DESMONTANDO EL MALWARE

Si bien existen muchas definiciones de malware, quizás una de las más acertadas es esta: "*malware es el término genérico utilizado para referirse a cualquier tipo de software malicioso o molesto que puede instalarse en los sistemas informáticos para llevar a cabo acciones sin el conocimiento del usuario".*

El alcance de esta definición es amplio. De hecho, actualmente el término "malware" sirve para agrupar dentro de un mismo concepto diferentes tipos de "virus informáticos", caballos de Troya y demás software malintencionado que durante muchos años han aparecido y también desaparecido. Si bien anteriormente las funciones de estos tipos de software (y por tanto su denominación) eran mucho más concretas, actualmente estas diferencias son más una herencia del pasado que un método eficaz de clasificación. A pesar de ello se sigue tratando de clasificar cada uno de los diferentes variantes del malware en función de la principal de sus funcionalidades.

A lo largo de este artículo es nuestro propósito profundizar en este concepto. Así, tras una introducción sobre qué es el malware, su objetivo y cómo llega a los equipos, se analizarán en profundidad los diferentes tipos de malware y se presentarán algunos ejemplos de renombre. El objetivo último es dar a conocer a los usuarios las distintas clases de malware para entender su funcionamiento y poder protegerse con mayor eficacia.

I ¿Qué busca el creador de malware?

Las palabras virus, troyano, gusano, etc. suelen asociarse a software con connotaciones negativas. Habitualmente, al cumplir su finalidad, la mayoría de las diferentes variedades de malware terminará provocando un perjuicio al usuario del equipo en que consigue instalarse. En los últimos años, este perjuicio ha estado habitualmente asociado a una motivación económica por parte de los creadores y compradores de malware, aunque existen otras motivaciones.

Una vez se comprenda qué puede interesar de un equipo infectado a un potencial atacante, será más fácil valorar las amenazas y comprender el porqué del funcionamiento de cada una.

Dinero

La económica es una de las principales motivaciones en la creación, difusión y utilización de malware. La obtención de beneficios económicos puede lograrse por diferentes medios, pero algunos se consideran una vía especialmente directa para ello.

Datos de formularios

Un punto desde donde se podrían obtener datos personales de interés son todos los formularios de las webs a las que se suele acceder. Los formularios más deseados por los atacantes son los relativos a compras online, en los que se introducen los datos cuya obtención puede traducirse rápidamente en beneficios económicos, como son por ejemplo los referentes a tarjetas de crédito y las tarjetas de coordenadas en el caso de servicios de banca electrónica.

Envío no consentido de mensajes premium

Con el incremento del uso de dispositivos móviles, se han ideado nuevas formas de sacar provecho a través de su infección. Una forma de obtener un dinero casi inmediato es aprovechar la capacidad de smartphones y tabletas de enviar mensajes de texto. La existencia de números de teléfono destinados a la recepción de mensajes premium[1] posibilita una recolección casi inmediata de los beneficios. De este modo el malware puede forzar que un dispositivo envíe peticiones de suscripción a estos servicios de tarifación especial, siendo el beneficiario de los mismos el atacante en cuestión.

Extorsión

El tercer método de obtención de ganancias económicas directas es la extorsión. A pesar de que habitualmente se ha considerado únicamente el pago de un "rescate" por información sensible que se haya podido sustraer, actualmente el malware posibilita el secuestro de los dispositivos, pudiendo pedirse un rescate para devolver el control del equipo.

Información

El segundo objetivo que se puede perseguir al atacar un equipo es la información que pueda alojar o procesar. Entre otros destacan:

Datos de acceso

Actualmente, el acceso a la mayoría de servicios (música online, redes sociales, etc.) requiere de un nombre de usuario y una contraseña. El malware podría tratar, por tanto, de conseguir a través de estos datos, acceder a información personal sensible, cuentas de correo de conocidos para el envío de correo basura o estadísticas para la personalización de mensajes de correo no solicitados, por mencionar algunos ejemplos.

[1] Números de tarificación especial que ofrecen servicios de notificación y envío de SMS a un precio superior al habitual.

Datos y documentos privados

Aparte de los datos personales específicos, también resulta de gran interés la obtención de documentos que sólo se encuentran disponibles en ciertos círculos cerrados. En este sentido podría incluirse el espionaje industrial, el robo de documentos de ámbito personal, fotografías, mensajes, correos electrónicos, etc.

Control de los recursos de procesamiento del equipo

Manejar al antojo del atacante el equipo infectado puede ser de utilidad para perseguir diversos objetivos, por ejemplo utilizar el equipo para enviar correo basura o atacar a otros sistemas. Más adelante se explicarán de forma más detenida los usos que actualmente se da en mayor medida a un ordenador controlado por un tercero (conocido como sistemas "zombi").

II ¿Cómo se disemina el malware?

Antes de tratar la forma en que los equipos informáticos llegan a ser infectados por malware, es necesario señalar que todo malware, para poder infectar un sistema, necesita no solamente llegar a dicho sistema, sino ser ejecutado. Es decir, una vez en el sistema, el malware necesita que una orden lo ponga en funcionamiento. A pesar de que lo habitual es que el usuario sea quien ejecute el malware, consciente o inconscientemente, no necesariamente es así, ya que existen ciertas formas de ejecución “automática” realizada por otros programas o por el sistema operativo.

Se enumeran a continuación las principales técnicas y vías utilizadas para intentar llegar a sus objetivos.

Dispositivos extraíbles

Todos los soportes – desde los primeros disquetes (cuando estos eran la única vía de comunicación entre los sistemas) hasta las memorias USB actuales – han sido utilizados como medios de propagación de malware.

Tradicionalmente, las posibilidades de infección a la hora de utilizar estos dispositivos de almacenamiento eran superiores a la actualidad, ya que la configuración por defecto de muchos sistemas permitía la ejecución automática de los programas alojados en ellos, contribuyendo así a las infecciones.

Actualmente esta funcionalidad está en desuso, por lo que el malware distribuido a través de dispositivos extraíbles ya no cuenta con la posibilidad de ejecutarse de forma automática en la mayoría de los equipos. Sin embargo, aún puede infectar estos dispositivos, y a través de ellos otros equipos, en caso de que el usuario o algún programa lo autorice, con o sin conocimiento de ello.

Vulnerabilidades

Ningún software, por alto que sea su nivel de madurez, está exento de fallos, situaciones inesperadas, falta de comprobaciones, etc. Estos posibles errores de diseño se conocen como vulnerabilidades.

En algunos casos, estas vulnerabilidades pueden llegar a ser aprovechadas para ejecutar ciertas instrucciones que permitirían a un atacante o malware acceder al sistema. Los ejemplos más habituales son abrir con un lector de archivos PDF un documento especialmente manipulado o utilizar un editor de texto para acceder a un archivo DOC. A pesar de ello, es necesario señalar que no solamente pueden aprovecharse los fallos a través de ficheros, sino que el simple hecho de visitar una página web puede llegar a explotar una vulnerabilidad del navegador.

Al acceder al sistema, los atacantes se encontrarían en una posición privilegiada para introducir cualquier tipo de malware en la máquina afectada. Habitualmente, se intenta atacar equipos cuyo sistema operativo y software se encuentre desactualizado, ya que de este modo los ataques son más efectivos al explotarse vulnerabilidades ya conocidas pero para las que no se han puesto en funcionamiento las soluciones existentes.

Ingeniería social

En una buena parte de las ocasiones, la vía de acceso más utilizada es intentar que el propio usuario introduzca la amenaza en su equipo sin ser consciente de ello. Ya que el dueño de la máquina en ningún caso querrá resultar afectado, se le presentarán aplicaciones con alguna funcionalidad interesante y aspecto inofensivo. Así, se puede intentar infectar mediante el envío de archivos adjuntos al correo, falsas actualizaciones de flash, Java, etc.

Esta forma de ataque se centra en la premisa más actual en seguridad: el componente más débil de los sistemas es el componente humano, por lo que los ataques más simples se llevan a cabo centrándose en ese componente.

III Tipología del malware y sus funcionalidades

En esta sección se presentan las diferentes denominaciones asignadas al malware para describir su objetivo o característica diferenciadora. Se estudiarán tanto los nombres que describen una funcionalidad en concreto, como los que definen una característica o comportamiento.

Antes de presentar las diferentes categorías, hay que señalar que el malware actualmente se encuentra en un estado de evolución en el cual es complejo encajar los diferentes ejemplares dentro de un tipo concreto, ya que suelen contener características compartidas entre varios tipos. Así, se pueden encontrar troyanos con características

víricas, de backdoor, etc. Como apunta Kurt Wismer[2], intentar en 2012 clasificar el malware como "virus", "troyano" o "gusano" es como intentar clasificar a un ser humano como "mamífero", "bípedo" o "vertebrado": lo es todo a la vez e independientemente, según el enfoque que se necesite en cada momento.

En la mayoría de las muestras de malware que son procesadas a diario por las casas antivirus, se suelen presentar simultáneamente varias de las características o funcionalidades existentes. Esto se debe a que los atacantes persiguen crear un software que consiga llevar a cabo su labor de la forma más eficaz y efectiva posible. Por tanto, la frontera que diferencia un tipo de malware de otro puede llegar a ser bastante difusa.

A pesar de ello, se recurre en muchos casos a nombres similares a los que veremos a continuación para determinar la característica más notable de cada muestra o tipo de malware aunque posea varias. En la actualidad no existe ninguna directiva o norma común consensuada sobre cómo asignar las diversas denominaciones al malware o las familias.

Además, no es inusual que cada casa antivirus nombre o clasifique una muestra de una manera completamente diferente a como lo hace cualquier otra, incluso llegando a clasificarla en grupos muy diferentes. En este sentido, el nombre que le dé cada firma ha perdido toda su utilidad para el usuario común.

Ilustración 1: Nombre del mismo malware según diferentes antivirus

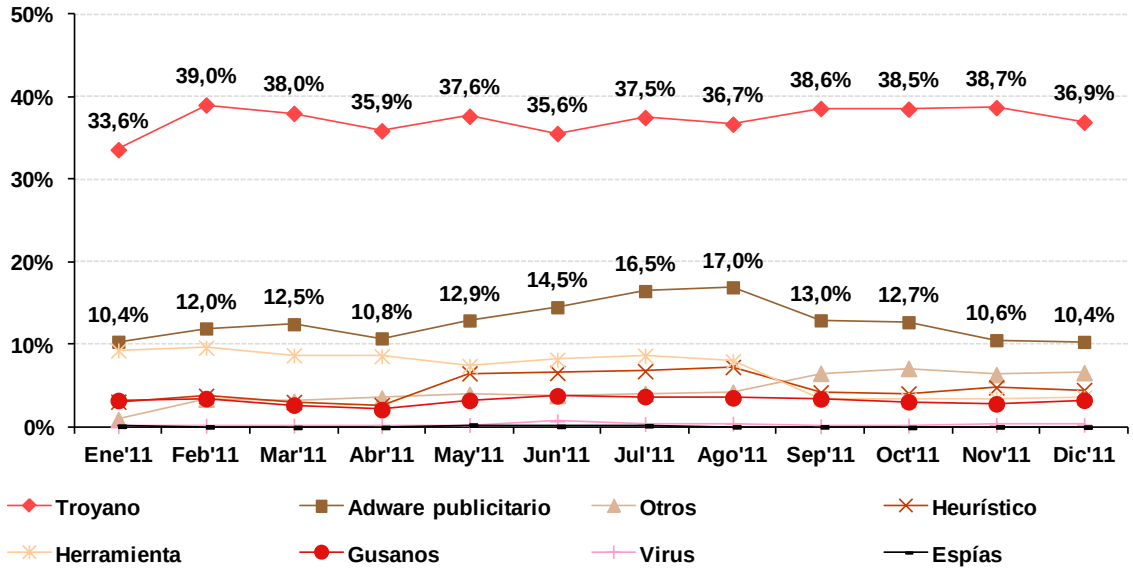
Antivirus	Resultado
AhnLab-V3	Dropper/Win32.Agent
AntiVir	TR/Defmid.azta
Antiy-AVL	Trojan/Win32.Foreign.gen
Avast	Win32:Kryptik-IFQ [Trj]
AVG	Generic27.BHZL
BitDefender	Trojan.Generic.KD.582581
Comodo	UnclassifiedMalware
DrWeb	Trojan.Siggen3.59142
Emsisoft	Trojan.Win32.Reveton!IK
eSafe	Win32.Kryptik.Adhn
F-Secure	Trojan:W32/Reveton.A
Fortinet	W32/Reveton.AF!tr
GData	Trojan.Generic.KD.582581

Fuente: INTECO

[2] www.anti-virus-rants.blogspot.com

Por otro lado, es necesario advertir de la verdadera dimensión que alcanza la propagación del malware, presente en el 45,2% de los equipos a finales de 2011[3].

Ilustración 2: Porcentaje de equipos que alojan malware según tipología, 2011



Fuente: INTECO

Virus

Fue el primer tipo de malware creado, y por tanto este término se ha convertido en una de las formas más comunes de referirse a todos los tipos de malware. Una prueba de lo arraigado del término es que al software destinado a combatir los diferentes tipos de amenazas recibe genéricamente el nombre de "antivirus", a pesar de contar actualmente con muchas otras funcionalidades.

La definición de un programa con un comportamiento considerado "vírico" es simple: cualquier programa cuyo objetivo sea asegurar su propia existencia, replicándose a sí mismo infectando a otros programas. Recibe su nombre por la similitud con los agentes biológicos que únicamente buscan la manera de sobrevivir multiplicándose una y otra vez infectando a los seres vivos con los que entran en contacto.

Una vez infectado un fichero, los virus podrían inutilizar o modificar su comportamiento, pero en los tiempos en los que el comportamiento vírico puro era más popular, habitualmente su principal objetivo era la simple copia de sí mismos a otros ficheros en el disco duro para poder infectar al mayor número de programas posibles. Por tanto, su fin

[3] Fuente: INTECO (2012) *Estudio sobre la seguridad de la información y la e-confianza de los hogares españoles, informe anual 2011 (17ª oleada)*. Disponible en: http://www.inteco.es/Seguridad/Observatorio/Estudios/Estudio_hogares_3C2011

era llegar a tantos sistemas como permitiera su funcionalidad, sin un claro objetivo para el creador más allá de la satisfacción de difundir "su obra".

En la actualidad, sin embargo, es muy poco común encontrar muestras de malware que realmente se comporten como virus "infectando a otros programas". Para replicarse ya no buscan otros programas donde esconderse y ejecutarse, sino que se copian a sí mismos.

Dialers o marcadores telefónicos

Se trata de otro de los primeros tipos de malware que se crearon, aunque actualmente se considera prácticamente desaparecido. La principal causa de su “extinción” se debe a que su funcionamiento se basa en la modificación del comportamiento de los módems, dispositivos de conexión en desuso debido a la implantación de tecnologías superiores.

Se trata de programas maliciosos que alteran el funcionamiento de los módems que se encuentren presentes en el sistema. El objetivo de esta alteración es enviar al módem órdenes para realizar llamadas dirigidas a números de tarificación adicional controlados por los atacantes. De este modo el atacante obtendría grandes ganancias económicas.

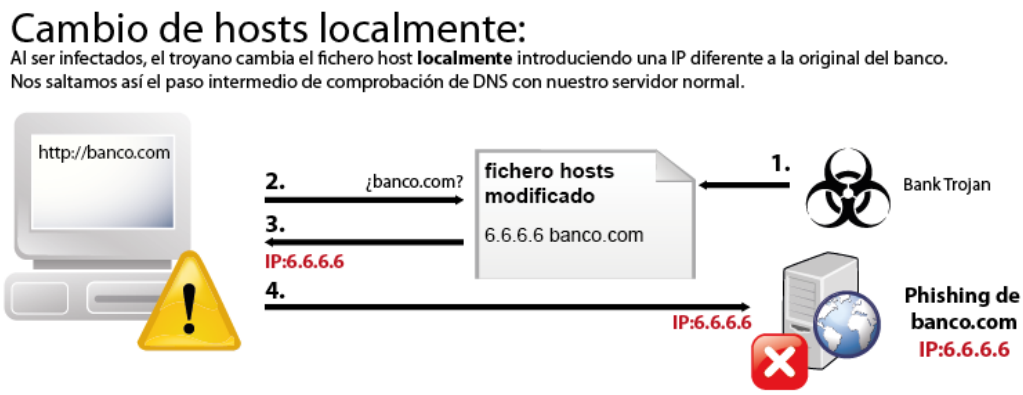
Redireccionadores

Son el tipo de malware cuyo fin es redirigir al usuario a ciertas páginas web, habitualmente páginas que se hacen pasar por otras ya existentes. En estas páginas, la víctima introducirá sus datos personales o su nombre de usuario y contraseña, pensando que se trata de la web legítima. De este modo el atacante podría hacerse con los datos de acceso a diferentes servicios, especialmente servicios bancarios y de comercio electrónico. Estas redirecciones se llevan a cabo esencialmente de dos maneras, modificando el archivo “hosts” de un equipo o sus servidores DNS.

Los ordenadores, para poder conectarse a una página web, necesitan conocer la dirección numérica (IP) de los dominios que se visitan (servidores). De esta manera el navegador sabe a qué servidor acudir. Los sistemas informáticos tienen básicamente dos maneras de realizar esta asociación: un fichero en el sistema llamado "hosts" (en el que se establece esta relación de forma manual y permanente) y los servidores DNS configurados en el sistema operativo (que normalmente proporciona el proveedor de conexión). Así, el malware redireccionador puede actuar de dos formas:

- Modificando el archivo hosts: Este método es común en el malware latinoamericano. El malware modifica el fichero hosts para que los dominios que interesan acudan a otra página creada en realidad por el navegador. Cuando la víctima introduzca la dirección de su banco en el navegador, acudirá a una dirección IP previamente modificada en el archivo hosts por el malware, y donde se aloja una web parecida a la que la víctima espera encontrar.

Ilustración 3: Esquema de funcionamiento de un malware que modifica el archivo hosts



Fuente: INTECO

- Modificando los DNS: En este caso, el malware modifica los servidores DNS del sistema operativo. Estos servidores DNS son controlados por el atacante, y puede hacer que la víctima sea redirigida a cualquier página web cuando introduce una dirección en su navegador. Este tipo de malware suele ser llamado DNSChanger[4], y ha alcanzado cierta relevancia en 2012, ya que el FBI tomó el control de los servidores DNS de algunas variantes y los apagaron el día 9 de julio de 2012.

Gusanos

Al igual que los virus, se caracterizan por su objetivo de replicarse a sí mismos. La diferencia entre ambos radica en la forma de reproducirse, ya que en este caso su objetivo no es infectar o afectar a otros programas, sino replicarse haciendo copias de sí mismos de forma automática. Su aparición también es de las primeras en el mundo del malware, dando lugar a especímenes bastante conocidos, como "Sasser", "Blaster" o "I Love You".

Sus objetivos primigenios solían ser la simple replicación y ralentización de sistemas. Hoy en día se trata más bien de una técnica de propagación que utilizan el malware y que busca en realidad otros fines una vez infectado el sistema. Los gusanos, o las técnicas de gusano en malware, son todavía habituales. Se considera que el malware utiliza características de gusano cuando se copian a sí mismos dentro de las memorias USB y también cuando busca en la red nuevos equipos a los que infectar a través de algún servicio, por ejemplo entre las carpetas compartidas.

[4] http://cert.inteco.es/Actualidad/Actualidad_Virus/DNSChanger/

Troyanos

Se conoce como caballos de Troya o simplemente troyanos a los programas que, presentándose a la víctima como legítimos, esconden una funcionalidad oculta, principalmente con fines maliciosos. En la actualidad es el tipo de malware al que más recurren los atacantes a la hora de buscar nuevas infecciones.

Su nombre se debe a la similitud en su comportamiento con el caballo de madera utilizado en la guerra de Troya para ocultar soldados y que las propias víctimas los introdujeran en la ciudad que más tarde tomarían. Del mismo modo, los troyanos inicialmente son aparentemente inofensivos y se les permite acceder al sistema, para posteriormente poder llevar a cabo su objetivo.

La finalidad del programa escondido habitualmente solía ser la de controlar totalmente el equipo, quedándose en modo residente en él, es decir, manteniéndose en funcionamiento constante, y siendo capaz de recibir órdenes del exterior. Así pues, se decía que el equipo se encontraba "troyanizado", de modo que el término "troyano" se refería tanto a la forma en la que se presentaba el malware, como a su funcionalidad.

En la actualidad, se le llama troyano a todo software que, sin advertir a la víctima, es capaz de recibir o enviar órdenes a un tercero y ejercer control sobre el sistema infectado, independientemente de cómo se presente a la víctima y cómo ésta sea infectada. Este comportamiento es muy utilizado en el malware actual.

Entre ellos, según su funcionalidad, se pueden diferenciar varios tipos, por ejemplo:

- **Downloader**: El troyano downloader es un "paso intermedio" entre una primera infección y una segunda. Descarga ficheros de Internet, principalmente archivos de configuración y nuevas versiones del troyano, que permiten seguir teniendo el control del equipo al tiempo que intenta pasar desapercibido. Puede tratarse de una funcionalidad de una primera etapa de un malware, o un malware en sí especializado en esta técnica.

- **Bancario**: Los troyanos bancarios se orientan al robo de credenciales, recurriendo a infinidad de funcionalidades para obtener datos de clientes de bancos.

- **Backdoor**: Funcionalidad utilizada para que el atacante pueda acceder de forma remota al dispositivo infectado. En el siguiente punto se explica con más detenimiento este tipo de funcionalidad debido a su importancia. Suele encontrarse en combinación con las anteriores.

Backdoors (o puertas traseras)

Pese a considerarse un tipo de troyano, o de funcionalidad de ellos por ser este el grupo en que más se presenta, esta funcionalidad está ampliamente extendida debido al gran abanico de posibilidades que ofrece.

Significa "puerta trasera", y su objetivo es permitir al atacante controlar el sistema infectado a través de una vía de acceso y control que se encuentra oculta para el usuario legítimo del equipo. A partir de aquí el controlador remoto puede realizar cualquier acción sobre el equipo (siempre que disponga de los permisos adecuados), desde instalar un "Keylogger" hasta mandar instrucciones para atacar otros ordenadores o enviar correos basura. En estas posibilidades de acción se pone de manifiesto la importancia de utilizar de forma habitual un perfil de usuario con permisos reducidos, en lugar de un perfil de administrador.

La existencia de un "backdoor", deja la máquina bajo el control del atacante. Este estado del equipo es comúnmente conocido como "zombi" o "bots", y desde el momento en el que se infecta puede pasar a formar parte de de las llamadas "botnets" o red de "zombis". Estas redes pueden ser utilizadas con diversos fines, y no siempre en perjuicio del propio infectado. En ocasiones el atacante que controla la botnet puede usar la máquina para el beneficio propio o en perjuicio de un tercero, siendo los daños al usuario infectado "efectos colaterales".

En los casos de redes "zombi", los sistemas infectados (bots) son manipulados por el atacante de una manera más automatizada, desde un panel, mientras que en el backdoor puro, la manipulación puede ser más "artesanal" y personalizada. La principal diferencia entre estas dos formas radica en si el control y manipulación del equipo se realiza de forma agregada dentro de toda una red de equipos infectados, o si se realiza individualmente, controlando ese único equipo.

Los principales ejemplos de uso de estas redes son:

- **Ataques DDoS** (Denegación de Servicio Distribuida por sus siglas en inglés): Se trata de ataques realizados por gran cantidad de máquinas con el fin de saturar al equipo atacado (normalmente un servidor web). El objetivo es generar desde los equipos infectados una gran cantidad de tráfico y solicitudes de acceso a información de la máquina víctima, llegando al punto en que ésta no sea capaz de satisfacer todas las peticiones y, por lo tanto, se produzca una denegación de acceso a los usuarios legítimos de los servicios. De este modo se utilizan los equipos infectados para que un determinado servicio web (una página, un servidor, etc.) no esté disponible para ningún usuario. En este caso se abusa del ancho de banda de la conexión que utilizan los equipos infectados.

- **Generación de bitcoins**[5]: Se pueden aprovechar todas las máquinas infectadas para generar este tipo de monedas, ya que esta labor requiere una gran capacidad de cómputo. Estas monedas podrán ser intercambiadas posteriormente por otras divisas. El equipo infectado ve mermada su capacidad de cómputo (o más bien la capacidad a disposición de su legítimo usuario) ya que es utilizada por el atacante.

- **Spam**: Los equipos infectados también se pueden utilizar para el envío de correos electrónicos no deseados. Este uso se debe a que el hecho de que el origen del correo basura se encuentre repartido entre diversas localizaciones dificulta en gran medida el bloqueo de todas ellas, además de proteger así la estructura central de control.

- **Alojar otras muestras de malware**: Los equipos infectados se pueden usar también como repositorio de nuevas muestras de malware que serán descargadas por otras víctimas. También pueden utilizarse como servidores donde alojar páginas de phishing, spam online, contenidos ilícitos, etc.

Adware (o software publicitario)

Se trata de un tipo de software destinado a generar un beneficio económico directo a su creador o comprador[6] a través de la publicidad no deseada e intrusiva. Su funcionamiento se basa en mostrar publicidad esperando que el usuario acceda a las páginas webs anunciadas.

Existen otras variedades de "adware" que en lugar de mostrar anuncios, realizan un trabajo más discreto, como es el caso de los llamados "clickers". Su objetivo es pulsar de forma automática (y inadvertida para la víctima) sobre ciertos anuncios de publicidad para generar así beneficios para el anunciante. Esto les permite eludir los controles de las compañías de publicidad, que penalizan las pulsaciones sobre anuncios que parezcan provenir de sistemas automatizados. Con una gran cantidad de usuarios infectados con estos "clickers" se puede conseguir que las visitas a la publicidad, aunque automatizada, provenga de diferentes equipos y con una cadencia más "aleatoria", simulando el comportamiento "normal" del usuario.

También existe "adware" que modifica los anuncios aparecidos en el navegador anteponiéndose a los legítimos.

[5] Bitcoin: Moneda electrónica cuya confianza no depende de ningún emisor central. La obtención de las divisas requiere la solución de problemas matemáticos de alta complejidad computacional, de ahí el interés por utilizar la capacidad de procesamiento de una botnet. Sitio oficial: http://bitcoin.org/

[6] En los últimos años se está extendiendo la práctica por la que el programador de cualquier tipo de malware no es el mismo que finalmente obtiene el beneficio resultante de las infecciones. Los programadores de las diferentes amenazas venden su producto para ser utilizado por otras personas.

Spyware (o software espía)

Se incluye en esta categoría el malware cuya función es recolectar información de la máquina infectada, monitorizando sus movimientos. Por ello son también conocidos como s*tealers* (en inglés, ladrones).

Entre los datos de interés que se encarga de recolectar se encuentran las credenciales almacenadas en el equipo (en el navegador o archivos de configuración), claves privadas, datos de tarjetas de crédito, etc.

También se puede recopilar otro tipo de información, con un beneficio menos directo, como son los hábitos de navegación de internet, útiles para conocer gustos, últimas tendencias, etc. y así poder presentar una publicidad más atractiva para los infectados (estas técnicas también suelen ser utilizadas por ciertas páginas con cookies de rastreo).En este punto en el que se llega a alterar el comportamiento del navegador, es donde la diferencia entre "adware" y "spyware" empieza a difuminarse. En todo caso podría considerarse que es "adware" que incluye características de "spyware".

Keyloggers (o capturadores de pulsaciones)

Se trata del software malicioso que registra todas las pulsaciones de teclas realizadas en la máquina infectada. Podría considerarse un tipo de spyware, pero actualmente suele incluirse dentro de los troyanos bancarios. Su principal fin es el obtener claves y cuentas de usuarios. La recopilación de todo el contenido tecleado suele ser enviada a través de internet a servidores controlados por el atacante. Para evitar este tipo de malware, los bancos suelen poner a disposición de sus clientes unos teclados virtuales, evitando así que las credenciales de los clientes puedan ser obtenidas.

Ilustración 4: Teclado virtual de una entidad bancaria

Fuente: INTECO

En este sentido, el malware ha evolucionado de forma que es capaz de capturar pequeñas imágenes de las pulsaciones en pantalla o grabaciones en vídeo del teclado virtual.

Además de poder utilizarse programas o malware para registrar las pulsaciones de teclado, también existen dispositivos físicos o hardware capaces de realizar estas funciones.

Rootkit

Este caso, más que un tipo de software malicioso, se puede considerar una característica presente en otros tipos de malware. El término "rootkit" se emplea para referirse a un conjunto de herramientas (kit) que tienen como objetivo que un atacante pueda conseguir y mantener acceso con los máximos privilegios o permisos de actuación (root), intentando pasar desapercibido para cualquier usuario del sistema.

Hasta este punto, la definición de "rootkit" se asemeja a la de un "backdoor", sin embargo, se incluye otra característica básica que los diferencia: se centran en una ocultación mucho más compleja. Modifican en mayor medida las raíces del sistema, y esto les permite permanecer ocultos ante el sistema y las soluciones de seguridad que se ejecuten en él. A efectos prácticos, las técnicas de "rootkit" suelen ser utilizadas para evitar o dificultar que tanto los antivirus como los usuarios o analistas los detecten.

Bomba lógica

Se trata de una funcionalidad incluida en diferentes tipos de malware que permite que un código o programa se ejecute cuando se cumplen ciertas condiciones pre-establecidas. De este modo, el malware constaría de dos partes: una carga útil y un disparador. La llamada carga útil es el código que se ejecutará, "lo que ocurrirá" cuando se den las condiciones para las cuales está preparada la bomba lógica, pudiendo ser un virus, un troyano, etc. El disparador es el código que se encarga de comprobar si se dan las condiciones idóneas o necesarias para lanzar su contenido.

Ransomware

Se trata de una variedad de malware aparecida en la década de los 90, pero que ha tenido su mayor auge en los últimos años. Como otros tipos de malware, busca un beneficio económico directo, en este caso recurriendo al chantaje a los usuarios del dispositivo infectado.

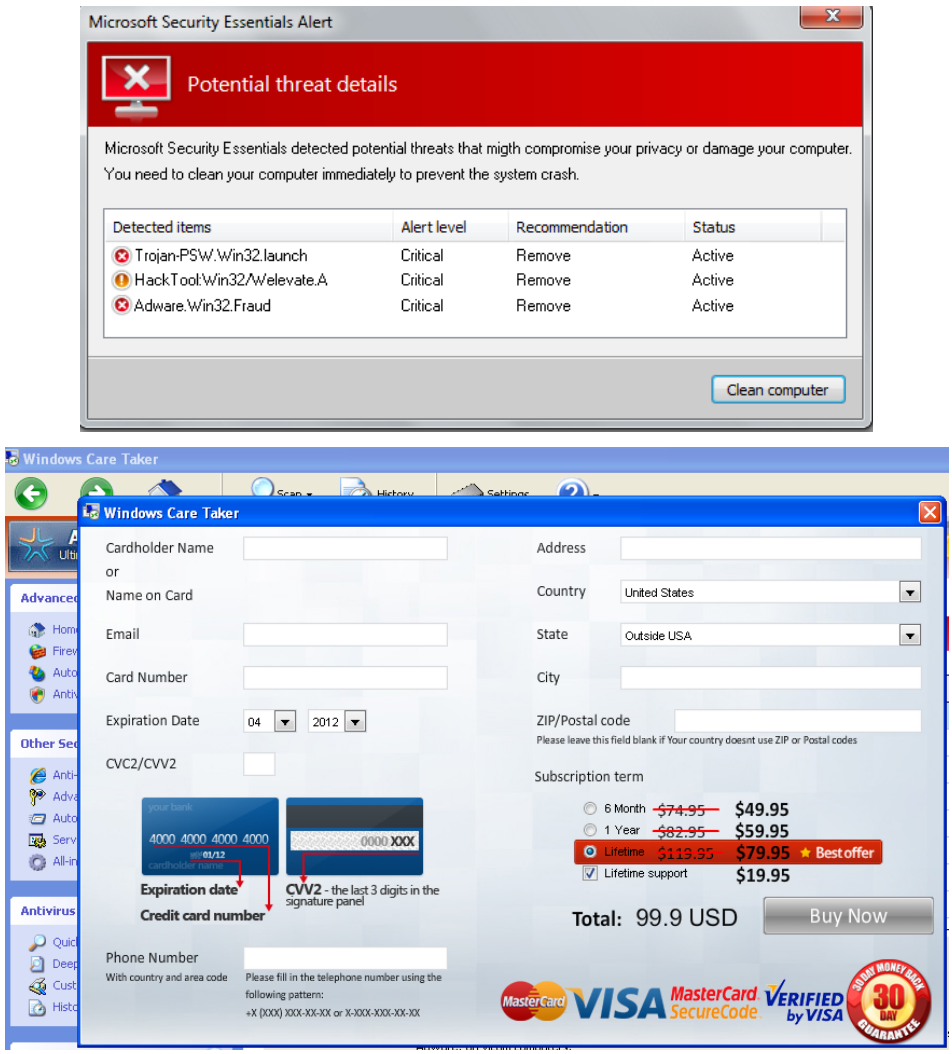
Al contrario que en la gran mayoría del malware, en este caso es necesario que el usuario sea consciente de la existencia de un comportamiento anómalo, que será utilizado para la coacción al plantearse el pago como única solución a ese comportamiento. Para aumentar su efectividad, se suele recurrir al bloqueo de cualquier tipo de acceso e interacción con el equipo (programas, archivos, administrador de tareas, etc.) que no sea estrictamente necesario para el envío del dinero.

Algunos de los casos más conocidos cifran los datos de interés para el usuario (documentos y fotografías) y piden el pago una cantidad económica para obtener la clave que era capaz de descifrar los archivos del usuario. En la gran mayoría de los casos, tras el pago no se obtiene el control de la máquina ni de los archivos cifrados.

Rogueware o Scareware

Este malware puede considerarse una variante del "ransomware". Suele presentarse en forma de antivirus, aunque realmente se trata de un falso antivirus. Su método para causar alarma en la víctima es informar sobre la presencia de diversos tipos de malware en el dispositivo tras simular haber realizado un escaneo del equipo. El "rogueware" se ofrece entonces a desinfectar la máquina, intentando descreditar así a la actual solución antivirus. Su único objetivo una vez instalado en la máquina del usuario es requerir la activación del supuesto producto a través de diversas formas de pago.

Ilustración 5: Ejemplos de antivirus falsos "Scareware"



Fuente: INTECO

IV Familias de malware destacadas

A pesar de la gran variedad de malware existente, ciertos ejemplares y familias han alcanzado una gran popularidad, ya sea por tener una gran incidencia o por su efectividad. A continuación se destacan algunos de los casos más reseñables.

Zeus y SpyEye

Se trata de los dos kits comerciales de troyanos que han destacado por su éxito tanto en infecciones como en adquisición de datos y ventas. El primero en conocerse, en 2006, fue Zeus (también conocido como Zbot) y más tarde SpyEye.

Estos kits no precisan de altos conocimientos en programación por parte de los compradores que deseen ponerlos en funcionamiento. Los kits son adquiridos previo pago y requieren de la posesión de una clave que sólo podrá ser utilizada en un único ordenador, evitando así que puedan ser usados sin el control del vendedor. El atacante podrá crear con el kit tantos troyanos bancarios como desee y con las características que necesite.

Con respecto a sus funcionalidades, se enumeran algunas de ellas:

- Afectan a la mayoría de navegadores más utilizados (Internet Explorer, Mozilla Firefox, Opera y Chrome entre otros), detectando la visita a entidades bancarias objetivo y modificando su web para requerir los datos que interesan al atacante.
- Se han creado variantes capaces de infectar teléfonos móviles y conseguir así acceso a los SMS con las claves enviadas por algunas entidades bancarias para el acceso a la banca electrónica.
- Permiten inyectar código HTML en el navegador. Esto significa que se consiguen modificar las páginas web que se deseen para, por ejemplo:
    - Pedir datos que serán enviados a los atacantes.
    - Ocultar los movimientos sospechosos en las cuentas de los afectados.
- Incluyen técnicas sofisticadas que dificultan su análisis (en general es una características bastante común en el malware).
- Incluyen funcionalidades de "keylogger", "rootkit" y “clicker”.
- Toma de capturas de pantalla. Útil cuando se utilizan teclados en pantalla.
- Cuentan con soporte para plugins o extensiones que permiten ampliar aún más sus funcionalidades.

- En su compra se incluye soporte técnico y actualizaciones.
- Permiten la automatización del uso de datos robados de tarjetas para "comprar" software del propio atacante. Este es un método para conseguir estafar a los usuarios con estas compras e incluso usado para "blanquear" dinero.

Ransomware en nombre de la Policía

Una de las maneras de "chantajear" a las potenciales víctimas de un fraude que más éxito ha obtenido en los últimos tiempos, es el caso del "virus de la policía". Este malware es una gran familia que ha evolucionado desde mediados de 2011, con diferentes funcionalidades, métodos y mejoras. En este caso se recurre a la imagen del Cuerpo Nacional de Policía para intentar dar una mayor credibilidad a la estafa. Tras infectar el equipo de la víctima, se presenta una imagen que impide el uso del ordenador, ocultando la barra de herramientas y el escritorio, ocupando toda la pantalla. Esta aplicación añade además varias protecciones para evitar que la persona infectada lo elimine, como la invalidación del arranque en modo seguro.

Ilustración 6: Pantalla de un ordenador infectado con ransomware

Fuente: INTECO

En la imagen presentada a la víctima se muestra el nombre y la imagen de la policía española acusándole de supuestos delitos como envío de correo basura y tenencia de

material considerado ilegal según la legislación. La presentación de datos personales de la máquina como el sistema operativo y navegador que utiliza, dirección IP, país, etc. intenta amedrentar a al víctima para que realice el pago de la supuesta multa impuesta. En la misma pantalla presentada se indicaba el método de pago de la multa con el fin de desbloquear el equipo. En las últimas versiones también se cifran los archivos del usuario. El éxito de este malware, desde noviembre de 2011, está siendo muy notable.

Stuxnet, Duqu y TheFlame

En los últimos dos años se han detectado tres muestras de malware muy concretas, clasificadas como "ciber-armas". El objetivo en estos casos no es robar dinero, enviar correo basura o acceder a datos personales, sino el controlar o espiar en entornos industriales muy específicos. Stuxnet, por ejemplo, estaba dirigido al espionaje industrial y sabotaje en instalaciones nucleares iraníes.

Se diferencian del malware común en su dispersión, ya que no intentan llegar al mayor número de equipos posible de forma indiscriminada, sino que pretenden quedarse durante el mayor tiempo posible dentro de un entorno del que pretenden obtener información.

También se diferencia en que se trata de un software especialmente creado "a medida", invirtiendo una gran cantidad de recursos como evidencian, por ejemplo, el uso de certificados válidos robados y de vulnerabilidades desconocidas. El alto grado de sofisticación y los recursos que se estima han sido necesarios para su desarrollo, han llevado a pensar que una gran organización se encuentra detrás de su creación.

En el caso de Stuxnet, se hacía uso de cuatro vulnerabilidades "0-day" en Windows (es decir, desconocidas incluso para el fabricante por lo que no existían parches que las solventasen), para poder pasar de un ordenador a otro. El caso de TheFlame, el más complejo descubierto hasta la fecha, es especialmente relevante, ya que consiguió mantenerse oculto durante al menos cinco años gracias a que se encontraba firmado por Microsoft. Si bien Microsoft no fue el responsable, los atacantes consiguieron, gracias a una cadena de errores de la compañía, firmar un software como si se tratara de Microsoft y pasar así desapercibido todo ese tiempo.