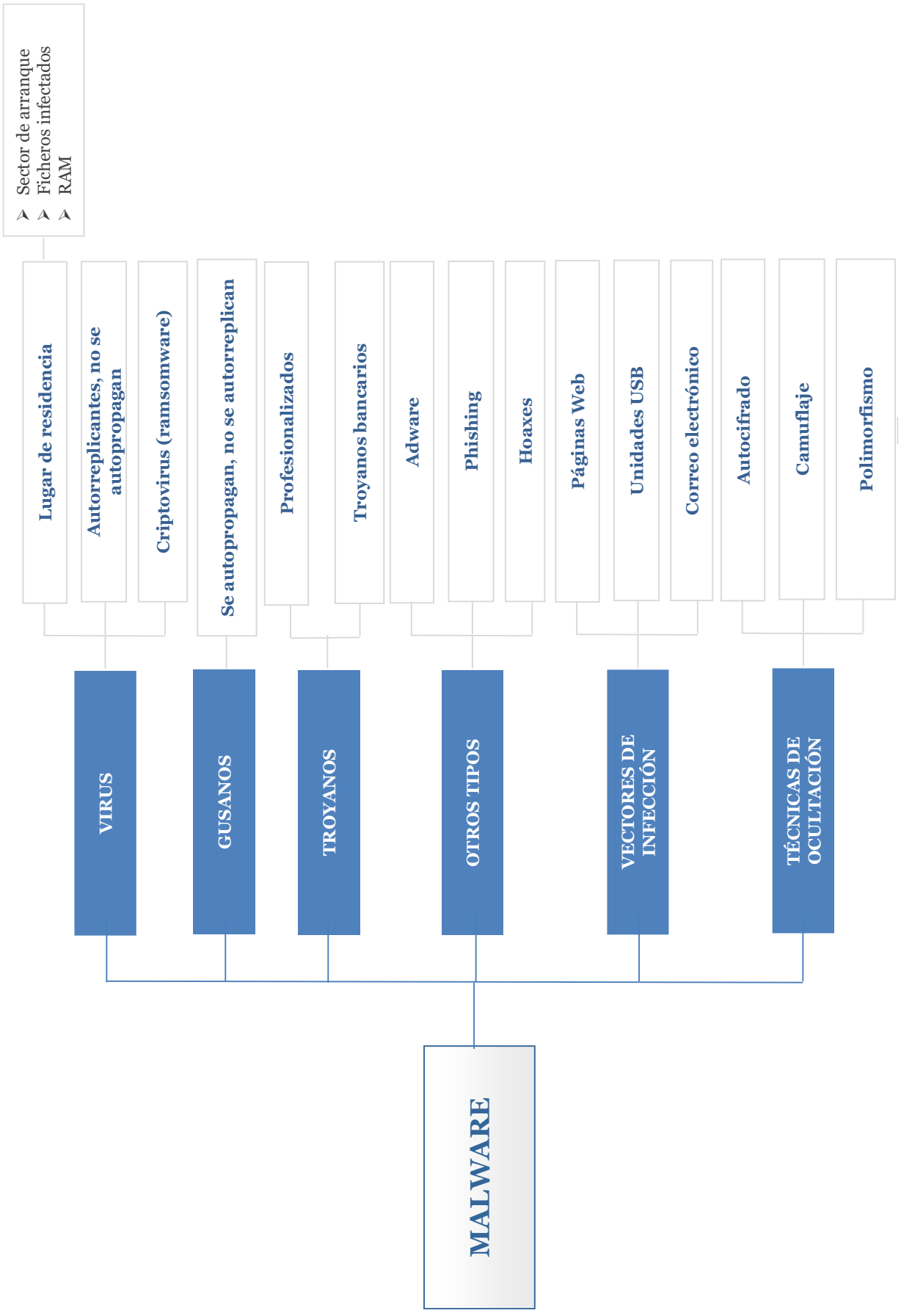
Malware y código malicioso

TEMA 11

Esquema


MALWARE
VIRUS
GUSANOS
TROYANOS
OTROS TIPOS
VECTORES DE INFECCIÓN
TÉCNICAS DE OCULTACIÓN
Lugar de residencia
Autorreplicantes, no se autopropagan
Criptovirus (ramsomware)
Se autopropagan, no se autorreplican
Profesionalizados
Troyanos bancarios
Adware
Phishing
Hoaxes
Páginas Web
Unidades USB
Correo electrónico
Autocifrado
Camuflaje
Polimorfismo
Sector de arranque
Ficheros infectados
RAM

Ideas clave

11.1. ¿Cómo estudiar este tema?

El estudio de este tema se realiza a través de los contenidos desarrollados en las **Ideas clave** expuestas a continuación.

En este tema realizaremos un viaje por la **historia de una de las principales amenazas actuales a cualquier sistema de información: el software malicioso o *malware***. Tan antiguo como la propia informática, sus inicios fueron casi inocentes; hoy, están lejos de eso, y se han profesionalizado en busca de todo tipo de credenciales, información que pueda usarse para extorsionar posteriormente a los usuarios y un largo etcétera.

Como siempre, comencemos por definir con precisión de qué estamos hablando, sus objetivos y algunos números sobre su exponencial crecimiento en los últimos años. Expondremos a continuación los principales tipos de malware existentes, clasificándolos en función a algunos parámetros como capacidad de propagación o autorreplicación.

Haremos hincapié en el caso de los troyanos de última generación, especialmente aquellos destinados a robar credenciales de autenticación. Analizaremos, además, la «economía» del *malware*, es decir, las motivaciones para escribir este tipo de malware, cómo se roba el dinero o cómo, incluso, se paga por ellos.

Finalmente, acabaremos el tema estudiando las **posibles soluciones y una serie de contramedidas efectivas para evitar ser víctima de este tipo de *malware***.

11.2. ¿Qué es el malware?

Mostrar la importancia de este tema al alumno, es muy sencillo: *phising*, el principal malware, ¿porqué?, cada persona es atacada por este tipo de malware múltiples veces a lo largo de un solo día, solo se debe consultar la papelera de correo no deseado, para ver el alcance de este tipo de malware.

Su finalidad es la obtención de las claves necesarias para acceder a datos personales, banca electrónica, obtención de claves de identificación, acceso a los datos privados de la víctima y finalmente trasferir y monetizar el importe económico defraudado. En este tema se engloba el proceso completo bajo el término ciclo del *Phishing*. A partir de aquí, concienciar al alumno con el resto del tema, es una tarea sencilla. Comencemos.

El *malware* es, sin duda, una de las amenazas más conocidas y peligrosas que pueden encontrarse en Internet. Por malware se entiende **«cualquier programa escrito con intenciones maliciosas»**, entre las que pueden encontrarse:

- **Robar credenciales de autenticación:** en los últimos años se ha convertido en el uso más común de todo tipo de malware. Estas credenciales pueden incluir contraseñas para multitud de aplicaciones o servicios, como banca online, sitios de subastas o plataformas de pago como eBay y PayPal, o servicios de mensajería instantánea como Microsoft Messenger, AOL y otros.
- **Mostrar publicidad no solicitada:** todo el mundo ha sufrido, con seguridad, este molesto tipo de malware, que se ha dado en llamar adware. Su misión es mostrar publicidad no solicitada ni autorizada durante la navegación del usuario, habitualmente a través de los molestos pop-ups, o ventanas emergentes.
- **Estudiar los hábitos de navegación:** estos programas, conocidos como spyware, se instalan y funcionan habitualmente sin que el usuario los advierta, recolectando información sobre los hábitos de navegación del usuario. Esta acción, que puede parecer inofensiva a primera vista, puede producir enormes beneficios a ciertas empresas, que llegan a pagar importantes cantidades de dinero por esos datos, que posteriormente se utilizan para personalizar la publicidad que el usuario recibe.
- **Secuestrar información:** un curioso tipo de malware, que se han denominado criptovirus, buscan y «secuestran» ciertos ficheros del disco duro, como archivos Word, de texto, hojas de cálculo, etc…, con la esperanza de que contengan información valiosa para el usuario y éste esté dispuesto a pagar dinero para recuperar los ficheros.

Algunos números

Para comprender en su totalidad la magnitud del problema que supone el malware en Internet, nada mejor que dar una serie de datos que lo ilustren. El más significativo quizás sea el espectacular incremento anual que ha sufrido la producción de este tipo de programas en los últimos años. Las cifras varían mucho entre diferentes estudios, pero una cifra conservadora podría rondar los 100.000 nuevos especímenes, ¡diariamente!

Muchos de ellos, es cierto, se generan de forma automática, o son meras variantes de otros especímenes existentes. De ellos, más del 90% son del tipo troyanos, cuyas características analizaremos a continuación. Algo menos del 5% son virus y el resto de amenazas, como gusanos, spyware, etc..., suman el 3,5% restante.

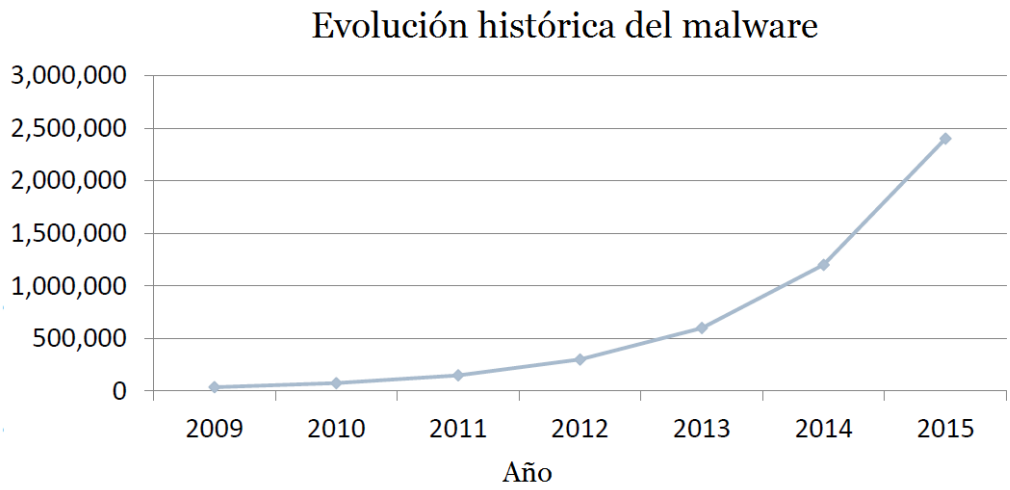


Figura 1. Evolución histórica y proyección futura del volumen del malware, en número de especímenes descubiertos anualmente. Fuente: Frost & Sullivan

Otro dato importante hace referencia a un cambio drástico de tendencia en el tipo de malware que se ha producido en los últimos años. De hecho, el 90% actual, perteneciente a troyanos, estaba constituido hace unos años por malware de tipo virus.
Sin embargo, la reciente profesionalización del cibercrimen, que ha permitido la entrada en escena de las mafias tradicionales, ha invertido claramente esta tendencia, sacando del olvido a los troyanos. La razón de este cambio es que un troyano, por sus características es el vehículo perfecto para realizar fraude en Internet. Tanto es así, que en la actualidad el 69% de los troyanos están diseñados para, específicamente, robar credenciales bancarias.

¿Quién escribe el malware?

Como hemos comentado, el cibercrimen está liderado hoy en día por grupos organizados de delincuentes, apoyados por las mafias tradicionales. Hace años que el *hacking* ha perdido su componente nostálgico y lejos quedaron los tiempos en que los escritores de virus únicamente pretendían demostrar sus conocimientos.

En la actualidad, la motivación principal de este tipo de personas es, cómo no, ganar dinero. Y realmente se trata de mucho dinero, pues las cifras de fraude no dejan de subir año a año y alcanzan ya los varios billones de dólares anuales en todo el mundo.

Sin embargo, existen también otras motivaciones algo más exóticas. Por ejemplo, se sabe que el gobierno chino tiene «en nómina» a un grupo de hackers, expertos informáticos, para que, entre otras tareas, encuentren vulnerabilidades en productos de Microsoft, utilizados por un porcentaje altísimo de usuarios en todo el mundo. De esta forma, las autoridades chinas quieren poder desarrollar troyanos u otro tipo de malware, del que pudieran hacer uso en caso de un hipotético conflicto con otra nación.

11.3. Tipos de malware

Aunque la clasificación de este tipo de programas puede hacerse en base a muchos criterios, vamos a realizar una primera taxonomía **en función de la capacidad de propagación del malware**. Según este criterio, podemos distinguir **tres grandes grupos**:

- **Virus:** fueron los primeros en aparecer y su característica más común es que no tienen capacidad de autopropagación. Es decir, no pueden infectar máquinas por sí mismos, sino que deben esperar a que el propio usuario los ejecute o actúe de vehículo de transmisión. Su nombre no podría ser más adecuado, pues su analogía con los virus biológicos es evidente.
- **Gusanos:** a diferencia de los virus, sí tienen capacidad de propagación. Por tanto, pueden infectar otras máquinas por sí mismos, habitualmente a través de la red en la que la máquina huésped está conectada.
- **Troyanos:** habitualmente no tienen capacidad de autorreplicación. Deben, por tanto, utilizar a los usuarios para poder propagarse. Sin embargo, a diferencia de los virus, que suelen tratar de ocultar su presencia, los troyanos utilizan una estrategia diferente: dicen ser programas benignos, como un juego, un salvapantallas o, incluso un antivirus, cuando, en realidad, tienen otras intenciones.

Por supuesto, existen muchísimos tipos más de malware, pero la gran mayoría puede englobarse en alguna de las categorías anteriores. Algunos de estos tipos incluyen los que hemos descrito en el punto anterior, como el *adware*, el *spyware*, aunque existen muchos más, como los *dialers*, *hoaxes* y otros, que analizaremos en los siguientes apartados.

11.4. Virus

Como hemos comentado, los virus pueden considerarse **el primer tipo de malware de la historia informática**, a pesar de que sus inicios fueron algo inocentes, pues únicamente trataban de demostrar que era posible escribir un programa que se autorreplicarse (inicialmente, sólo en la memoria del ordenador).

Pero, como era previsible, no tardaron en aparecer los primeros casos de programas que eran capaces de infectar disquetes y viajar ocultos en ellos, como el famoso caso del virus ***Viernes 13***.

En cualquier caso, los virus tienen características propias, que los diferencian respecto a otros tipos de *malware*:

- **Se reproducen infectando** ciertos ficheros o programas.
- Al ejecutarse **llevan a cabo acciones molestas** y/o **dañinas** para el usuario.

Existe una **analogía clara entre los virus informáticos y los biológicos**: del mismo modo que los virus biológicos **se introducen en el cuerpo humano e infectan una célula, que a su vez infectará nuevas células al inyectar su contenido en ellas, los virus informáticos se introducen en los ordenadores e infectan ficheros insertando en ellos su «código»**. Cuando el programa infectado se ejecuta, el código entra en funcionamiento y el virus sigue extendiéndose. Además, ambos tipos de virus presentan síntomas que avisan de su presencia y, mientras que los virus biológicos son micro-organismos, los virus informáticos son micro-programas.

¿Dónde se encuentran?

Una vez que el virus ha infectado un ordenador, podemos encontrar **rastros del mismo en distintos lugares**, incluyendo:

- **La memoria principal del ordenador**, o memoria RAM. Los virus quedan residentes en ella, esperando a que se den las circunstancias adecuadas para entrar en acción. Por esta razón, ésta también es un área que cualquier antivirus rastrea en busca de *malware*.
- Evidentemente, los propios **ficheros infectados**, que hacen de huéspedes para el virus. Cada vez que uno de ellos es ejecutado, el virus toma el control y lleva a cabo sus acciones.
- El **sector de arranque**, que es un área especial de cualquier disco, que almacena información sobre sus características y su contenido. Algunos virus se alojan en ella para poder ejecutarse antes incluso de que el sistema operativo arranque.
- Los **ficheros con macros** suponen, también, un escondite perfecto para ciertos virus. Las macros son pequeños programas que ayudan a realizar ciertas tareas y están incorporados dentro de muchos productos de Microsoft, como la suite ofimática Office. Al tratarse, en esencia, de programas, las macros pueden ser infectadas.

Síntomas de infección

En ocasiones puede ser difícil decidir, sin el uso de herramientas adecuadas, si un ordenador está infectado por un virus. Sin embargo, sí que existen **ciertos síntomas que delatan la posible presencia de virus**:

- La **lentitud no habitual** con la que repentinamente funciona un ordenador, sin ninguna causa aparente. Es un síntoma engañoso, pues puede deberse a varios motivos ajenos a un virus, dado, sobre todo, la creciente voracidad en recursos de memoria y CPU de los programas actuales.
- En ocasiones, la **imposibilidad de abrir ciertos ficheros** o de trabajar con determinados programas puede deberse a que un virus los haya eliminado, o que haya suprimido los ficheros que éstos necesitan para funcionar adecuadamente. De nuevo, el problema también puede deberse a que estos archivos se han corrompido por causas que no tienen que ver en absoluto con un virus.
- La **desaparición de ficheros y carpetas** es uno de los efectos más comunes de los virus.

- En otras ocasiones puede ser **imposible acceder al contenido de ciertos ficheros**. Los virus también suelen modificar ficheros, dejándolos inservibles. Al abrirlos, se mostrará un aviso de error.
- La **aparición en pantalla de avisos o mensajes** de texto inesperados puede ser un síntoma claro de infección por virus u otro tipo de malware. Generalmente, estos avisos contienen textos que, claramente, no son bien intencionados, de carácter absurdo, jocoso, hiriente, de contenido sexual, etc…
- La **disminución repentina del espacio en disco** o de la capacidad de la memoria es también un síntoma de infección por un virus, que puede llegar a ocupar todo el espacio libre. En tal caso se muestran avisos indicando que no hay más espacio.
- La **alteración inesperada en las propiedades de un fichero** puede ser también un síntoma de infección. La mayoría de virus modifican los ficheros que infectan, aumentando su tamaño, alterando su fecha de creación y modificación o sus atributos, etc.
- Si el **sistema operativo muestra mensajes de error**, puede ser debido a un error real o a la presencia de virus que no han funcionado correctamente. Sin embargo, los sistemas operativos de Microsoft son propensos a mostrar este tipo de errores por diversas causas, por lo que no puede considerarse un signo claro o definitivo de infección.
- Los **problemas al iniciar el sistema operativo** pueden deberse a varios motivos, pero la infección por parte de un virus puede ser uno de ellos.
- **El ordenador se apaga repentinamente** sin motivo aparente y vuelve a arrancar. Algunos virus necesitan este reinicio para activarse y asegurar su funcionamiento, por lo que ellos mismos provocan este tipo de situaciones.
- Otros efectos extraños, claros síntomas de la infección por troyanos, pueden ser que la **bandeja del CD-ROM se abra y se cierre automáticamente**, que el teclado y el ratón no funcionen correctamente o lo hagan al azar o que desaparezcan ventanas repentinamente, etc…

Quizás con excepción del último de los síntomas, ninguno de los anteriores puede considerarse un signo inequívoco de infección. Sin embargo, si varios de estos síntomas se producen simultáneamente las posibilidades de que se trate de un virus aumentan considerablemente.

Vectores de infección

Como hemos visto, los virus se diferencian de los gusanos en que tienen **capacidad de *autorreplicación***, es decir, capacidad para copiarse a sí mismos en otros lugares, como ficheros o disquetes, pero no cuentan con capacidad de ***autopropagación***.

Por tanto, no pueden salir de la máquina infectada sin que participe un humano, de alguna forma, en el proceso. Por ejemplo, llevando el disquete, o la llave USB, con un fichero infectado hasta ordenador y ejecutando allí dicho fichero. Este proceso, que permite que el virus infecte una nueva víctima, se conoce con el nombre de **vector de infección**.

A continuación listamos algunos de los vectores más comunes, que los virus utilizan para suplir su incapacidad de propagación y lograr extenderse:

- Las **páginas Web** están escritas en un determinado lenguaje y pueden contener elementos, como applets Java y controles ActiveX, que permiten a los virus esconderse en ellos. Al visitar la página, se produce la infección.
- Recientemente, las **unidades USB** y discos duros externos.
- Los **mensajes de correo electrónico** son los escondites preferidos de los virus, pues se trata del medio de propagación más rápido. Estos mensajes pueden contener ficheros infectados o incluso producir la infección con su simple lectura y apertura. En este sentido, algunos virus incluyen de forma automática código HTML en el campo de **Autofirma** de los mensajes de correo.
- Instalación y activación del virus con la simple visualización del mensaje a través de la **Vista previa** de ciertos clientes de correo.
- **Inclusión de código que provoca**, al abrir un mensaje infectado, **la ejecución automática del fichero incluido dentro del mismo**, aprovechando fallos, conocidas como *vulnerabilidades*, del navegador Internet Explorer y de los programas de correo electrónico Outlook y Outlook Express.
- **Uso de unidades de disco y directorios compartidos de red**, para disponer de información, utilidades o servicios comunes a los usuarios.
- **Uso de redes P2P de intercambio de archivos, como eMule.** Debido al auge de estas redes, éste se ha convertido recientemente en el vector de infección más común. Se estima que el 80% de los ficheros ejecutables que pueden encontrarse en este tipo de redes están infectados con algún tipo de *malware*, ya sean virus u otros.

Técnicas de ocultación

Los virus **intentan ocultarse de los antivirus** y demás sistemas de protección utilizando una combinación de **complejas técnicas**: camuflaje, autocifrado y polimorfismo.

1. Camuflaje

Los virus que utilizan esta técnica intentan pasar desapercibidos **ocultando los síntomas que normalmente delatan su presencia**. Algunos de los trucos utilizados incluyen los siguientes:

- Cuando un fichero es infectado generalmente aumenta de tamaño. Para que esto no se aprecie, el virus sólo incluye su código de infección en las secciones libres (sin contenido) del fichero. De este modo, aunque aumente el tamaño del fichero, el virus hará creer al sistema que éste no ha variado.
- Tras la infección se produce una modificación en la fecha y hora de último acceso al fichero. El virus evita esto manteniendo la fecha y hora que estuvieran establecidas antes de la infección.
- Para no levantar sospechas, los virus ocultan algunos de los ficheros que infectan, cambiando sus atributos y estableciéndolos en modo oculto.

2. Autocifrado

Los antivirus funcionan, básicamente, **buscando determinados grupos de instrucciones o cadenas de caracteres en el contenido de los ficheros**. Estas cadenas son características de cada espécimen concreto de virus, y es lo que permite su identificación. Para defenderse, éstos cifran u ofuscan partes de su código de forma que no sea fácilmente detectable.

Por supuesto, siempre debe existir una porción de código que no puede ser alterado con este sistema, pues de lo contrario el virus no sería capaz de ejecutarse correctamente y llevar a cabo sus acciones. Habitualmente esta sección de código se encarga de descifrar el resto del mismo, antes de éste sea ejecutado.

Tomando en cuenta esto, **los antivirus modernos son capaces de encontrar e identificar esta sección de código que**, recordemos, **no puede ser cifrada**.

Polimorfismo

El polimorfismo **hace referencia a la capacidad de algunos virus de cambiar o mutar la apariencia de su código sin que se modifique su funcionamiento**. Los virus que utilizan esta técnica cambian su aspecto de forma diferente en cada una de las infecciones que realizan.

Esto dificulta enormemente la detección por parte de los programas antivirus. Como la modificación no debe alterar su funcionalidad, el cambio se lleva a cabo, por ejemplo, introduciendo porciones de código que no realizan ninguna función útil o realizando saltos atrás y adelante en el código de forma aleatoria para volver a mismo sitio desde el que se comenzó.

11.5. Criptovirus (*ransomware*)

El primer criptovirus de la historia, aunque técnicamente fuera un troyano, lo encontramos en el año 1989, a través de un paquete que era distribuido por correo postal a las empresas farmacéuticas. El paquete contenía un disquete con un programa, en teoría con supuesta información sobre el virus (humano) del SIDA.

Sin embargo, el disquete contenía un virus que, tras ejecutarse, tomaba el control y quedaba a la espera, evaluando ciertas condiciones. Cuando éstas se producían, procedía a cifrar el disco duro y presentaba una «factura» a la víctima para recuperar la clave de cifrado. El programa en cuestión se llamó, como no podía ser de otra forma, *AIDS*, acrónimo inglés equivalente a SIDA.

Más tarde, en 1996, **Moti Yung** y **Adam Young** escribieron un artículo académico en el que desarrollaban el concepto teórico de un virus que utilizaba criptografía asimétrica, a diferencia de la simétrica que había sido utilizada por el troyano AIDS, para cifrar información del usuario.

¿Cómo funcionan?

El código malicioso **infecta la computadora del usuario por los medios normalmente utilizados por cualquier malware y acto seguido cifra los documentos que encuentre, generalmente ofimáticos, eliminando los originales y dejando un archivo de texto con las instrucciones para recuperarlos**.

Hasta el momento el cifrado se ha llevado a cabo utilizando claves simétricas simples, que son aquellas que utilizan la misma clave para cifrar y descifrar un documento, por lo que, utilizando ingeniería inversa sobre el código del virus, es posible obtener las claves de cifrado y, posteriormente, recuperar los archivos secuestrados.

Normalmente el rescate que se pedía ha sido el depósito de dinero en una cuenta determinada por el creador del virus. Una vez que el dinero era depositado, en teoría las claves para descifrar los archivos eran entregadas al usuario. Aunque, por supuesto, no había ninguna garantía de que esto fuera a ser así.

El futuro

Hasta ahora, las técnicas de cifrado utilizadas por estos virus han sido bastante rudimentarias, lo que ha permitido que recuperar los archivos secuestrados sea relativamente fácil.

Sin embargo, es fácil imaginar que, cuando estos métodos se perfeccionen, ocurrirá lo inevitable y las técnicas de cifrado utilizadas se aproximarán al modelo de Young-Yung, la criptografía asimétrica, lo que imposibilitará el descifrado de los archivos.

11.6. Gusanos

Siguiendo con nuestro recorrido por los tipos de malware, nos encontramos con los **gusanos**, que son programas muy similares a los virus, ya que también se autorreplican y tienen efectos dañinos para los ordenadores, pero se diferencian en que no necesitan infectar otros ficheros para reproducirse.

Básicamente, los gusanos se limitan a realizar copias de sí mismos, sin tocar ni dañar ningún otro fichero, pero se reproducen a tal velocidad que pueden colapsar por saturación las redes en las que se infiltran. Principalmente se extienden a través del correo electrónico, como el conocido ***I love you***, que enviaba copias de sí mismo a cada entrada de la libreta de contactos del usuario.

11.7. Adware

Adware es una palabra inglesa que nace de la contracción de las palabras ***Ad****vertising* *Soft****ware***, es decir, programas que muestran anuncios.

En general, se denomina adware al **software que muestra publicidad, empleando cualquier tipo de medio, como ventanas emergentes, *banners* o cambios en la página de inicio o de búsqueda del navegador**. La publicidad está asociada a productos y servicios ofrecidos por los propios creadores del adware o por terceros.

El adware puede ser instalado con el consentimiento del usuario y su plena conciencia, pero en la inmensa mayoría de ocasiones no es así. Lo mismo ocurre con la falta de conocimiento acerca de sus funciones y cómo éstas son llevadas a cabo.

11.8. Spyware

Los *programas espía*, también conocidos como *spyware*, son **aplicaciones informáticas que recopilan datos sobre los hábitos de navegación, preferencias y gustos del usuario**. Los datos recogidos son transmitidos a los propios fabricantes o revendidos a terceros.

El **spyware** puede ser instalado en el sistema a través de numerosas vías, entre las que podemos citar las siguientes:

- Troyanos, que los instalan sin consentimiento del usuario.
- Visitas a páginas web que contienen determinados controles ActiveX o código que explota una determinada vulnerabilidad.
- Aplicaciones con licencia de tipo shareware o freeware descargadas de Internet, etc.

El spyware es instalado habitualmente de forma oculta, sin solicitar en ningún momento ni de ninguna forma el consentimiento del usuario. Como era previsible, existe también una falta total de información sobre el proceso de recopilación de datos y del uso que se va a realizar de los mismos.

11.9. Hoaxes

Los ***hoaxes*** no son virus, sino **mensajes de correo electrónico engañosos, que se difunden masivamente por Internet sembrando la alarma sobre supuestas infecciones víricas y amenazas contra los usuarios**.

Los hoaxes tratan de ganarse la confianza de los usuarios aportando datos que parecen ciertos y proponiendo una serie de acciones a realizar para librarse de la supuesta infección.

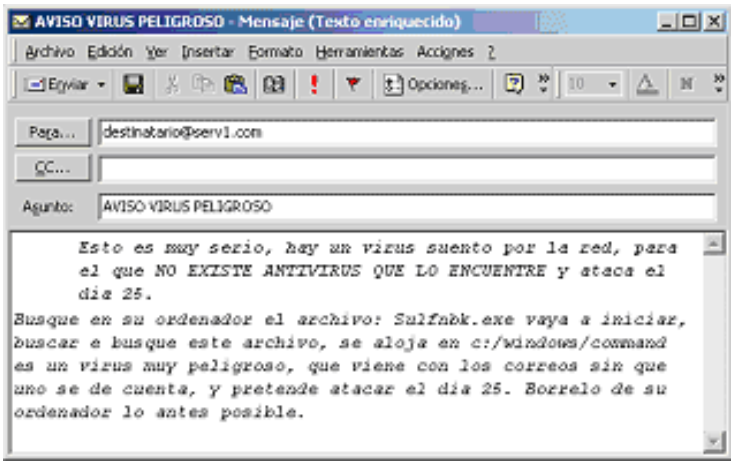


Figura 2. Hoax de ejemplo

11.10. *Phishing*

El ***phishing*** es una de las últimas amenazas en aparecer en el panorama telemático y, sin duda, se ha convertido **en una de las más conocidas y mediáticas**.

Consiste en el **envío masivo de correos electrónicos que, aparentando provenir de fuentes fiables, típicamente de entidades bancarias, intentan obtener datos confidenciales del usuario**.

Para ello, suelen incluir un enlace que, al ser pulsado, lleva a páginas web falsificadas. De esta manera, el usuario, creyendo estar en un sitio de confianza, introduce la información solicitada que, en realidad, va a parar a manos del delincuente.

La magnitud del problema, que no ha dejado de crecer durante los últimos años, ha llevado a que prácticamente la totalidad de bancos y cajas de ahorros españolas hayan sufrido, en mayor o menor medida, intentos de *phishing*. Pero el atrevimiento de los estafadores no tiene límites e, incluso organismos oficiales, como el Instituto Nacional de Estadística (INE), la Agencia Tributaria o el propio Banco de España, han sido objetos de intentos de fraude.

A continuación reproducimos uno de estos correos, correspondiente a un intento real de *phishing* contra una caja de ahorros española:

De: atencioncliente@ibercaja.es [mailto:atencioncliente@ibercaja.es]
Asunto: RENOVACION DE INFORMACION BANCARIA
Importancia: Alta

Estimado cliente,

Es muy importante y obligatorio a leer!

Posiblemente Usted notó que la semana pasada nuestro sitio www.ibercaja.es funcionaba inestable y se observaban frecuentes intermitencias. Hemos renovado nuestras instalaciones bancarias y ahora el problema está resuelta.
Pero para activar un sistema nuevo de protección de los datos y una capa cidad de trabajo correcta de sus cuentas bancarias, le pedimos a Usted a introd ucir los detalles completos de la cuenta para que pudamos renovar nuestra base de los clientes y comprobar la capacidad de trabajo de nuestro nuevo sistema de protección de los datos.
Si Usted no active su cuenta bancaria, no va a tener las posibilidades compleme ntarias de la defensa de seguridad en su cuenta.
Si Usted tiene una cuenta bancaria personal, pase a la referencia:
https://www.ibercaja.es/particulares/

Compruebe, por favor, este informe pulsando en acoplamiento inferior de Oficina Internet

Esta carta se automaticamente manda a cada cliente del Grupo Ibercaja, no es necesario a responderla.
Gracias por comprensión y apoyo.

Con respeto,
El servicio del mantenimiento técnico del Banco.

Como puede observarse fácilmente, hay dos cosas que llaman la atención del texto:

- El correo contiene tal cantidad de **errores gramaticales y ortográficos** que resulta prácticamente ininteligible. Afortunadamente, gracias a esta circunstancia, el impacto de este tipo de fraude no ha sido mayor, pues despertaba recelo entre algunos usuarios. Curiosamente, sin embargo, este es un hecho que no ha mejorado durante los años de vida del *phishing*, como podría esperarse.
- La **dirección de origen parece ser correcta** o, al menos, proveniente del dominio de la entidad financiera. Hay que recordar, sin embargo, que falsificar la dirección de origen de un correo electrónico es una tarea extremadamente sencilla, por lo que no debe nunca confiarse en el contenido de un correo basándonos únicamente en la dirección desde donde supuestamente ha sido enviado. En este caso, por supuesto, la dirección ha sido falsificada para hacer más creíble el correo.

Otras de las **características más comunes** que pueden presentan este tipo de mensajes de correo electrónico son:

- **Direcciones web con la apariencia correcta**. Como hemos visto, el correo fraudulento suele conducir al lector hacia sitios web que replican el aspecto de la entidad que está siendo atacada. En realidad, tanto los contenidos de las páginas como la dirección web son falsos y se limitan a imitar los contenidos reales. Incluso la información legal y otros enlaces no vitales pueden redirigir al usuario a la página web real.

- **Factor «miedo»**. La ventana de oportunidad de los delincuentes es muy breve, ya que una vez se informa a la compañía de que sus clientes están siendo objeto de este tipo de prácticas, el servidor que aloja al sitio web fraudulento y sirve para la recogida de información se cierra en el intervalo de unos pocos días. Por lo tanto, es fundamental para el defraudador el conseguir una respuesta inmediata por parte del usuario. En muchos casos, el mejor incentivo es amenazar con una pérdida, ya sea económica o de la propia cuenta existente, si no se siguen las instrucciones indicadas en el correo recibido, y que usualmente están relacionadas con nuevas medidas de seguridad recomendadas por la entidad.

Por último, para tratar de que el usuario no advierta que el dominio al que está siendo enviado no es el correspondiente a la entidad bancaria, **algunos casos de *phishing* utilizan dominios muy similares al original**, que pueden inducir fácilmente a error.

Pero la imaginación, y la «caradura» de los phishers no conoce límites y el profesor de esta asignatura, a lo largo de su carrera profesional, se ha encontrado casos realmente curiosos. Como el siguiente: una entidad bancaria decidió empezar a utilizar tarjetas de coordenadas para el acceso a su banca electrónico, lo que supone una buena idea y han terminado haciendo muchas de ellas, en un intento de reducir el impacto del *phishing* entre sus clientes.

Sin embargo, los phishers, ni cortos ni perezosos, decidieron que, a grandes males, grandes remedios, y enviaron correos electrónicos solicitando toda la tarjeta de coordenadas completa, como puede apreciarse en la Figura 3.

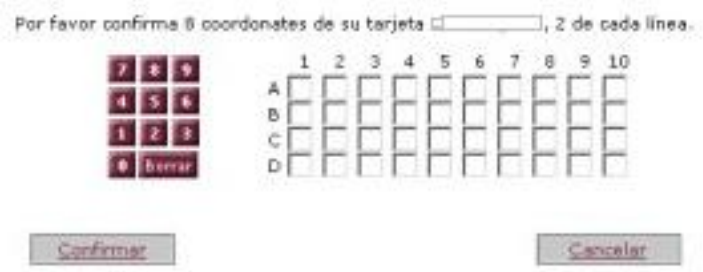


Figura 3. Intento de *phishing* real, en el que se solicitaba al usuario toda la tarjeta de coordenadas

En otro caso, aún más descabellado, se pedía que se enviara una copia de la tarjeta, ¡por fax! Lo más triste del caso es que, según nos consta, realmente algún usuario cayó en el engaño y envió su copia correspondiente.

Logística del *phishing*: los muleros

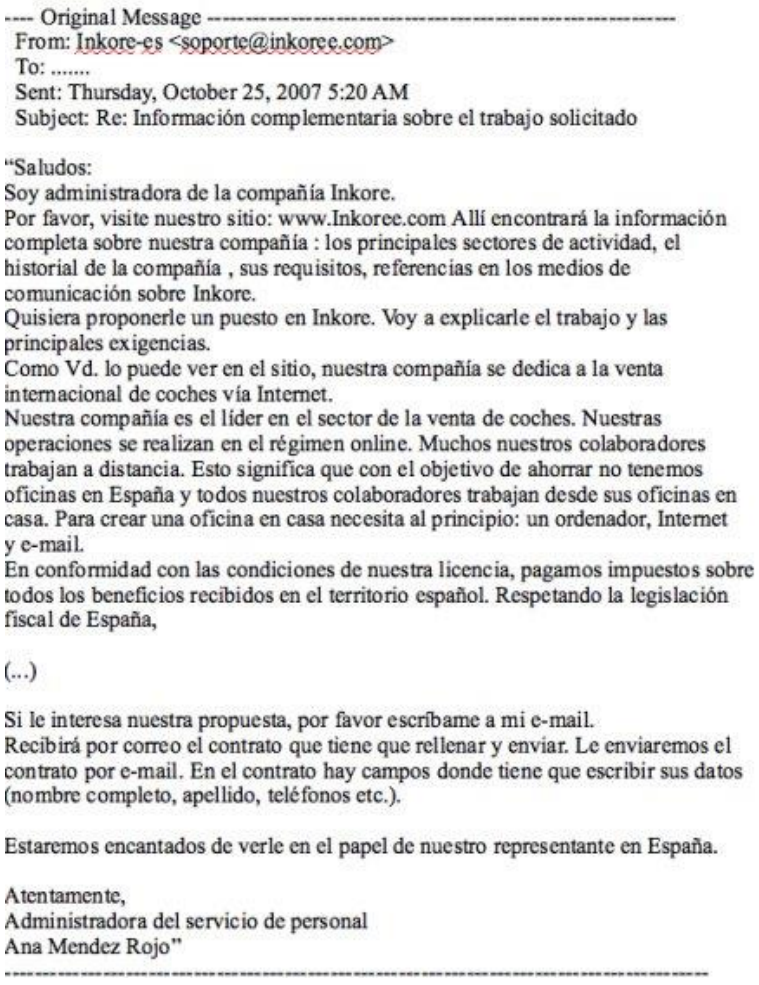
Una vez que el usuario ha sido víctima del engaño y ha proporcionado sus claves, estas son utilizadas lo más rápidamente posible para realizar una transferencia desde su cuenta.

Para ocultar el rastro dejado por estas transferencias, los delincuentes utilizan lo que se ha dado en llamar **mulas** o **muleros**. Una mula **es una persona que, siendo consciente o no de las posibles consecuencias, acepta una oferta de trabajo falsa, de las que circulan cientos por la red, y que ofrecen teletrabajar desde casa a cambio de una comisión suculenta por cada operación realizada**.

Las tareas consisten básicamente en abrir una cuenta bancaria, recibir una cantidad de dinero de supuestos clientes de una empresa falsa y, posteriormente, reenviar esa cantidad, menos la comisión por operación, a través de entidades como *Western Union* o *Money Gram*, a cuentas bancarias de otros países.

Evidentemente esto es una estafa, conocida como ***scam***, potencialmente muy peligrosa, pues puede provocar acusaciones por estafa o blanqueo de capitales penadas con hasta 6 años de prisión.

Esta estafa, el scam, así como el propio *phishing*, se ha profesionalizado mucho en los últimos años, generando cada vez anuncios y procesos de selección más creíbles (puedes encontrar un ejemplo real en la **Figura 4**. Por supuesto, el único propósito de los delincuentes al emplear a estas mulas es «encadenar» varias de ellas en el traspaso de fondos desde la cuenta del usuario engañado por el *phishing* hasta la cuenta final, habitualmente situada en algún banco de Europa del Este.



---- Original Message ----------
From: Inkore-es <soporte@inkoree.com>
To: .....
Sent: Thursday, October 25, 2007 5:20 AM
Subject: Re: Información complementaria sobre el trabajo solicitado

"Saludos:
Soy administradora de la compañía Inkore.
Por favor, visite nuestro sitio: www.Inkoree.com Allí encontrará la información completa sobre nuestra compañía : los principales sectores de actividad, el historial de la compañía , sus requisitos, referencias en los medios de comunicación sobre Inkore.
Quisiera proponerle un puesto en Inkore. Voy a explicarle el trabajo y las principales exigencias.
Como Vd. lo puede ver en el sitio, nuestra compañía se dedica a la venta internacional de coches vía Internet.
Nuestra compañía es el líder en el sector de la venta de coches. Nuestras operaciones se realizan en el régimen online. Muchos nuestros colaboradores trabajan a distancia. Esto significa que con el objetivo de ahorrar no tenemos oficinas en España y todos nuestros colaboradores trabajan desde sus oficinas en casa. Para crear una oficina en casa necesita al principio: un ordenador, Internet y e-mail.
En conformidad con las condiciones de nuestra licencia, pagamos impuestos sobre todos los beneficios recibidos en el territorio español. Respetando la legislación fiscal de España,

(...)

Si le interesa nuestra propuesta, por favor escríbame a mi e-mail.
Recibirá por correo el contrato que tiene que rellenar y enviar. Le enviaremos el contrato por e-mail. En el contrato hay campos donde tiene que escribir sus datos (nombre completo, apellido, teléfonos etc.).

Estaremos encantados de verle en el papel de nuestro representante en España.

Atentamente,
Administradora del servicio de personal
Ana Mendez Rojo"

Figura4. Ejemplo real de correo enviado para captar mulas

De esta forma, se dificulta y enlentece mucho el rastreo de dichos movimientos, lo que les permite ganar tiempo para retirar el dinero en efectivo antes de que las cuentas sean bloqueadas.

Es importante repetir que, si usted recibe un correo ofreciendo un trabajo de este tipo, no debe hacer ningún caso. Sería aconsejable además, que denunciara el caso ante la Brigada de Investigación Tecnológica de la Policía Nacional o el Grupo de Delitos Telemáticos de la Guardia Civil.

El *phishing* en cifras

Hablar sobre cifras de número de usuarios o entidades afectadas es difícil, pues existe una fuerte reticencia por parte de éstos a aceptar que han sido víctimas de una estafa y de las entidades a aceptar todos los casos que realmente se han producido por miedo a daños en su reputación pública.

Sin embargo, el **Instituto Nacional de Tecnologías de la Comunicación (INTECO)**, publicó en octubre de 2007 un amplio e interesante informe sobre el fenómeno del *phishing*, que ofrece cifras que podrían considerarse una buena aproximación. Citamos a continuación **algunas de las conclusiones más importantes** del mismo:

- El 29,9% de los usuarios reconocen haber sufrido algún intento de fraude online, aunque sólo afirman haber sufrido un perjuicio económico el 2,1% de los usuarios españoles de Internet.
- La media de perjuicio económico se sitúa en 593€, si bien en más de dos de cada tres casos no supera los 400€ que es el límite establecido en el ordenamiento jurídico español para que tenga la consideración de delito.
- El 24,8% de los ataques no alcanza los 50€. Este hecho contribuye a que, en muchas ocasiones, los fraudes no sean detectados al camuflarse entre los apuntes bancarios corrientes.
- Un 80,2%, de aquellos usuarios de Internet que han sido objeto de un intento de fraude no modifican sus hábitos de utilización del servicio de banca online, y un 73,1% no modifican sus hábitos de comercio electrónico.
- Incluso cuando dicho intento conlleva un perjuicio económico, no se produce un abandono masivo de los servicios de banca ni compra online: no alteran su comportamiento un 52,4% y un 31,9% respectivamente.

Evolución del *phishing*: *troyanos*

Aunque aún hoy en día siguen existiendo casos, y víctimas que «pican» en los mismos, afortunadamente el *phishing* ha ido perdiendo efectividad paulatinamente, conforme ha ido siendo conocido por un mayor número de usuarios. Los phishers se han encontrado por tanto, con la necesidad de buscar nuevos métodos para seguir llevando a cabo sus estafas. Y para ello, han encontrado la herramienta perfecta: **los troyanos bancarios**.

11.11. Troyanos

Cuenta Homero cómo Ulises, el más astuto de los mortales, ideó la argucia de construir un enorme caballo de madera, donde se ocultarían más de 3000 guerreros, para poder traspasar las murallas de Troya, que llevaba más de diez años resistiéndose a los envites del ejército griego. Tras simular éste su retirada, los troyanos abandonaron confiados su ciudad y, al encontrar el enigmático caballo, decidieron introducirlo en su interior. Ebrios como estaban, celebrando su segura victoria sobre los griegos, no opusieron mucha resistencia al selecto grupo de soldados que emergió entonces del interior del caballo.

Sin duda los griegos lo hubieran tenido mucho más fácil si, entre todo el legado de conocimiento que nos dejaron, hubiesen inventado también Internet. En ese caso les habría bastado con camuflar un programa maligno en el interior de otro aparentemente inocuo y conseguir que sus enemigos lo ejecutasen en sus ordenadores. Hubiesen inventado, así, el primer **caballo de troya informático** de la historia.

Por suerte o por desgracia no lo hicieron y tenemos que esperar hasta la década de los 80 para encontrar los primeros ejemplos, basados en el sistema operativo DOS. Desde entonces su complejidad se ha elevado enormemente pero, en lo esencial, su funcionamiento y comportamiento siguen siendo los mismos.

En pocas palabras, un **troyano** es un código malicioso que aparenta ser un programa inofensivo, como un salvapantallas, un juego o, incluso, un antivirus. Una vez que este programa es ejecutado, el troyano toma el control y queda residente en la máquina, listo para llevar a cabo la tarea para la que ha sido programado. A diferencia de los gusanos, los troyanos no tienen capacidad de autorreplicación, de modo que tienen que hacer uso de la siempre efectiva picaresca o ingeniería social para propagarse.

Los caballos de troya han recorrido un largo camino desde sus inicios a principios de la década de los 80. Con la reciente profesionalización del cibercrimen, este tipo de *malware* vive una segunda época dorada, pues está siendo utilizado como el vehículo perfecto para que los delin9*cuentes perpetren sus fechorías.

Además, por supuesto, los troyanos se han sofisticado muchísimo en los últimos años, hasta el punto de que en la actualidad hacen uso de todo tipo de técnicas de ocultación y autoprotección.

Primeros casos

Los primeros casos de este tipo de troyanos utilizaban viejas técnicas víricas, como la captura de las pulsaciones del teclado, en busca de palabras como «password». Para combatirlos, los bancos comenzaron a utilizar los teclados virtuales, tan extendidos hoy en día (puedes encontrar un ejemplo en la **Figura 5**)

Figura 5. Ejemplo de teclado virtual de una institución bancaria española

El siguiente movimiento de los delincuentes no se hizo esperar y consistió en dotar a los troyanos de la capacidad de tomar capturas de pantalla, e incluso, pequeñas secuencias de vídeo.

El juego del gato y el ratón continuó con nuevas técnicas, algunas algo burdas, como la que trataba de ocultar la barra de direcciones del navegador con una imagen que contenía la dirección legítima del banco, en lugar de la falsa a la que el usuario estaba siendo redireccionado.

Ante el escaso éxito de estos intentos, pronto empezaron a utilizar otros métodos, como el ***pharming***. Este consiste, en pocas palabras, en **engañar al sistema de resolución de nombres, de forma que éste devuelva una dirección IP falsa para un dominio concreto**. En los sistemas operativos de Microsoft, por ejemplo, basta modificar el archivo *hosts*, situado habitualmente en la ruta *\Windows\system32\drivers\etc*. De esta forma, el troyano puede redirigir el sitio web de cualquier entidad bancaria a un dominio fraudulento, donde se habrá colocado una copia del sitio original.

El problema se agravaba en aquellos momentos porque *Internet Explorer* contaba con ciertas vulnerabilidades que permitían visualizar una URL en la barra de direcciones cuando, en realidad, se estaba visitando otra. Afortunadamente, estos problemas fueron solucionados y este tipo de ataques son más difíciles de llevar a cabo en la actualidad.

Vectores de infección

Como es previsible, un método de propagación natural para estos troyanos son las redes de **intercambio de archivos P2P**, en las que no existen mecanismos de seguridad integrados. Según algunos estudios recientes, casi el 50% de los programas ejecutables que pueden encontrarse en este tipo de redes están infectados con alguna clase de *malware*.

Para incrementar el atractivo de los binarios y conseguir que el máximo número posible de usuarios los descarguen y ejecuten, muchos de ellos suelen estar camuflados utilizando el aspecto del reclamo más viejo del mundo: el sexo.

Otro vector muy utilizado por los delincuentes, la más utilizada hoy en día, de hecho, es la infección vía web. Aprovechando ciertas vulnerabilidades en los navegadores pueden conseguir que un usuario, por el mero hecho de visitar un sitio web malicioso, quede infectado. El proceso comienza con el compromiso de sitios web existentes, tanto mejor cuando más conocidos y visitados sean éstos. Para ello suelen utilizar herramientas automáticas, que explotan vulnerabilidades concretas, y que, en poco tiempo, pueden reunir una colección de cientos de máquinas comprometidas.

Acto seguido, se instala en cada una de ellas un pequeño código, de unos pocos kilobytes, que suele conocerse con el nombre de ***dropper***. A continuación se modifica el código fuente de la página web, a menudo sin alterar el comportamiento ni el aspecto de la misma, de forma que, cuando el usuario la visite, se explote la vulnerabilidad del navegador y se provoque la descarga y ejecución del *dropper* al ordenador de la víctima.

A partir de ese momento, el *dropper* toma el control y comienza su misión, consistente en descargar el verdadero troyano. Para ello cuenta una lista de direcciones donde, previamente, los creadores del troyano han colocado copias del mismo. Comenzará probando con la primera de ellas y, en el caso de que falle, seguirá avanzando por la lista hasta agotarla.

De esta forma, los delincuentes consiguen aumentar la resistencia del sistema y que éste siga funcionando aunque las autoridades cierren uno o varios de los sitios de descarga. Sirve, incluso, para generar distintas versiones de los troyanos, con mejoras o personalizaciones, de forma que no es necesario modificar el código del sitio web comprometido para que se descarguen las nuevas versiones.

Una vez que el *dropper* encuentra un sitio activo comienza la descarga del troyano. Luego lo ejecuta y … ¡*game over*! Todo este proceso se lleva a cabo, por supuesto, sin que el usuario note que algo extraño está sucediendo. En la siguiente figura puede observarse un esquema del ciclo completo.

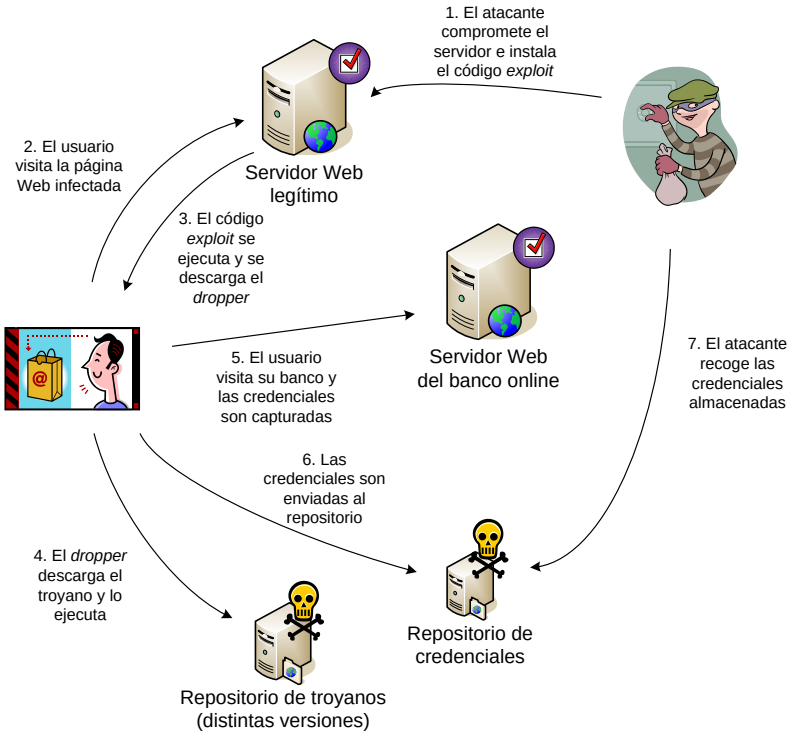


Figura 6. Ciclo completo de infección por un troyano vía Web

Últimas técnicas: inyección de código HTML

Estos troyanos son especialmente peligrosos cuando utilizan una técnica recientemente ideada por los delincuentes, la llamada ***inyección de código HTML***. Ésta consiste, en pocas palabras, en manipular el código HTML de la página web que está visitando el usuario, habitualmente la de un banco, antes de que ésta sea presentada en el navegador.

Los troyanos bancarios **utilizan este ataque para insertar campos fantasmas en los formularios de autenticación**, engañando al usuario para que introduzca datos que habitualmente no se piden, como se ilustra en la siguiente figura:

Debido a que la manipulación la lleva a cabo el propio navegador, a través de la extensión BHO instalada por el troyano, **resulta totalmente indetectable para un usuario no experto que utilice las medidas de seguridad habituales**.

Por ejemplo, el famoso candado, sobre el que tanto se insiste a los usuarios, está cerrado, ya que el certificado presentado por el banco es perfectamente legítimo. Por otra parte, tampoco puede apreciarse nada extraño en la URL visitada, puesto que realmente la página proviene del banco legítimo, sólo que ha sido modificada en el último instante antes de que ésta sea presentada al usuario.

Aunque es cierto que éste es un problema que afecta mayoritariamente a Internet Explorer, la extensión del mismo va más allá. Y, en realidad, tiene poco o nada que ver con la vieja y estéril polémica sobre la seguridad intrínseca de cada navegador. Parece lógico pensar que si Internet Explorer es el navegador más atacado no se debe a que sea más inseguro, sino porque es el más utilizado y, por tanto, más atractivo para los atacantes.

El fondo del asunto radica en el hecho de que, dado que en este tipo de ataque los datos se manipulan en la capa de aplicación, una sesión SSL, que actúa sólo protegiendo niveles inferiores, no es garantía de seguridad ante este tipo de amenazas. Puede decirse que los navegadores han dejado de ser, si alguna vez lo fueron, una plataforma confiable para mostrar información sensible.

Técnicas de ocultación

Desde que se han convertido en el juguete favorito de los ciberdelincuentes, la evolución de los troyanos en los últimos años ha sido inmensa. Los fabricantes de antivirus han reaccionado mejorando sensiblemente sus técnicas de detección, por lo que han obligado a los troyanos a utilizar sofisticadas medidas de protección y ocultación.

Algunas de ellas incluyen **técnicas para detectar y evitar la depuración**, **desensamblado o ejecución de los troyanos en entornos virtuales**. Si este detecta que está siendo depurado, con el fin de estudiar su comportamiento, simplemente no actúa o trata de jugar al despiste con el analista, entrando en bucles infinitos.

Lo mismo ocurre cuando se trata de estudiar al troyano ejecutándolo en entornos virtuales, como *VirtualBox* o *VMWare*, con el fin de contener el riesgo y proteger la máquina real. Es habitual que, en estas situaciones, el troyano no realice las acciones programadas o que, incluso, se niegue a infectar la máquina en cuestión. Esto supone una dificultad añadida para las compañías dedicadas a combatir este tipo de *malware* pues, al enorme volumen de especímenes existentes, que hace imposible un análisis manual, se suma el hecho de que no puedan utilizar entornos virtuales en los que automatizar, en lo posible, la tarea.

Por otra parte, **es habitual que este tipo de troyanos tengan una tasa de mutación altísima, hasta seis variantes diarias, con el fin de evitar la detección de los antivirus**. Evidentemente ese ritmo no puede alcanzarse de forma manual, sino que utilizan utilidades escritas por ellos mismos para crear las variantes de forma automática.

11.12. Economía del *malware*

Hace tiempo que la creación de *malware* dejó de ser una actividad exclusiva de *freaks* quinceañeros. Según las compañías antivirus, el 75% del malware detectado en el último trimestre del año pasado estaba diseñado para obtener dinero fraudulentamente. Hoy día es un negocio muy lucrativo, que mueve muchos millones de euros en todo el mundo, y que ha ido siendo progresivamente ocupado en parte por las mafias tradicionales, que pueden usar fácilmente sus redes ya establecidas de blanqueo de dinero.

Como todo negocio que crece, se hace necesaria la especialización, de modo que la cadena del fraude *online* se ha fragmentado en partes claramente diferenciadas. El primer eslabón lo componen los **escritores del *malware***, con conocimientos técnicos suficientes, que venden sus creaciones utilizando todo tipo de estrategias de marketing, al más puro estilo «teletienda».

Y es una afirmación literal, pues en los foros especializados, donde se vende este tipo de *malware*, es fácil encontrar ofertas del tipo 2x1, descuentos por volumen comprado o garantías de que los troyanos no son detectados por ningún antivirus.

Una vez que el comprador ha elegido el «producto», la forma más común de contacto es través de *ICQ*, a través del que puede hablarse directamente con el vendedor y negociar el precio final.

Por último, la transacción se realiza habitualmente a través de *WebMoney*, el nuevo sistema de pago electrónico preferido de los delincuentes, después de que en noviembre de 2006 *eGold*, plataforma más utilizada por los *phishers* en ese momento, decidiera dejar de hacer oídos sordos a las acusaciones de connivencia que llevaba años recibiendo por parte de las autoridades norteamericanas. De hecho, a menudo los precios pueden encontrarse anunciados en *WMZ*, la moneda oficial de *WebMoney*, equivalente a 1 dólar USA.

11.13. Posibles soluciones

Ahora que se conocen los riesgos es posible preguntarse, ¿cómo arreglar esta situación? Lo primero que parece claro es que los consejos habituales dados por las entidades financieras como «Compruebe el candado del navegador», «No haga clic en ningún enlace, escriba directamente la URL» o «Mantenga su antivirus actualizado» han dejado de ser ya una garantía de seguridad. Esta limitación no significa, por supuesto, que no sean válidas o deban dejar de seguirse. Simplemente, no son suficientes.

Un número cada vez mayor de bancos online están empezando a optar por soluciones que impliquen un ***doble factor de autenticación***, como las **tarjetas de coordenadas o el DNI electrónico**. Estos esquemas se basan en comprobar que el usuario, además de conocer cierto secreto asociado a él, es decir, su contraseña, posee físicamente un dispositivo, con el fin de evitar ataques de suplantación.

Este dispositivo puede ser tan simple como un cartón con una serie de números anotados en él, una tarjeta de coordenadas, o algo más complejos, como el DNI electrónico, con capacidad de realizar validaciones criptográficas.

Sin embargo, existen inconvenientes para que este sistema se generalice, pues supone ciertas molestias para los usuarios, que pueden olvidar o perder su tarjeta, y un coste elevado para los bancos. Por estas razones, algunos han pensado en un sistema ingenioso (aunque no novedoso, pues lleva años utilizándose en otros países europeos), que consiste en crear un pseudo-token **OTP (*One-Time Password*)** utilizando el teléfono móvil del usuario.

El sistema es sencillo: cuando el usuario necesite realizar una transferencia, u otra operación potencialmente peligrosa, la entidad bancaria envía un mensaje de texto al móvil de éste, con un código de un sólo uso, que debe introducir junto con su contraseña habitual para poder realizar la operación.

Otro sistema que, sin duda, será útil en el futuro es el famoso **DNI electrónico**. Dejando al margen la polémica que le rodea sobre la idoneidad de los algoritmos criptográficos que utiliza, es innegable que puede suponer una herramienta valiosa en la lucha contra el fraude. Sin embargo ésta lleva ya unos años librándose, y parece que aún quedan otros tantos hasta que el DNIe sea una realidad suficientemente extendida como para que suponga una ayuda efectiva.

Contramedidas

A pesar de que el panorama que hemos analizado no es muy halagüeño, esto no significa que no pueda obtenerse un alto nivel de seguridad en un ordenador de propósito general. Si, por ejemplo, fuera necesario realizar una transacción bancaria desde un ordenador, la siguiente tabla recoge contramedidas efectivas para todas las amenazas que hemos estudiado:

Amenaza	Peligrosidad	Contramedida
Phishing	Baja	Borre el correo e informe a las autoridades
Keylogger software	Alta	Software antivirus
Keylogger hardware	Alta	Habitualmente instalados en cibercafés. Nunca opere desde allí.
Troyano tradicional	Media	Software antivirus
Troyano inyección código	Alta	Arrancar un nuevo sistema operativo desde un CD

Lo + recomendado

No dejes de leer…

Phishing techniques in mobile devices

Amro, B. (2018). Phishing techniques in mobile devices. *Journal of Computer and Communications,* 6, 27-35.

La rápida evolución de los dispositivos móviles y la tecnología de la comunicación ha supuesto un aumento drástico del número de usuarios del dispositivo móvil. Y con ello el uso para realizar muchas tareas de *hacking* y estafas en medios de pago.

Accede al artículo a través del aula virtual o desde la siguiente dirección web:
https://arxiv.org/ftp/arxiv/papers/1802/1802.04501.pdf

No dejes de ver…

Generate phishing domains easily with dnstwist

Tutorial sobre cómo encontrar dominios para ataques de *phishing* con Dnstwist.

Accede al vídeo a través del aula virtual o desde la siguiente dirección web:
https://www.youtube.com/watch?v=ne8SPEoDe8o

Lección de la *Intypedia* sobre *malware*

En esta lección de la *Intypedia* se presenta un resumen muy interesante de la mayoría de los tipos de *malware* que hemos analizado en este tema. No dejes de verla como repaso, o para comprobar que realmente has entendido los principales conceptos estudiados en nuestro tema.

Accede al vídeo a través del aula virtual o desde la siguiente dirección web:
https://www.youtube.com/watch?v=NPsjN8AvNQM

Conferencia: «Nuevas amenazas al comercio y la banca en línea»

En esta conferencia, vuestro profesor de esta asignatura presenta ejemplos concretos de algunos de los troyanos avanzados, que hemos analizado en este tema. Puede verse uno de estos troyanos en acción, afectando a una conocida entidad financiera española.

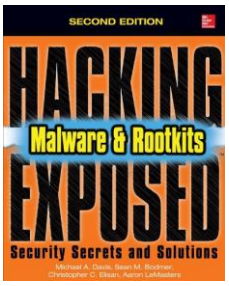
Accede al vídeo a través del aula virtual o desde la siguiente dirección web:
https://www.youtube.com/watch?v=7TE92IoZ95U

+ Información

A fondo

Hacking Exposed Malware & Rootkits

Davis, M.; Bodmer, S. & Lemasters, A. (2014). *Hacking Exposed Malware & Rootkits*. McGrawHill**.** ISBN: 0071823077



Este libro resulta muy interesante porque contiene multitud de casos de estudio reales, donde se analizan las técnicas concretas que utiliza actualmente el malware para atactar las redes y sobrepasar las medidas de protección. Como es habitual, muestra también una serie de contramedidas útiles para protegerse contra este tipo de malware.

Test

1. Una de las principales características de los virus es que:

A. Pueden reproducirse rápidamente y agotar los recursos de la máquina
B. Pueden transmitirse a través de la red
C. No tienen capacidad de autorreplicación
D. El principal vector de infección son las redes P2P

2. El polimorfismo de un virus hace referencia a:

A. Su capacidad de mutar su código sin afectar a su funcionalidad
B. Su capacidad de cambiar rápidamente la forma de infección
C. Su capacidad de mutar su código y funcionalidad en cada infección
D. Su capacidad de cambiar su funcionalidad manteniendo intacto su código

3. El *ransomware*, o criptovirus, es un tipo de virus que suele habitualmente:

A. Buscar ciertos ficheros en el disco duro infectado y borrarlos
B. Ocultarse utilizando para ello primitivas criptográficas (como el polimorfismo)
C. Buscar ciertos ficheros en el disco duro infectado y cifrarlos con el fin de, posteriormente, pedir un rescate económico por su recuperación
D. Buscar ciertos ficheros en el disco duro infectado y enviarlos a una máquina remota controlada por el atacante, borrándolos del disco duro. Posteriormente, suelen pedir un rescate económico por su recuperación

4. El *phishing* no es, estrictamente hablando, un tipo de malware, pero es, sin embargo, una amenaza que sigue estando muy vigente hoy en día. Consiste básicamente en:

A. Crear un sitio Web lo más parecido posible al original, habitualmente con el fin de robar credenciales
B. Realizar un ataque de *man-in-the-middle* al usuario e interceptar su tráfico cuando éste visite el sitio Web legítimo
C. Realizar un ataque de denegación de servicio a un sitio Web
D. Capturar tráfico dirigido a otras máquinas

5. Las principales características distintivas de un troyano es que:

A. No necesita ningún huésped, pues puede propagarse por la red
B. Dispone de capacidad de autorreplicación
C. No dispone de capacidad de autorreplicación, y oculta siempre su presencia
D. Suele ocultarse en medios de almacenamiento extraíbles, como unidades de CD o USB

6. El principal vector de infección de los troyanos actualmente es:

A. Vía correo electrónico
B. Vía redes P2P
C. Vía medios extraíbles, como unidades de CD o USB
D. Vía navegación Web

7. Una contramedida que suele utilizar la banca electrónica para combatir la amenaza de los troyanos es:

A. Comprobar si los usuarios tienen instalado un antivirus antes de operar con ellos
B. Los esquemas de doble factor de autenticación
C. Obligar a los usuarios a que arranquen en el ordenador un nuevo sistema operativo desde un CD
D. Realizar una comprobación telefónica de la identidad del usuario

8. En el entorno del *phishing* y, en general, del fraude en Internet, un mulero es:

A. Una persona que los delincuentes utilizan para transferir el dinero a la cuenta de destino final
B. El nombre en jerga con el que se conoce a los propios atacantes
C. Una víctima del *phishing*
D. Una persona que envía correos falsos, que dan comienzo al *phishing*

9. Un día recibes en tu bandeja de entrada del correo electrónico un mensaje con el siguiente texto. ¿Qué tipo de amenaza es la que has recibido?

«NO ADMITAS EN TU MESSENGER a: J_???????_FERREIRA@HOTMAIL.COM
ES UN VIRUS EXTREMADAMENTE POTENTE QUE SE TRANSMITE A TODOS TUS CONTACTOS Y TE
FORMATEA EL ORDENADOR.
MANDALE ESTE MAIL A TODA LA GENTE QUE TENGAS EN TU MSN. ESTO DEBE SABERLO TODA TU LISTA DE E-MAIL PORQUE SI NO LO MANDAS A TI TAMBIEN TE PUEDE AFECTAR, PORQUE SI ERES CONTACTO DE UNA PERSONA QUE LO ACEPTO A TI TAMBIEN TE LLEGA EL VIRUS»

A. Un phishing
B. Un troyano
C. Un hoax
D. Un virus

10. El *dropper* es uno de los elementos que suele formar parte de los:

A. Virus
B. Gusanos
C. Troyanos
D. Spyware