

Medidas de protección contra troyanos bancarios

Autores: Chema Alonso

<http://elladodelmal.blogspot.com/>

Recopilación: Lic. Cristian Borghello, CISSP

Fecha Publicación: 30 de noviembre de 2008

Estos documentos han sido escritos y publicados por Chema Alonso en su Blog y en Artículo publicado en PCWorld Profesional Septiembre 2008.

Indice

Medidas de protección contra troyanos bancarios	1
Indice	2
Medidas de protección contra troyanos bancarios (I de VI).....	3
Conoce a tu enemigo.....	3
Fuego Purificador	3
Grano no hace Granero... ..	4
Medidas de protección contra troyanos bancarios (II de VI)	5
Sacar la pasta	5
El principio	6
Más vale prevenir que curar	6
Medidas de protección contra troyanos bancarios (III de VI)	7
Antivirus	7
Mutaciones.....	8
Antivirus estratégicos	9
Medidas de protección contra troyanos bancarios (IV de VI).....	10
Software Actualizado	10
Medidas de protección contra troyanos bancarios (V de VI)	13
Mínimo Privilegio Posible	13
Fortifica tu navegador.....	14
Medidas de protección contra troyanos bancarios (VI de VI).....	15
Zonas de Seguridad	15
Sitios Fraudulentos de Phishing.....	15
Recomendaciones Finales.....	16

Medidas de protección contra troyanos bancarios (I de VI)

<http://elladodelmal.blogspot.com/2008/07/medidas-de-proteccion-contra-troyanos.html>

Desde hace ya un tiempo todos los que trabajan en la industria de la lucha contra el malware parecen estar de acuerdo en que se acabó el romanticismo. ¿Romanticismo? Sí, esa época en la que los virus y los troyanos estaban creados por un autor o un grupo reducido y cuyo único objetivo era el destrozar tu ordenador para dejar claro que puede hacerlo o tener controlado tu PC con el único deseo de pasar un buen rato. Hoy en día la cosa está un pelín más difícil.

Alguna vez hemos ido comentando en un taxi como está el tema de la industria de robar pasta y al final del viaje el taxista, con los ojos inyectados en preocupación nos ha dicho: *“Oigan, disculpen, yo uso el Banco Pepito por Internet, ¿no me robarán el dinero, verdad?”* A lo que le hemos contestado que por supuesto que no, que tranquilo, que...Vale teníamos prisa, y no podíamos sentarnos a explicarle todas las precauciones que debe tomar para intentar mitigar la amenaza.

Conoce a tu enemigo

Sí, es tu enemigo, lo quieras o no te va a perjudicar de una u otra manera, así que más te vale que sepas como actúa. Si piensas que *“es que hay que ser muy tonto para caer en las estafas”* es que eres una víctima propicia.

El *“Phishing”* basado en correos escritos en muchos casos utilizando un traductor automático para decirte que *“Garche esta ancla”* fueron sólo las primeras apariciones de lo que se iba a convertir en una gran industria de generación de herramientas y mecanismos para robar pasta de los que los troyanos bancarios, con cien mil variaciones y mutaciones, son el máximo exponente tecnológico.

Sí ya hay que hablar de una industria detrás, una gran maquinaria de personas y técnicos que buscan la forma de tomar control de tu ordenador pero sin molestarte. Ya se ha pasado esa época en la que querían hacerle daño a tu ordenador, no quieren que tu procesador de textos favorito deje de funcionar, no quieren que no puedas jugar, no quieren que no puedas navegar por internet. No, al contrario, son como el Venom de Spiderman, quieren vivir contigo, en tu ordenador, ser parte de tu maquinita, tu dirección IP, tu proveedor de Internet y por supuesto tus cuentas bancarias. El daño no se lo quieren hacer al ordenador, te lo quieren hacer a ti.

Fuego Purificador

Para entender cómo funcionan los troyanos bancarios hoy en día lo primero que tienes que preguntarte es: ¿Tú cuándo vas al médico? ¿Vas periódicamente? ¿O sólo cuando te duele algo? Seguro que podemos mirar en nuestra agenda y responder a esta pregunta fácilmente. La mayoría sólo vamos al médico cuando nos duele algo. No somos de revisiones anuales, semestrales o trimestrales dónde nos hagamos una revisión completa. Con nuestro ordenador sucede lo mismo, ¿vas a buscar algún troyano en tu equipo cuando no tienes ningún síntoma? *“Mi equipo va bien, no me hace nada raro ergo estoy seguro”* es una reflexión no del todo cierta y que sólo será verdad (y nunca comprobable al 100 %) si has tomado todas las

precauciones necesarias.

Los fabricantes de malware buscan evitar que tu ordenador vaya al médico, que notes tu presencia en el ordenador y lo que es aún peor, que apliques el famoso “fuego purificador”, es decir, que reinstales tu equipo completamente. Esto no gusta nada a los troyanos bancarios.

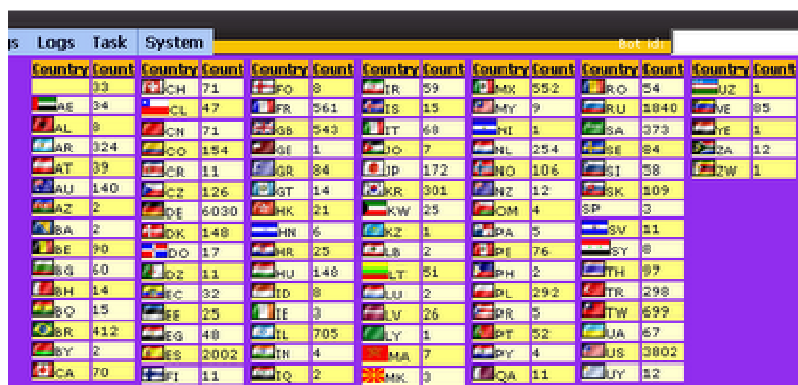
Grano no hace Granero...

¿Para qué quieren vivir conmigo en mi máquina? La primera y más fácil respuesta a esto es que quieren estar en tu máquina para grabar tus acciones cuando te conectas a un banco y así robar tus credenciales. No, no vas a estar seguro ni aunque la contraseña no se vea, ni aunque se use un teclado virtual, ni aunque ese teclado virtual vaya aleatorizando la posición de los números cada vez, ni aunque aparezca un candadito de seguridad autenticando el servidor.

Los troyanos bancarios están preparados para grabar las pulsaciones del teclado en tu ordenador o para grabar la zona de pantalla dónde has hecho clic cada vez que lo haces, por lo tanto siempre van a saber qué acciones has tomado cuando te enfrentas a una aplicación web bancaria.

Una vez recogida esta información es transmitida hasta un servidor controlado dónde se van almacenando los datos de las cuentas bancarias robadas. Hoy en día, los sistemas de almacenamiento son cada vez más elegantes, siendo controlados por paneles de control que clasifican directamente las cuentas robadas por países y bancos en función de las direcciones IP en las que han sido robados.

Esto es muy importante, ya que las entidades bancarias tienen sistemas de alertas cuando una cuenta está realizando movimientos fuera de su perfil de uso. Es decir, si una cuenta siempre se usa desde Francia y de repente se empieza a utilizar desde Korea entonces saltan las alarmas en los sistemas de los bancos.



Country	Count	Country	Count	Country	Count	Country	Count	Country	Count
CH	71	FR	561	IR	59	MX	552	RO	54
AE	34	CL	47	IS	15	MY	9	RU	1040
AL	8	CH	71	GB	543	IT	60	SA	373
AR	324	CO	154	SI	1	DO	7	NL	254
AT	39	CR	11	GR	84	JP	172	NO	106
AU	140	CZ	126	GT	14	KR	301	HK	12
AZ	2	DE	6030	HK	21	KW	25	OM	4
BA	2	DK	148	HN	6	KZ	1	PA	5
BE	90	DO	17	HR	25	LB	2	PE	76
BG	60	DZ	11	HU	148	LT	51	PH	2
BH	14	EC	32	ID	8	LU	2	PL	292
BQ	15	EE	25	IE	3	LV	26	PR	5
BR	412	EG	48	IL	705	LY	1	PT	52
BY	2	ES	2002	IN	4	MA	7	PY	4
CA	70	FI	11	IQ	2	MX	9	QA	11
								UY	12

Imagen: Panel de Control de un troyano Bancario publicado por Hispasec Sistemas

Medidas de protección contra troyanos bancarios (II de VI)

http://elladodelmal.blogspot.com/2008/07/medidas-de-proteccion-contr-troyanos_08.html

Sacar la pasta

Una vez que se tienen las cuentas robadas y clasificadas, ¿cómo se accede al dinero? Esto es una industria cada vez más profesionaliza y en muchos casos son gente distinta. Por un lado la gente que roba las credenciales bancarias se las vende a mafias que van a realizar la extracción del dinero.

Para sacar la pasta lo primero es sacarla desde el propio país, es decir, si vamos a robar dinero en cuentas en España se tiene que hacer desde un ordenador en la red de España. Para ello, nuestros queridos troyanos vienen configurados para permitir que el “amo” tome el control de la máquina y pueda realizar las transferencias desde un ordenador situado en España. Así se evitan el uso de proxys anónimos que los bancos los tienen marcados en blacklists. Es suficiente con entrar a una máquina de una víctima en el país dónde se va a robar el dinero y desde ella realizar cierto número de transacciones. Luego se coge otra y otra hasta que se roba en todas las cuentas.

Pero... ¿a qué cuenta se envía? Si la cuenta esta en otro país es más probable que salten las alarmas por lo que, mediante el uso de e-mailings masivos utilizando técnicas de SPAM o anuncios publicitarios en distintos medios se “contrata” a una persona para actuar de lo que se llama “Mulero”. Los correos de Spam no se envían desde servidores de la mafia sino desde equipos troyanizados que no están en blacklists de correo, por lo que basta con cambiar cada poco de víctima para seguir enviando correo SPAM.

El mulero que se va a contratar tiene que ser del país en el que se va a robar, es decir, si tienen 2000 cuentas bancarias con sus correspondientes números de personas en España se contrata a un mulero en España.

Los anuncios suelen ofrecer un trabajo por horas sin mucha cualificación y ofrecen un buen dinero a cambio. Suelen plantear una situación en la que una empresa de otro país precisa de la ayuda de un “representante” para gestionar los cobros de sus clientes. Para ello nuestro flamante recién incorporado a la cola de ir a la cárcel solo debe abrirse una cuenta en el banco a su nombre en la que va a recibir “los pagos”. Una vez esté el dinero en la cuenta él debe sacarlo, quedarse con su comisión y enviar el resto por una empresa de envío de dinero a otros países.

Así la transferencia es, en nuestro ejemplo, de España a España reduciéndose el número de alarmas que se pueden disparar.

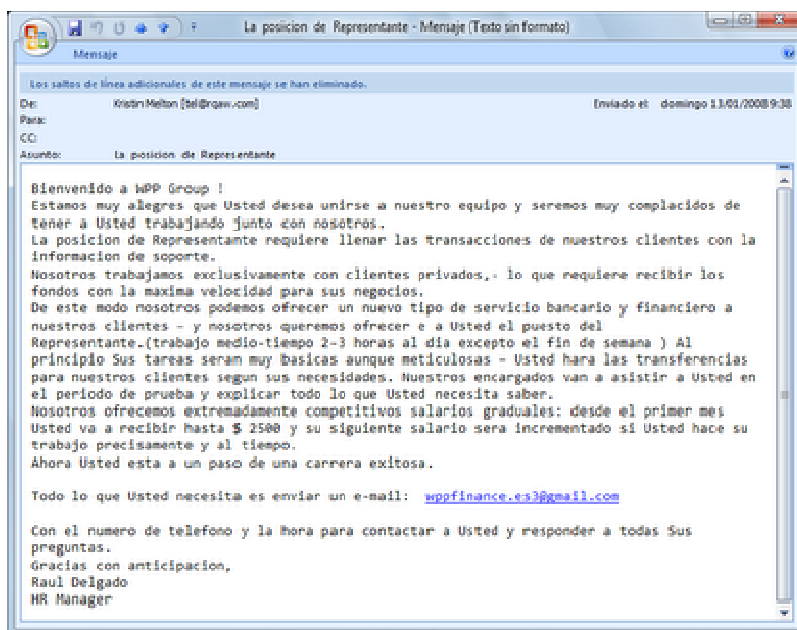


Imagen: Oferta de trabajo "Mulero"

Una vez el dinero esté en manos de la mafia, adiós muy buenas y los que han dejado todos los rastros han sido los equipos desde los que se envía el SPAM y desde los que se hacen las transferencias y los datos del mulero y ellos han permanecido en un completo anonimato.

El principio

Claro, como se puede ver, todo parte de tener máquinas controladas con troyanos. Troyanos que van a permitir robar los datos bancarios, tomar el control de la máquina para realizar las transferencias desde ella, mediante la instalación de servidores proxys en ella o directamente desde el control remoto de la máquina, troyanos para enviar el spam. Troyanos bancarios pero... ¿cómo se meten en el ordenador? Esa es la clave, evitar que se puedan meter en tu equipo. Para ello vamos a ver que podemos realizar para protegernos de ellos.

Más vale prevenir que curar

Una vez que un troyano se ha colado en tu equipo es posible que se oculte para toda herramienta informática instalada o que se vaya a instalar haciendo que su detección y eliminación sea más que un duro trabajo. Además, una vez introducido un troyano en tu máquina no hay garantía de que no se haya hecho nada más en el ordenador y que por tanto, tras el borrado del troyano, tu equipo se ha quedado totalmente limpio. Intenta por tanto no tener que buscar troyanos en tu equipo.

Para evitar tener problemas con los troyanos existen una serie de precauciones que se deben seguir. Ninguna es 100 % efectiva sin no se aplican todas y aún así, por desgracia, en este mundo cambiante en el que vivimos no se puede garantizar el 100 % de seguridad aún siguiéndolas pero sí se podrá reducir el riesgo.

Medidas de protección contra troyanos bancarios (III de VI)

<http://elladodelmal.blogspot.com/2008/10/medidas-de-proteccion-contr-troyanos.html>

Antivirus

Vivir peligrosamente porque se tiene un antivirus es igual suicida que vivir sin antivirus por el mero hecho de que los antivirus no puedan detectar todo. Esto es algo que las compañías de antivirus saben. No se puede detectar todo el malware ya que en todo caso se podría detectar el 100 % del malware conocido y esto siempre va a ser mucho menor que el malware existente. Hay que tener en cuenta que, aunque se utilicen “honey pots” [1] para intentar recoger la máxima cantidad de malware, hoy en día es tanta la cantidad que se hace difícil poder analizarlo todo, y aun así no hay garantía de que se haya obtenido el 100 % del malware existente.

Es fácil coger cualquier malware y subirlo a [Virus Total](#) y hacer algunas pruebas que demuestren esta afirmación. Virus Total es un servicio gratuito de análisis de malware que fue pionero en el mundo. Fue creado por Hispasec Sistemas, una empresa con base en Málaga y en Virus Total, el objetivo es poder ofrecer un informe de análisis de malware formado en la actualidad por los resultados de más de 30 motores de antivirus. Es fácil subir distintos troyanos bancarios y ver como ningún motor es capaz de detectar todos.



Virustotal es un [servicio de análisis de archivos sospechosos](#) que permite detectar virus, gusanos, troyanos, y malware en general. [Más información.](#)

Análisis del archivo **troyano.ex_** recibido el 26.03.2007 04:06:43 (CET)
Estado actual: **análisis terminado**
Resultado: **9/32 (28.12%)**

Imagen: Troyano Bancario sólo reconocido por 9 motores cuando llevaba un tiempo funcionando



Virustotal es un [servicio de análisis de archivos sospechosos](#) que permite detectar virus, gusanos, troyanos, y malware en general. [Más información.](#)

Análisis del archivo **troyano2.ex_** recibido el 02.02.2008 11:54:13 (CET)
Estado actual: **análisis terminado**
Resultado: **26/32 (81.25%)**

Imagen: Troyano Bancario casi un año después es detectado por 26 de 32 motores

Esta información no debe asustarnos, sino simplemente tener en cuenta que el uso de antivirus no es una garantía de seguridad total y que la ausencia de él es un riesgo aún mayor para la seguridad del equipo.

Además de tener antivirus, este debe estar funcionando en tiempo real, es decir, que escanee todos los archivos antes de que puedan ser ejecutados. Un antivirus parado que va a ser utilizado sólo para escaneos periódicos pierde gran parte de su efectividad.

Mutaciones

Uno de los principales problemas a la hora de detectar los troyanos bancarios es la enorme cantidad de mutaciones a las que son sometidos para evitar ser detectados. Así, un mismo troyano bancario, con el único objetivo de robar a un determinado conjunto de bancos, es reescrito n veces cambiando los códigos, las estructuras, las compilaciones, las compresiones utilizadas en los archivos ejecutables, etc... con el fin de que la firma generada por la compañía de antivirus no lo detecte. De hecho, se venden por internet troyanos 100 % indetectables a la carta.



VirusTotal es un [servicio de análisis de archivos sospechosos](#) que permite detectar virus, gusanos, troyanos, y malware en general. [Más información...](#)

Análisis del archivo `troyano2_mutado_pero_poco.ex` recibido el 03.02.2008
11:06:32 (CET)
Estado actual: **análisis terminado**
Resultado: **21/31 (67.75%)**

Imagen: Mismo troyano con ligera mutación (cambio de algunas cadenas ASCII de mayúsculas a minúsculas). Pasa a ser detectado por 21 de 31 motores.

Si vas a ejecutar un archivo en tu ordenador que procede de “algún sitio no confesable”, quiero decir, que te ha sido descargado de alguna web, o de alguna red P2P o que viene junto con alguna otra cosa, es una de las fuentes más peligrosas para coger una infección. Una buena idea puede ser enviar a analizar el archivo a Virus Total y que te de la opinión de los 30 motores de antivirus antes de “jugártela”. Para eso puedes usar el [Virus Total Uploader](#). Esta sencilla utilidad pone en el botón derecho del menú contextual del archivo una opción con la que con un simple clic se envía el archivo a Virus Total.

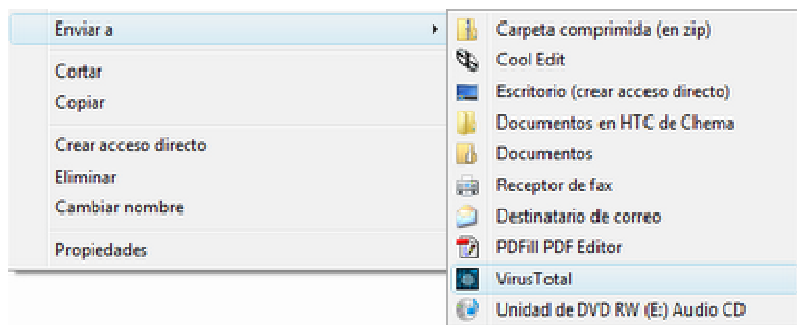


Imagen: Enviar a Virus Total con VTuploader

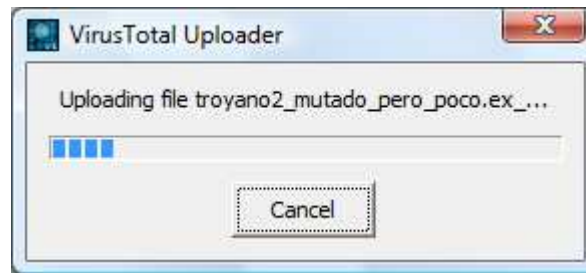


Imagen: Archivo siendo enviado a Virus Total

Antivirus estratégicos

No solo el antivirus de la máquina debe existir si estamos trabajando en una red corporativa. Una estrategia multinivel de antivirus ayudará a mitigar el impacto de los troyanos bancarios. Para ello hay que poner antivirus en el servidor de correo para evitar los troyanos que se difunden mediante cadenas de “cosas divertidas” o los que los usuarios se descargan “inocentemente” buscando “otras cosas” de servidores FTP o redes P2P por lo que también necesitaríamos configurar un Antivirus a nivel de red integrado en el firewall y que escanee todos los ficheros transmitidos por diversos protocolos. Una de las recomendaciones para subir el ratio de detección es utilizar diferentes motores de antivirus para subir el ratio de detección. Esta es una de las principales características por las que muchas empresas confían como antivirus de correo en Microsoft Forefront Security Server que integra hasta 9 motores de antivirus distintos para escanear el correo en los servidores.

Medidas de protección contra troyanos bancarios (IV de VI)

http://elladodelmal.blogspot.com/2008/10/medidas-de-proteccion-contra-troyanos_12.html

Software Actualizado

Si no es por las buenas... pues será por las malas. Conseguir que todos los usuarios “piquen” o sean “descuidados” en lo que ejecutan no es siempre posible. Muchos usuarios, temerosos de lo que pueda pasar hacen un uso “estable” del equipo, es decir, mejor no tocar lo que está funcionando así que evitan instalar cosas nuevas y “tocar nada”. Este uso “estable” es igual de peligroso pues para este tipo de usuarios se busca la infección mediante la detección de vulnerabilidades. Todo el software debe ser actualizado ya que periódicamente se van detectando fallos de seguridad. La primera recomendación es tener configuradas las opciones de actualizaciones automáticas dentro de tu PC. Esto reducirá el impacto que pueda tener una vulnerabilidad que permita a un atacante ejecutar código en tu máquina.

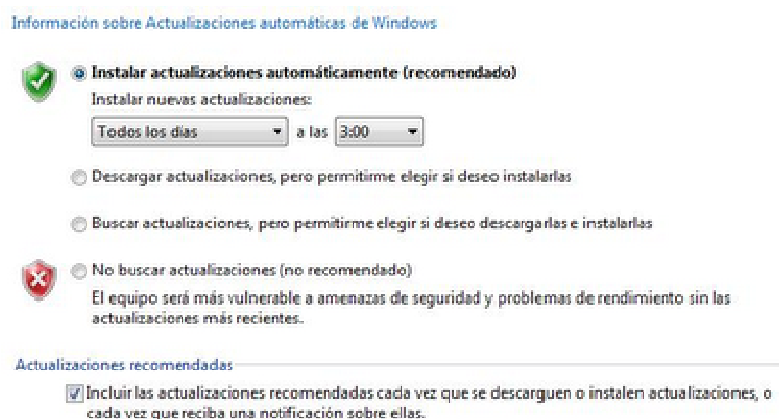


Imagen: Configuración de Windows Update en Windows Vista.

Esta opción actualiza todo el software del sistema operativo Windows, pero no programas de uso común en la plataforma como por ejemplo el plug-in de Flash para el navegador, el reproductor multimedia Winamp, el Adobe Acrobat Reader, la máquina virtual de Java, el reproductor Quick Time, el navegador de Internet Firefox, los codecs de divx, el compresor Winrar o cualquier otro software. Las empresas que desarrollan software intentan mantener un sistema de actualizaciones más o menos robusto, así, cuando, por ejemplo la Fundación Mozilla tiene una nueva actualización de Firefox te avisa de ello para que actualices tu versión. Igual hacen muchas otras empresas, pero no todas... Para ello es conveniente contar con alguna utilidad que chequee las versiones de tus productos instalados y te avise de cuáles de ellos deben ser actualizados y cuales están en un riesgo de seguridad. Existen varias utilidades que realizan estas funciones:

Secunia Personal Software Inspector

Esta es una herramienta muy completa para uso personal que actualmente se encuentra en RC3, es decir, a punto de ser versión final. Está disponible para descarga en la siguiente URL: [Secunia PSI](#). Es una herramienta que analiza el

equipo completamente para averiguar qué programas se encuentran instalados. Después comprueba si las versiones cuentan con fallos de seguridad conocidos que las hacen inseguras o no y que pueden ser utilizados para atacar el equipo. Para cada programa inseguro que deba ser actualizado se da una completa información técnica sobre cuál es el problema, cuál es la solución y dónde está la descarga. Muy cómo y sencillo para mantener el equipo actualizado y lejos de problemas innecesarios.



Imagen: Secunia Personal Software Inspector

La gente de Secunia cuenta también con una versión para redes que actualmente se encuentra en versión 2.0 y cuyo nombre es Network Secunia Software Inspector: [Secunia NSI](#). Por último, desde no hace mucho tiempo, está también disponible el servicio de escaneo Online llamado OSI (Online Software Inspector): [Secunia OSI](#)

Software Update Monitor (SUMO)

SUMO realiza las mismas acciones que PSI, está en version final y es software Libre con una versión descargable desde la siguiente URL:

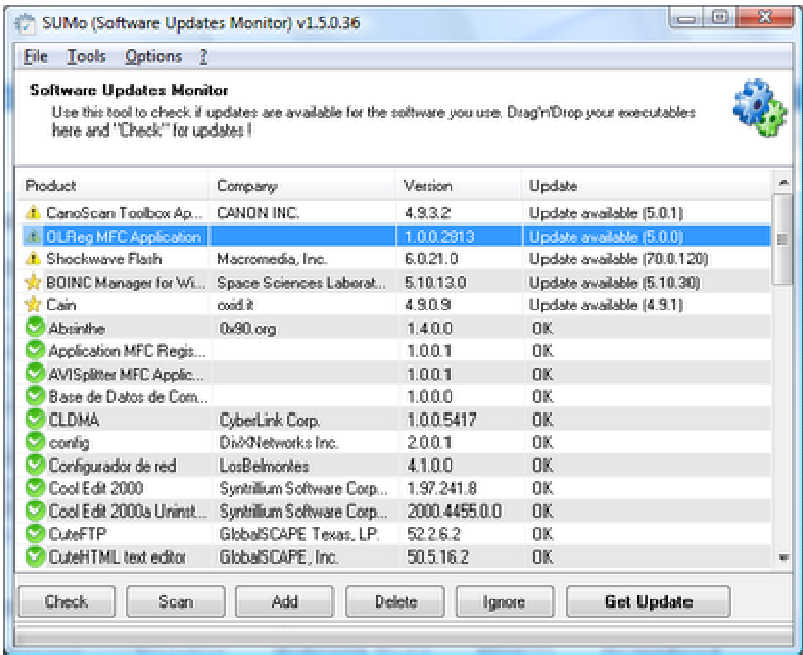
<http://www.kcsoftwares.com/index.php?sumo>

La herramienta avisa con una señal de peligro cuando la versión del software es insegura, con una estrella cuando no es insegura pero existe una versión más moderna y con una señal verde cuando el software está actualizado a la última versión.



Imagen: SUMO. Software Update Monitor

Como regla de oro, si una utilizad no la estás utilizando ni la vas a utilizar entonces quítala de tu sistema y reduce así la superficie de exposición de tu máquina.



Informe SUMO

Medidas de protección contra troyanos bancarios (V de VI)

http://elladodelmal.blogspot.com/2008/10/medidas-de-proteccion-contr-troyanos_18.html

Mínimo Privilegio Posible

Cuando salimos a la calle no solemos llevar todos nuestros ahorros encima por si acaso sucede algo. Bien, pues cuando salgas a Internet o vayas a trabajar con tu ordenador no lles todos tus privilegios encima. Esto es algo a lo que tenemos que acostumbrarnos. Si vas a escribir unos documentos con tu Microsoft Office o vas navegar un rato por Internet o vas manejar algún programa en tu ordenador... ¿por qué conectarse con un usuario administrador? La conexión con un usuario no administrador debe ser la forma normal de uso de tu equipo y única y exclusivamente debes conectarte como administrador cuando vayas a realizar una tarea de configuración del sistema.

Si aún así te has conectado como un usuario administrador porque es necesario para tu actividad normal, entonces debes navegar con un usuario no privilegiado porque en Internet no necesitas exponerte con todos tus privilegios. Si navegaras por una página que atacara una vulnerabilidad no conocida o no parcheada de tu navegador favorito el programita adquiriría automáticamente los privilegios de tu cuenta.

Para evitar esto, en las versiones de Windows XP existe la opción de “Ejecutar Como...”. Esto permite que antes de ejecutar el navegador elijas la cuenta de usuario que vas a utilizar para correr este programa. Para ello ten listo un usuario sin privilegios en tu sistema que utilices solo para navegar por Internet.

Windows Vista es un sistema operativo mucho más seguro y pensado desde cero en seguridad e incorpora una opción que se llama UAC (User Account Control) o “Control de Cuentas de Usuario”. Esta forma de trabajar con el sistema hace que, accedas al sistema con el usuario que accedas, todos los programas se ejecutan sin privilegios y si algún privilegio es necesario entonces el sistema solicita la autorización del sistema. Nunca otorgues ningún privilegio a ningún programa que desconozcas o que no sea una herramienta de administración de tu equipo.

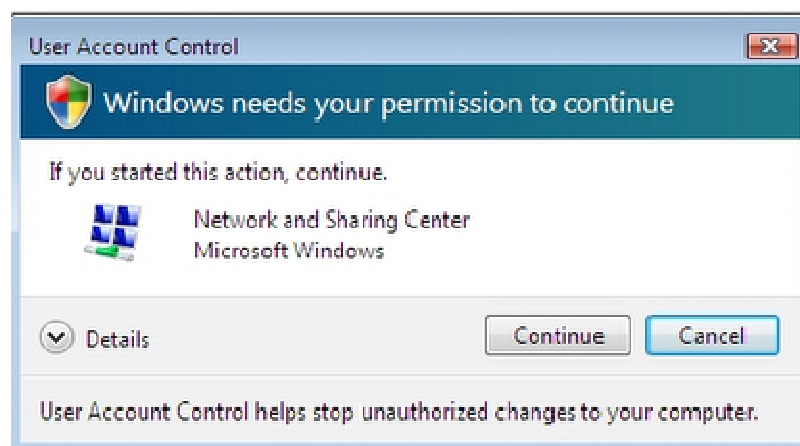


Imagen: UAC en gestión de redes

Fortifica tu navegador

Los navegadores de Internet cuentan con una amplia serie de opciones de seguridad. El uso apropiado de ellas ayuda a fortificar la seguridad y la entrada de troyanos por tu equipo. Configura el uso de bloqueo de pop-ups. Presta atención a las alertas de seguridad de certificados que da el servidor y no clasifica los sitios de confianza de tu equipo.

Internet Explorer 7 cuenta con una opción que se llama Modo Protegido. Esta opción del sistema hace uso de una característica que viene con Windows Vista y que se llama MIC (Mandatory Integrity Control). Cada proceso del sistema operativo se ejecuta con un nivel de Integridad, impidiendo que ningún proceso de nivel de integridad inferior pueda acceder a un proceso/objeto de nivel de integridad superior. Así, cuando el modo protegido está activado, ningún programa podrá acceder desde el navegador, por ejemplo, al sistema de ficheros sin autorización expresa y entrega de permisos por parte de un usuario.

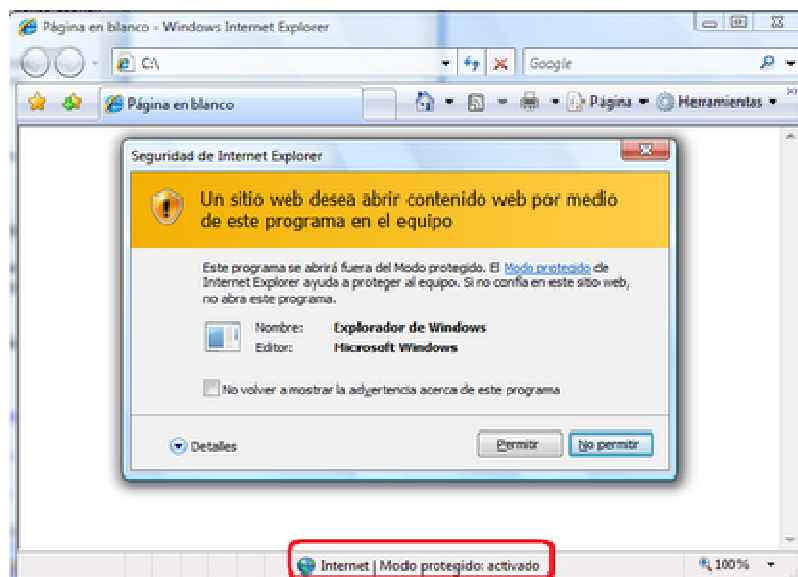


Imagen: Modo Protegido

Medidas de protección contra troyanos bancarios (VI de VI)

http://elladodelmal.blogspot.com/2008/10/medidas-de-proteccion-contra-troyanos_26.html

Zonas de Seguridad

El uso de las zonas de Seguridad en tu equipo permite que puedas permitir algunas opciones, como los comandos javascript, los objetos Applet, o los controles Activex sólo en sitios de confianza y no para todos los sitios que se visitan en Internet. Son muchas las veces en las que mediante el uso de técnicas de engaño con javascript, usando sistemas de publicidad atacados, lanzando exploits a través de lenguajes script o simplemente usando servidores comprometidos se infecta a los visitantes de una web.

Otra opción interesante que permite Internet Explorer es el aislamiento total de la navegación entre zonas no permitiendo que compartan navegador en las mismas pestañas. Esto permite un mayor aislamiento de las opciones de seguridad.

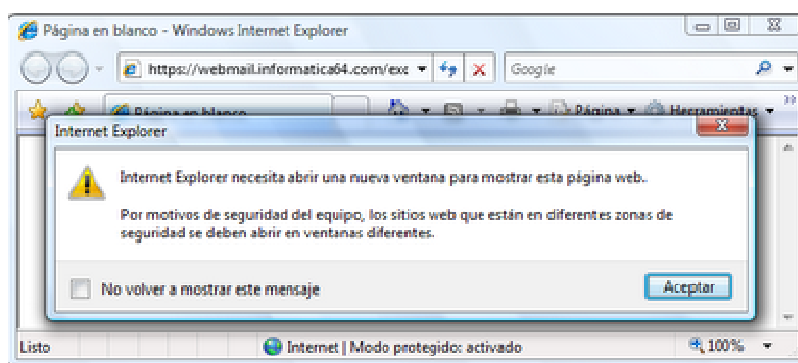


Imagen: Aislamiento de zonas de seguridad

Sitios Fraudulentos de Phishing

Muchos de los troyanos bancarios, aunque no los más modernos y avanzados, siguen utilizando sitios fraudulentos en servidores web para simular sitios bancarios. Para evitar que estos sitios engañen a los usuarios, cuando un nuevo servidor es contrastado como un sitio que realiza robo de datos bancarios las empresas de seguridad lo meten en bases de datos de sitios ilegítimos. Estas bases de datos son consultadas por los navegadores con filtros antiphishing para mostrar una alerta de seguridad severa cuando alguien accede a uno de estos sitios.

Además del filtro basado en consulta de bases de datos, Internet Explorer 7 realiza un análisis heurístico de la página mostrada al usuario por si contiene información superpuesta, textos escondidos o cualquier estructura utilizada comúnmente en ataques de fraude bancario con lo que saldrá un aviso de seguridad en el caso de que exista algo “extraño”.

Por último si cualquier usuario detecta un sitio fraudulento, por ejemplo, una web que representa a una entidad bancaria y que está en un dominio no perteneciente a esa entidad, se puede reportar como sitio de phishing. No es peligroso, pues antes de marcar ese sitio como de phishing los equipos de seguridad realizan una verificación para saber si es o no un sitio de fraude. Si se comprueba

que es un sitio ilegítimo pasará a formar parte de la base de datos y se procederá a intentar quitarlo.

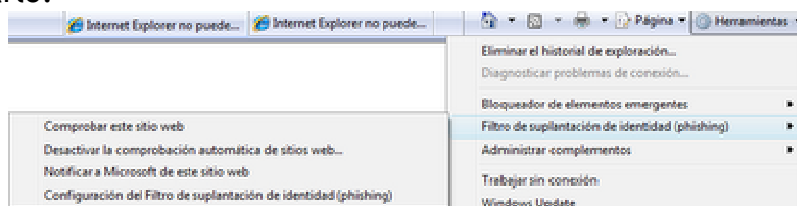


Imagen: Notificación de Sitio de Phishing. Paso 1.

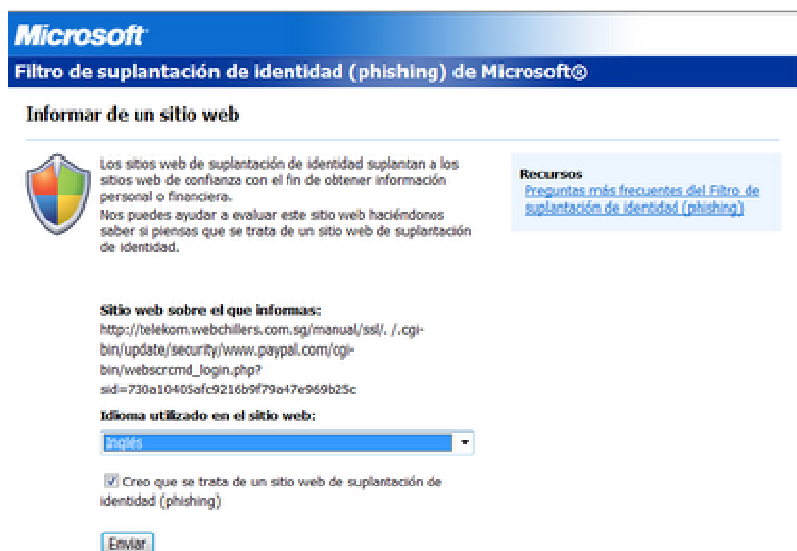


Imagen: Notificación de sitio de Phishing. Paso 2.

Recomendaciones Finales

Si el ordenador es compartido por varios miembros de la familia, que todos estén educados en las medidas de seguridad y que todos tengan mucho cuidado con lo que se ejecuta en cada máquina. Si tienes un ordenador nuevo con Vista, no le instales un Windows XP, las mafias conocen bien Windows XP y Windows Vista trae muchos controles de seguridad extras que les dificultan "su trabajo". Ellos estarán contentos si usas versiones antiguas de los navegadores de Internet, versiones antiguas de sistemas operativos o de cualquier software, así que actualiza.

Además, como recomendación añadida, procura fortificar tus buzones de correo. No sigas links desde el correo, activa las comprobaciones antispam que te filtren el máximo de correos maliciosos y ten el antivirus enchufado también al correo. El spam es uno de los motores en la distribución de troyanos bancarios, ya sea directamente, mediante referencias a webs que te van a intentar infectar, etc...

Estate siempre alerta, en cualquier rincón de una web, en cualquier esquina de un archivo, en cualquier trocito de link o en cualquier arhivito adjunto puede venir "el premio".

Por lo tanto, como dijo un día un amigo mío: **"Se rápido con la mente y lento con el doble clic"**.