LISTA DE SPYWARE

AdProtector
AdwareHunter (adwarehunter.com, browser-page.com)
AdWareRemoverGold (adwareremovergold.com)
BPS Spyware & Adware Remover (bulletproofsoft.com)
InternetAntiSpy (internetantispy.com)
NoAdware (noadware.net, netpalnow.com)
Online PC-Fix SpyFerret
PurityScan (purityscan.com, puritysweep.com)
Real AdWareRemoverGold (adwareremovergold.com, sg08.biz)
SpyAssault (spyassault.com)
SpyBan (spyban.net)
SpyBlast (spyblast.com, advertising.com)
Spyblocs/eBlocs.com (eblocs.com)
Spybouncer (spybouncer.com)
SpyDeleter (spydeleter.com, 209.50.251.182)
SpyEliminator (securetactics.com)
SpyFerret (onlinepcfix.com)
SpyGone (spygone.com)
SpyHunter (enigmasoftwaregroup.com, spywareremove.com, spybot-spyware.com)
SpyKiller (spy-killer.com, maxionsoftware.com, spykiller.com, spykillerdownload.com)
SpyKillerPro (spykillerpro.com)
Spyware Annihilator (solidlabs.com)
SpywareBeGone (spywarebegone.com, freespywarescan.org)
SpywareCleaner (www.checkforspyware.com, www.spw2a.com/sc/)
SpywareCrusher (spywarecrusher.com)
SpywareInfoooo.com
SpywareKilla (spywarekilla.com)
SpywareNuker (spywarenuker.com, trekblue.com, trekdata.com, spyware-killer.com)
SpywareRemover (spy-ware-remover.com, spywareremover.com)
SpywareThis (spywarethis.com)
SpywareZapper (spywarezapper.com)
SpyWiper (mailwiper.com)
ssppyy pro (ssppyy.com)
TZ Spyware Adware Remover (trackzapper.com)
VBouncer/AdDestroyer (spywarelabs.com, virtualbouncer.com)
Warnet (warnet.com)
XoftSpy (download-spybot.com, paretologic.com, downloadspybot.com, no-spybot.com)
ZeroSpyware (zerospyware.com, zeroads.com)

AdProtector

Categoría: Misceláneo
AdProtector pretende remover spywares pero ciertamente actúa de forma contraria constituyendo una intrusión en el sistema a componer. La aplicación se sabe que actúa como restrador del escritorio del sistema, páginas de inicio y busquedas en Internet.
Este spyware posee las siguientes características:

- Causa Inestabilidad en el Sistema
  Causa Inestabilidad en el Sistema debido a un excesivo uso del ancho de banda del sitema. Aplicaciones maliciosas ejecutan tareas en modo oculto, de manera que logran provocar un uso exagerado, logrando en conjunto, una compleja inestabilidad del sistema.
- Conecta a Internet
  Intenta establecer una conexión externa. Estos Spywares lo realizan tipicamente para descargar sus actualizaciones o reportar la información de la víctima infectada.
- Muestra publicidad
  Muestra un popup no solicitado o una publicidad aleatoria. Dicha publicidad puede aparecer o no en el explorador HTML predeterminado. Por ejemplo: Internet Explorer.
- Modificación o "Rapto" del Explorador
  Modifica las propiedades del navegador predeterminado (generalmente Internet Explorer) y redirecciona la página de inicio y las páginas de búsqueda a sitios no solicitados de publicidad. Algunos son tan complejos que pueden llegar a modificar hasta las páginas de errores 404 inclusive.
- Instala Archivos
  Instala numerosos archivos necesarios para su ejecución. Cuantos mas archivos instala en su ordenador, mas cantidad de aplicaciones maliciosas pueden tener control sobre su ordenador y su sistema..
- Modifica el Registro del Sistema
  Altera el Registro del sistema creando o modificando entradas ya existentes. Es común que este Spyware modifique las llaves del registro de modo que se ejecute automaticamente en el inicio del sistema.

Web3000
Categoría: Adware
Web3000 es un componente adware que muestra publicidad en forma de pop-up y cambia las propiedades del navegador. La aplicación se instala tipicamente como un agregado a utilidades freewares; sin embargo, Web3000 también utiliza un exploit o "hueco" del navegador web logrando instalarse de forma forzada e imperceptible a cualquier usuario. Web3000 descarga anuncios no solicitados, "rapta" las páginas de búsqueda del Internet Explorer (especialmente nos damos cuenta cuando encontramos que se presentan cientos de anuncios de avisos o hasta contenido adulto), relentiza el explorador de Internet, y el sistema operativo en general.
Este spyware posee las siguientes características:

- Conecta a Internet
  Intenta establecer una conexión externa. Estos Spywares lo realizan tipicamente para descargar sus actualizaciones o reportar la información de la víctima infectada.
- Muestra publicidad
  Muestra un popup no solicitado o una publicidad aleatoria. Dicha publicidad puede aparecer o no en el explorador HTML predeterminado. Por ejemplo: Internet Explorer.

- Loguea los hábitos de navegación en Internet
  Guarda las "huellas" de su explorador de Internet y sus hábitos de compras online, enviando de esta forma información centralizada sobre sus gustos. Esta información es normalmente utilizada para proveer publicidad relacionada con la información que recogieron de su ordenador.
- Permanece Residente en la Memoria
  Permanece residente en la memoria esperando no ser detectado o removido por un detector de Spywares. Su funcionamiento oculto hace que sea muy difícil de remover por aplicaciones anti-espías. Sin embargo, Sin-Espías lo reconoce y elimina correctamente.

¿Qué es webHancer?
webHancer es un programa ejecutable malicioso que generalmente se instala sin el consentimiento o el conocimiento del usuario. webHancer puede tener la capacidad de controlar, registrar y transmitir en secreto la actividad de la computadora. Los posibles síntomas de webHancer incluyen, pero no se limitan a, rendimiento lento del sistema, fallas frecuentes del sistema, anuncios comerciales (publicidades emergentes) y/o elevado uso de la CPU, entre otras características. webHancer también puede causar una conexión lenta a Internet debido al uso en aumento del ancho de banda. La reproducción no es frecuente con webHancer. No obstante, se recomienda eliminar webHancer.
¿Cómo obtuve webHancer?
Los métodos de infección por webHancer varían. Muy probablemente, webHancer estaba integrado con otra aplicación descargada intencionalmente. Los programas de comunicaciones entre pares también podrían ser una fuente de infección. Otras tácticas de distribución de webHancer incluyen vulnerabilidades del explorador, cuadros emergentes engañosos diseñados para aparecer como cuadros de diálogo legítimos de Windows y/o descargas encubiertas de archivos.
¿Cómo elimino webHancer?
Es más que probable que webHancer se haya incrustado por sí mismo en su sistema, lo cual dificultará la eliminación manual. Por fortuna, existe gran cantidad de soluciones Anti-Spyware preparadas para hacer el trabajo por usted. Y, si bien no podemos garantizar la eficacia de todo el software que aparece en InternetSecurityZone.com, podemos recomendar (y de hecho lo hacemos) STOPzilla. Haga clic aquí para descargar STOPzilla y elimine webHancer ahora mismo.
GoHip: Programa que ofrece publicidad en su PC.
Created by: Creado por: GoHip.com, Inc. GoHip.com, Inc
Extracción manual: Usted puede obtener una herramienta de remover
http://www.gohip.com/remove.exe

	Conducent-Timesink
Nombre técnico:	Spyware/Conducent-Timesink
Peligrosidad:	 Spyware de peligrosidad Baja
Alias:	Conducent-Timesink
Tipo:	Spyware
Efectos:	*Conducent-Timesink* realiza las siguientes acciones: • Realiza conexiones a Internet en segundo plano sin el

consentimiento del usuario para descargar publicidad.
- Muestra mensajes publicitarios en cualquier momento mientras se esté ejecutando.
- Guarda datos del usuario en ficheros encriptados que posteriormente son enviados a la empresa que lo desarrolló.
- Guarda y envía información sobre hábitos de uso de Internet, páginas *web* visitadas, etc.
- Se ejecuta cada vez que se inicia Windows y se coloca residente en memoria.
- No ofrece herramientas para su desinstalación.

Plataformas que infecta:	Windows 95/98/ME/NT/2000/XP
Fecha de aparición:	14 de Octubre de 2003 a las 12:20 horas

Conducent-Timesink es un programa espía, que acompaña a otras aplicaciones que pueden descargarse desde Internet.
Conducent-Timesink realiza conexiones a Internet en segundo plano, sin el conocimiento del usuario, y descarga publicidad que será mostrada en cualquier momento mientras se esté ejecutando.
Conducent-Timesink guarda datos del usuario en ficheros encriptados que son almacenados en el disco duro, para posteriormente ser enviados a la empresa que lo desarrolló. *Conducent-Timesink* también guarda información sobre los hábitos de uso de Internet, páginas *web* visitadas, etc.
La empresa que desarrolló *Conducent-Timesink* no sigue activa en el mercado, por lo que no es probable que afecte a nuevos ordenadores. Sin embargo, es posible que muchos usuarios sigan albergando este programa espía en su equipo.

Síntomas visibles:

Conducent-Timesink es difícil de reconocer a simple vista, ya que no muestra mensajes o avisos que alerten sobre su presencia.

LISTA DE VIRUS

DOWNLOAD.TROJAN
- Caballo de Troya, afecta a NT y 2K.
- Se conecta con los sitios web y de FTP de su autor.
- Trae desde allí troyanos, virus, gusanos y los componentes de éstos hacia la máquina infectada.
- Cada vez que se trae archivos desde Internet, se auto ejecuta.
- SOLUCIÓN: Borrado manual.

FAKE SERVER TROJAN
- Afecta sólo archivos .exe.
- SOLUCIÓN: Borrado manual.

HACK V1.12.TROJAN

- Afecta sólo archivos .exe.
- SOLUCIÓN: Borrado manual.

JS.EXITW.TROJAN

- No afecta NT ni 2K.
- Hace que Windows arranque y se cierre inmediatamente.
- SOLUCIÓN: Borrado manual.

JS.FORTNIGHT

- Afecta a NT y 2K. Híbrido de gusano/troyano.
- Modifica la configuración del programa Outlook Express y envía un link al sitio del hacker, escondido en la firma del usuario.
- Configura una página pornográfica como página de inicio del Internet Explorer.
- SOLUCIÓN: Borrado manual. Luego, corregir a mano el registro .

JS.FORTNIGHT.B

- Igual al anterior. Además, re direcciona toda URL a la URL que el hacker desea y inhabilita la solapa "Seguridad" del Internet Explorer.
- SOLUCIÓN: Borrado manual. Luego, corregir a mano la registry .

JS.FORTNIGHT.C

- Igual a los anteriores, pero no inhabilita la solapa del IE5.
- SOLUCIÓN: Borrado manual. Luego, corregir a mano la registry.

MMC.EXE

- Es el Caballo de Troya del W32.Nimda.A@mm (ver).
- SOLUCIÓN: Borrado manual.

MSBLAST.EXE

- Es el Caballo de Troya del W32.Blaster. Worm (ver).
- SOLUCIÓN: Borrado manual.

NETBUS.170.W95.TROJAN

- Muy peligroso. Afecta NT y 2K.
- Troyano backdoor. Le da a su creador acceso y permisos FULL CONTROL para atacar el equipo infectado. Estas capacidades incluyen enviar archivos del usuario al sitio del hacker, ejecutar aplicaciones, robar documentos y borrar archivos en forma remota.
- SOLUCIÓN: Borrado manual. Luego, corregir a mano la registry .

NETBUS.2.TROJAN

- Este troyano es la aplicación cliente de la herramienta de hackeo Netbus 2.0. Se conecta desde un sistema remoto y gana control de acceso sobre la máquina infectada.
- SOLUCIÓN: Borrado manual.
- PRETTYPARK.WORM
- Conocido gusano de red.
- Es parecido al Happy99. Dispara un troyano (prettypark.exe) que a veces hace correr el salvapantallas de las cañerías.
- Se conecta solo a un servidor IRC, a un canal específico y monitorea para recibir los comandos que el dueño le manda desde ese canal.

- Le entrega al hacker las claves de discado para conexión de la víctima, toda la información del sistema y la configuración del ICQ.
- A su vez, el hacker (siempre vía IRC) tiene acceso a recibir, crear, borrar y ejecutar cualquier archivo.
- SOLUCIÓN: Ejecutar el reparador . Luego, corregir a mano la registry, si se encuentran daños en ella.

TROJAN.ADCLICKER

- Funciona en NT y 2K.
- La función de este troyano es que la máquina de la víctima haga clic permanentemente en las publicidades de las páginas web de las que es dueño su programador.
- SOLUCIÓN: Borrado manual. Luego, corregir a mano la registry .

TROJAN.DOWNLOAD.CHECKIN

- Este Caballo de Troya es, aparentemente, parte de una aplicación de adware.
- Se conecta a varios sitios e IPs diferentes y chequea si hay nuevas versiones de sí mismo. Si la respuesta es afirmativa, las baja en la máquina infectada y las ejecuta. Como no hace chequeo de CRC ni integridad antes de ejecutar, si el troyano bajó corrupto los resultados son imprevisibles.
- SOLUCIÓN: Borrado manual. Luego, corregir a mano la registry.

LISTA DE WORM's MÁS POPULARES

W32.BLASTER.WORM

- Gusano de red híbrido gusano/troyano, de alta peligrosidad (Grado 4). Tercero en el ranking de peligrosidad de Symantec (1-9-03, Symantec Security Response Newsletter, 22 de agosto, 2003). Daño: Alto. Distribución: Alta. Presencia en libertad: Alta.
- Explota la vulnerabilidad de seguridad en el servicio DCOM RPC, utilizando el puerto TCP 135.
- El virus está pensado para 2K y XP. Aunque NT es vulnerable también, el Blaster no se replica en esta plataforma, a menos que se lo instale y ejecute manualmente. Afecta especialmente a Windows 2K Server.
- No tiene funcionalidad de envío masivo de e-mail.
- El virus trae el troyano msblast.exe, lo coloca en \system32 y lo ejecuta, siempre los días 16 del mes si el mes es anterior a agosto, y todos los días desde el 16 de agosto hasta el 31 de diciembre.
- Hace un DOS (Denial of Service, Denegación de Servicio) contra www.windowsupdate.com, para evitar que el usuario pueda bajar e instalar los parches que corrigen la vulnerabilidad del RPC.
- Un error en su código hace fallar los equipos NT infectados y además abre una pantalla cmd.exe en la máquina del hacker, para que pueda ejecutar comandos en forma remota en el equipo infectado. El usuario no se percata de ello.

- Genera IPs similares a la del equipo infectado y trata de conectarse con las demás máquinas de la red. Para ello, utiliza los puertos UDP 69 y TCP 135 y 4444, usando la vulnerabilidad del servicio DCOM RPC. La LAN se satura de solicitudes del puerto 135. El servicio RPC falla. El servicio svchost.exe comienza a saturar la máquina de errores. Si el operador reinicia el equipo, vuelve a ejecutar el troyano.
- El virus monitorea en el puerto TCP 4444 los comandos DOS que recibe desde la pantalla que creó en la máquina del dueño del virus. También monitorea en el puerto UDP 69 las respuestas de las máquinas a las que les preguntó (por el TCP 135) si tenían corriendo un DCOM RCP no parchado. A las que le dicen que sí, les manda, instala y ejecuta el troyano msblast.exe.
- SOLUCIÓN: Con el equipo desconectado de la red, ejecutar el reparador localizado aquí. A continuación, instalar el parche para NT que está localizado aquí. Para los servidores 2K, hay un parche diferente. Verificar luego, a mano, que no se encuentren en la registry los daños producidos por el mencionado virus, comparándola con la registry normal que se describe aquí.

W32.BUGBEAR.B

- Variante del gusano Bugbear, con una muy eficiente funcionalidad para envíos masivos de e-mail e infección masiva de LANs. Alta peligrosidad, Nivel 4. Cuarto en el ranking de amenazas mundiales de Symantec: Existencia en libertad: Alta; Daños: Medio; Distribución: Alta.
- Se trata de uno de los nuevos gusanos polimórficos, que muta para evitar ser detectado.
- Registra las pulsaciones de teclas en el logon para interceptar las claves y enviárselas a su dueño. Abre backdoors para permitirle tomar posesión de los equipos.
- Ataca una variedad de archivos .exe.
- Se defiende de los antivirus más comunes y es capaz de atravesar firewalls.
- Explota la vulnerabilidad MIME de Microsoft que permite que el IE corra automáticamente los adjuntos.
- Por un error de código, satura los buffers de las impresoras de red, haciendo que impriman basura (en realidad, lo que intenta hacer es imprimirse a sí mismo y lo que vemos en papel es la interpretación que hace la impresora del código del virus).
- Está dedicado en especial a enviarle al hacker los datos financieros que encuentra (claves para páginas de bancos, números de tarjetas de crédito, etc.).
- Si un antivirus no funciona en un equipo, la causa más probable es que esté infectado con el Bugbear.
- Su troyano, PWS.Hooker.Trojan, registra las claves, las encripta y se las manda al autor del gusano.
- SOLUCIÓN: Con el equipo desconectado de la red, ejecutar el reparador localizado aquí. Luego, instalar en cada equipo el parche localizado aquí (observando que sea para la versión correcta del IE. Ambos son sólo para Internet Explorer con Service Pack 1. El IE5 (cualquier versión) con SP2 no es vulnerable al Bugbear y no es necesario instalar estos parches.

W32.BUGBEAR.B.DAM

- Versión corrupta del anterior.
- No es funcional. No causa daños, no se replica ni se autoenvía.
- SOLUCIÓN: Borrado manual.

W32.GANDA.A@MM

- Mail masivo, se autoenvía a todos los que están en la libreta de direcciones.
- Agrega un troyano a muchos ejecutables.
- Impide que se ejecuten varios productos antivirus.
- SOLUCIÓN: Borrado manual; luego, verificar la integridad de la registry según se describe aquí.

W32.GANDA.A@MM.ENC

- Es la versión codificada como MIME del virus anterior, que se puede ejecutar automáticamente (es decir, sin que uno abra el mensaje). Contiene el virus vivo y activo (ver arriba).
- SOLUCIÓN: Ídem anterior.

W32.HLLP.SPREDA

- En un virus (no gusano) que se propaga dentro de los archivos .exe que se bajan por el KaZaA. Está escrito en C++.
- SOLUCIÓN: Mediante un buen antivirus. Si no puede reparar los archivos, eliminarlos a mano.

W32.KLEZ.H@MM

- Gusano de red, de peligrosidad Grado 3: Existencia salvaje: Alta; Daño: Medio; Distribución: Alta; Solución: Difícil.
- Es la versión mejorada del Klez.E, que no sólo se dispersa por e-mail sino a través de las LANs.
- Infecta ejecutables, se autoreenvía masivamente y libera junto con su propia copia todo tipo de documentos de la máquina del usuario.
- SOLUCIÓN: Correr el reparador. Luego, revisar los posibles daños virales en la registry, comparándola con una normal.

W32.KLEZ.H@MM.ENC

- Versión codificada MIME del anterior (ver). Tiene el virus activo.
- SOLUCIÓN: Ídem anterior.

W32.KWBOT.C.WORM

- Se expande a través de los archivos bajados del KaZaA o del IMesh.
- Deposita un troyano que tiene tales capacidades de generar backdoors que otorga al hacker el control total sobre el equipo infectado.
- Abre puertos ocultos, tanto TCP como UDP.
- SOLUCIÓN: Remoción manual. Luego, comparar la registry .

W32.LIRVA.A@MM

- Gusano de mediana peligrosidad, Grado 2.
- Se transmite, además del e-mail, a través de IRC, KaZaA e ICQ.
- Utiliza la misma vulnerabilidad de IE y Outlook Express que explota el Bugbear.

- Se dispara los días 7, 11 y 24 de cada mes, se conecta con una página erótica y muestra una animación.
- Elude a los programas antivirus y los firewalls, y envía a su autor las claves de discado de conexión de los equipos basados en 95, 98 y Me.
- SOLUCIÓN: Ejecutar el reparador . Luego, comparar los daños en la registry.

W32.MAPSON.WORM

- Gusano de red. Se autoreenvía a todos los contactos de MSN Messenger. Además, se propaga a través de KaZaA, KaZaA Lite, eDonkey2000, Gnucleus, Limewire, Morpheus, ICQ y Grokster.
- Está escrito en Delphi y comprimido por UPX.
- Muestra algunos mensajes en el mes de julio.
- SOLUCIÓN: Borrado manual.

W32.MIMAIL.A@MM

- Gusano de red de Grado 3, quinto en el ranking de Symantec.
- Muy peligroso porque está destinado a robar información de la máquina infectada y enviarla por un e-mail oculto al programador del virus.
- Utiliza las vulnerabilidades de Microsoft MS02-15 y MS03-14.
- Simula ser el programa de manejo de la placa de video, por lo que es imposible no ejecutarlo al iniciar Windows.
- Captura el texto de las ventanas que está abriendo el usuario y lo reenvía por e-mail.
- Tiene su propio cliente SMTP de correo incorporado. Busca y encuentra la DNS del host del usuario. Contacta al mailserver del dominio en cuestión, y, a través del mismo, se conecta con el hacker en forma directa.
- SOLUCIÓN: Ejecutar el reparador . A continuación, instalar en todas las máquinas el parche de Microsoft . Por último, verificar que no hayan quedado daños por modificaciones efectuadas por el gusano en la registry del equipo.

W32.MIMAIL.A@MM.ENC

- Versión MIME autoejecutable del anterior (ver).
- SOLUCIÓN: Ídem anterior.

W32.NAVIDAD

- Eficiente gusano de e-mail, explota la vulnerabilidad de MAPI. Se expande a través de Outlook Express, Outlook y todos los cliente de e-mail que usan MAPI.
- Contiene errores que hacen que el equipo falle al ejecutar el gusano. Esto ocurre porque hace cambios erróneos en la registry.
- SOLUCIÓN: Ejecutar el reparador.Luego, verificar que la registry no contenga errores, comparando sus valores.

W32.NICEHELLO@MM

- Es un gusano que se reenvía a todas las direcciones a través del correo.
- Roba las claves del MSN Messenger y se las envía a su programador.
- Abre el puerto 53 y se conecta con el servidor DNS 65.173.56.33. A través de él, envía al hacker las claves que acaba de robar, a una cuenta de Yahoo! o de Olimpo.
- SOLUCIÓN: Borrado manual. Luego, hay que verificar que la registry esté limpia.

W32.NIMDA.A@MM

- Gusano de red de peligrosidad Grado 2.
- Luego de infectar la máquina, espera diez días antes de hacer nada.
- Se reenvía a todas las direcciones por e-mail.
- Explota la vulnerabilidad Unicode Web Traversal de Microsoft y la ya conocida vulnerabilidad MIME.
- Su nombre es "Admin" escrito al revés, y se debe a que el gusano comparte los recursos del equipo infectado, se hace cargo de la cuenta Guest (o "invitado") y se otorga a sí mismo, registrado con ella, privilegios de Administrator.
- Penetra en todos los equipos y web servers vulnerables.
- SOLUCIÓN: No es sencilla en el caso del Nimda. Por empezar es imprescindible ejecutar el reparador en su equipo. Si usted está en una LAN, deberá hacerlo en todos los equipos de la red local, INCLUYENDO TODOS LOS SERVIDORES. Para ello, hay que desconectar los equipos de la red o del teléfono UNO POR UNO antes de correr el reparador. Luego de ejecutarlo, reiniciar cada equipo. La herramienta no borrará todos los e-mails infectados. Reparará el system.ini corrompido por el virus, quitará los derechos administrativos de la cuenta Invitado e inhabilitará el grupo Invitados. Recuperará las modificaciones hechas al Internet Explorer y dejará sin compartir las unidades compartidas por Nimda.
- Sin embargo, en Windows NT/2K/XP, el reparador no puede distinguir correctamente las elecciones de compartir que fueron hechas por el virus de las que hace el mismo sistema operativo (C$, por ejemplo). Por lo tanto, todos los permisos de todos los equipos deben ser verificados manualmente por los administradores luego de haber ejecutado esta herramienta.
- El reparador restaura todos los valores del Explorador de Windows a los de por defecto. Esto también tiene que ser verificado a mano, en caso de querer que conserve valores especiales.
- Dado que los equipos infectados por el Nimda son accedidos por el hacker desde afuera, la herramienta no garantiza la integridad del sistema ni de los datos, ni su correcto funcionamiento. Verificar tales condiciones a mano.
- Es muy probable que, luego de correr el reparador, algunos programas como Microsoft Word o Excel se llenen de errores o ni siquiera arranquen. Esto se debe a que el virus ha corrompido un archivo llamado riched20.dll. Para ello, si el sistema operativo es Windows NT, hay que borrar la .dll mencionada, desinstalar el Service Pack, reiniciar el equipo, y volver a instalar el Service Pack de la misma versión que tenía el equipo.
- Si el problema anterior se ocasionara en un Windows 2000, hay que seguir las instrucciones de remoción que se indican en la página de Symantec Corporation.
- Si las fallas de Word y Excel continúan, estas aplicaciones se deberán reinstalar. Si aún así no funcionan, reinstale el Office completo (desinstalando y reiniciando primero).
- La misma .dll está infectada si, al terminar de correr el reparador, aparece un mensaje parecido a "The file NOT is infected and FUCKING repaired".

- A continuación, debe instalar parches para la vulnerabilidad del sistema operativo.
- Por último, verificar que todos los cambios que el virus hizo en registry se hayan corregido: Si todavía persisten daños, el operador deberá hacer una copia de respaldo de la registry en otro equipo no infectado e intentar corregirlos a mano.

W32.NIMDA.A@MM.ENC

- Es la versión MIME del anterior (ver).
- SOLUCIÓN: Íd. Anterior.

W32.PINFI

- Es un virus residente en memoria que infecta .exe y .scr. Es polimórfico, y se expande a través de unidades mapeadas y por las IPs de las LANs.
- SOLUCIÓN: Remoción manual, con revisión de los posibles daños ocasionados en la registry.

W32.SIRCAM.WORM

- Gusano de red de peligrosidad media, Grado 3.
- Posee su propio motor SMTP pero, por un error de código, no es capaz de replicarse en equipos con tecnología basada en NT .
- SOLUCIÓN: A pesar de que no se propaga en NT, un equipo que fue infectado con este virus puede no permitir que se ejecuten fixes con extensión .exe, por eso la herramienta es un .com.
- Sí será necesario verificar la registry, porque los cambios pueden estar allí.

W32.SOBIG.F

- Gusano de red de alta peligrosidad, Grado 4, ubicado en el primer lugar del ranking mundial de amenazas virales.
- Se propaga por e-mail a todas las direcciones y a través de las LANs.
- No se puede extender a los mapeos de red por un error de código.
- El último día en que se replicó fue el 9 de septiembre de 2003. El 10 de septiembre los SoBig.F se autodesactivaron, pero en fecha próxima su autor va a liberar la versión G, con todos los errores detectados corregidos y mejores funcionalidades.
- La desactivación sólo se aplica al e-mail y la propagación por red. Esto significa que el virus sigue vivo en los equipos, y que ese día le va a preguntar a su propio server si está lista la nueva actualización de sí mismo. Como la respuesta va a ser afirmativa (hasta ahora nunca falló), se la va a bajar, se va a autoactualizar y seguirá operando, ya mejorado. Por lo tanto, aunque el F ya no actúa, no está de más quitarlo de su equipo y protegerse contra la futura versión G.
- Se dedica a reenviarse por e-mail y a robar información de sistema y contraseñas, que son enviadas a su amo.
- SOLUCIÓN: Primero, desconecte los equipos infectados de su cable de red o de la línea telefónica. Segundo, ejecute el reparador .Luego verifique que no hayan quedado daños permanentes en la registry, y en caso necesario, corríjalos. Puede seguir la guía que se encuentra.
- W32.SUPOVA.WORM

- Gusano de red, que simula ser algún programa muy popular (porno, juegos, etc.) y que por ello se propaga a través de KaZaA.
- SOLUCIÓN: Manual o a través del antivirus. Si le quedaron modificaciones en la registry.

W32.YAHA.F@MM.ENC

- Gusano de red de e-mail masivo, que se reenvía a todas las direcciones de la Libreta de Direcciones, a todos los contactos de ICQ, a todos los contactos de Messenger y a todos los contactos de Yahoo! Pager.
- Elude a los antivirus y a los firewalls.
- SOLUCIÓN: Ejecutar el reparador . (hay que ser Administrador y desconectar el cable de red o el módem). Es muy posible que, si el gusano ya ha sido ejecutado, el reparador no lo pueda eliminar. En ese caso, habrá que removerlo a mano. Desde la misma página verificar si hay daños en la registry, comparándola con la que se muestra.

W32.YAHA.P@MM.ENC

- Variante del Yaha.L. Además de las vías de dispersión del anterior, también viaja a través del .NET Messenger.
- SOLUCIÓN: Remoción manual, siguiendo las instrucciones de Symantec .
- W95.HYBRIS.WORM
- Gusano con funcionalidad de dropper, de alta peligrosidad (Nivel 4).
- Lo implanta el virus W95.Hybris.gen, y se lo encuentra tanto en los rígidos como en los e-mails originales infectados.
- SOLUCIÓN: Manual o con antivirus.

LISTA DE VIRUS DE MACRO

W97M.CHACK.AH.GEN

- Virus de macro, infecta todas las versiones de Office anteriores al Service Release 1.
- Muestra una imagen porno al infectar archivos todos los sábados, o al crear nuevos documentos los martes.
- SOLUCIÓN: Remoción manual o vía antivirus.

W97M.ETHAN.EK.SRC

- Macro, infecta .doc de Word y la plantilla normal.dot.
- Cambia los acentos ortográficos de los documentos.
- SOLUCIÓN: Manual o por el antivirus.

W97M.MARKER.GEN

- Macro.
- Desactiva los mensajes normales de Word.
- SOLUCIÓN: Borrado manual o con el antivirus.

W97M.TITCH.D

- Virus de macro.
- Cambia las configuraciones de Word (sobre todo en lo que hace a protección de documentos).

- SOLUCIÓN: Borrado manual o con un antivirus.

LISTA DE TROYANOS MÁS POPULARES

- SCRIPT.INI: el primero de ellos. Apareció aproximadamente en enero de 1.998, y rápidamente se esparció por la red. Afecta sólo al mIRC de versión 5.3 o anterior. Consiste en un fichero, script.ini, que reemplaza al verdadero utilizado por el mIRC. Al infectar, intentará mandar el fichero script.ini a cualquier otro PC que acceda al mismo canal IRC donde esté el infectado. Además, permite ciertas acciones de control remoto sobre el cliente mIRC. Se elimina simplemente borrando el fichero script.ini y sustituyéndolo por uno correcto. Lo más facil es volver a instalar el mIRC.

- DMSETUP.EXE: el más dañino de los troyanos de tipo IRC, y también muy extendido. Existen al menos cinco variantes distintas. Afecta también al mIRC. También intenta infectar a los PCs que entran en el canal donde esta el infectado. Además crea multitud de copias de sí mismo en el disco duro, altera el C:\AUTOEXEC.BAT, y crea algunos ficheros propios, como el C:\CONFIGG.SYS, y otros en el subdirectorio del mIRC. También permite el control remoto del cliente IRC. La eliminación suele ser muy problemática, incluso en el caso de la variantes 4ª, suele ser necesario el formateo del disco duro.

- WINHELP.EXE: otro troyano que afecta al mIRC, aunque bastante menos extendido. Modifica el fichero MIRC.INI y el WIN.INI. Se propaga de la misma manera que los otros.

En http://www.irchelp.org/irchelp/security/trojan.html hay información más clara y abundante sobre los troyanos de IRC.

- BACK ORIFICE (BO): creado en agosto de 1.998 por el grupo cDc (Cult of Dead Cows), se ha extendido peligrosamente por la red, hasta el punto de que en España ha llegado a estar infectado el 10% de los PCs conectados a internet. La parte servidora puede ser configurada para ejecutarse con cualquier nombre y para utilizar cualquier puerto UDP, aunque por defecto utiliza el nombre " .EXE" (un blanco antes del punto), y el puerto de 37331. En cualquier caso, el icono del programa es un blanco (aparece sin icono en el Explorador de Windows). Cuando se ejecuta, se instala en C:\WINDOWS\SYSTEM, donde además del ejecutable de la parte server aparece el fichero WINDLL.DLL. Además, al instalarse graba en el registro una entrada en HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices, con el nombre del ejecutable del server. Esto hace que el server se ejecute siempre que se arranque Windows, y permanece en todo momento ejecutandose en oculto, sin aparecer como tarea de Windows. La parte cliente consta de dos ejecutables, una en version de comandos DOS (BOCLIENT.EXE), y la otra en versión de interfaz gráfica de usuario (BOGUI.EXE). Las dos tienen las mismas funcionalidades:
  - Ping individual o a una lista de IPs, barrido en una subred para encontrar servers, o en una lista de subredes.

- Utilización de passwords para restringir el acceso.
- Manejo de ficheros: creado, borrado, renpmbrado, lista, envio, recepción, etc.
- Manejo de directorios: creado, borrado, lista.
- Comandos del sistema: información, passwords en caché, mandar ventanas de dialogo, logs de teclas pulsadas, reboot, permitir la navegacion en su disco duro por http, impedirla, bloquear el PC.
- Manejo del entorno de comunicaciones del PC.
- Envío, ejecución o listado de plugins.
- Listar, ejecutar o matar procesos del sistema.
- Control del registro de Windows.
- Ejecución de sonidos, de video, volcado de pantalla.
- Redireccionamiento del tráfico TCP/IP a otros host y otros puertos.
- listado, ejecución y eliminación de aplicaciones de consola, como COMMAND.COM, NETSTAT.EXE, etc.

- NETBUS: creado por Karl Fredrik Neikter poco despues que el BO, es otro de los más populares troyanos. También está muy extendido por la red. Al instalarse se graba en C:\WINDOWS el ejecutable de la parte cliente, con el nombre que tuviera el programa al ser ejecutado. Puede ser ejecutado con parámetros, de manera que no se rearranque cada vez que se arranque Windows, o se arranque ajuste el troyano para funcionar por un puerto TCP distinto del de por defecto (12345), o para pedir password ante el acceso de la parte cliente. La parte server frecuentemente va camuflada en un juego, el Whackjob. Al ejecutarse el troyano, si se ejecuta sin el parámetro /NOADD o sin el parámetro /REMOVE (que, como indica, lo elimina), graba una entrada en el registro de Windows, en HKEY_LOCAL_MACHINES\SOFTWARE\ Microsoft\Windows\CurrentVersion\Run, graba tambien el fichero KEYHOOK.DLL en C:\WINDOWS, y en el caso de la version 1.70, crea en ese mismo directorio un fichero INI con las opciones de configuracion. Las funcionalidades que presenta son muchas. En esencia, las mismas que el BO, más algunas como apertura y cierre del CD, control del ratón (intercambio de funcion de teclas, control de movimientos), mas posibilidad de envío de mensajes al server, envío de texto y recepción de teclas pulsadas, intercepción del teclado, etc. La eliminación del troyano puede hacerse modificando el registro y borrando los ficheros implicados (para eso, en la entrada correspondiente del registro viene el nombre del ejecutable). Tambien puede hacerse a mediante la parte cliente del NETBUS, que permite eliminar el troyano. Dada su popularidad, también han aparecido algunos programas tanto para su detección o eliminación (NETBUSTER) como para crackear las passwords (NETRUST21A o el BUSCONQUERER13). Incluso los últimos scripts para mIRC (por ejemplo, el orbital) detectan barridos de puertos buscando el NETBUS, o buscan clientes IRC conectados que esten infectados con el BO o el NETBUS (por ejemplo, el RIP).

- Sockets De Troie: también llamado MSchv32.EXE por ser el nombre del ejecutable de la parte server en las primeras versiones. Creado por un tal JC`zic, y con textos exclusivamente en francés, es otro programa de control remoto ligeramente posterior al BO. Además del idioma, tiene la peculiaridad de que la versión 2.5 es realmete un virus, y se propaga como tal. Cuando se ejecuta,

generalmente sale un mensaje de error también en francés (excepto cuando el infector es el fichero Cheval sans msg.exe, en cuyo caso no hay mensaje).Al infectar, en el caso de la version 1.0 graba el fichero MSchv32.EXE en C:\WINDOWS\SYSTEM y crea una entrada de registro en KEY_CURRENT_USER\Software\Microsoft\Windows\ CurrenVersion\Run. En el caso de las versiones 2.x crea tres ficheros: RSRCLOAD.EXE (en c:\WINDOWS), MGADESKDLL.EXE (en C:\WINDOWS\SYSTEM) y CSMCTRL32.EXE (en el mismo sitio) y crea tres entradas en el registro, una para cada uno de los ficheros:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run (MGADESKDLL.EXE)

HKEY_LOCAL_MACHINES\Software\Microsoft\Windows\CurrentVersion\Run (RSCRLOAD.EXE)

HKEY_LOCAL_MACHINES\Software\Microsoft\Windows\CurrentVersion\RunServices (CSMCTRL32.EXE).

A diferencia del BO y del NETBUS, no corre en invisible, y por tanto aparece en la ventana de tareas. La versión 1.0 utiliza el puerto 5000, mientras las 2.x utilizan por defecto el 50505. Como funcionalidades presenta más o menos las mismas que el BO, con alguna funcionalidad añadida como arma ofensiva en IRC, del tipo de los nukes ICMP o SSPING. Para eliminarlo basta cerrar la tarea, y eliminar los ficheros y las entradas del registro. También existen programas específicamente dedicados a detectar y eliminar este troyano, como por ejemplo el ANTISOCKETS.

- GIRL FRIEND: Este es un troyano bastante reciente (diciembre 1.998) creado por General Failure en Delphi. La parte server (el troyano) se llama GIRL FRIEND mientras que la parte cliente se llama BOY FRIEND. El troyano, al instalarse, se copia en C:\WINDOWS\SYSTEM con el nombre WINDLL.EXE, y crea una entrada de registro en HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ Windows\CurrentVersion\Run. El puerto utilizado por defecto es el 21554, aunque es configurable. Todos los datos del GF los va grabando en el registro, en HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\General. Tiene las funcionalidades típicas de los programas de acceso remoto, aunque sin control de periféricos. En cambio es muy potente para acceso a passwords, pues va grabando todas aunque la parte cliente no este conectada. Tiene también como peculiaridad, además de fallar más que una escopeta de feria, el que cuando está arrancado, si el cliente no está conectado, el puerto que utiliza no está abierto, de manera que no se puede detectar con el NETSTAT. También aparece oculto en la ventana de tareas.

- MASTER OF PARADISE: otro troyano más basado en los mismos principios que los anteriores. Este fue creado por Dan Lehmann, un alemán que por lo menos tuvo el detalle de traducir la parte cliente al inglés, aunque los mensajes de error siguen saliendo en alemán. El programa es muy completo. De hecho, podría ser el mejor de todos los troyanos actuales, si no fuera porque también falla con demasiada frecuencia. Tiene las mismas utilidades del NetBus, más algunas otras como el control de la barra de tareas, y mejor gestión de la pantalla del servidor. Además, la interfase gráfica es muy clara. El troyano ejecutable se llama AGENT.EXE por defecto, pero puede darse con cualquier nombre, y tambien puede presentarse enmascarado en un juego. De todas formas, este troyano no se ejecuta en oculto. Aparece en la barra de tareas, y puede ser parado como cualquier otro proceso de la barra de tareas..

- BACKDOOR 2.03, GATECRASHER, DEEPTHROAT: son tres ejemplos de troyanos relativamente recientes y poco conocidos pero bastante potentes. Tienen más o menos las mismas funcionalidades que el Masters of Paradise. Incluso uno de ellos, el GATECRASHER, se transmite mediante macros en un documento Word. Próximamente ampliaré la información sobre estos troyanos, pues probablemente acaben sustituyendo al BO y al NETBUS.