FRAUDE EN INTERNET: DEL PHISHING AL PHARMING

1. INTRODUCCION:

En un informe anterior de Recovery Labs se hacía un exhaustivo estudio sobre el fenómeno del phishing, su repercusión y las diferentes formas de combatirlo. Hoy en día el phishing sigue evolucionando y está cada vez más presente en los mensajes que recibimos y también cada vez en un mayor número de países e idiomas. Pero su evolución final ha culminado con la aparición del **Pharming,** aún más peligrosa y, en caso de llegar a realizarse, mucho más efectiva que el phishing tradicional.
En el presente informe vamos a analizar la actualidad del phishing, sus nuevas técnicas de engaño y estadísticas de expansión actuales. Y en segundo lugar explicaremos claramente el fenómeno del pharming y cómo luchar ante éste.

2. ¿QUÉ SON?

Toda la información necesaria acerca de qué es el phishing, cómo funciona o cómo evitarlo la encontraremos en el anterior informe, que se puede localizar en la siguiente dirección: http://www.recoverylabs.com/press/informes.htm

No obstante, a modo de recordatorio y como paso preliminar para explicar qué es el pharming, diremos que el PHISHING no es más que la suplantación de sitios de Internet. Se tratan de correos electrónicos engañosos y páginas Web fraudulentas que aparentan proceder de instituciones de confianza (bancos, entidades financieras, etc.), pero que en realidad están diseñados para embaucar al destinatario y conseguir que divulgue información confidencial. Por este motivo el phishing se considera un fraude que se vale de la "ingeniería social", por lo que su éxito está limitado ya que no todos los usuarios caen en sus trucos. La ingeniería social consiste en la manipulación de las personas para que voluntariamente realicen actos que normalmente no harían. En este caso sería facilitar, por ejemplo, claves o datos personales.

En cambio, el PHARMING es una técnica para llevar a cabo estafas online aún más peligrosa que el phishing, puesto que no necesita utilizar técnicas de ingeniería social. El pharming consiste en manipular las direcciones DNS (Domain Name Server) que utiliza el usuario, con el objetivo de engañarle y conseguir que las páginas que el usuario visite no sean realmente las originales, aunque su aspecto sea idéntico. Estas páginas falsas han sido creadas previamente por los delincuentes informáticos con el objetivo de conseguir datos e información sensible y personal, sobre todo la relacionada con los bancos, cajas, o entidades financieras.

3. ¿COMO FUNCIONA?

3.1 PHISHING

Funciona a través de un mensaje electrónico, simulando proceder de una fuente fiable (por ejemplo, de tu banco), se intentan recoger los datos necesarios para estafar al usuario. Normalmente se trata de mensajes con textos como:"Por motivos de seguridad…", o "Su cuenta se debe confirmar…", o "Usuarios del banco advierten", indicando al usuario que se están realizando cambios y que por seguridad debe introducir sus datos personales y códigos bancarios pinchando en un link que ellos te indican. Al pinchar se redirecciona a una página con gran similitud a la de tu banco habitual. La verdad es que esa página pertenece al estafador, quien no tiene más que copiar los datos que el usuario rellena.
Otras veces el mismo mail te pide que rellenes los datos y pulses "enviar", sin necesidad de redireccionarte a otra página.

3.2 PHARMING

El pharming consiste en manipular direcciones DNS para engañar al usuario y cometer fraude. Para entender mejor y con mayor claridad el pharming, debemos entender exactamente en qué consiste la manipulación de las direcciones DNS.
Cuando se teclea una dirección web determinada (URL) en el navegador de Internet, para poder acceder a ella, esta URL debe convertirse a la dirección IP real de la página que se quiere visitar. El formato IP es: 000.000.000.000.
Obviamente, esto se hace porque sería extremadamente complejo poder recordar secuencias de números que identificasen todas las webs que visitamos. Por lo tanto, es más sencillo escribir en nuestro navegador, por ejemplo, www.cajamadrid.es, y luego convertirlo a la numeración correspondiente a su IP real. Ahora bien, normalmente el navegador no puede realizar esta conversión, por lo que se necesita un servidor DNS para que realice esta acción.
A modo de ejemplo, al teclear **cajamadrid.es** estamos enviando este nombre a un servidor DNS. Éste tiene un registro que administra esos nombres y les otorga su correspondiente secuencia numérica, para conducir finalmente al usuario a la página deseada.

El pharming realiza su ataque sobre estos servidores DNS. Su objetivo es cambiar la correspondencia numérica a todos los usuarios que lo utilicen. Al cambiar esta correspondencia, usted escribe en su navegador cajamadrid.es, pero el DNS le otorga otra correspondencia numérica distinta a la original y real, llevando al usuario a una página idéntica a la de cajamadrid, pero que en realidad ha sido creada por los delincuentes. A partir de aquí, el usuario ve en su navegador que está en www.cajamadrid.es y realiza sus movimientos con total tranquilidad. El delincuente informático tan sólo tiene que utilizar las claves que el usuario escribe.

Otro tipo de pharming, aún más peligroso y efectivo es el que se realiza a nivel local, es decir, en cada equipo individualmente. Tan sólo es necesario modificar un archivo denominado **"HOSTS",** y que contiene cualquier ordenador que funciona bajo el sistema operativo Windows y que utilice Internet Explorer para navegar por Internet.
El fichero **hosts** actúa de tal forma que no es necesario acceder al servidor DNS para reconducirnos a la web deseada. Éste almacena una pequeña tabla con las direcciones de servidores y direcciones IP que más suele utilizar el usuario.
Al modificar este fichero, por ejemplo, con falsas direcciones de bancos online sucederá como en el caso anterior, es decir, en el navegador se escribirá el nombre, pero nos enviará a una página que no corresponde con la real.
Suponemos que a estas alturas la pregunta que nos formulamos todos es: ¿Cómo modifica una tercera persona en un ordenador personal un fichero concreto? Esto puede hacerlo directamente el delincuente entrando en el ordenador de forma remota a través de alguna vulnerabilidad del sistema, o bien mediante un código malicioso (virus o troyanos). Algunos ejemplos de troyanos reconocidos con la capacidad de realizar estos cambios en el fichero hosts son los de las familias **Bancos, Banker o Banbra**. Estos troyanos suelen ser malwares disfrazados que suelen esconderse en ficheros adjuntos, o bien se descargan al acceder a páginas falsas creadas con este objetivo.

4. ¿COMO EVITARLO?

4.1 EVITAR EL PHISHING

Toda la información necesaria acerca de cómo evitarlo la encontraremos en el anterior informe, que se puede localizar en la siguiente dirección:
http://www.recoverylabs.com/press/informes.htm

No obstante, las técnicas de ingeniería social siguen evolucionando, por lo que mostraremos ejemplos de los últimos casos encontrados.

Los bancos online con el típico mensaje alertando que por algún motivo se deben introducir los datos personales siguen siendo los más perjudicados en ataques de phishing. Aunque su evolución al pharming está empezando a generar nuevos engaños de ingeniería social cuyo objetivo es que el usuario se dirija a páginas falsas que contienen códigos malware, para posteriormente utilizarlo y conseguir información del usuario. A continuación analizaremos unos ejemplos:

CASO 1. Terra: Un amigo le ha dedicado una canción

Como se puede observar, el mensaje está en portugués y de momento sólo se ha identificado en Brasil. Es una claro ejemplo de la utilización del phishing para realizar pharming. El usuario recibe un falso mail con el siguiente asunto: *"Hemos dedicado música para ti"*. El resto del texto dice: *"Un amigo/a te ha dedicado una canción. Con cariño!!!. Para escuchar la canción clique aquí".*

Si hacemos clic en ***clique aquí***, un archivo ejecutable se descarga desde la web del delincuente. En el momento en que ejecutemos dicho archivo, un código malicioso se instala en el equipo. Éste puede ser:

- **Keylogger**: se trata de un tipo de troyano capaz de registrar las pulsaciones de su teclado al conectarse a determinadas páginas web. Por ejemplo, en el momento en que el usuario se conecta a su banco, si éste está en la lista del troyano, comienza a registrar las teclas que el usuario pulsa, consiguiendo el delincuente de ésta forma los códigos. Existen troyanos de éste tipo que incluso realizan pantallazos y posteriormente los envían al delincuente.
- **Troyanos** que cambian el archivo hosts: son los que mencionábamos anteriormente.

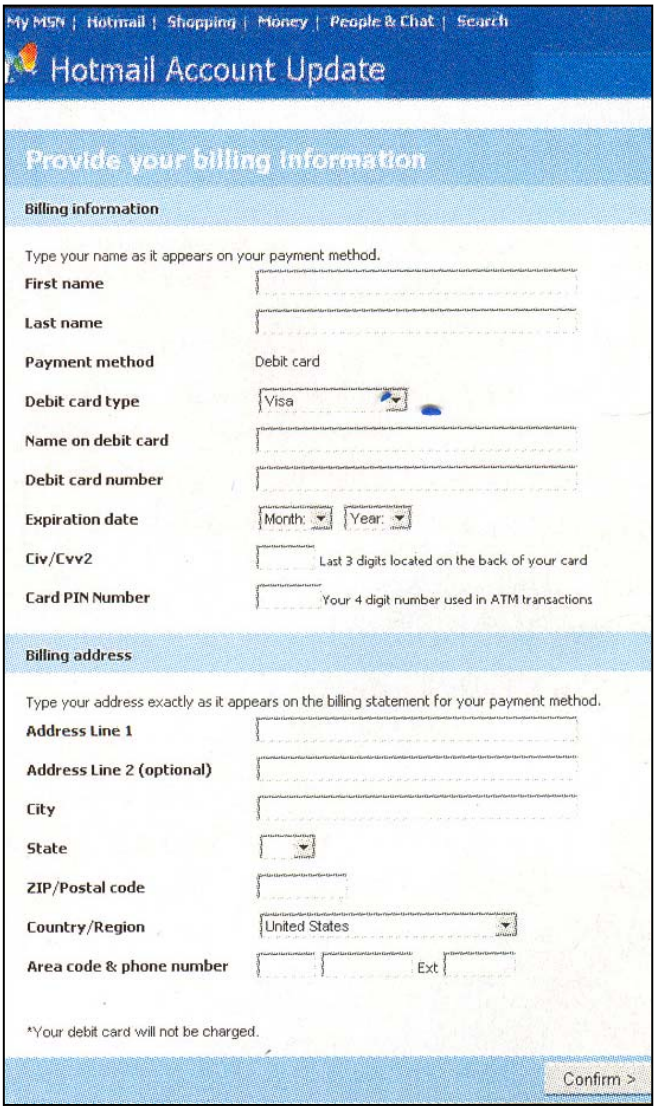
CASO 2. Norton: Información de un nuevo gusano

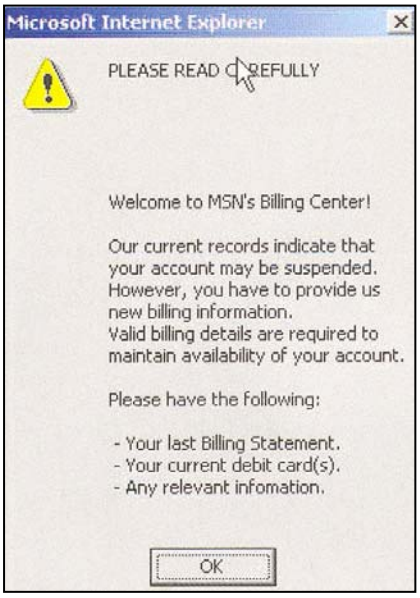
Este caso es similar al ejemplo 1, y la finalidad también es que se acceda a una página para que se descargue un troyano y así poder cometer el fraude. El mensaje es diferente y nos alerta ante la aparición de un nuevo gusano que por supuesto no es real. El texto del mensaje dice;

> *"Detectamos que su e-mail está enviando mensajes contaminados con el virus* ***w32.Bugbear.B@mm:***
>
> *- Se trata de una variante del virus w32.Bugbear@mm*
> *- Es una gusano de distribución masiva que también se propaga a través de redes compartidas*
> *- Es polifórmico y también afecta a una lista selecta de archivos ejecutables*
> *- Registra actividades del teclado y habilita puertas traseras*
> *- Intenta finalizar los procesos de numerosos antivirus y firwalls*
> *- Actualización crítica*
>
> *Descárguese el parche para eliminar el virus de su sistema"*
>
> ***DESCARGAR AQUÍ***

Cuando pinchamos en DESCARGAR AQUÍ, sucede lo mismo que en el anterior ejemplo.

Queremos recordarle que el phishing no es algo nuevo y que no se extiende únicamente a entidades financieras. En general debemos ser cautelosos y sospechar ante cualquier ventana emergente que nos pida datos bancarios. Otros fraudes con mensajes engañosos se pueden encontrar en falsas ventanas o e-mails enviados a usuarios de Hotmail. Otro de los sectores más perjudicados es el de subastas y ventas on-line.





4.2 EVITAR EL PHARMING

La mejor forma de evitarlo es, en primer lugar, asegurándonos que la página web que se está visitando es la correcta y, en segundo lugar, no permitir que se instale un malware en nuestro equipo.

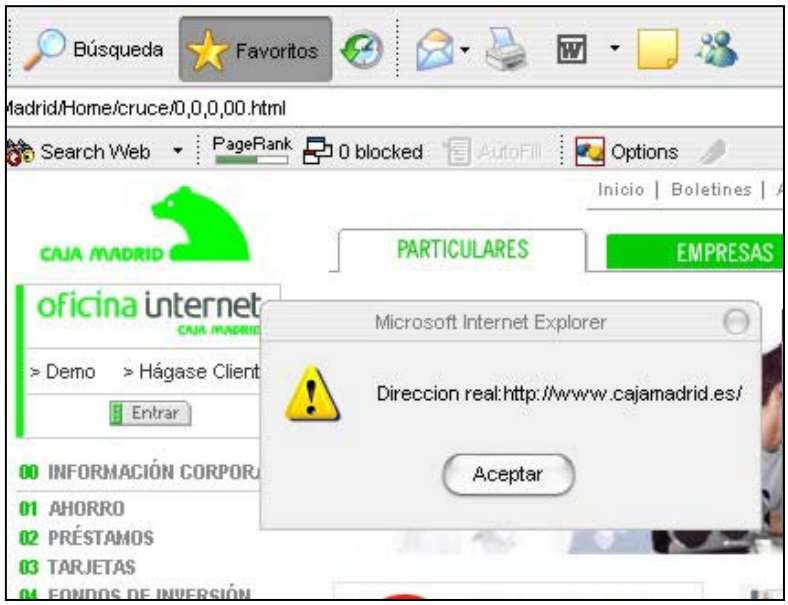
1- **¿Cómo se puede saber que la dirección que aparece en la barra de navegación es la verdadera?**

Es muy fácil con el siguiente truco:

Debemos teclear en el navegador y exactamente lo siguiente:

javascript:alert("Direccion real:"+ location.protocol + "//" + location.hostname + "/")

Al pinchar sobre "IR", aparecerá una ventana indicando la dirección verdadera de la web en la cual nos encontramos. Lo más cómodo sería configurar este javascript en favoritos. Para ello, escribiremos el java en el navegador, lo agregamos como ***Favoritos*** y le llamamos, por ejemplo: "WEB REAL". A continuación abrimos ***Favoritos*** y con botón derecho sobre "WEB REAL" vamos a propiedades. Donde pone URL, lo cambiamos de nuevo por el java y aceptamos. A partir de aquí, cuando el usuario navegue por cualquier página, sólo debe pinchar sobre "WEB REAL", y aparecerá la ventana con la información. Incluso se puede colocar como botón en la barra de vínculos de Internet Explorer.



2- **Para evitar que se instale un malware en nuestro equipo los mejores consejos que se deben seguir son:**

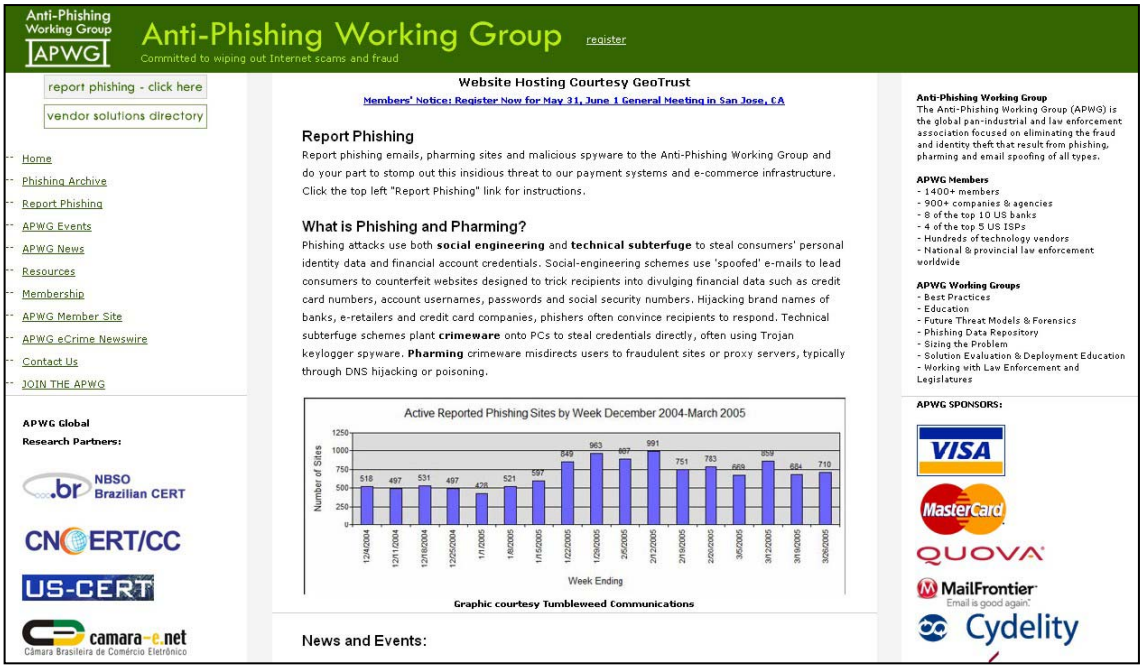
- No abra archivos adjuntos si desconfía de su procedencia
- Mantenga su sistema al día con las últimas actualizaciones
- Mantenga actualizado su antivirus diariamente y páselo por el sistema en busca de malware
- Utilice un firewall o cortafuegos.

5. LUCHANDO CONTRA EL PHISHING Y EL PHARMING

5.1 ANTI-PHISHING WORKING GROUP" (APWG)

En Estados Unidos se ha creado la "**Anti-Phishing Working Group"(APWG).** Se trata de una asociación de industrias cuyo principal objetivo es acabar con el robo de identidad y fraudes resultantes del creciente problema del phishing en correos electrónicos fraudulentos. Si quieres ampliar información sobre esta organización, puedes visitar su página Web: **http://www.antiphishing.org**; y en caso que detectes un caso de estafa sobre phishing o pharming, puedes denunciarlo y enviarles un email a **reportphishing@antiphishing.org**

Hace tan sólo unos meses sólo se ocupaba de los casos de phishing (de ahí su nombre), pero después de la aparición del pharming se han visto obligados a adaptarse e incluirlo dentro de su lucha.



Esta organización realiza un informe mensual analizando todos los ataques de phishing denunciados a APWG. Su último informe publicado corresponde a Marzo de 2005 y lo podemos encontrar en su página Web (en inglés). A continuación os reproducimos los datos más relevantes del informe.

5.2 DATOS

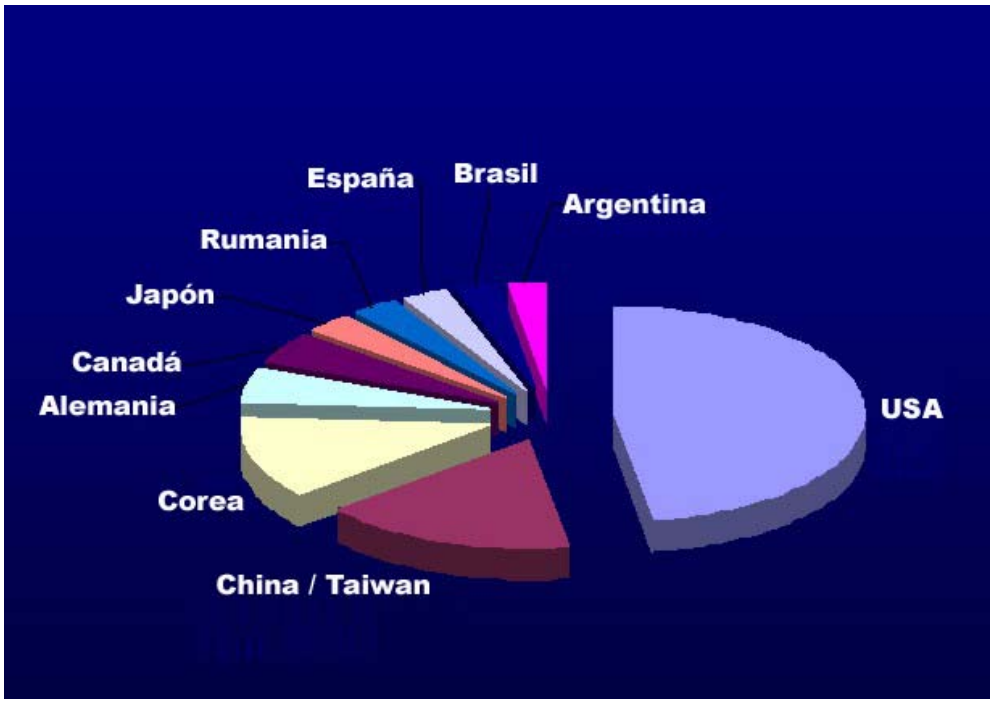
- Número de ataques únicos de phishing* reportados durante marzo: **13.353 ataques**
- Media mensual del ratio de crecimiento desde julio 04 a Marzo 05: **50%**
- Sectores industriales más atacados : **Servicios financieros**
- País con mayor número de Webs alojadas de phishing: **Estados Unidos**
- Media de vida de una página web de phishing activa: **5.8 días**

***Un "ataque único de phishing" se define en este análisis como un solo envío masivo de correos electrónicos enviados de una vez, destinados a una compañía u organización, y escritos en una misma línea de texto.**

- ***PAISES CON MAYOR NÚMERO DE WEBS ALOJADAS DE PHISHING***

Estados Unidos es una vez más el país "líder" en número de alojamiento de webs con phishing. Aparecen en la tarta países que en el 2004 ni siquiera aparecían, como España y Brasil. Esto se debe a problemas de idiomas. Antes todos los ataques se lanzaban en inglés, y ahora están empezando a personalizarlos en diferentes idiomas.

Países con mayor número de webs alojadas de phishing



6. GLOSARIO

CÓDIGO O LENGUAJE DE VIRUS (VBSCRIPT, JAVASCRIPT, HTML): Los virus Script están escritos en lenguaje de programación script, como VBScript y JavaScript. Los virus VBScript (Visual Basic Script) y JavaScript utilizan el Scripting Host (servidor de códigos) de Windows de Microsoft para activarse e infectar otros archivos. Desde que Scripting Host de Windows está disponible en Windows 98 y Windows 2000, los virus se pueden activar simplemente al hacer doble click en los archivos *.vbs o *.js de Windows Explorer.Para hacer daño, los virus HTML utilizan scripts insertados en archivos HTML. Estos códigos insertados actúan en el momento de abrir la página HTML desde un navegador habilitado para scripts.

DIRECCION IP: Dirección numérica obligatoria de un dominio 'Internet'. Está compuesta por cuatro cifras (de 0 a 255) decimales separadas por puntos.

DNS: 1) Acrónimo de Domain Name System [Sistema de nombres de dominio] 2) Acrónimo de Domain Name Service [Servicio de nombre de dominio] 3) Acrónimo de Domain Name Server [Servidor de nombre de dominio] Los dos primeros acrónimos simbolizan la misma idea siendo el tercero el equipo servidor que resuelve en sí la conversión que se realiza entre direcciones 'IP' y los nombres de dominio propiamente dichos. 'DNS' se creó con el fin de evitar la incomodidad de manejar números para identificar una dirección 'IP' ideando para ello un sistema basado en nombres compuestos de variasÿpalabras. Este es el sistema por el que se rige 'Internet' para poder comunicar ordenadores y usuarios por la red. Los servicios de denominación simbólica 'DNS' fueron instaurados en 1984.

FIREWALL / CORTAFUEGOS: Su traducción literal es *muro de fuego*, también conocido a nivel técnico como *cortafuegos*. Es una *barrera* o protección que permite a un sistema salvaguardar la información al acceder a otras redes, como por ejemplo Internet.

INGENIERÍA SOCIAL: consiste en la manipulación de las personas para que voluntariamente realicen actos que normalmente no harían. En este caso sería facilitar, por ejemplo, claves o datos personales.

MALWARE: Cualquier programa, documento o mensaje, susceptible de causar perjuicios a los usuarios de sistemas informáticos. *MAL*icious software.

TROYANO O CABALLO DE TROYA: También conocido como caballo de Troya, es un programa que realiza algunas acciones inesperadas o no autorizadas, generalmente malignas, tales como desplegar mensajes, borrar archivos o formatear un disco. Un caballo de Troya no infecta otros archivos, por lo que no es necesario limpiar. Para deshacerse de un troyano, simplemente borre el programa.

El glosario ha sido extraído de: http://catinello.webcindario.com/glosario/MN.html y de http://www.pandasoftware.es/virus_info/glosario/