Seguridad Informática

Versión 1.0

Dante Alighieri N 453 Villa Las Palmas Comuna de Maipú Santiago de Chile
Teléfono 09-397.26.01 E-Mail: **contactos@ucaisia.cl**

CONTROL DE VERSIONES

Versión	Fecha	Autor	Principales Cambios
1.0.	21/10/2007	Ulises Cáceres Rui-Perez	Versión original.

INDICE

INTRODUCCIÓN

Este documento ha sido creado con el objeto de entregar a la comunidad informática y a todos aquellos usuarios que les interese saber más de **¿Cómo?**, proteger de una manera eficiente y segura la información que contiene su computador.

Los enlaces son directos de aquellos que en la red proveen de información y de aquellos que se dedican a realizar productos para la seguridad informática.

La información de éste documento es una recopilación de nuestra empresa en casos reales y de documentación obtenida desde los muchísimos sitios que comentan sobre el tema.

Programa Espía

Los **programas espías** o **Spyware** son aplicaciones que recopilan información sobre una persona u organización sin su conocimiento. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas, pero también se han empleado en círculos legales para recopilar información contra sospechosos de delitos, como en el caso de la piratería de software. Además pueden servir para enviar a los usuarios a sitios de Internet que tienen la imagen corporativa de otros, con el objetivo de obtener información importante. Dado que el Spyware usa normalmente la conexión de una computadora a Internet para transmitir información, consume ancho de banda, con lo cual, puede verse afectada la velocidad de transferencia de datos entre dicha computadora y otra(s) conectada(s) a Internet.

Pueden tener acceso por ejemplo a: el correo electrónico y el password; dirección IP y DNS; teléfono, país; páginas que se visitan, qué tiempos se está en ellas y con qué frecuencia se regresa; qué software está instalado en el equipo y cuál se descarga; qué compras se hacen por Internet; tarjeta de crédito y cuentas de banco.

Los programas espía pueden ser instalados en un ordenador mediante un virus, un troyano que se distribuye por correo electrónico, como el programa Magic Lantern desarrollado por el FBI, o bien puede estar oculto en la instalación de un programa aparentemente inocuo.

Los programas de recolección de datos instalados con el conocimiento del usuario no son realmente programas espías si el usuario comprende plenamente qué datos están siendo recopilados y a quién se distribuyen.

Los cookies son archivos en los que almacena información sobre un usuario de Internet en su propio ordenador, y se suelen emplear para asignar a los visitantes de un sitio de Internet un número de identificación individual para su reconocimiento subsiguiente. La existencia de los cookies y su uso generalmente no están ocultos al usuario, quien puede desactivar el acceso a la información de los cookies; sin embargo, dado que un sitio Web puede emplear un identificador cookie para construir un perfil de un usuario y que dicho usuario éste no conoce la información que se añade a este perfil, se puede considerar al software que transmite información de las cookies, sin que el usuario consienta la respectiva transferencia, una forma de Spyware. Por ejemplo, una página con motor de búsqueda puede asignar un número de identificación individual al usuario la primera vez que visita la página, y puede almacenar todos sus términos de búsqueda en una base de datos con su número de identificación como clave en todas sus próximas visitas (hasta que el cookie expira o se borra). Estos datos pueden ser empleados para seleccionar los anuncios publicitarios que se mostrarán al usuario, o pueden ser transmitidos (legal o ilegalmente) a otros sitios u organizaciones.
Algunos ejemplos de programas espía conocidos son Gator, Bonzi Buddy, o Kazaa

Principales síntomas de infección

- Cambio de la página de inicio, la de error y búsqueda del navegador.
- Aparición de ventanas "pop-ups", incluso sin estar conectados y sin tener el navegador abierto, la mayoría de temas pornográficos y comerciales (por ejemplo, la salida al mercado de un nuevo producto).
- Barras de búsquedas de sitios como la de Alexa, Hotbar, MyWebSearch, FunWeb, etc.. que no se pueden eliminar.
- Creación de carpetas tanto en el directorio raíz, como en "Archivos de programas", "Documents and Settings" y "WINDOWS".
- Modificación de valores de registro.
- La navegación por la red se hace cada día más lenta, y con más problemas.
- Es notable que tarda más en iniciar el computador debido a la carga de cantidad de software Spyware que se inicia una vez alterado el registro a los fines de que el Spyware se active al iniciarse la computadora.
- Al hacer clic en un vínculo y el usuario retorna de nuevo a la misma página que el software espía hace aparecer.
- Botones que aparecen en la barra de herramientas del navegador y no se pueden quitar.
- Aparición de un mensaje de infección no propio del sistema, así como un enlace Web para descargar un supuesto antispyware.
- Al acceder a determinados sitios sobre el escritorio se oculta o bloquea tanto el panel de control como los iconos de programas.
- Denegación de servicios de correo y mensajería instantánea.

Programas Antiespías

Los antivirus más recientes son capaces de eliminar programas espía, como Norton, Kaspersky y Zone Alarm También hay programas especializados en eliminar o bloquear programas espía. Se recomienda no usar un solo programa antiespías sino una combinación de varios, dado que en muchas ocasiones uno de ellos detecta algunas cosas que no encuentran los otros, y viceversa, por lo que el uso combinado, de varios de ellos, ofrece una protección mucho más completa.

Antiespías gratuitos (para uso personal):
Anti-Espías Basados en Firmas:

- Spybot - Search & Destroy
- Ad-Aware
- **AVG Antispyware**
- **Spyware Doctor**
- **Spy Sweeper**
- **SUPERAntispyware**
- **Zone Alarm**
- **Windows Defender**
- **Panda Antivirus**
- **HijackThis**

Antimalwares sin Firmas:

- **Prevx**
- **CiberHawk Pro 2.0**
- **Primary Response Safeconect**

Inmunizadores (impide la instalación de Malware conocido):

- SpywareBlaster

Por otro lado, existen según Spyware warrior hasta 349 programas que se presentan como "antiespías" y en realidad no lo son. Algunos de ellos hacen lo contrario de lo que predican, instalan espías. Ver abajo, en enlaces externos, para una lista sobre estos programas sospechosos o no confiables que de ninguna manera deben instalarse en el computador.
Los Más populares son:

1. AdwareSheriff
2. Antispyware Soldier
3. Antivirus-Golden
4. AntiVermins
5. Error Safe
6. MalwareWiper
7. Perfect Codec
8. PestTrap
9. PSGuard
10. P.S.Guard
11. QualityCodec
12. Silver Codec
13. SpyAxe
14. SpyFalcon
15. Spy-Heal
16. SpyTrooper
17. SpySheriff
18. SpywareQuake
19. SpywareSheriff
20. SpywareStrike
21. SpywareHeal
22. SystemDoctor 2006 Free
23. Spyware Soft Stop
24. Super Codec
25. VirusBlast
26. Virus-Burst
27. VirusBurster
28. Video ActiveX Object
29. WinAntiVirus Pro 2006
30. Sin Espías

¿Qué es el Spyware?

Existe algo peor que los virus? Algo con un rango de acción más amplio y extendido por toda la Internet. Algo que no mata inmediatamente, pero que envenena poco a poco su PC.

Ya hemos hablado en otras ocasiones de él, pero nunca analizamos en profundidad el daño que hace. Es una enfermedad que se extiende como epidemia, que comienza a ralentizar su computadora, a hacerla perder funciones, a navegar más lento, a inhabilitar programas... hasta que lo fuerce a usted a formatear y reinstalar Windows periódicamente.
El villano invitado en esta historia es el **Spyware**.

¿Cuál es la naturaleza del Spyware?

El Spyware es software espía. Son programas que se instalan en su PC de modo automático o que vienen camuflados en la instalación de programas más respetables. En el primer caso, si usted ha navegado por páginas porno gratis, es común que las mismas instalen en su PC algún Spyware. Pero las páginas pornográficas no son las únicas que utilizan estos métodos. Portales de apariencia respetable también lo hacen. Y, en el segundo caso, es frecuente en los programas freeware que uno instala, que los mismos tengan algún componente espía. Sin ir más lejos, la versión Standard del **Kazaa** y otros programas de intercambios de archivos, los packs de emoticones para **MSN Messenger** y otros servicios de mensajería - que no sean los oficiales de **Microsoft**, por ejemplo -, bastantes programas aceleradores de downloads, juegos gratis, y en general todo caballo regalado que hay por Internet tiene un componente Spyware.

¿Cómo actúa el Spyware?

El software espía tiene básicamente dos métodos de acción :

- **forzar al usuario a ver determinadas cosas / utilizar determinados programas e interfases**
- **extraer información de la computadora del usuario**

El primer caso es el más evidente, pero no el menos dañino. Muchas páginas de descargas gratis fraudulentas instalan, por ejemplo, algún discador (*dialer*) en su computadora. Usted entra a un portal para bajar determinados archivos (ringtones, emoticones, etc.) y mientras navega, se instala subrepticiamente un software en su PC. Cuando llega a la sección donde realmente puede realizar la descarga del software que le interesa, **el dialer ya instalado "corta" su conexión a Internet (teóricamente) e inmediatamente disca un número de teléfono internacional para acceder a una Intranet (una Internet privada).** En los hechos, usted notará cierta demora en la navegación, pero no hay ningún indicio de que usted salió de Internet e ingresó a una red privada en otro país. Y mientras tanto, la cuenta de su teléfono corre...

Decimos teóricamente porque para que esta estafa funcione (en ningún momento el usuario sabe que en realidad está discando larga distancia, la Web no le advierte de esto), su conexión a Internet debería ser *dial up* (de discado por teléfono, tipo 56 KB), o si posee ADSL / Cable MODEM, al menos que su PC tuviera una línea de teléfono conectada (por ejemplo, gente que usa Internet por cable, pero que usa teléfono para enviar faxes desde la misma PC). **Debe haber un teléfono de línea conectado a la computadora como para que el dialer pueda hacer uso de él.**

Otra vía de acción del primer caso, son los programas que se instalan para modificar el funcionamiento habitual de **Windows**, el navegador **Explorer** u otros utilitarios vinculados a Internet. El **Internet Explorer** es la víctima boba y habitual de estas invasiones: **ya sea instalando una barra de búsqueda no deseada (Web Search, por ejemplo), o instalando programas que comienzan a lanzar popup (ventanas emergentes) de publicidad**. Si usted visita páginas reconocidas (**Google**, **Yahoo**), las mismas no tienen popup. Si a usted le aparecen cuando las navega, es porque en su computadora se ha instalado un Spyware (no es que dichas webs hayan comenzado con esa práctica o instalen software espía).

El segundo caso es verdaderamente espionaje electrónico. Un software espía se instala en su PC y comienza a mandar información hacia algún Server en especial. Esta información puede ser: leer las cookies de su navegación, monitorear y sacar estadísticas de qué páginas navega, analizar qué programas tiene usted en su PC e informarlos y así. Las cookies, recordemos, son pequeños archivos que muchos portales instalan en su computadora, y que es una práctica totalmente normal. Esos pequeños archivos memorizan cuándo estuvo el usuario en ese portal, recuerdan claves y logines, etc. Sin ir más lejos, cada vez que usted entra a **Hotmail** y aparece su nombre y password automáticamente cargados en la página de acceso, se debe a que la Web está leyendo una cookie que posee dichos datos y está en su PC. **Eso es normal y es razonable**. **Una cookie no es un programa espía.** Pero lo que sí hace un programa espía es leer cookies propias y ajenas, y despachar esa información por Internet a alguien que está esperando dichos datos para leerlos.

Acá es importante diferenciar entre software espía y una invasión de hacking. El software espía extrae información con fines puramente estadísticos - aunque nadie lo diga, es más que probable que **Microsoft** tenga un dispositivo de este tipo para, por ejemplo, tener una idea real de la base de instalaciones de **Windows** legales que existe en el mundo -. Esto sirve para hacer estudios de marketing, evaluar campañas publicitarias o analizar la base de visitantes de un portal / usuarios de un programa. **Es muy diferente a que un hacker acceda a su PC, saque la información de sus logines y claves, y se meta a usar sus casillas de correo o sus tarjetas de crédito**. Mientras que el software espía es estadístico y sus datos se acumulan con los de miles de otros usuarios, el ataque hacker es individual y tiende a explotar esa información para beneficio propio y abusar de servicios en su nombre. **Pero en ambos casos sigue siendo una invasión a la privacidad.**

El tema está en el grado de invasión que realiza el Spyware. Muchos software espías son realmente invisibles, salvo que usted haga una análisis pormenorizado de su computadora. Otros son mas toscos y evidentes, viendo algún ícono no deseado junto al de la conexión de Internet, o notando que su navegación se ha vuelto más lenta (claro, **hay otro usuario que está utilizando su PC al mismo tiempo que usted**). En algunos casos resulta hasta aceptable que haya un software espía instalado, si es el precio para poder utilizar otro programa mucho más útil. Un acelerador de descargas gratuito, por ejemplo, puede tener un software espía atachado - al cual no podemos inutilizar, porque también lo haríamos con el software de descargas -, pero son más las ventajas que las contras.

Otros software espía se instalan generalmente porque el usuario simplemente no lee las advertencias, o porque indican otra cosa que lo que realmente es. En el caso del **Kazaa Standard** (no el **Lite**, que es una versión depurada sin Spyware), cuando uno lo instala, la instalación común indica que van a ir agregados 4 o 5 programas adicionales que pueden no ser instalados. Pero como muchos usuarios no entienden inglés o no saben del alcance real de estos programas (**Web Search**, **Gator** que es un acelerador de descargas, aceleradores de navegaciones Web varias, etc.), instalan todo y después comienza el infierno de los popup y de la navegación a mitad de velocidad.

El verdadero problema del Spyware

El mayor problema del Spyware es que es aceptado. No está visto como dañino, a lo sumo como molesto. No es repudiado universalmente como los virus y, por tal motivo, no hay herramientas permanentes para prevenirlos. Hablando en términos reales, hoy en día hay que ser bastante idiota para que un virus le explote en la nariz. Teniendo un antivirus instalado que se actualice automáticamente por Internet (como el **AVG** o el **Norton**, por ejemplo), usted está cubierto en el 90% de los casos. El 10% restante responde a que usted sea de aquellos que abren todos los correos y todos los archivos atachados extraños, o bien que lo sorprenda un virus altamente dañino creado hoy, y que aún no haya actualización disponible de su antivirus para descargar. Y hablo de los usuarios domésticos, porque el panorama es diferente si hablamos de servidores de Internet, que son bombardeados permanentemente con los virus.

Pero, mientras que existen programas que custodian permanentemente nuestra PC de virus, no existe lo mismo para el Spyware. Usted puede instalar un *Firewall* para protegerlo de ataques hacker (como el **Zone Alarm**, que es gratis y recomiendo), y que puede detectar la mayoría de programas que intentan instalarse sin autorización en su PC, o bien si ya se han instalado, le advierte que intenta sacar datos hacia Internet. Pero no tienen el grado de monitoreo constante de un antivirus.

El mayor inconveniente del Spyware está en cómo se instala en su PC. En muchos casos es sumamente complejo o incluso imposible anularlos. Algunos Spyware poseen su propio desinstalador pero no está a la vista. Puede ir al **Panel de Control** de **Windows** y encontrarse en *"Agregar / Quitar Programas"* que hay software que simplemente usted nunca instaló, y ni siquiera encuentra un ícono en el escritorio o en la barra de inicio. Desde allí puede desinstalarlo. Y, en otros casos más graves, el software espía se disemina y actúa como un verdadero virus. **No destruye su PC ni datos, es cierto, pero cada vez que usted lo borra se vuelve a instalar.** En el caso de ciertas barras de búsqueda (**Web Search**) instalan un programa protegido en la carpeta **Temp** de **Windows**... que no se puede borrar - está protegido como sólo lectura, vive en memoria y se clona en el disco -. Es posible, en algunos casos, que usted deba examinar dicha barra (que se superpone a la del **Internet Explorer**), y encontrar, muy escondida, una opción de desinstalación, que generalmente llama a la Web del programa y le hace descargar un desinstalador - *que no siempre funciona* -. Entonces lo habitual es reiniciar la computadora en modo texto o **DOS**, ir a la carpeta donde se encuentra el archivo y borrarlo manualmente (con comandos **DOS**). Pero aún así, el daño está hecho.

El tema es que el software espía no es simplemente un programa que se instala en su PC. Es una garrapata que se prende en muchos lugares, principalmente en el registro de Windows, que es el núcleo del sistema operativo y que indica cómo deben funcionar los programas. Si usted, en el caso anterior, borró la barra **Web Search** a mano, puede que su **Internet Explorer** no se pueda ejecutar, emita mensajes de error o que funcione, pero no navegue.

El software Anti espía es un remedio que, a la larga, resulta tan dañino como el software espía. Ad Aware o **Spybot Search and Destroy** consiguen, en la mayoría de los casos, inutilizar al Spyware, pero a costa de *manosear* el registro de Windows. La primera desinfección estará OK, pero a medida que pase el tiempo y continúe desinfectando, su PC comenzará a tener problemas, específicamente **Windows** comenzará a mostrar errores y los programas no funcionarán como corresponde.

¿Cómo combatir al Spyware?

Hay una serie de reglas que pueden ayudarle a prolongar la vida útil de su sistema operativo. Ciertamente el Spyware es un fenómeno generalizado, nadie está exento de ello, y **es probable que cada año y medio o más - dependiendo de cuánto use Internet - deba reinstalar Windows desde cero en su PC**. Pero algunos consejos le permitirán dilatar este engorroso proceso:

- Primero, **no descargue programas en páginas desconocidas**, hágalo en portales de prestigio (**Download.com**, **Superarchivos.com.ar**, etc.). Las páginas desconocidas pueden instalarle dialers.
- Segundo, **no descargue packs de emoticones que no sean de Microsoft ni que figuren en otra Web que no sea la de Microsoft.com**
- Tercero, **instale un Firewall** como el **Zone Alarm**, el **Kerio**, el **Personal Firewall** u otros gratuitos, que le alertarán de intentos de egreso e ingreso de datos de su PC por otro que no sea usted
- Cuarto, si instala software, **instale solo el programa que le interesa, no instale programas adicionales gratis** (*bundle*) que pueda contener
- Quinto, **si ha detectado que hay software espía en su PC, identifíquelo e intente desinstalarlo normalmente como cualquier software**. Vaya en primer lugar al **Panel de Control / Agregar - Quitar Programas** y vea si puede quitarlo desde allí. De no ser así, busque y ejecute el programa espía, analícelo y vea si en el mismo programa hay una opción para desinstalar. Y, de no ser así, busque el nombre de dicho programa en **Google** u otro buscador. **Seguramente encontrará foros de usuarios molestos que le ha sucedido lo mismo que a usted, y le dirán las recetas de cómo borrar dichos archivos**.
- Sexto, **utilice como último recurso los programas anti Spyware como el Ad Aware o el Spybot Search and Destroy**. Le recomiendo el primero porque es muy fácil de utilizar y automático. Si se encuentra con una verdadera lacra aferrada a su sistema operativo, utilice el Spybot. Pero **recuerde siempre que estos programas a la larga terminan modificando el registro de Windows - no es culpa de ellos sino del Spyware; es como extraer un tumor maligno a costa de perder algún órgano - y es preferible utilizarlos lo menos posible (y desinstalar el Spyware por medios naturales como cualquier programa).**

Lista de antispyware sospechosos o no confiables

¿Qué son los parásitos?

Los "parásitos", son aplicaciones comerciales que se instalan en nuestra computadora, sin nuestro consentimiento, y sin ser solicitadas. Dentro de este tipo de código, podemos catalogar al Spyware (software que recoge información de nuestros hábitos de navegación, por ejemplo), y al Adware (agrega publicidad a los programas, generalmente como forma de pago por el uso del software).

Actualmente, existen numerosos productos que se encargan de limpiar los sistemas afectados por estos parásitos. Sin embargo, no todos ellos cumplen lo que prometen, o lo que es peor, muchos agregan a su vez programas espías o realizan modificaciones en el sistema que se supone deberían limpiar. Y por supuesto, sin siquiera advertir al usuario.

Muchos de estos productos, que son gratuitos, apelan a tácticas condenables, vendiéndose a patrocinantes inescrupulosos con la esperanza de sobrevivir (los menos), o de lucrar.

Y no nos referimos al clásico banner publicitario que aparece en algunos productos de uso gratuito, sino a verdaderos espías que una vez instalados recogen toda la información posible del usuario, incluyendo en ocasiones sus direcciones electrónicas, las que luego son empleadas para enviarle correo no solicitado.

Por otra parte, conocer los hábitos de navegación, puede servir para obligar al usuario a visitar sitios específicos que aparecen misteriosamente como páginas de inicio, o al realizar una búsqueda manipulada sin el conocimiento y por supuesto sin el consentimiento de la víctima.

También existen aquellos programas, que aunque no agregan software malicioso, pueden detectar Adware y Spyware que otros no han detectado, pero que solo pueden ser eliminados cuando pagamos por el producto. Lo sospechoso es que detecten cosas que otros productos no, o cosas que directamente no son consideradas Adwares o Spywares, dejando la duda de si no se tratará de inventos como parte de un inescrupuloso marketing de venta.

La siguiente es una lista actualizada de estos programas (al menos de los conocidos y comprobados), ninguno de los cuáles debería instalar o ejecutar en su computadora, si no desea correr el riesgo de, o bien infectarse con la misma basura que irónicamente muchos de ellos dicen quitar, o bien ser engañados por productos que mienten a la hora de detectar malwares (deliberadamente o no), para que el usuario termine comprándolos.

Productos Anti Spywares sospechosos o no confiables:

- #1 Spyware Killer
- 1 Click Spy Clean
- 100 Percent Anti-Spyware
- 1-2-3 Spyware Free
- 1stAntiVirus
- 2004 Adware/Spyware Remover & Blocker
- about:blank 2005
- AdDriller
- Ad-Eliminator
- Ad-Protect
- AdProtector
- Ad-Purge Adware & Spyware Remover
- ADS Adware Remover
- Ads Alert
- Advanced Spyware Remover
- Adware & Spyware Firewall
- Adware Agent
- Adware Cops
- Adware Filter
- Adware Finder
- Adware Hitman
- Adware Remover
- Adware Sheriff
- AdWare SpyWare Blocker & Removal
- Adware Striker
- Adware/Spyware Remover
- AdwareAlert
- AdwareBazooka
- AdwareDelete
- AdwareDeluxe
- AdwareHunter
- Adware-Nuker

- AdwarePatrol
- AdwarePro
- AdwarePunisher
- AdwareRemover
- AdwareSafe
- AdwareSafety
- AdwareSpy
- AdwareTools
- AdwareX
- AdwareX Eliminator
- Ad-Where 2005
- Agent Spyware
- AGuardDog Adware/Spyware Remover
- AlertSpy
- AlfaCleaner
- Anti Virus Pro
- Anti-Spyware Blocker
- AntiSpyware Soldier
- AntiSpyZone
- AntiVermins
- Antivirus Email
- AntiVirus Gold
- AntiVirus Golden
- AntiVirus Protector
- Antivirus Solution
- Anti-Virus&Spyware
- AntivirusPCSuite
- ArmorWall
- AVSystemCare
- BestGuardPlatinum
- Botsquash
- BPS Spyware & Adware Remover
- Brave Sentry
- CleanX
- CoffeeCup Spyware Remover
- Consumer Identity
- CyberDefender
- CheckFlow CheckSpy & Anti Spyware 2005
- Doctor Adware
- Doctor Adware Pro
- Doctor Alex
- eAcceleration/Veloz Stop-Sign
- Easy Erase Spyware Remover
- Easy SpyRemover
- Easy Spyware Killer
- Elimiware
- Emco Malware Bouncer
- ETD Security Scanner
- ExpertAntiVirus
- Flobo Free Anti Spyware Clean
- Freeze.com AntiSpyware
- Froggie Scan
- GarbageClean
- GoodbyeSpy
- GuardBar

- HitVirus
- IC Spyware Scanner
- Intelligent Spyware Cleaner
- Internet Cleanup
- InternetAntiSpy
- InternetShield
- iSpyKiller
- JC Spyware Remover & Adware Killer
- KaZaaP
- KillAllSpyware
- KillAndClean
- KillSpy
- Malware Stopper
- MalwareScanner
- MalwareWipe
- MalWhere
- Max Privacy Protector
- MaxNetShield (MNS Spyware Remover & History Eraser)
- MicroAntivirus
- MyNetProtector
- MyPCTuneUp
- MySpyFreePC
- MySpyProtector
- NeoSpace
- NetSpyProtector
- NoAdware
- NoSpyX
- Oxford Spyware Remover
- PAL Emergency Response
- PAL Spyware Remover
- PC AdWare SpyWare Removal
- PC Health Plan
- PCArmor
- pcOrion
- PerfectCleaner
- PestBot
- PestProtector
- PestTrap
- PestWiper
- Privacy Crusader
- Privacy Champion
- Privacy Defender
- Privacy Tools 2004
- Protect Your Identity
- PSGuard
- PurityScan /
- PuritySweep
- QuickCleaner
- RazeSpyware
- Real AdWareRemoverGold
- RegFreeze
- RemedyAntiSpy
- RemoveIT Pro
- Safe & Clean (Scan & Clean)
- SafeWebSurfer

- SamuraiSpy
- Scan & Repair Utilities 2006
- ScanSpyware
- Scumware-Remover
- SecureMyPC
- Security iGuard
- SlimShield
- SmartSecurity
- SpwareRemoval
- SpwareRemover
- Spy Annihilator
- Spy Crusher
- Spy Defence
- Spy Detector
- Spy Emergency 2005
- Spy Reaper
- Spy Sniper
- Spy Sniper Pro
- Spy Stalker
- Spy Striker
- Spy-Ad Exterminator Pro
- SpyAdvanced
- SpyAssassin
- SpyAssault
- SpyAway
- SpyAxe
- SpyBan
- SpyBeware
- SpyBlast
- Spy-Block
- SpyBlocs/eBlocs.com
- SpyBouncer
- SpyBurn
- SpyClean
- SpyCleaner
- SpyContra
- Spy-Control
- Spy Crush
- SpyCut
- SpyDawn
- SpyDeface
- SpyDeleter
- SpyDemolisher
- SpyDestroy Pro
- SpyEliminator
- SpyFalcon
- SpyFerret
- SpyFighter
- SpyFirewall
- SpyGuardian Pro
- SpyHeal
- SpyHunter
- SpyiBlock
- SpyiKiller
- Spyinator

- Spy-Kill
- SpyKiller
- SpyKiller 2005
- SpyKillerPro
- SpyLax
- SpyLocked
- SpyNoMore
- SpyOnThis
- Spy-Out
- SpyPry
- SpyRemover
- SpySheriff
- SpyShield
- Spy-Shield
- SpySoldier
- SpySpotter
- SpyToaster
- SpyTrooper
- SpyVampire
- SpyVest
- SpyViper
- Spyware & Adware Removal
- Spyware & Pest Remover
- Spyware & Pop-Up Utility
- Spyware Annihilator
- Spyware Blaster
- Spyware Bomber
- Spyware C.O.P.
- Spyware Cleaner
- Spyware Cleaner & Pop-Up Blocker
- Spyware Cops
- Spyware Defense
- Spyware Destroyer
- Spyware Detector
- Spyware Disinfector
- Spyware Immobilizer
- Spyware IT)
- SpyWare Killer
- Spyware Knight
- Spyware Medic
- Spyware Protection Pro
- Spyware Quake
- Spyware Removal Wizard
- Spyware Remover)
- Spyware Remover
- Spyware Remover
- Spyware Remover
- Spyware Scrapper
- SpyWare Secure
- Spyware Sheriff
- Spyware Shield
- Spyware Slayer
- Spyware Sledgehammer
- Spyware Snooper
- Spyware Soft Stop

- Spyware Stormer
- Spyware Striker Pro
- Spyware Suite 2005
- Spyware Terminator (invender .nl)
- Spyware Vanisher
- Spyware Wizard
- SpywareAssassin
- SpywareAvenger
- SpywareBeGone
- SpywareBot
- SpywareCleaner
- SpywareCrusher
- SpywareHospital
- SpywareHound
- SpywareKill
- SpywareKilla
- SpywareNo!
- SpywareNuker
- SpywareRemover
- Spyware-Stop
- SpywareStrike
- SpywareTek / Spyware Removal System
- SpywareThis
- SpywareXP
- SpywareZapper
- SpyWiper
- Spyzooka
- StartGuard
- StopGuard
- StopItBlockIt 2005
- Super Spyware Remover
- System Detective
- SystemStable
- TeoSoft Anti-Spyware
- Terminexor
- The Adware Hunter
- The SpyGuard (Adware Punisher)
- The Spyware Detective
- The Spyware Shield
- The Web Shield
- TheSpywareKiller
- Titan AntiSpyware
- TitanShield AntiSpyware
- Top10Reviews SpyScan
- True Sword
- TrueWatch
- Trust Cleaner
- TZ Spyware Adware Remover
- UControl
- Ultimate Cleaner
- Ultimate Defender
- Ultimate Spyware-Adware Remover
- UnSpyPC
- VBouncer/AdDestroyer
- VirusBlast

- VirusBurst
- VirusBursters
- VirusGuard
- VirusRescue
- WareOut Spyware Remover
- WebSafe Spyware Secure
- WinAntiSpy 2005
- WinAntiSpyware 2005
- WinAntiSpyware 2006
- WinAntivirus 2005
- WinAntiVirus 2006
- Wincleaner Antispyware
- Winhound Spyware Remover
- Winkeeper
- WinSOS
- WorldAntiSpy
- X-Con Spyware Destroyer
- Xmembytes AntiSpyware
- XoftSpy
- Xspyware
- X-Spyware
- XSRemover
- ZeroSpyware
- ZoneProtect Antispyware

NOTA sobre SpywareRemover se refiere al producto relacionado con los siguientes sitios: hijack-this.com, msantispy.com, microsoftantispyware.net, microsoftantispy.com, free-spybot.com, spy-bot.com)

NOTA sobre "Spyware Terminator" (spywareterminator.com, spyterm.com, crawler.com): Según informa el sitio Spyware Warrior (http://www.spywarewarrior.com/rogue_anti-spyware.htm#spyterm_note), Spyware Terminator fue sacado de la lista de programas sospechosos o no confiables, lista a la que ingresó por su conexión con IBIS, un conocido distribuidor de Adware, con productos como Wintools, Websearch, y Huntbar. La razón de quitarlo de la lista, es que la propia IBIS anunció oficialmente que dejaba el negocio del Adware (ver "IBIS Discontinues Distribution of Controversial WebSearch Toolbar", http://www.websearch.com/pr/pr_release.aspx). Esta decisión fue tomada luego de tres meses de prueba, para asegurarse que el programa Spyware Terminator no presentaba ninguna clase de problemas al usuario, y que por lo tanto, se trata de un programa recomendado. **NOTA: No confundir Spyware Terminator de Crawler.com (http://www.spywareterminator.com/), con Spyware Terminator 4 de Invender.nl, ni con Spyware X-terminator de Stompsoft.**

NOTA sobre Spyware Blaster: Spyware Blaster (spyware-blaster-software.com), es un antispyware que se vale maliciosamente del nombre de la utilidad legítima "SpywareBlaster" de Javacool, pero no tiene ninguna relación con dicho programa. La verdadera utilidad SpywareBlaster recomendada por VSAntivirus se puede encontrar en el siguiente enlace: "SpywareBlaster, previene la instalación de parásitos", http://www.vsantivirus.com/spywareblaster.htm

NOTA sobre "No-Spy / Sin-Espías" (http://www.sin-espias.com/): Según informa el sitio Spyware Warrior (http://www.spywarewarrior.com/rogue_anti-spyware.htm#no-spy_note), este antispyware fue incluido en esta lista debido a que la versión gratuita provocaba un falso positivo. Desde abril de 2005, fecha del lanzamiento de una nueva versión y de nuevas definiciones, este problema fue solucionado. Cómo en VSAntivirus solo publicamos el listado, y no agregamos los comentarios incluidos en la página original, resolvimos quitar dicho programa de la lista de Anti Spywares sospechosos o no confiables, después de haber testeado durante junio y julio de 2005 la versión gratuita de Sin-Espías (No-Spy) en nuestro propio laboratorio, y haber comprobado que efectivamente no existe ninguna razón para incluirlo aquí.

NOTA sobre SpywareBot: El sitio de SpywareBot explota el nombre del antispyware "Spybot Search & Destroy" (Search & Destroy Spyware and Adware today!), pero no tiene ninguna relación con éste programa.

Sitios relacionados con los Anti Spywares sospechosos o no confiables:

Esta lista de sitios Web, corresponde a los sitios oficiales de los productos no confiables o sospechosos indicados antes.

- 1clickspyclean.com
- 1clicksuite.net
- 1spywarekiller.com
- 1stantivirus.com
- 209.50.251.182
- 3bsoftware.com
- 66.79.171.75
- 6d-antivirus.com
- aboutblankremover.com
- actualresearch.com
- achtungachtung.com
- adaware.com
- ada-ware.com
- addriller.com
- ad-eliminator.com
- adeliminator.net
- adprotect.com
- adprotector.com
- adprotectplus.com
- adremovergold.com
- advancedsearchbar.com
- advertising.com
- adware.com
- adware .privacy-solution.com
- adware .storesbiz.com
- adwarealert.com
- adwarebazooka.com
- adwarecops.com
- adwaredelete.com
- adwaredeluxe.com
- adwarefilter.com
- adwarefinder.com
- adwarehitman.com
- adwarehunter.com
- adwarepatrol.com
- adwarepro.com

- adwareprotectionsite.com
- adwarepunisher.com
- adware-remover.net
- adwareremover.ws
- adwareremovergold.com
- adwaresafe.com
- adwaresafety.com
- adwaresheriff.com
- adwaresoft.com
- adwarespy.com
- adwarespyware.net
- adwarespywareremoval.com
- adwarestriker.com
- adwaretools.com
- adwarexeliminator.com
- ad-where.com
- affiliatesuccess.net
- agentspyware.com
- aguarddog.com
- aladdinsys.com
- alertspy.com
- alfacleaner.com
- aluriasoftware.com
- alwaysfreealways.com
- allume.com
- anonymizer.com
- antispylab.com
- antispynow.com
- antispywarebox.com
- anti-spyware-review.com
- antispywaresoldier.com
- antispyzone.com
- antivermins.com
- antivirus-email.com
- anti-viruses.net
- anti-viruses.net
- antivirus-gold.com
- antivirusgolden.com
- antiviruspcsuite.com
- antiviruspremium.com
- anti-virus-pro.com
- antivirusprotectionsite.com
- antivirusprotector.com
- armor2net.com
- ascentive.com
- athivision.com
- avsystemcare.com
- bestguardplatinum.com
- botsquash.com
- bravesentry.com
- browser-page.com
- bulletproofsoft.com
- cashunlim.com
- cdmworldsoftware.com
- certified-safe-downloads.com

- cleanx.co.kr
- clickspring.net
- coffeecup.com
- consumeridentity.com
- cosmi.com
- cyberdefender.com
- cyber-defender.com
- checkflow.com
- checkforspyware.com/sc/
- checkspy.com
- doctoradware.com
- doctoradwarepro.com
- doctor-alex.com
- dreamenstudio.com
- eacceleration.com
- eanthology.net
- easyerase.com
- easyspyremover.com
- easyspywarekiller.com
- eblocs.com
- elimiware.com
- emco.is
- engagemarketing.com
- enigmasoftwaregroup.com
- esunsofttechnologies.com
- etdscanner.com
- etrust-spyware.com
- expertantivirus.com
- fastlink2.com
- floborecovery.com
- flyyasoft.com
- freepcscan.com
- free-spybot.com
- free-spyware-scan.com
- freespywarescan.org
- freeze.com
- genericscanner.com
- goggle.com
- gsiconcepts.com
- guardbar.com
- guardwall.com
- halt-spyware.com
- haltspyware.info
- healthycomputerclub.com
- hijack-this.com
- hijack-this.net
- hitvirus.com
- hotwinupdates.com
- idownload.com
- incodesolutions.com
- inicom.dk
- innovagest2000.com
- interesoft.com
- internetantispy.com
- internetshield.com

- invender.nl
- ispykiller.com
- jcspyware-remover.com
- jeanharris.com
- kazaap.org
- killallspyware.com
- killandclean.com
- killercash.com
- killersoftware.com
- killspy.net
- logiguard.com
- mailwiper.com
- mainstreamdollars.com
- malwarepanacea.com
- malware-stopper.com
- malwarewipe.com
- malwhere.com
- maximumsoftware.com
- maxionsoftware.com
- maxnetshield.com
- maxprivacyprotector.com
- maxtheater.com
- microantivirus.com
- microantivirusxp.com
- microsoftantispy.com
- microsoftantispyware.net
- mntolympus.org
- msantispy.com
- mynetprotector.com
- mypctuneup.com
- myspyfreepc.com
- myspyprotector.com
- myspywarecleaner.com/sc/
- myspywarescan.com
- neosoftlabs.com
- neospacelab.com
- netspyprotector.com
- networkdynamicscorp.com
- noadware.biz
- no-adware.com
- noadware.net
- no-adware.net
- no-spy-ware.com
- nospyware.info
- nospyx.com
- nuker.com
- onlinepcfix.com
- oreware.com
- oxfordspywareremover.com
- palsol.biz
- palsol.com
- palsol.net
- paretologic.com
- pcadwareremoval.com
- pcarmor.net

- pcorion.com
- pcprivacysoftware.com
- pcsafe.com
- pcsecurityshield.com
- pcspytool.com
- pchealthplan.com
- perfect-cleaner.com
- pestbot.com
- pestprotector.com
- pesttrap.com
- pestwiper.com
- pest-wiper.com
- pimasoft.com
- platinumparter.com
- platinumpartner.com
- privacycash.com
- privacychampion.com
- privacytools2004.com
- professionalcash.com
- protectorsuite.com
- psguard.com
- purityscan.com
- puritysweep.com
- qspyware.com
- quickcleaner.com
- razespyware.com
- razespyware.net
- rebrandsoftware.com
- redemptionengine.com
- redv.net
- registry-doctor.com
- remedyantispy.com
- rizalsoftware.com
- rosecitysoftware.com
- safer-networking.com
- safewebsurfer.com
- samuraispy.com
- scanandclean.com
- scanandrepair.com
- scanspyware.net
- scosoft.com
- scumware-remover.org
- securemywindows.com
- securetactics.com
- securityiguard.com
- securitystronghold.com
- shareware4web.com
- sheriffcash.com
- shootspyware.com
- slimshield.com
- smartestsearch.com
- smartpctools.com)
- smart-security .info
- softbulldog.com
- softdd.com

- softsky.com.ua
- software4yoursuccess.com
- softwareoasis.cc
- softwareonline.com
- softwareprofit.com
- solidlabs.com
- spy .storebiz4u.com
- spyadvanced.com
- spyassassin.com
- spyassault.com
- spy-away.com
- spyaxe.com
- spyban.net
- spybeware.com
- spyblast.com
- spybloc.com
- spy-block.com
- spyblocs.com
- spy-bot.com
- spybot-spyware-removal.com
- spybouncer.com
- spyburn.palsol.biz
- spyclean.com
- spycleaner.net
- spycleaner-gold.com
- spycontra.com
- spy-control.com
- spycrush.com
- spy-crusher.com
- spycut.com
- spydawn.com
- spydeface.com
- spydefence.com
- spydeleter.com
- spydemolisher.com
- spydestroy.com
- spydetector.net
- spy-emergency.com
- spyfalcon.com
- spyferret.com
- spyfighter.com
- spyfirewall.com
- spyheal.com
- spyiblock.com
- spyikiller.com
- spyinator.com
- spy-kill.com
- spykiller.com
- spy-killer.com
- spykillerdownload.com
- spykillerpro.com
- spylocked.com
- spynomore.com
- spyonthis.net
- spy-out.com

- spyout.net
- spypry.com
- spyreaper.com
- spysheriff.com
- spy-sheriff.com
- spy-shield.com
- spyshield.org
- spysniper.net
- spysoldier.com
- spyspotter.com
- spystalker.com
- spystriker.com
- spytoaster.com
- spytrooper.com
- spy-trooper.com
- spyvampire.com
- spyvest.com
- spyviper.com (SpyViper)
- spywarealert.com
- spywareassassin.com
- spywareavenger.com
- spyware-b1aster-software.com
- spywarebegone.com
- spywareboard.com
- spywarebomber.com
- spywarebot.com
- spyware-cash.com
- spywarecleanerdownload2.com
- spyware-cop.com
- spywarecops.com
- spywarecrusher.com
- spywarecure.net
- spywaredefense.com
- spyware-destroyer.com
- spywaredetector.net
- spywaredisinfector.com
- spywaredollars.com
- spywarehospital.com
- spywarehound.com
- spywareit.com
- spywarekill.com
- spywarekilla.com
- spywarekiller.net
- spywareknight.com
- spywarelabs.com
- spywareno.com
- spywarenuker.com
- spyware-pest-remover.com
- spywarequake.com
- spywarequake.info
- spyware-removal.net
- spywareremoval.ws
- spywareremovalwizard.com
- spywareremove.com
- spywareremover.com

- spy-ware-remover.com
- spywarescrapper.com
- spyware-secure.com
- spywaresheriff.com
- spywaresledgehammer.com
- spywaresnooper.com
- spywaresoftstop.com
- spywarespy.com
- spyware-stop.com
- spywarestormer.com
- spywarestrike.com
- spywaretek.com
- spywarethis.com
- spywarevanisher.com
- spyware-wiper.com
- spywarewizard.com
- spywarexp.com
- spywarezapper.com
- spyxpress.com (SpyViper)
- spyzooka.com
- startguard.net
- stingware.com
- stopguard.com
- stopitblockit.com
- stop-sign.com
- surfertools.com
- swanksoft.com
- synergeticsoft.com
- systemdetective.com
- systemstable.com
- tekeffect.com
- teocash.com
- teosoft.biz
- teosoft.com
- terminexor.com
- theadwarehunter.com
- thespyguard.com
- thespywaredetective.com
- thespywarekiller.com
- thespywareshield.com
- titanantispyware.com
- titanshield.com
- topantispy.com
- topdownloads.net
- topics-ent.com
- toptenreviews.com
- trackzapper.com
- trekblue.com
- trekdata.com
- truesuite.com
- trustcleaner.com
- udefender.com
- ultimatecleaner.com
- uninstallxupiter.com
- unspypc.com

- untdd.com
- vantagesoftware.com
- veloz.com
- virtualbouncer.com
- virusblast.com
- virusburst.com
- virusguard.com
- virusrescue.com
- virusscansite.com
- wareout.com
- webalias.com/spybot
- websafesecure.com
- websoftsecure.com
- whenu.com
- winantispy.com
- winantispyware.com
- winantivirus.com
- wincleaner.com
- winhound.com
- winkeeper.net
- winsoftware.com
- winsos.com
- worldantispy.com
- x-conspywaredestroyer.com
- xmembytes.com
- xp67.com
- x-spyware.com
- xspyware.net
- xsremover.com
- xtremeinnovations.net
- your-soft.com
- zendmedia.com
- zeroads.com
- zerospyware.com
- zoneprotect.com
- zzztech.com

Sitios de Anti Spywares sospechosos o no confiables:

En los últimos años, a medida que los problemas con el spyware y el Adware han empezado a hacerse más notorios, han surgido varios sitios Web para proporcionar información e incluso recomendar ciertos programas anti spyware. Pero la mayoría de estos sitios no son confiables como guías para defendernos del spyware.

Especialmente malos son aquellos que pretenden hacer revisiones de programas anti spyware, alegando hacer un análisis "objetivo", cuando en realidad empujan al usuario a utilizar muchos de los productos anti Spywares sospechosos o no confiables que se listan arriba. En realidad, muchos de estos webs están afiliados con los productos que ellos dicen examinar y luego recomiendan. La mayor parte de estos sitios incluso se anuncian de forma bastante agresiva en Google, como usted mismo puede ver cada vez que hace una búsqueda por algún tema relacionado.

- ✓ 2004spywareremovers.com
- ✓ 2dollarfix.com
- ✓ 5spynetwork.com
- ✓ add-aware.com
- ✓ adwarereport.com
- ✓ adware-spyware-review.com
- ✓ antispyware .neonant.com
- ✓ anti-spyware-review
- ✓ Anti-Spyware-Review.com
- ✓ anti-spyware-reviews.net
- ✓ bewareadware.com
- ✓ compareeasy.com
- ✓ CompareSpywareRemoval.com
- ✓ CompareSpywareRemovers.com
- ✓ compu3.com/spyware .html
- ✓ download-spybot.com
- ✓ e-Spyware.com
- ✓ likesurfing.com
- ✓ mambomarket.com
- ✓ megalithusa.com
- ✓ merign.org
- ✓ noadware.com
- ✓ nontoxic-internet.com
- ✓ no-spybot.com
- ✓ online-survival-lab.com
- ✓ pcspyremover.com
- ✓ privacysoftwarereport.com
- ✓ radownload.com
- ✓ RateSpywareRemovers.com
- ✓ removespyware.com
- ✓ removespyware.ru
- ✓ revieweasy.com/spy/
- ✓ safespy.net
- ✓ scanner .altmaster.net
- ✓ sdspybot.com
- ✓ spyads.com
- ✓ spybot.com
- ✓ spybot.net
- ✓ spybot.org
- ✓ spybot-spyware.com
- ✓ spy-deleter.com
- ✓ spyforce.com
- ✓ spyhunter.com
- ✓ spy-hunter-detector.com
- ✓ spy-review.com
- ✓ spysoftcentral.com
- ✓ spyware .1000recursos.com
- ✓ spyware.com-rr.com
- ✓ spyware .junglebee.com
- ✓ spyware.net
- ✓ spyware .speedylearning.com
- ✓ spyware-adware-download.com
- ✓ spyware-adware-removal.net
- ✓ spywarealert.com
- ✓ spywareblaster.com

- ✓ spyware-blaster-software.com
- ✓ spywarehelp.net
- ✓ spywarehub.com
- ✓ SpywareInfoooo.com
- ✓ spywareonline.org
- ✓ spyware-removal.blogspot.com
- ✓ spywareremoval.ec-force.com
- ✓ SpywareRemovalAuthority.com
- ✓ spywareremovalutilities.com
- ✓ spywareremove.org
- ✓ SpywareRemoverComparisons.com
- ✓ spyware-removers.org
- ✓ spywareremovers/
- ✓ SpywareRemoversReview.com
- ✓ spywarereview.info
- ✓ spywarescanreview.com
- ✓ spyware-spybot.net
- ✓ successalert.com
- ✓ teslaplus.com
- ✓ theshopontop.com/
- ✓ the-spyware-review.com
- ✓ the-spyware-zone.com
- ✓ topspywareremovers.com
- ✓ toptenreviews.com
- ✓ Trojan-Scan.com

NOTA sobre Spywareblaster.com: SPYWAREBLASTER.com es un sitio que se vale maliciosamente del nombre de la utilidad legítima "SpywareBlaster" de Javacool, pero no tiene ninguna relación con dicho programa. La verdadera utilidad SpywareBlaster recomendada por VSAntivirus se puede encontrar en el siguiente enlace: "SpywareBlaster, previene la instalación de parásitos", http://www.vsantivirus.com/spywareblaster.htm

Programas aconsejados:

Ad-aware
http://www.lavasoft.de/spanish/default.shtml
Pest Patrol
http://www.ca.com/products/pestpatrol/
Spybot Search & Destroy
http://spybot.safer-networking.de/es/index.html
Webroot Spy Sweeper
http://www.webroot.com/es/index.php
Windows Defender (Beta 2) (ex Microsoft AntiSpyware).
Ver "NOTA sobre Windows Defender (Beta 2) (ex Microsoft AntiSpyware)"
http://www.microsoft.com/athome/security/spyware/software/default.mspx
Ver también "Parásitos en nuestra computadora",
http://www.vsantivirus.com/ev-parasitos.htm

Complemento aconsejado:

SpywareBlaster, previene la instalación de parásitos
http://www.vsantivirus.com/spywareblaster.htm

Sobre NOD32

NOD32, el antivirus de ESET distribuido por VSAntivirus en Uruguay, posee la certificación de Checkmark sobre Spyware, por lo que los usuarios de este antivirus están doblemente protegidos (contra toda amenaza viral y también contra Spywares). Más información:

NOD32 consigue la nueva certificación de Checkmark
http://www.vsantivirus.com/nod32-checkmark.htm
Eset lanza la nueva versión de NOD32 en español
http://www.vsantivirus.com/nod32-250.htm
Sobre NOD32 y descargas de evaluación:
http://www.vsantivirus.com/nod32.htm
http://www.nod32.com.uy/

NOTA sobre Windows Defender (Beta 2) (ex Microsoft Antispyware)
La versión beta actual ha resuelto los problemas que ocurrían cuando se intentaba instalar sobre versiones de Windows que no fueran en inglés (incluidas versiones en español de Windows).

Ver el siguiente artículo para más información:
Mensaje de error cuando se intenta instalar Beta 2 de Defensor de Windows:" Error 1609." Se produjo un error hasta aplicar configuración de seguridad. "Usuario no es un usuario o un grupo válidos."

http://support.microsoft.com/?kbid=915087

Fuente: Spyware Warrior

http://www.spywarewarrior.com/rogue_anti-spyware.htm

Malware

Malware (del inglés ***mal****icious* ***soft****ware*, también llamado **badware** o **software malicioso**) es un software que tiene como objetivo infiltrarse en o dañar un computador sin el conocimiento de su dueño y con finalidades muy diversas ya que en esta categoría encontramos desde un troyano hasta un spyware.

Y si bien puede instalarse a través de algún correo electrónico, lo puede hacer a través de una página falsa que se enlaza desde el buscador.

Esta expresión es un término general muy utilizado por profesionales de la computación para definir una variedad de softwares o programas de códigos hostiles e intrusivos.

Muchos usuarios de computadores no están aún familiarizados con este término y otros incluso nunca lo han utilizado. Sin embargo, la expresión "virus informático" es más utilizada en el lenguaje cotidiano y a menudo en los medios de comunicación para describir todos los tipos de malware.

Se debe considerar que el ataque a la vulnerabilidad por malware, puede ser a una aplicación, una computadora, un sistema operativo o una red.

Existen varios factores que hacen a un sistema más vulnerable:

- Homogeneidad - Cuando todas las computadoras en una red funcionan con el mismo sistema operativo, si pueden corromper ese SO, podrán afectar cualquier computadora que lo corra.
- Defectos - la mayoría de los sistemas contienen errores que se pueden dañar por el malware, mientras no se ponga el parche correspondiente.
- Código sin confirmar - un código en un diskette, en CD-ROM o USB, se puede ejecutar sin la responsabilidad del usuario.
- Sobre-privilegios del usuario - algunos sistemas permiten que todos los usuarios modifiquen sus estructuras internas.
- Sobre-privilegios del código - la mayoría de los sistemas operativos permiten que el código sea ejecutado por un usuario con todos los derechos.

Una causa no citada de la vulnerabilidad de redes, es la homogeneidad del software multiusuario. En particular, Microsoft Windows tiene una gran parte del mercado que al concentrarse en él permitirá a crackers derribar una gran cantidad de sistemas.

La mayoría de los sistemas contienen los Bugs (insectos) que pueden ser aprovechados por el malware. Los ejemplos típicos son los buffer, en los cuales un interfaz diseñado para almacenar datos en un área pequeña de la memoria permite que sea ocupada y después sobrescriben sus estructuras internas. Esto puede ser utilizado por el malware para forzar al sistema a ejecutar su código.

Originalmente, las PC tenían que ser booteadas (iniciadas) con un floppy diskette, y hasta hace poco tiempo era común que fuera el dispositivo de arranque por default. Esto significó que un diskette corrupto podría dañar la computadora durante el booting, e igual se aplica a CDs. Aunque eso es menos común ahora, sigue siendo posible olvidarse de que el equipo se inicia por default, en un medio removible.

En algunos sistemas, los usuarios no-administradores son sobre-privilegiados por diseño, en el sentido que se les permite modificar las estructuras internas del sistema.

En algunos ambientes, los usuarios son sobre-privilegiados porque les han concedido privilegios inadecuados de administrador o el estado equivalente. Éste es sobre todo una decisión de la configuración, pero en los sistemas de Microsoft Windows la configuración por default es sobre-privilegiar al usuario.

Esta situación existe debido a las decisiones tomadas por Microsoft para priorizar la compatibilidad con viejos sistemas sobre la necesidad de una nueva configuración de seguridad y porque las aplicaciones típicas fueron desarrollados sin tomar en cuenta a los usuarios sin privilegios.

Consecuentemente, muchas aplicaciones existentes que requieren exceso de privilegio (código sobre-privilegiado) pueden tener problemas con la compatibilidad con Vista.

Sin embargo, la característica del control de la cuenta del usuario de Vista procura remediar las aplicaciones no diseñados para los usuarios no privilegiados, actuando como apoyo para resolver el problema del acceso privilegiado inherente en las aplicaciones legales.

Los Malware, funcionando como código sobre-privilegiado, pueden utilizar estos privilegios para cambiar el sistema. Casi todos los sistemas operativos populares, y también muchas aplicaciones escritas no prohíben algunos códigos también con muchos privilegios, generalmente en el sentido que cuando un usuario ejecuta el código, el sistema no prohíbe a ese código los derechos de usuario.

Esto hace a usuarios vulnerables al malware en la forma de anexos de E-mail, que pueden o no pueden ser disfrazados. Dado esta situación, se advierte a los usuarios que abran solamente los archivos en que confían, y ser cuidadosos de códigos recibido de fuentes desconocidas.

Es también común para los sistemas operativos que sean diseñados de modo que reconozcan más dispositivos de los diversos fabricantes y cuenten con sus drivers de estos hardwares, aun algunos que pueden no ser muy confiables.

Existen muchísimos tipos de malware, aunque algunos de los más comunes son los virus informáticos, los gusanos, los troyanos, los programas de spyware/adware o incluso los bots.

Dos tipos comunes de malware son los *virus* y los *gusanos* informáticos, este tipo de programas tienen en común la capacidad para auto replicarse, es decir, pueden contaminar con copias de sí mismo que en algunas ocasiones ya han mutado, la diferencia entre un gusano y un virus informático radica en que el gusano opera de forma más o menos independiente a otros archivos, mientras que el virus depende de un portador para poderse replicar.

Los virus informáticos utilizan una variedad de portadores. Los blancos comunes son los archivos ejecutables que son parte de las aplicaciones, los documentos que contienen macros, y los sectores de arranque de los discos de 3,1/2 pulgadas. En el caso de los archivos ejecutables, la rutina de infección se produce cuando el código infectado es ejecutado, originando al mismo tiempo el código del virus. Normalmente la aplicación infectada funciona correctamente. Algunos virus sobrescriben otros programas con copias de ellos mismos, el contagio entre computadoras se efectúa cuando el software o el documento infectado van de una computadora a otra y es ejecutado.

Cuando un software produce perdidas económicas en el usuario del equipo también se clasifica como **software criminal o Crimeware**, término dado por Peter Cassidy, para diferenciarlo de los otros tipos de software malignos, en que estos programas son encaminados al aspecto financiero, la suplantación de personalidad y el espionaje utilizando la llamada Ingeniería social (seguridad informática), que es conseguir la información confidencial del propio usuario al identificar sus pulsaciones en el teclado o los movimientos del ratón o creando falsas páginas de bancos o empresas de contratación y empleo para con ello conseguir número de cuenta e identificaciones, registros oficiales y datos personales con el objetivo de hacer fraudes o mal uso de la información.

Adware

Este software muestra o baja anuncios publicitarios que aparecen inesperadamente en el equipo, pudiendo hacerlo simultáneamente a cuando se esta utilizando la conexión a una pagina Web o después de que se ha instalado en la memoria de la computadora.

Algunas empresas ofrecen software "gratuito" a cambio de publicitarse en su pantalla y puede ser que al instalar un programa, le instale un Spyware sin que lo note.

También existen programas a prueba shareware que mientras no son pagados, no permiten algunas opciones como puede ser imprimir o guardar y además en ocasiones cuentan con patrocinios temporales que al recibir la clave libera de tales mensajes publicitarios y complementan al programa.

Backdoor

Una puerta trasera (también conocidos como *Backdoor*) es un software que permite el acceso al sistema de la computadora ignorando los procedimientos normales de autenticación o facilita la entrada a la información de un usuario sin su permiso o conocimiento. Según como trabajan e infectan a otros equipos, existen dos tipos de puertas traseras. El primer grupo se asemeja a los caballos de Troya, es decir, son manualmente insertados dentro de algún otro software, ejecutados por el software contaminado e infecta al sistema para poder ser instalado permanentemente. El segundo grupo funciona de manera parecida a un gusano informático, el cuál es ejecutado como un procedimiento de inicialización del sistema y normalmente infecta por medio de gusanos que lo llevan como carga.

Badware Alcalinos

Este es un tipo de Malware mitad spyware, mitad Backdoor, suele residir en las ventanas del sistema observando incesantemente hasta que se echa al acecho de un usuario.

Bomba Fork

Programa que se auto réplica velozmente para ocupar toda la memoria y capacidad de proceso del computador donde se ejecutan, debido a que su forma de ataque es del tipo Denial of service (DoS) que es un ataque al servidor o a la red de computadoras para producir la inconectibilidad a una red debido a que consume el ancho de banda atacado, al crear programas y procesos simultáneos muy rápidamente, saturando el espacio disponible e impidiendo que se creen procesos reales del usuario.

Bots

Es un programa robot, que se encarga de realizar funciones rutinarias, pero que también creaban cuentas en los diferentes sitios que otorgan e-mailes gratuitos, para con estas cuentas realizar daños.

En algunos casos este bot, puede encargarse de fingir ser un humano dando contestación a preguntas como es el caso de supuestos adivinos que dan el futuro a aquellos que pagan por este servicio o fingir ser una mujer u hombre con quien se esta teniendo una candente platica, pero también son juegos de Internet programados para jugar contra supuestamente una serie de contrincantes que lo son en forma virtual, pudiendo pedir cantidades de dinero para poder participar y con ello además poder tener datos de cuentas de tarjetas de crédito.

También son programas que a través de órdenes enviadas desde otra computadora controlan el equipo personal de quien quiere afectar, es decir robotizándola.

Bug

Es todo error en la programación, que impiden funcionar bien a los equipos de cómputo, se le llama así por la entrada de una polilla encontrada atrapada entre los puntos en el relé # 70, panel F, de la Mark II , Construida por Aiken, cuando era probada en la Universidad de Harvard, el 9 de septiembre de 1945.

Se dice que fue Grace Murray Hopper, quien identificó a la polilla dando el término Bug (anglicismo que significa error o fallo en un programa o sistema), cuando ella trabajaba en el equipo de programación de la marina, escribió en su cuaderno de trabajo: "moth in relay, First Actual case of bug being found" (polilla en relé, primer caso real de insecto encontrado). Puso la palabra "debugging" a computer program es decir, de que "habían eliminado errores del programa de cómputo" y anexo al insecto.

Caballo de Troya

Un **programa caballo de Troya** (también llamado Troyano) es una pieza de software dañino disfrazado de software legítimo. Los caballos de Troya no son capaces de replicarse por sí mismos y pueden ser adjuntados con cualquier tipo de software por un programador o puede contaminar a los equipos por medio del engaño.

Su nombre es equívoco y dado en alusión al popular caballo de madera con que los aqueos (griegos) engañaron a los troyanos. De modo similar actúa este software entrando en la computadora, oculto en otros programas aparentemente útiles e inofensivos pero que al activarse crean problemas al desarrollar la acción de estos archivos infecciosos. Debería llamarse "griego".

Se considera que el primer troyano aparece a finales de los 80s, pero eran poco comunes al ser necesario que el programa se distribuyera casi manualmente, fue hasta que se generalizó la comunicación por Internet, que se hizo más común y peligroso al entrar ocultos e instalarse cuidadosamente sin que se percatara el usuario del equipo, con lo que se han considerado una de las más temibles invasiones ilegales en las estaciones de trabajo, servidores y computadoras personales, que toman el control de estos equipos, y los dañan tanto físicamente como económicamente al espiar y robar información o contribuyen a la descarga e instalación de programas que desencadenan una amplia variedad de software malicioso de sus sitios Web.

Cookies


Es el tipo de almacenamiento de información guardado en el propio equipo que puede hacer normalmente el seguimiento de las preferencias en Internet, dándole una clave que su creador podrá identificar para con ello tener una referencia de visitas en ocasiones con la finalidad de medir preferencias de mercado. Pero también por lo mismo puede ser usada por hackers para chequear qué páginas consulta un usuario regularmente quitándole intimidad. Estas cookies se pueden aceptar o evitar en nuestros equipos, por medio de la configuración de la carpeta de privacidad de las opciones de Internet.

Crackers

Además de referirse a hackers con malas intenciones, son programas que monitorean las contraseñas en las aplicaciones de la máquina. Se conocen también como ladrones de contraseñas.

Cryptovirus Ransomware o Secuestradores

Es el programa que entra a la computadora y cifra los archivos del disco duro, pidiendo que se envié el pago vía Internet (rescate) para obtener la clave de dicha codificación (la liberación del rehén).

Dialers

Los dialers son programas que llaman a un número de larga distancia, para a través de su módem entrar con o sin su consentimiento principalmente a páginas de juegos o pornográficas.

Exploit o Xploit

Un Exploit es aquel software que ataca una vulnerabilidad particular de un sistema operativo. Los Exploits no son necesariamente maliciosos –son generalmente creados por investigadores de seguridad informática para demostrar que existe una vulnerabilidad. Y por esto son componentes comunes de los programas maliciosos como los gusanos informáticos.

Hijacker

Programa que realiza cambios en la configuración de la página de inicio del navegador, que lo redirige a otra de características indeseables como son las pornográficas y más peligrosamente a copias casi fieles de las bancarias.

Hoaxes, Jokes o Bulos

Son bromas que semejan ser virus, pero que, ciertamente no los son. Normalmente una persona conocida nuestra recibe una “alarma” de un supuesto virus y nos hace el favor de notificarnos para que tomemos precauciones en nuestro equipo.

El objetivo de la persona que inició el rumor o hoax se ha cumplido, al preocupar al usuario con la broma y que, en muchos casos, pueden hacer al usuario auto eliminar el supuesto archivo contaminado y cual podría afectar realmente al funcionamiento del sistema.

Keystroke o Keyloggers

Son programas espías, enviados por medio de troyanos que radicados en un computador, monitorea el sistema, registrando las pulsaciones del teclado, para robar las claves y passwords en páginas financieras y correos electrónicos del equipo utilizado para saber lo que la víctima hizo, y enviarle de forma periódica, dicha información al cracker creador, por medio de un archivo o por Internet al sitio del servidor Web, previamente establecido para el robo de dicha información.

Pueden ser también aparatos o dispositivos electrónicos colocados intencionalmente en equipos públicos o en carátulas de cajeros automáticos que copian la banda magnética de la tarjeta de crédito y copian el password pulsado en el teclado con lo que se realizará la estafa.

Ladilla Virtual

Conocido como (virtual crab). Este tipo de programa maligno que, como analogía al parásito de transmisión sexual, entra en una computadora a través del sexo virtual, sitios pornográficos o cualquier aplicación relacionada. Los sitios Web pornográficos suelen ser un gran caldo de cultivo para estos Malwares virtuales.

Leapfrog

Las ranas como también se conocen en español son programas que entran a los equipos para conocer las claves de acceso y las cuentas de correo almacenadas para ser utilizadas en la replicación de estos.

Parásito Informático

Este tipo de malware es el que se adhieren a archivos (especialmente ejecutables), como lo haría un parásito. Ese archivo ejecutable es denominado portador (o Host) y el parasito lo utiliza para propagarse. Si el programa es ejecutado, lo primero que se ejecuta es el parasito informático y luego, para no levantar sospechas, se ejecuta el programa original. Muchas veces es aquí donde los parásitos fallan, porque hay programas que detectan estas modificaciones y lanzan errores (incluso errores de advertencias de presencia de Malware).

Pharming

Es el software maligno que suplanta al DNS, en el Host local, para conducirnos a una página Web falsa, con lo cual al intentar entrar en nuestro navegador a un determinado nombre de dominio nos redirección al que el hacker, ha cambiado.

Por ejemplo la página de un banco como pudiera ser www.banco.com (xxx.156.24.196), nos lo cambia por www.ban**ka**.com (YYY.132.30.60), con lo que al parecerse, no nos percatamos normalmente que nos esta enviando a otra página controlada por el bandido cibernético.

Para poder instalarnos en la página que realizara el direccionamiento, se instalará en nuestro sistema algunos programas malware ejecutables, que recibimos a través de un correo electrónico o descargas por Internet.

Siendo en este momento el más común el envió de una supuesta tarjeta de Gusanito.com, que al entrar en el vinculo contenido en el correo electrónico, no solo nos da la sorpresa de la tarjeta, sino que, ha realizado la descarga correspondiente que se encargara de auto ejecutarse creando el Host que redirecciona nuestro navegador a las IP de las paginas falsas administradas por el hacker.

Phishings

Del inglés "fishing" (pescando), se utiliza para identificar la acción fraudulenta de conseguir información confidencial, vía correo electrónico o página Web, con el propósito de que los usuarios de cuentas bancarias lo contesten, o entren a páginas aparentemente iguales a la del banco o de los portales con ingreso por contraseña.

El phishing se basa en el envío por parte de un estafador de un mensaje electrónico o enlace de una empresa supuestamente respetable.

Éstas a menudo conducen a una página Web falsificada que han creado, y te engañan para que introduzcas tu contraseña y tu información personal.

Así te convierten en un blanco fácil del robo de información personal o financiera de manera electrónica utilizando el nombre de un tercero (banco) y últimamente las páginas del acceso al e-mails de compañías como Yahoo¡.

Nunca dé información de sus cuentas bancarias por otros medios que no sean en las sucursales correspondientes a su banco, ya que, por medio de correos electrónicos con enlaces supuestamente del banco le pueden solicitar sus números de cuentas y contraseña, con lo que les está dando todo para que puedan cometer el fraude.

El método de entrar a las páginas Web de los diferentes Bancos de algunos países, es usando el generador de claves dinámicas de las compañías Secure Computing y el RSA SecurID, con lo que se espera terminar con los Phishing.

Por lo tanto, ahora el ataque de los pescadores de datos (fishing), es pidiéndole que sincronice su generador de claves, con lo que inmediatamente entran a la cuenta del usuario sacando lo que puedan y cambiando hasta las claves de acceso.

También Yahoo nos da protección por medio de la creación del llamado sello de acceso personalizado, que consiste en colocar una imagen o texto, el cual debe aparecer cada vez que se inicie sesión en Yahoo, en la computadora en que se ha colocado, púes se vincula a ella y no al usuario del correo.

Si el sello de acceso **NO** está, es probable que sea una página falsificada creada por un estafador para robar los datos personales.

Pornware

Describe programas que usan el MODEM de la computadora para conectarse a servicios de pago por evento pornográfico o para bajar contenidos pornográficos de la Web. Es un caso particular de Dialers.

Es un auténtico fraude mediante información engañosa, manifiestan que es completamente gratuito, el sitio a visitar es en efecto sin costo, pero solo se tiene acceso por vía telefónica (MODEM), que resulta con una alta tarifa por minuto que se refleja en el recibo telefónico (por lo regular utilizan una clave de larga distancia internacional (900) con un cargo aproximado de $20.00 USD por minuto). Esta técnica fraudulenta se utiliza también usando como señuelo videojuegos, salva pantallas, programas o cualquier otra falacia que requiera acceso mediante un MODEM telefónico.

Primero se descarga desde algún sitio que ofrece todo absolutamente gratis un pequeño programa ejecutable, que coloca en el escritorio de la PC un llamativo ícono para que cualquier incauto con un simple clic haga el enlace mencionado, aparecen insistentes mensajes sugiriendo de que todo es completamente gratis y sin límite de tiempo.

Sin embargo, se están extinguiendo por dejarse de lado los Modems convencionales de 56Kbps y usarse Tarifas Planas en Red Ethernet de Banda ancha o ADSL

Rabbit o Conejos

Reciben este nombre algunos gusanos informáticos, cuyos códigos malignos llenan el disco duro con sus reproducciones en muy poco tiempo y que también pueden saturar el ancho de banda de una red rápidamente.

Riskware

Programas originales, como las herramientas de administración remota, que contienen agujeros usados por los crackers para realizar acciones dañinas.

Rootkit

Los rootkit son programas que son insertados en una computadora después de que algún atacante ha ganado el control de un sistema. Los rootkit generalmente incluyen funciones para ocultar los rastros del ataque, como es borrar los Logs de entradas o encubrir los procesos del atacante. Los rootkit pueden incluir puertas traseras, permitiendo al atacante obtener de nuevo acceso al sistema o también pueden incluir exploits para atacar otros sistemas y evitan ser desinstalados o eliminados a toda costa, pues cuenta con protección para no permitirlo, con lo cual se convierte en un programa indeseable y molesto.

Scumware o Escoria

Scumware o escoria es cualquier software que hace cambios significativos en la apariencia y funciones de las páginas Web sin permiso del Administrador (Webmaster) o propietarios. Por ejemplo, un número de productos sobreponen la publicidad de los banners con otros anuncios, a veces para los productos de la competencia. El Scumware puede agregar híper links desautorizados a la sección opinión de una página Web - a veces usar de un usuario acoplamientos a los sitios posiblemente desagradables. Tales programas pueden interferir con hipervínculos (híper links) existentes agregando otros destinos a los previstos. A veces, el Scumware es conocido como thiefware.

Spam

Se le llama a los e-mailes basura, que son mandados a direcciones electrónicas compradas por empresas con la finalidad de vender sus productos. Últimamente han surgido páginas con mensajes que aparecen en un corto instante de tiempo (efecto *flash*) tratando de producir en el inconsciente de la mente la necesidad de comprar el producto anunciado como si de un mensaje subliminal se tratara.

Spyware

Los Spywares o Programa espía, son aplicaciones que se dedican a recopilar información del sistema en el que se encuentran instaladas para luego enviarla a través de Internet, generalmente a alguna empresa de publicidad. Todas estas acciones se enmascaran tras confusas autorizaciones al instalar terceros programas, por lo que rara vez el usuario es consciente de ello. Normalmente trabajan y contaminan sistemas como lo hacen los caballos de Troya.

Ventanas Emergentes / POP-UPS

Son ventanas muy molestas que normalmente aparecen al navegar y muestran publicidad o información que es difícil de eliminar y que aparece constantemente.

Son una forma en línea de publicidad en el World Wide Web, que aumentan el tráfico de la red o que son también usadas para capturar direcciones del e-mail. Trabaja cuando ciertos sitios abren una ventana del buscador para exhibir los anuncios.

La ventana pop-up que contiene un anuncio es generada normalmente por JavaScript, pero se puede generar por otros medios también.

Una variante en las ventanas pop-up es hacer aparecer el anuncio debajo de la ventana activa, con lo cual el usuario no se percata cuando surge, sino hasta que cierra su navegación, con lo que difícilmente puede identificar junto a que página surgió, sobre todo en aquellas sesiones en que se tienen varios documentos abiertos.

Worms o Gusanos

Los **gusanos** informáticos son similares a los virus, pero los gusanos no dependen de archivos portadores para poder contaminar otros sistemas. Estos pueden modificar el sistema operativo con el fin de auto ejecutarse como parte del proceso de inicialización del sistema. Para contaminar otros sistemas, los gusanos explotan vulnerabilidades del objetivo o utilizan algún tipo de ingeniería social para engañar a los usuarios y poderse ejecutar.

Métodos de Protección

- Utilizar una cuenta de usuario con pocos privilegios (no administrador) en su equipo, solo utilizar la cuenta de administrador cuándo se deba cambiar una configuración o instalar un software de confianza. De todas maneras, se debe ser cauteloso con lo que se ejecuta.
- Cada vez que se transfiera un archivo desde o hacia Internet se debe tener la precaución de revisarlo contra virus, crimeware o malwares, pero lo más importante saber de dónde proviene.
- Se debe comprobar todos y cada uno de los medios magnéticos (Diskettes, ya en desuso), soportes ópticos (CDs, DVD, Blueray) o tarjetas de memoria (SD, MMC, XD, compact Flash), que se introduzcan en el ordenador.

- Comprobar los archivos comprimidos (ZIP, RAR, ACE, CAB, 7z..).
- Hacer copias de respaldo de programas y documentos importantes, podrías guardarlos en un Pendrive, CD, DVD, entre otros medios externos.
- No instalar programas de dudoso origen.
- Evita navegar por sitios potencialmente dañinos buscando cosas como "pornografía gratis", "programas gratis", "mp3 gratis", claves, licencias o cracks para los programas comerciales (existen alternativas gratis).
- Evita descargar programas, archivos comprimidos o ejecutables, desde redes peer-to-peer ya que no sabes el real contenido de la descarga.
- Mantener actualizado tu sistema operativo. Por ejemplo si usas Windows XP, no se te olvide tener el Service Pack 2 instalado y también las posteriores actualizaciones.
- Tener un programa antivirus y firewall llamados también cortafuegos instalados en tu computador, así como también anti-espías.
- También es importante tener actualizados estos programas, ya que, cada día aparecen nuevas amenazas.
- Desactivar la interpretación de Visual Basic VBS y permitir JavaScript JS, ActiveX y cookies sólo en páginas Web de confianza.
- Usar preferentemente navegadores como Opera o Firefox entre otros.
- Seguir las políticas de seguridad de éste documento
- Por último, también puedes probar alternativas diferentes como sistema operativo, tales como alguna distribución de GNU/Linux.

Referencias

Cuidado con algunas de estas referencias.

1. vulnerabilidad de Windows por Marcos González
2. John von Neumann, "Theory of Self-Reproducing Automata", Part 1: Transcripts of lectures given at the University of Illinois, Dec. 1949, Editor: A. W. Burks, University of Illinois, USA, 1966.
3. congreso sobre seguridad en la UNAM
4. Peter Cassidy
5. publicidad en Internet
6. cita del acontecimiento
7. Las 7 cosas a saber de los creadores de virus
8. IP irreal del banco
9. IP falso que seria el del hacker
10. Secure Computing,
11. RSA SecurID
12. Sello de acceso de Yahoo¡
13. http://www.networkworld.com/newsletters/sec/2002/01331360.html/
14. compañía espía
15. medidas básicas con Windows XP
16. navegador opera
17. mozilla firefox
18. documento de políticas de seguridad de la información [14]
19. Linux

Enlaces Externos

Información sobre Malware por Symantec

Información de las páginas de las Compañías de Antivirus []

Avast
AVG Free Advisor
Avira AntiVir
Bit Defender
Central Command
Command Antivirus
Computer Associates
Corydoranetworks
F-Secure
Grisoft
Kaspersky
Mcafee
Neosecurity
NOD32
Norman
Norton
OpenAntivirus (GNU)
Panda security
PC Cillin
Redhat
Sophos
Sybari
Trend Micro
Hacking & Security Latin Team

Véase También

Heurística

Heurísticas en antivirus

Los productos antivirus suelen tener técnicas de reconocimiento inteligente de códigos maliciosos (virus, gusanos, caballos de Troya, etc.), las cuales se conocen comúnmente bajo el nombre de heurísticas. El término general implica funcionalidades como detección a través de firmas genéricas, reconocimiento del código compilado, desensamblado, desempaquetamiento, entre otros. Su importancia radica en el hecho de ser la única defensa posible frente a la aparición de nuevos códigos maliciosos de los cuales no se posean firmas.

Técnicas Heurísticas

Firmas Genéricas

Muchos códigos maliciosos son modificados en forma constante por sus autores para crear nuevas versiones. Usualmente, estas variantes contienen similitudes con los originales, lo cual se denomina como una familia de virus. Gracias a las similitudes dentro del código del virus, los antivirus pueden llegar a reconocer a todos los miembros de la misma familia a través de una única firma o vacuna genérica. Esto permite que al momento de aparecer una nueva versión de un virus ya conocido, aquellos antivirus que implementan esta técnica puedan detectarlo sin la necesidad de una actualización.

Reconocimiento de código compilado

Cuando un programa es compilado para poder convertirlo en un archivo ejecutable, la codificación resultante representa instrucciones que se le darán al sistema para realizar ciertas acciones. Las implementaciones de heurística de algunos antivirus utilizan técnicas para reconocer instrucciones comúnmente aplicadas por los códigos maliciosos, y así poder identificar si un archivo ejecutable puede llegar a ser un código malicioso.

Desensamblado

Todo archivo ejecutable puede ser desensamblado con el objetivo de obtener el código fuente del programa en lenguaje ensamblador. La heurística de algunos productos antivirus es capaz de analizar el código fuente de los programas sospechosos con el fin de reconocer en él técnicas de desarrollo que normalmente sean usadas por los programadores de virus y así reconocer un código malicioso nuevo sin la necesidad de una actualización.

Desempaquetamiento

Los programadores de códigos maliciosos suelen usar empaquetadores de archivos con el fin de modificar la "apariencia" del virus a los ojos del análisis antivirus. Empaquetadores como UPX, son ampliamente utilizados para esto. Para evitar ser engañados por un código malicioso antiguo, reempaquetado, los antivirus incluyen en sus técnicas heurísticas métodos de desempaquetamiento con el fin de poder analizar el código real del programa, y no el empaquetado.

Evaluaciones Retrospectivas

La Heurística es un aspecto muy difícil de probar en los productos antivirus, dado que se requiere realizar las denominadas evaluaciones retrospectivas.

¿Qué son las Evaluaciones Retrospectivas?

Para poder analizar correctamente el funcionamiento de las capacidades heurísticas o *proactivas* de un antivirus, lo que se hace es detener la actualización de firmas del producto durante un período de tiempo **X**. En ese lapso, se acumulan muestras de códigos maliciosos nuevos, para que una vez recolectada una cantidad suficiente, se analice si los productos antivirus las reconocen o no. Al no haber sido actualizados para detectar esas muestras, el antivirus solo podrá reconocer si están infectadas o no a través de sus capacidades heurísticas.

Gracias a estas evaluaciones se puede conocer en detalle el rendimiento de los productos antivirus frente a virus nuevos o desconocidos.

Ejemplos

Existen varios organismos independientes que realizan evaluaciones retrospectivas, como por ejemplo:

AV-Comparatives (en inglés)
Hispasec (en castellano)

Antivirus

Los **antivirus** son programas cuya función es detectar y eliminar Virus informáticos y otros programas maliciosos *(a veces denominados malware).*

Básicamente, un antivirus compara el código de cada archivo con una base de datos de los códigos (también conocidos como firmas o vacunas) de los virus conocidos, por lo que es importante actualizarla periódicamente a fin de evitar que un virus nuevo no sea detectado. También se les ha agregado funciones avanzadas, como la búsqueda de comportamientos típicos de virus (técnica conocida como Heurística) o la verificación contra virus en redes de computadoras.

Normalmente un antivirus tiene un componente que se carga en memoria y permanece en ella para verificar todos los archivos abiertos, creados, modificados y ejecutados en tiempo real. Es muy común que tengan componentes que revisen los adjuntos de los correos electrónicos salientes y entrantes, así como los scripts y programas que pueden ejecutarse en un navegador Web (ActiveX, Java, JavaScript).

Los virus, gusanos, spyware, etc. son programas informáticos que se ejecutan normalmente sin el consentimiento del legítimo propietario y que tienen las características de ejecutar recursos, consumir memoria e incluso eliminar o destrozar la información.

Una característica adicional es la capacidad que tienen de propagarse. Otras características son el robo de información, la pérdida de esta, la capacidad de suplantación, que hacen que reviertan en pérdidas económicas y de imagen.

Daños y Perjuicios

Dado que una característica de los virus es el consumo de recursos, los virus ocasionan problemas tales como pérdida de productividad, cortes en los sistemas de información o daños a nivel de datos.

Otra de las características es la posibilidad que tienen de ir *replicándose* en otras partes del sistema de información. Las redes en la actualidad ayudan a dicha propagación.

Los daños que los virus dan a los sistemas informáticos son:

- Pérdida de información (evaluable según el caso)
- Horas de contención (Técnicos de SI, Horas de paradas productivas, tiempos de contención o reinstalación, cuantificables según el caso, más horas de asesoría externa)
- Pérdida de imagen (Valor no cuantificable)

Hay que tener en cuenta que cada virus es una situación nueva por lo que es difícil cuantificar a prioridad, lo que puede costar una intervención. Tenemos que encontrar métodos de realizar planificación en caso de que se produzcan estas contingencias.

Métodos de Contagio

Existen dos grandes grupos de *contaminaciones*, los virus donde el usuario en un momento dado ejecuta o acepta de forma inadvertida la instalación del virus, o los gusanos donde el programa malicioso actúa replicándose a través de las redes.

En cualquiera de los dos casos, el sistema operativo infectado comienza a sufrir una serie de comportamientos anómalos o no previstos. Dichos comportamientos son los que nos dan la traza del problema y tienen que permitir la recuperación del mismo.

Dentro de las contaminaciones más frecuentes por interacción del usuario están las siguientes:

- Mensajes que ejecutan automáticamente programas (como el programa de correo que abre directamente un archivo adjunto)
- Ingeniería social, mensajes como *ejecute este programa y gane un premio*.
- Entrada de información en discos de otros usuarios infectados.
- Instalación de software pirata o de baja calidad.
- Todos los nuevos métodos que vayan apareciendo conforme las tecnologías de la información vaya ganando terreno.

Seguridad Métodos de Protección

Tener en cuenta este reto, es el primer paso para obtener seguridad. Existen múltiples medios de intentar combatir el problema. Sin embargo hemos de ser realistas. Conforme nuevos programas y sistemas operativos se introduzcan en el mercado más difícil va a ser tener controlados a todos y más sencillo va a ser que a alguien se le ocurran nuevas formas de infectar el sistema.

Ante este tipo de problemas están los software llamados antivirus. Estos antivirus tratan de descubrir las trazas que ha dejado un software malicioso, para eliminarlo o detectarlo, y en algunos casos contener o parar la contaminación.

Los métodos para contener o reducir los riesgos asociados a los virus pueden ser los denominados activos o pasivos.

Antivirus (activo)

Estos programas como se ha mencionado tratan de encontrar la traza de los programas maliciosos mientras el sistema este funcionando.

Tratan de tener controlado el sistema mientras funciona parando las vías conocidas de infección y notificando al usuario de posibles incidencias de seguridad.

Como programa que esté continuamente funcionando, el antivirus tiene un efecto adverso sobre el sistema en funcionamiento. Una parte importante de los recursos se destinan al funcionamiento del mismo. Además, dado que están continuamente comprobando la memoria de la maquina, dar más memoria al sistema no mejora las prestaciones del mismo.

Otro efecto adverso son los **falsos positivos**, es decir al notificar al usuario de posibles incidencias en la seguridad, éste que normalmente no es un experto de seguridad se acostumbra a dar al botón de **autorizar** a todas las acciones que le notifica el sistema. De esta forma el antivirus funcionando da una sensación de **falsa seguridad**

TIPOS DE VACUNAS

CA: SOLO DETECCION: son vacunas que solo detectan archivos infectados sin embargo no pueden eliminarlos o desinfectarlos.
CA: DETECCIÓN Y DESINFECCIÓN: son vacunas que detectan archivos infectados y que pueden desinfectarlos.
CA: DETECCIÓN Y ABORTO DE LA ACCIÓN: son vacunas que detectan archivos infectados y detienen las acciones que causa el virus.
CA: DETECCIÓN Y ELIMINACION DE ARCHIVO/OBJETO: son vacunas que detectan archivos infectados y eliminan el archivo u objeto que tenga infección.
CB: COMPARCIÓN DIRECTA: son vacunas que comparan directamente los archivos para revisar si alguno esta infectado
CB: COMPARACION POR SIGNATURA: son vacunas que comparan las signaturas de archivos sospechosos para saber si están infectados.
CB: COMPARACION DE SIGNATURA DE ARCHIVO: son vacunas que comparan las signaturas de los atributos guardados en tu equipo.
CB: POR MÉTODOS HEURÍSTICOS: son vacunas que usan métodos heurísticos para comparar archivos.
CC: INVOCADO POR EL/LA USUARIO/LA: son vacunas que se activan instantáneamente con el usuario.
CC: INVOCADO POR ACTIVIDAD DEL SISTEMA: son vacunas que se activan instantáneamente por la actividad del sistema

Filtros de ficheros (activo)

Otra aproximación es la de generar filtros dentro de la red que proporcionen un filtrado más selectivo. Desde el sistema de correos, hasta el empleo de técnicas de firewall, proporcionan un método *activo* y eficaz de eliminar estos contenidos.

En general este sistema proporciona una seguridad donde el usuario no requiere de intervención, puede ser más tajante, y permitir emplear únicamente recursos de forma más selectiva.

Cuando el número de puestos a filtrar crece puede ser conveniente

Copias de seguridad (pasivo)

Mantener una política de copias de seguridad garantiza la recuperación de los datos y la respuesta cuando nada de lo anterior ha funcionado.

Asimismo las empresas deberían disponer de un plan y detalle de todo el software instalado para tener un plan de contingencia en caso de problemas.

Planificación

La planificación consiste en tener preparado un plan de contingencia en caso de que una emergencia de virus se produzca, así como disponer al personal de la **formación adecuada** para reducir al máximo las acciones que puedan entrañar riesgo.

Consideraciones de software

El software es otro de los elementos clave en la parte de planificación. Se debería tener en cuenta la siguiente lista de comprobaciones:

I. Tener el software imprescindible para el funcionamiento de la actividad, nunca menos pero tampoco más. Tener controlado al personal en cuanto a la instalación de software es una medida que va implícita. Así mismo tener controlado el software asegura la calidad de la procedencia del mismo (no debería permitirse software pirata o sin garantías). En todo caso un inventario de software proporciona un método correcto de asegurar la reinstalación en caso de desastre.
II. Disponer del software de seguridad adecuado. Cada actividad forma de trabajo métodos de conexión a Internet requieren una medida diferente de aproximación al problema. En general, las soluciones domésticas, donde únicamente hay un equipo expuesto, no son las mismas que las soluciones empresariales.
III. Métodos de instalación rápidos. Para permitir la reinstalación rápida en caso de contingencia.
IV. Asegurar licencias. Determinados softwares imponen métodos de instalación de una vez, que dificultan la reinstalación rápida de la red. Dichos programas no siempre tienen alternativas pero ha de buscarse con el fabricante métodos rápidos de instalación.
V. Buscar alternativas más seguras. Existe software que es famoso por la cantidad de agujeros de seguridad que introduce. Es imprescindible conocer si se puede encontrar una alternativa que proporcione iguales funcionalidades pero permitiendo una seguridad extra.

Consideraciones de la red

Disponer de una visión clara del funcionamiento de la red permite poner puntos de verificación filtrado y detección ahí donde la incidencia es más claramente identificable. Sin perder de vista otros puntos de acción es conveniente:

I. Mantener al máximo el número de recursos de red en modo de sólo lectura. De esta forma se impide que computadoras infectadas los propaguen.
II. Centralizar los datos. De forma que detectores de virus en modo batch puedan trabajar durante la noche.
III. Realizar filtrados de firewall de red. Eliminar los programas de compartición de datos, como pueden ser los P2P; Mantener esta política de forma rigurosa, y con el consentimiento de la gerencia.
IV. Reducir los permisos de los usuarios al mínimo, de modo que sólo permitan el trabajo diario.
V. Controlar y monitorizar el acceso a Internet. Para poder detectar en fases de recuperación cómo se ha introducido el virus, y así determinar los pasos a seguir.

Política General

Partiendo de la base que las actualizaciones e incorporaciones de nuevas tecnologías por parte de las empresas implican una cantidad muy importante de nuevas tecnologías por día, pensamos que es muy complicado mantener todos los sistemas de información con un nivel muy alto de seguridad.

Formación: *Del usuario*

Esta es la primera barrera de protección de la red.

Antivirus

Es conveniente disponer de una licencia activa de antivirus. Dicha licencia se empleará para la generación de discos de recuperación y emergencia. Sin embargo no se recomienda en una red el uso continuo de antivirus.

El motivo radica en la cantidad de recursos que dichos programas obtienen del sistema, reduciendo el valor de las inversiones en hardware realizadas.

Aunque si los recursos son suficientes. Este extra de seguridad puede ser muy útil.

Sin embargo los filtros de correos con detectores de virus son imprescindibles, ya que de esta forma se asegurará una reducción importante de decisiones de usuarios no entrenados que pueden poner en riesgo la red.

Firewalls

Filtrar contenidos y puntos de acceso. Eliminar programas P2P que no estén relacionados con la actividad. Tener monitorizado los accesos de los usuarios a la red, permite asimismo reducir la instalación de software que no es necesario o que puede generar riesgo para la continuidad del negocio.

Reemplazo de software

Los puntos de entrada en la red son generalmente el correo, las páginas WEB, y la entrada de archivos desde discos, o de PC's que no están en la empresa (portátiles...)

Muchas de estas computadoras emplean programas que pueden ser reemplazados por alternativas más seguras.

Es conveniente llevar un seguimiento de cómo distribuyen bancos, y externos el software, valorar su utilidad e instalarlo si son realmente imprescindibles.

Centralización y backup

La centralización de recursos y garantizar el backup de los datos es otra de las partes fundamentales en la política de seguridad recomendada.

La generación de inventarios de software, centralización del mismo y la capacidad de generar instalaciones rápidas proporcionan métodos adicionales de seguridad.

Es importante tener identificado donde tenemos localizada la información en la empresa. De esta forma podemos realizar las copias de seguridad de forma adecuada.

Control o separación de la informática móvil, dado que esta está más expuesta a las contingencias de virus.

Empleo de sistemas operativos más seguros

Para servir archivos no es conveniente disponer de los mismos sistemas operativos que se emplean dentro de las estaciones de trabajo, ya que toda la red en este caso está expuesta a los mismos retos. Una forma de prevenir problemas es disponer de sistemas operativos con arquitecturas diferentes, que permitan garantizar la continuidad del negocio.

Temas acerca de la seguridad

Existen ideas instaladas parte por las empresas de antivirus parte en la cultura popular que no ayudan a mantener la seguridad de los sistemas de información.

- **Mi sistema no es importante para un hacker**. Este tema se basa en la idea de que no introducir passwords seguras en una empresa no entraña riesgos pues ¿Quién va a querer obtener información mía?. Sin embargo, dado que los métodos de contagio se realizan por medio de programas *automáticos*, desde unas máquinas a otras, estos no distinguen buenos de malos, interesantes de no interesantes... Por tanto, abrir sistemas y dejarlos sin claves es facilitar la vida a los virus.
- **Estoy protegido pues no abro archivos que no conozco**. Esto es falso, pues existen múltiples formas de contagio, además los programas realizan acciones sin la supervisión del usuario poniendo en riesgo los sistemas.
- **Como tengo antivirus estoy protegido**. Únicamente estoy protegido mientras el antivirus sepa a lo que se enfrenta y como combatirlo. En general los programas antivirus no son capaces de detectar todas las posibles formas de contagio existentes, ni las nuevas que pudieran aparecer conforme las computadoras aumenten las capacidades de comunicación.
- **Como dispongo de un firewall no me contagio**. Esto únicamente proporciona una limitada capacidad de respuesta. Las formas de infectarse en una red son múltiples. Unas provienen directamente de accesos a mi sistema (de lo que protege un firewall) y otras de conexiones que realizó (de las que no me protege). Emplear usuarios con altos privilegios para realizar conexiones tampoco ayuda.

Resumen

Los retos de seguridad son cada vez mayores, conforme se confía en el desempeño de tareas a los sistemas de información los daños que la pérdida de información puede llegar a poner en peligro la **continuidad** del negocio.

Hemos de disponer de una visión global en cuanto a la seguridad:

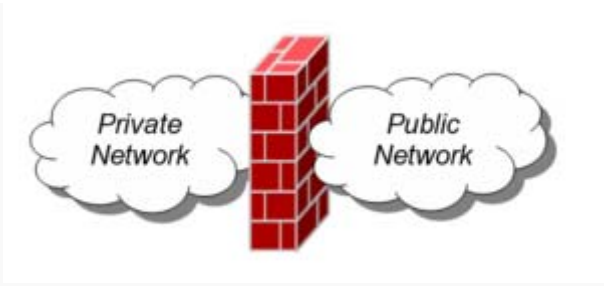
- Contraseñas difíciles de averiguar.
- Disponer de elementos pasivos/activos de detección de riesgos.
- Mantener los sistemas de información con las actualizaciones que más impacten en la seguridad.
- Evitar programas cuyo comportamiento respecto a la seguridad no sea idóneo.
- Mantener separación de sistemas operativos.
- Mantenimiento progresivo de la computadora en la que se trabaja.

Firewall

El término **Firewall** puede referirse a:

- ✓ un **cortafuegos (informática)**, un elemento utilizado en redes de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas;

Cortafuegos (Informática)



Un **cortafuegos** (o ***firewall*** en inglés), es un elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red. Su modo de funcionar es indicado por la recomendación RFC 2979, que define las características de comportamiento y requerimientos de interoperabilidad. La ubicación habitual de un cortafuego es el punto de conexión de la red interna de la organización con la red exterior, que normalmente es Internet; de este modo se protege la red interna de intentos de acceso no autorizados desde Internet, que puedan aprovechar vulnerabilidades de los sistemas de la red interna.

También es frecuente conectar al cortafuego una tercera red, llamada zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

Un cortafuego correctamente configurado añade protección a una instalación informática, pero en ningún caso debe considerarse como suficiente. La Seguridad informática abarca más ámbitos y más niveles de trabajo y protección.

Tipos de Cortafuegos

Cortafuegos de capa de red o de filtrado de paquetes

Funciona a nivel de red (nivel 3) de la pila de protocolos (TCP/IP) como filtro de paquetes IP. A este nivel se pueden realizar filtros según los distintos campos de los paquetes IP: dirección IP origen, dirección IP destino. A menudo en este tipo de cortafuegos se permiten filtrados según campos de nivel de transporte (nivel 4) como el puerto origen y destino, o a nivel de enlace de datos (nivel 2) como la dirección MAC.

Cortafuegos de capa de aplicación

Trabaja en el nivel de aplicación (nivel 7) de manera que los filtrados se pueden adaptar a características propias de los protocolos de este nivel. Por ejemplo, si se trata de tráfico HTTP se pueden realizar filtrados según la URL a la que se está intentando acceder. Un cortafuego a nivel 7 de tráfico HTTP es normalmente denominado Proxy y permite que los computadores de una organización entren a Internet de una forma controlada.

Cortafuego personal

Es un caso particular de cortafuegos que se instala como software en un computador, filtrando las comunicaciones entre dicho computador y el resto de la red y viceversa.

Ventajas de un Cortafuegos

- ✓ **Protege de intrusiones.** El acceso a ciertos segmentos de la red de una organización, sólo se permite desde máquinas autorizadas de otros segmentos de la organización o de Internet.
- ✓ **Protección de información privada.** Permite definir distintos niveles de acceso a la información de manera que en una organización cada grupo de usuarios definido tendrá acceso sólo a los servicios y la información que le son estrictamente necesarios.
- ✓ **Optimización de acceso.-** Identifica los elementos de la red internos y optimiza que la comunicación entre ellos sea más directa. Esto ayuda a reconfigurar los parámetros de seguridad.

Limitaciones de un Cortafuegos

- ✓ Un cortafuego no puede protegerse contra aquellos ataques que se efectúen fuera de su punto de operación.
- ✓ El cortafuego no puede protegerse de las amenazas a que esta sometido por traidores o usuarios inconscientes. El cortafuego no puede prohibir que los traidores o espías corporativos copien datos sensibles en disquetes o tarjetas PCMCIA y sustraigan éstas del edificio.
- ✓ El cortafuego no puede proteger contra los ataques de Ingeniería social
- ✓ El cortafuego no puede protegerse contra los ataques posibles a la red interna por virus informáticos a través de archivos y software. La solución real esta en que la organización debe ser consciente en instalar software antivirus en cada máquina para protegerse de los virus que llegan por medio de disquetes o cualquier otra fuente.
- ✓ El cortafuego no protege de los fallos de seguridad de los servicios y protocolos de los cuales se permita el tráfico. Hay que configurar correctamente y cuidar la seguridad de los servicios que se publiquen a Internet.

Políticas del Cortafuegos

Hay dos políticas básicas en la configuración de un cortafuego y que cambian radicalmente la filosofía fundamental de la seguridad en la organización:

- ✓ **Política restrictiva**: Se deniega todo el tráfico excepto el que está explícitamente permitido. El cortafuego obstruye todo el tráfico y hay que habilitar expresamente el tráfico de los servicios que se necesiten.
- ✓ **Política permisiva**: Se permite todo el tráfico excepto el que esté explícitamente denegado. Cada servicio potencialmente peligroso necesitará ser aislado básicamente caso por caso, mientras que el resto del tráfico no será filtrado.

La política restrictiva es la más segura, ya que es más difícil permitir por error tráfico potencialmente peligroso, mientras que en la política permisiva es posible que no se haya contemplado algún caso de tráfico peligroso y sea permitido por defecto.

Enlaces Externos

- Request for Comment 2979 - Comportamieto y requerimientos para los cortafuegos de Internet (en inglés)
- Comparativas de firewalls personales
- Gestión Unificada Control de Amenazas - UTM Firewall y Análisis de tráfico Protección Perimetral.