Android-with-Exploitation-Framework-2.jpg/
http://www.gizmodo.es/2012/08/06/crear-malware-para-android-nunca-fue-tan-facil-gracias-a-afe.html
http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2011.pdf
http://android-so.com/estadisticas-sobre-el-uso-de-smartphones-y-de-android-en-eeuu
http://www.elandroidelibre.com/2012/02/android-y-la-

seguridad-google-responde-con-bouncer.html
http://www.xatakamovil.com/aplicaciones/bouncer-el-servicio-para-combatir-el-malware-en-android-market
http://www.seguridad.unam.mx/noticia/?noti=205

- Malware para MAC OS

http://www.baquia.com/posts/2011-05-25-apple-admite-brecha-de-seguridad-y-lanza-un-antivirus
http://www.dailytech.com/Apple+Admits+Its+Macs+Have+a+Malware+Problem/article24451.htm
http://www.descubreapple.com/apple-modifica-informacion-marketing-admite-vulnerable-cierto-tipo-malware.html
http://www.descubreapple.com/version-desarrolladores-mountain-lion-actualiza-importantes-mejoras-seguridad.html
http://www.descubreapple.com/mountain-lion-fondo-gatekeeper-duplicacion-airplay-game-center-safari.html
http://aprenderinternet.about.com/od/SeguridadPrivacidad/a/Que-Es-Mac-Defender.htm
http://www.ubergizmo.com/2011/05/apple-automatically-remove-mac-defender-malware-next-os-x-update/
http://www.engadget.com/2012/04/10/apple-publishes-support-page-for-flashback-malware-is-working-o/
http://fairerplatform.com/2012/09/mac-malware-flashback/
http://www.viruslist.com/sp/analysis?pubid=207271183

12 REFERENCIAS DE LAS ILUSTRACIONES

- Ilustración 1:
  Gráfico elaborado por el alumno
- Ilustración 2:
  Gráfico elaborado por el alumno
- Ilustración 3:
  Gráfico elaborado por el alumno
- Ilustración 4:
  Gráfico elaborado por el alumno
- Ilustración 5:
  http://www.ionlitio.com/virus-informaticos/
- Ilustración 6:
  http://www.ionlitio.com/virus-informaticos-ii/
- Ilustración 7:
  http://cybercrime.pandasecurity.com/bredolab/how_works.php?lang=es
- Ilustración 8:
  Extraído del documento ¿Qué son y cómo actúan los troyanos bancarios? de INTECO
- Ilustración 9:
  Extraído del documento ¿Qué son y cómo actúan los troyanos bancarios? de INTECO
- Ilustración 10:
  Extraído del documento ¿Qué son y cómo actúan los troyanos bancarios? de INTECO
- Ilustración 11:
  http://www.keylogger-for-windows-7.com/
- Ilustración 12:
  Extraído del documento ¿Qué son y cómo actúan los troyanos bancarios? de INTECO
- Ilustración 13:
  Captura de la web https://www.openbank.es/
- Ilustración 14:
  Extraído del documento ¿Qué son y cómo actúan los troyanos

- Ilustración 28:
  Correo electrónico personal del alumno
- Ilustración 29:
  Correo electrónico personal del alumno
- Ilustración 30:
  http://tecnolatino.com/como-bloquear-sitios-web-en-firefox/
- Ilustración 31:
  http://www.taringa.net/posts/hazlo-tu-mismo/10983745/Bloquear-paginas-web-con-el-HOST_-facil-y-rapido_-_XP-Y-7_.html
- Ilustración 32:
  http://lh3.ggpht.com/_HFWqTWZY0Nc/TQfIDi5lFqI/AAAAAAAAB3s/U5ROvYAPJt0/p1-v3.jpg
- Ilustración 33:
  http://2.bp.blogspot.com/_ZeeLp9OkVRA/S_hEq1scGSI/AAAAAAAAPXk/uNOYY4fyUKA/s1600/reloj-despertador-bomba.jpg
- Ilustración 34:
  http://edwinnajera.wordpress.com/2009/04/30/bombas-logicas/
- Ilustración 35:
  http://ilmaistro.com/cmo-crear-un-virus-que-apague-la-pc/
- Ilustración 36:
  http://ilmaistro.com/cmo-crear-un-virus-que-apague-la-pc/
- Ilustración 37:
  http://www.jprogr.com/2010/11/hoaxes-que-son-y-como-identificarlos.html
- Ilustración 38:
  http://blogs.eset-la.com/laboratorio/category/hoax/
- Ilustración 39:
  http://www.satinfo.es/blog/?p=8958
- Ilustración 40:
  https://www.osi.es/es/actualidad/avisos/2012/01/virus-muestra-un-falso-mensaje-del-cuerpo-nacional-de-policia
- Ilustración 41:
  http://fasterpccleanclean.com/trojan-downloader-xs-removal/
- Ilustración 42:
  http://blog.webroot.com/2012/02/08/researchers-intercept-two-client-side-exploits-serving-malware-campaigns/

- Ilustración 57:
  http://laopiniondelcuco.blogcindario.com/2012/06/00974-eurovegas-el-timo-del-nigeriano.html
- Ilustración 58:
  http://ingenieriasocialsigloxxi.wordpress.com/category/3-como-se-hace-ing-social/3-1-phishing/
- Ilustración 59:
  http://www.thetechherald.com/articles/Facebook-password-scam-circulates-online/8130/
- Ilustración 60:
  http://www.virusno.es/pendrives-o-memorias-usb-libres-de-virus/
- Ilustración 61:
  Extraído del documento ¿Qué son y cómo actúan los troyanos bancarios? de INTECO
- Ilustración 62:
  Extraído del documento ¿Qué son y cómo actúan los troyanos bancarios? de INTECO
- Ilustración 63:
  http://www.elladodelmal.com/2011/09/al-pan-pan-y-al-mulero-mulero.html
- Ilustración 64:
  http://www.dinero20.com/2011/03/17/informe-actualizado-sobre-estafas-y-apuestas-online/
- Ilustración 65:
  Extraído del documento ¿Qué son y cómo actúan los troyanos bancarios? de INTECO
- Ilustración 66:
  Extraído del documento ¿Qué son y cómo actúan los troyanos bancarios? de INTECO
- Ilustración 67:
  Captura de pantalla de https://www.openbank.es/
- Ilustración 68:
  Extraído del documento ¿Qué son y cómo actúan los troyanos bancarios? de INTECO
- Ilustración 69:
  Extraído del documento ¿Qué son y cómo actúan los troyanos bancarios? de INTECO

http://samkear.com/security/refref-latest-denial-service-tool-anonymous

- Ilustración 85: http://samkear.com/security/refref-latest-denial-service-tool-anonymous
- Ilustración 86: http://samkear.com/security/refref-latest-denial-service-tool-anonymous
- Ilustración 87: http://www.auditoriaswireless.net/index.php/topic,2306.0.html
- Ilustración 88: http://samkear.com/security/refref-latest-denial-service-tool-anonymous
- Ilustración 89: http://samkear.com/security/refref-latest-denial-service-tool-anonymous
- Ilustración 90: Extraído del documento "Informe Hacktivismo 2011" de la compañía Arbor Networks
- Ilustración 91: Extraído del documento "Informe Hacktivismo 2011" de la compañía Arbor Networks
- Ilustración 92: http://armannd.com/security-firm-thinks-it-determined-the-identity-of-anonymous-gets-stomped-on.html/
- Ilustración 93: http://reflets.info/sequence-%C2%AB-clownesque-%C2%BB-avec-acslaw-et-hbgary-2/
- Ilustración 94: http://dagblog.com/reader-blogs/hb-gary-federal-anonymous-and-wikileaks-8912
- Ilustración 95: http://www.dailymail.co.uk/sciencetech/article-1354890/Cyber-warfare-breaks-security-firms-threat-expose-pro-WikiLeaks-hackers.html
- Ilustración 96: http://arstechnica.com/tech-policy/2011/02/anonymous-

speaks-the-inside-story-of-the-hbgary-hack/

- Ilustración 97: http://blog.segu-info.com.ar/2011/09/apt-advanced-persistent-threats.html#axzz24qzSNd5Y
- Ilustración 98: http://hackmageddon.com/tag/0-day-vulnerability/
- Ilustración 99: http://investigacion.us.es/investigacion/apoyo/certificados-digitales/comprobar-seguridad
- Ilustración 100: http://securitywatch.pcmag.com/none/283762-who-s-behind-stuxnet-the-americans-the-israelis
- Ilustración 101: http://www.curiosasnoticias.com/eugene-kaspersky-califica-a-stuxnet-como-el-nacimiento-de-un-nuevo-mundo/85561/
- Ilustración 102: http://intentodehacker.wordpress.com/2012/07/19/stuxnet-y-la-ciberguerra-13-2/
- Ilustración 103: http://www.veriluma.com/2010/11/origins-of-stuxnet/
- Ilustración 104: http://securityaffairs.co/wordpress/3716/malware/duqu-cyber-weapons-factory-still-operating-its-just-the-beginning.html
- Ilustración 105: http://eleconomista.com.mx/tecnociencia/2011/04/28/quien-hackeo-playstation-network
- Ilustración 106: http://www.slashgear.com/mcafee-android-malware-problem-getting-worse-now-most-targeted-platform-24174009/
- Ilustración 107: http://www.gadgec.com/find-and-call-trojan-app-store/
- Ilustración 108: http://macdailynews.com/2012/05/24/idc-android-surges-opens-gaping-lead-over-apples-ios-in-global-smartphone-unit-share/
- Ilustración 109: http://www.hellriegel.net/2011/11/07/smartphone-market-

expands-62-of-mobile-users-in-the-u-s-aged-25-34-use-smartphone/

- Ilustración 110: http://straighttalkandroid.blogspot.com.es/2012/08/experts-demonstrate-security-holes-in.html
- Ilustración 111: http://georgedao123.wordpress.com/2012/08/17/more-and-more-viruses-and-malwares-on-android/
- Ilustración 112: http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2011.pdf
- Ilustración 113: http://www.xatakamovil.com/aplicaciones/bouncer-el-servicio-para-combatir-el-malware-en-android-market
- Ilustración 114: http://www.descubreapple.com/apple-modifica-informacion-marketing-admite-vulnerable-cierto-tipo-malware.html
- Ilustración 115: http://www.ubergizmo.com/2011/05/apple-automatically-remove-mac-defender-malware-next-os-x-update/
- Ilustración 116: http://www.ubergizmo.com/2011/05/apple-automatically-remove-mac-defender-malware-next-os-x-update/
- Ilustración 117: http://es.engadget.com/2012/04/11/apple-reconoce-la-existencia-del-malware-flashback-y-promete-una/
- Ilustración 118: http://fairerplatform.com/2012/09/mac-malware-flashback/
- Ilustración 119: http://www.addictivetips.com/mac-os/fix-app-cant-be-opened-because-it-is-from-an-unidentified-developer-error-in-mountain-lion/
- Ilustración 120: http://www.viruslist.com/sp/analysis?pubid=207271183

13 GLOSARIO DE TÉRMINOS

[1]**Black Friday:** día en el que se inaugura la temporada de compras navideñas en USA (con significativas rebajas en muchas tiendas minoristas). Se realiza un día después del Día de Acción de Gracias, el cual se celebra el cuarto jueves del mes de noviembre.
(Fuente: http://es.wikipedia.org/wiki/Viernes_Negro_(compras))

[2] **Técnica del salami:** Técnica basada en la perpetración de robos a pequeña escala sobre un número extraordinariamente alto de víctimas, siendo el robo final una cantidad muy significativa. Esta técnica toma su nombre de la comparación con cortar rebanadas muy finas de una barra de salami sin que se vea significativamente reducido el volumen final del mismo.
(Fuente:
http://dmi.uib.es/~dmiamp/TEGP/Tema%202/Delito%20informatico%20I%20pres.pdf)

[3] **Spyware:** Software basado en la recopilación de todo tipo de información emitida desde un sistema informático y transmitida a un equipo externo sin el consentimiento del usuario legítimo del sistema.
(Fuente: http://www.masadelante.com/faqs/que-es-spyware)

[4] **Keylogger:** Software dedicado al almacenamiento de manera ilícita de toda la información transmitida mediante un teclado físico en un sistema informático. Normalmente, esta información contiene todos los datos escritos por parte del usuario legítimo del sistema, y es almacenada en un fichero o archivo que se envía a una entidad ajena al propietario del sistema informático.
(Fuente: http://www.alegsa.com.ar/Dic/keylogger.php)

[5] **Hacks:** Acciones llevadas a cabo por los hackers.
(Fuente: http://es.wikipedia.org/wiki/Hacker)

[6] **Intranet:** Red privada formada únicamente por usuarios autorizados y de acceso restringido al resto de clientes.
(Fuente: http://www.hosting-peru.net/que_es_intranet.html)

[7] **Crack:** Parche que modifica el comportamiento inicial de un programa software, con el objetivo de poder romper ciertas restricciones impuestas por los fabricantes y desarrolladores, generalmente para poder realizar actividades como la "piratería" y obtener un beneficio económico de las mismas.

n crack informático es un parche cuya finalidad es la de modificar el comportamiento del software original y creado sin autorización del desarrollador del programa. Debido al aumento de la piratería a

(Fuente: http://es.wikipedia.org/wiki/Crack_inform%C3%A1tico)

[8] **Ingeniería inversa:** Proceso de descubrir los principios tecnológicos de un dispositivo, objeto o sistema, a través de razonamiento abductivo de su estructura, función y operación.
(Fuente: http://www.alegsa.com.ar/Dic/ingenieria%20inversa.php)

[9] **Ondas radiales:** Ondas usadas frecuentemente en las comunicaciones, son un tipo de radiación electromagnética.
(Fuente: http://www.ecured.cu/index.php/Ondas_de_radio)

[10] **CopyHackers:** Personas que se valen de la ingeniería social para poder relacionarse y contactar con Hackers, a los que normalmente copian los métodos de ruptura de un sistema para obtener un beneficio económico con su posterior venta.
(Fuente: http://informateca-dothoez.blogspot.com.es/2008/11/hacking.html)

[11] **Cifra negra:** Cuantifica el número de delitos y delincuentes que no han llegado a ser descubiertos o condenados.
(Fuente: http://es.wikipedia.org/wiki/Cifra_negra)

[12] **Dirección IP:** Conjunto de números que sirven como identificador de un dispositivo informático dentro de una red que haya sido configurada con el protocolo IP (Internet Protocol). Un ejemplo de este tipo de redes sería Internet.
(Fuente: http://www.alegsa.com.ar/Dic/direccion%20ip.php)

[13] **Spoofing:** Técnica basada en la suplantación de identidad. Dado que cualquier tecnología de red puede sufrir este tipo de técnica, existen varios subtipos de spoofing, como el IP spoofing, ARP spoofing, etc.

(Fuente: http://es.wikipedia.org/wiki/Spoofing)

[14] **Tablet:** Dispositivo informático que consta de una computadora y una pantalla táctil mediante la cual se pueden realizar tareas similares a las de cualquier smartphone.
(Fuente: http://es.wikipedia.org/wiki/Tableta)

[15] **Redes P2P:** Acrónimo de Peer-to-peer. Red descentralizada que no tiene clientes ni servidores fijos, sino que tiene una serie de nodos que se comportan simultáneamente como clientes y servidores de los demás nodos de la red. Cada nodo puede iniciar, detener o completar una transacción compatible. Contrasta con el modelo cliente-servidor.
(Fuente: http://www.alegsa.com.ar/Dic/p2p.php)

[16] **Ingeniería social:** Técnica que tiene como objetivo obtener información confidencial de un usuario, de tal forma que se puede emplear cualquier tipo de método que permita conseguir dicha información. Generalmente, se utilizan habilidades sociales o técnicas psicológicas para extraer la información a la víctima.
(Fuente:
http://es.wikipedia.org/wiki/Ingenier%C3%ADa_social_(seguridad_inform%C3%A1tica))

[17] **Firewall:** Programa que controla cualquier tipo de movimiento (tanto de entrada como de salida) que se ejecuta en un dispositivo informático. Sirve como filtro para detectar posibles amenazas que puedan estar intentando penetrar en un sistema informático. Su función puede ir desde limitar la conexión a Internet en una empresa a impedir la apertura de determinados archivos susceptibles de contener algún tipo de malware. Se suele ubicar entre una red local e Internet, para controlar el flujo de información entrante y saliente.
(Fuente: http://www.definicion.org/firewall)

[18] **IRC:** Es el acrónimo de Internet Relay Chat. Protocolo de comunicación en tiempo real basado en texto. Su uso principal es conocido coloquialmente como la acción de "chatear", permite el intercambio de mensajes de texto entre uno o varios usuarios, tanto dentro de canales (salones de chat) IRC como de forma privada.
(Fuente: http://www.monografias.com/trabajos87/diccionario-de-informatica/diccionario-de-informatica.shtml)

[19] **FTP:** Es el acrónimo de File Transfer Protocol. Permite a los usuarios copiar archivos entre sistemas remotos en una red IP, y es usado tanto por usuarios como por programas de aplicación. Mediante este protocolo los usuarios pueden mover, copiar, pegar, etc. un determinado archivo de forma remota.
(Fuente: http://www.pergaminovirtual.com.ar/definicion/FTP.html)

[20] **HTTP:** Es el acrónimo de HyperText Transfer Protocol. Protocolo usado para acceder a la Web (WWW). Su función es procesar las peticiones de un cliente y resolverlas para poder visualizar el contenido de una determinada dirección web. Tiene

funciones adicionales como el envío de formularios con mensajes.
(Fuente: http://ciscomodulo1.wikispaces.com/Protocol)

[21] **Script:** Conjunto de instrucciones normalmente recopiladas en un archivo de texto, que deben ser interpretados línea a línea en tiempo real para su ejecución. A diferencia de los programas, deben ser convertidos a un archivo binario ejecutable para ejecutarlos. Los scripts pueden estar embebidos en otro lenguaje para aumentar las funcionalidades de este, como es el caso los scripts PHP o Javascript en código HTML.
(Fuente: http://www.alegsa.com.ar/Dic/script.php)

[22] **Backups:** Copia de seguridad que contiene cualquier tipo de información que el usuario ha considerado que se debe almacenar en un segundo dispositivo. Normalmente se almacenan datos críticos o importantes para una entidad.
(Fuente: http://www.alegsa.com.ar/Dic/backup.php)

[23] **Dropbox:** Servicio de alojamiento de archivos multiplataforma en la nube, operado por la compañía Dropbox. Los usuarios de esta herramienta pueden almacenar y sincronizar archivos en línea y entre computadoras y compartir archivos y carpetas con otros. Dependiendo del tipo de cuenta que el usuario posea (gratuita o de pago) se dispondrán de una serie de servicios u otros.
(Fuente: http://dropbox-informacioon.blogspot.com.es/2012/04/definicion-de-dropbox.html)

[24] **Discos RAID:** RAID es el acrónimo de "Redundant Array of Inexpensive Disks", (conjunto redundante de discos independientes). Es un sistema de almacenamiento, el cual mediante el uso de múltiples discos duros permite distribuir o replicar datos. Existen varias configuraciones, y cada una de ellas aporta una serie de beneficios respecto a un único disco. Así, se puede obtener una mayor integridad, mayor tolerancia a fallos, mayor rendimiento o una mayor capacidad.
(Fuente: http://es.wikipedia.org/wiki/RAID)

[25] **ADSL:** Son las siglas de Asymmetric Digital Subscriber Line (Línea de Abonado Digital Asimétrica). Consiste en una línea digital de alta velocidad, apoyada en el par simétrico de cobre que lleva la línea telefónica convencional o línea de abonado.
(Fuente: http://www.pergaminovirtual.com.ar/definicion/ADSL.html)

[26] **WiFi:** (Wireless Fidelity) Conjunto de estándares para redes inalámbricas basado en las especificaciones IEEE 802.11, creado para redes locales inalámbricas, pero que también se utiliza para

acceso a Internet.
(Fuente: http://www.gsmspain.com/glosario/?palabra=wifi)

[27] **Webmaster:** Persona que maneja un determinado sitio web.
(Fuente: http://www.masadelante.com/faqs/webmaster)

[28] **Dirección MAC:** Es el acrónimo de *Media Access Control address.* Sirve como identificador inequívoco de una tarjeta o interfaz de red. Su longitud es de 48 bits. Es individual, cada dispositivo tiene su propia dirección MAC determinada y configurada por el IEEE (los últimos 24 bits) y el fabricante (los primeros 24 bits).
(Fuente:http://cxo-community.com/articulos/glosario.html?task=list&glossid=150&letter=M)

[29] **Método POST:** El método POST se refiere normalmente a la invocación de procesos que generan datos que serán devueltos como respuesta a la petición. Además se utiliza para aportar datos de entrada a esos programas. En este caso los pares atributo-valor son incluidos en el cuerpo de la petición separados por *ampersand*.
(Fuente: http://www.infor.uva.es/~jvegas/cursos/buendia/pordocente/node15.html)

[30] **Método GET:** El método GET se utiliza para pasar una pequeña cantidad de información al servidor en forma de pares atributo-valor añadidos al final del URI detrás de un símbolo de interrogación, ?.
(Fuente: http://www.infor.uva.es/~jvegas/cursos/buendia/pordocente/node15.html)

[31] **SMTP:** Es el acrónimo de Simple Mail Transfer Protocol. Protocolo que se usa para el envío de correos electrónicos entre diferentes servidores.
(Fuente: http://www.mastermagazine.info/termino/6706.php)

[32] **Dead-line:** Un deadline es una fecha de entrega parcial o total en un proyecto.
(Fuente: http://iaap.wordpress.com/2009/08/10/fecha-de-entrega-deadline/)

[33] **Logs:** Un log es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué un evento ocurre para un dispositivo en particular o aplicación.
(Fuente: http://e-archivo.uc3m.es/bitstream/10016/12011/1/PFC_Jessica_Perez_Sandoval.pdf)

[34] **Open Source:** Cualquier tipo de software cuyos autores permiten la libre distribución del mismo.
(Fuente: http://www.ocitel.net/index.php?option=com_content&view=article&id=51:concepto-de-open-source&catid=38:infosoftware)

[35] **Hacktivismo:** Conjunto de usuarios, normalmente con grandes

capacidades tecnológicas, que mediante el uso de las nuevas tecnologías reivindican el pleno respeto a los derechos fundamentales de los seres humanos como la educación, la seguridad, el derecho a la información, etc.
(Fuente: https://www.underground.org.mx/index.php?topic=23221.0)

[36]**Anonymous:** Surgido en un comienzo como un movimiento por diversión, desde el 2008 Anonymous se manifiesta en acciones de protesta a favor de la libertad de expresión, de la independencia de Internet y en contra de diversas organizaciones, siendo hasta el momento un grupo muy difuso y difícil de identificar dada sus características basadas en el anonimato de sus integrantes y la carencia de organización formal alguna. En sus inicios, los participantes actuaban solamente en Internet, pero con el paso del tiempo, se han ido atribuyendo acciones como diversas manifestaciones a este grupo.
(Fuente: http://es.wikipedia.org/wiki/Anonymous)

[37]**Código ascii:** Código de caracteres basado en el alfabeto latino creado a partir de la evolución de los códigos usados en telegrafía. Utiliza 7 bits para representar cada uno de los caracteres.
(Fuente: http://es.wikipedia.org/wiki/ASCII)

[38]**Benchmark:** Este término se podría traducir como "comparativa" y engloba a las técnicas utilizadas para medir el rendimiento de un sistema o un componente del mismo.
(Fuente: http://es.wikipedia.org/wiki/Benchmark)