DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

Nombre:	**W32/Singu** **Alias:** Troj/Backdoor.Singu, Backdoor.Singu, Backdoor.Singu.g
Tipo:	Troyano
Tamaño:	218,274 bytes
Origen:	Internet
Destructivo:	SI
En la calle (in the wild):	SI
Detección y eliminación:	The Hacker 5.3 al 25/10/2002.

Descripción:

W32/Singu, es un troyano que permite el acceso remoto y no permitido de un intruso a la computadora infectada, además intenta actualizarse así mismo a través de internet, para ello utiliza el puerto 2002.

Cuando este se ejecuta se copia en :

C:\WINDOWS\Services.exe

Además crea la siguiente entrada en el registro para poder ejecutarse en cada reinicio del sistema:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

"winlogon"="C:\WINDOWS\Services.exe

También crea el archivo llamado Winservices.dll, este archivo tiene la configuración del troyano.

C:\WINDOWS\Winservices.dll

Nombre:	**VBS/Helvis** **Alias:** VBS.Helvis
Tipo:	Troyano
Tamaño:	5,590 bytes
Origen:	Internet
Destructivo:	NO
En la calle (in the wild):	SI
Detección/Eliminación:	The Hacker 5.3 al 27/10/2002

Descripción

VBS/Helvis, es un troyano que roba mensajes recibidos y enviados de la computadora infectada, las cuales envia a su creador. Para ello utiliza Outlook.

Cuando el troyano se ejecuta modifica la siguiente entrada en el registro del sistema:

HKEY_LOCAL_MACHINE\Microsoft\Windows Scripting Host\Settings Timeout=0

Además abre la siguiente página web en el Internet Explorer, el cual contiene una foto de un imitador del cantante Elvis Presley.

http:\\www.madblast.com
Seguidamente el troyano crea un nuevo script, que solo funcionará en determinados sistemas :
C:\WINNT\profiles\all users\start menu\programs\startup\VirusChecker.vbs
Este archivo **VirusChecker.vbs**, realiza la acción de envio de mensajes pero solo con mensajes que tengan de uno a tres días, solo funciona en sistemas con Windows NT.
Luego busca la bandeja de entrada y de elementos enviados y procede a enviarlos a la siguiente dirección **vcheckpr@hotmail.com**, el asunto en los mensajes de la bandeja de entrada es modificado por el siguiente texto:
Asunto : ibox1 [Nombre de asunto original]
A los mensajes de la bandeja de elementos enviados le agrega el siguiente asunto :
Asunto : sbox1 [Nombre de asunto original]

Nombre:	**W32/Downloader-BT** **Alias:** Downloader-BT,
Tipo:	Adware
Tamaño:	65,536 bytes
Origen:	EE.UU
Destructivo:	NO
En la calle (in the wild):	SI
Detección y eliminación:	The Hacker 5.4 al 21/01/2003.

Descripción:
W32/Downloader-BT, es una aplicación Adware que simula ser una aplicación de busquedas de elementos en Internet, cuya finalidad es la de permitir la muestra masiva de publicidad no deseada en el computador atacado.
Esta aplicación puede llegar a través del correo electrónico simulando ser una aplicación, necesita de la intervención del usuario para poder ejecutarse.
Este se adiciona como un proceso llamado WINNET.EXE, se le puede ver con el administrador de tareas.

Nombre:	**W32/Downloader-BS** **Alias:** Downloader-BS,
Tipo:	Troyano
Tamaño:	5,120 bytes
Origen:	Internet
Destructivo:	NO
En la calle (in the wild):	SI
Detección y eliminación:	The Hacker 5.4 al 15/01/2003.

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

Descripción:

W32/Downloader-BS, es un troyano que al ser ejecutado intenta descargar archivos desde un sitio Web mediante HTTP, los archivos son aplicaciones tipo **"PORNDIAL"** (aplicación dialer (marcación) que se conecta con servidores pornográficos para descargar peliculas, imagenes, etc, cada vez que se inicie el sistema esta aplicación se ejecuta e intenta conectarse a servidores pornográficos, es como si se estuviera haciendo una llamada telefónica)

Este se copia a sí mismo en:

C:\WINDOWWS\SYSTEM\MSFINDOS.EXE

Además crea las siguientes entradas en el registro para poder ejecutarse en el siguiente reinicio del sistema

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
"msfindosa.exe"="C:\WINDOWS\SYSTEM\Msfindosa.exe"
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
"msfindosa.exe"="C:\WINDOWS\SYSTEM\Msfindosa.exe"

Nombre:	**W32/Downloader-BO.dr** **Alias:** Downloader-BO.dr.b
Tipo:	Troyano
Tamaño:	11,046 bytes
Origen:	Internet
Destructivo:	SI
En la calle (in the wild):	SI
Detección y eliminación:	The Hacker 5.4 al 22/01/2003.

Descripción:

W32/Downloader-BO.dr, es un troyano que llega adjunto en un Email difundido como SPAM, el archivo adjunto tiene la extensión .HTA y tiene oculto el código Visual Basic Script.

Caracteristicas del Mensaje de Email:

Asunto: Mail delivery failed: returning message to sender
Archivo Adjunto : messages.hta

Cuando **Messages.hta** es descargado y ejecutado, este ejecuta a otro troyano y se copia en:

C:\Mware.exe

Seguidamente muestra una pantalla en blanco

Nombre:	**Troyan/Downloader.MY** **Alias:** Downloader-MY
Tipo:	Troyano Downloader
Tamaño:	6,656 bytes
Origen:	Internet

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

Destructivo:	NO
En la calle (in the wild):	SI
Detección y eliminación:	The Hacker 5.6 al 21/07/2004.

Descripción:
Trojan/Downloader.MY, es un troyano que al ser ejecutado intenta descargar y ejecutar archivos desde sitios Web remotos, los archivos son aplicaciones tipo dialer, spywares, etc.
Cuando el troyano se ejecuta se copia a sí mismo dentro de las siguientes ubicaciones:
%system%\drivers\cd_load.exe
%system%\inetsrv\MSCStat.exe
Además crea las siguientes entradas en el registro para poder ejecutarse en el siguiente reinicio del sistema:
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
"CashToolbar"="%system%\inetsrv\MSCStat.exe"
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
"ClickTheButton"="%system%\drivers\cd_load.exe"
Seguidamente muestra el siguiente falso mensaje de error:
Windows Error
Windows has detected Spyware on your computer
Download Spyware Remover
[OK] [Cancel]
Si se presiona el botón [OK] el troyano intentará descargar archivos desde sitios remotos.

Nombre:	**Trojan/Allclicks** **Alias:** Trojan.Allclicks.A, TrojanClicker.NetBuie.a, Trojan/Win32.Elitec, Trojan.NetBuie.A, Troj/Allclicks.A, Allclicks
Tipo:	Troyano
Tamaño:	32,768, 47,718, 20,480 y 400,938 bytes
Origen:	Internet
Destructivo:	NO
En la calle (in the wild):	SI
Detección y eliminación:	The Hacker 5.2 al 15/06/2002.

Trojan/Allclicks, simula ser un programa emulador de la consola de juegos de Microsoft Xbox, si se ejecuta lo que hace es conectarse periodicamente a paginas de Internet especificas.
Cuando es ejecutado este trojano realiza los siguiente, copia el siguiente archivo en:
C:\WINDOWS\Escritorio\Xbox_emulator.0.34.exe (Contiene al falso emulador del juego)
Ademas copia los siguientes archivos en :

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS
C:\WINDOWS\SYSTEM\Archive.exe
C:\WINDOWS\SYSTEM\NetBUIE.exe
C:\WINDOWS\SYSTEM\RegUpdate.exe
C:\WINDOWS\SYSTEM\Sucess.exe
Tambien modifica algunas entradas en el registro para poder ejecutarse en cada inicio del sistema:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
"NetBUIE dll loopback - Inserted by Dr. Watson" ="C:\windows\system\NetBUIE.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Run
"NetBUIE dll loopback - Inserted by Dr. Watson" ="C:\windows\system\NetBUIE.exe"

Nombre:	**QDel359** **Alias:**
Tipo:	Troyano
Tamaño:	19,968 bytes
Origen:	Internet
Destructivo:	SI
En la calle (in the wild):	SI
Deteccion/Eliminación:	The Hacker 5.3 y 5.4 al 24/12/2002.

Descripción
QDel359, es un troyano que tiene una rutina de eliminación de archivos de la unidad **"C:"**, para lograr esto modifica el archivo **AUTOEXEC.BAT**. Este Troyano necesita de la intervención del usuario para poder ejecutarse y propagarse.
Cuando el troyano se ejecuta reinicia el sistema y procede a borrar todos los archivos en la unidad **C:** para ello utiliza el archivo **deltree.exe,** el troyano llega en un archivo llamado **MIRC PATCH.EXE,** simulando ser una actualización (parche) de la aplicación mIRC
Despues de su ejecución no queda residente en memoria, además no hace cambios en el registro para que se ejecute en el siguiente reinicio del sistema, para que se vuelva a ejecutar necesariamente necesita ser ejecutado manualmente.
Además muestra el siguiente mensaje cuando se esta ejecutando:
synix.w32 ... infected.

Nombre:	**QDel356** **Alias:** Troj/QDel356
Tipo:	Troyano
Tamaño:	16,384 bytes
Origen:	Internet
Destructivo:	SI
En la calle (in the wild):	SI
Deteccion/Eliminación:	The Hacker 5.3 ó 5.4 al 11/12/2002.

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

Descripción

QDel356, es un troyano que tiene una rutina de eliminacion de archivos importantes de la carpeta Windows. Este Troyano necesita de la intervención del usuario para poder ejecutarse y propagarse. Simula ser un detector de virus.

Cuando el troyano se ejecuta muestra un mensaje con el siguiente texto :

Congratulations! No more virus on your computer!
Experiment completed! No any destructives! Thank you!
[all virus-related files removed successfully]
[OK]

Seguidamente el troyano busca en la carpeta de Windows los siguientes archivos

- taskbar.bak
- taskbar.exe
- notepad.ini
- win64.ini
- winstat.ini
- wbackup.ini
- wcurrent.ini
- winhelp.ini

Si los encuentra procederá a borrarlos. Despues de su ejecución no queda residente en memoria, además no hace cambios en el registro para que se ejecute en el siguiente reinicio del sistema, para que se vuelva a ejecutar necesariamente necesita ser ejecutado manualmente.

Nombre:	**QDel297**
Tipo:	Troyano
Tamaño:	29,696 bytes (.exe) 54 bytes (.bat)
Origen:	Internet
Destructivo:	SI
En la calle (in the wild):	SI
Deteccion/Eliminación:	The Hacker 5.3 al 14/11/2002.

Descripción

QDel297, es un troyano que tiene una rutina de eliminacion de archivos del sistema infectado. Este Troyano necesita de la intervención del usuario para poder ejecutarse y propagarse, esta escrito en Visual Basic, además copia al computador infectado un archivo **AUTOEXEC.BAT** que hace que el computador infectado se reinicie.

Al reiniciarse el troyano ejecuta el archivo **AUTOEXEC.BAT** y muestra el siguiente mensaje :

subnix owns you

Seguidamente intentará eliminar todo los archivos que encuentre en el computador infectado, ejecutando el comando **DELTREE.EXE**. (no mostrara el mensaje de confirmación de la acción a realizar)

En este caso la única manera de volver a ejecutar correctamente la computadora, es volver a instalar Windows, y todos sus software.

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

Nombre:	**QDel234** **Alias:** Troj/QDe1234
Tipo:	Troyano
Tamaño:	320,512 bytes
Origen:	Internet
Destructivo:	SI
En la calle (in the wild):	SI
Deteccion/Eliminación:	The Hacker 5.2 al 20/05/2002.

Descripción

QDel234, es un troyano que tiene una rutina de eliminacion de archivos importantes del sistema infectado. Este Troyano necesita de la intervención del usuario para poder ejecutarse y propagarse, llega como un archivo adjunto en un email, en el cuerpo del mensaje llega el texto de alguien que dice haber hackeado su pagina web o algun otro sitio determinado, tratando de engañar a su victima a que abra y ejecute los archivos que prueban dicha acción.

Cuando el troyano se ejecuta muestra el siguiente mensaje en modo MS-DOS:

Warning
Actually what I feel is, you have reached to the end....
And your guards, firewaalls, bridgs, mount towers and crack filters are not configured properly or they are out of service in your server
Better to update that.Then you will not come across with this kind of problems Thank you.
Please note.
You can not take an action against this, because Sri Lanka is away from Computer Misuse Act 1990
Press any key to continue ...

Si la victima pulsa alguna tecla, el troyano borrara los siguientes archivos en la computadora del usuario:

C:\WINDOWS\SYSTEM*.ini
C:\WINDOWS\SYSTEM*.exe
C:\WINDOWS*.dll
C:\WINDOWS*.exe

En este caso la unica manera de volver a ejecutar correctamente la computadora, es volver a instalar Windows, y todos sus software.

Nombre:	**PHC2002_TROYANO**
Variantes y Alias:	TROJAN_PHC, PHC, PHC2002.EXE, Trojan/W32.PHC (Panda), Trojan.Win32.Killav.l (AVP), AVKill-J (Mcafee), Troj/KillAV-C (Sophos)
Tipo:	Troyano
Tamaño:	Varía

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

Origen:	Perú
Destructivo:	SI
En la calle (in the wild):	NO
Detección y eliminación:	The Hacker 5.3 al 21/08/2002 tiene todas las variantes conocidas

PHC2002_TROYANO y variantes son troyanos DAÑINOS reportados en Perú hace algunos meses, hay varias variantes conocidas, las últimas variantes son detectadas como PHC2002_TROYANO por The Hacker 5.3. El troyano ha sido escrito por un grupo de creadores de virus Peruanos conocidos como PHC.

Al igual que otros virus como W32/Bandera que atacan a los antivirus McAfee, Panda, AVP y Per el troyano PHC2002_TROYANO y sus variantes tienen como único objetivo atacar a The Hacker.

Cada una de las variantes tiene características específicas y están escritas igualmente para versiones específicas del antivirus, entre sus múltiples acciones podemos indicar:

- **Modificación de los procesos del antivirus en Memoria vía API de Windows (CreateProcess, WriteProcessMemory, etc):** Hay diferentes variantes que realizan tal acción, cada versión del troyano es específica a una versión del antivirus, si el troyano se ejecuta en una versión para la cual no está programado colgará el proceso del antivirus.

- **Sobreescribe el Virus Scanner Engine (th32.dll):** El troyano sobreescribe esta librería DLL para evitar su detección, igualmente si el troyano encuentra una DLL para el cual no está programado aparecen mensajes de error de Windows en la librería afectada..

- **Sobreescribe las librerías de búsqueda (th32eng.dll, th32mac.dll, etc):** Las últimas versiones del troyano atacan este archivo para evitar su detección, el troyano sobreescribe algunas areas en la librería de búsqueda, los resultados podrían variar desde cuelgues hasta mal funcionamiento del antivirus. Al igual que en los puntos anteriores el troyano es específico a una versión.

- **Sobreescribe el registro de virus (thact.dat, etc):** En algunas variantes, este troyano "corta a la mitad" el archivo thact.dat tratando de evitar su detección, por ejemplo si el archivo thact.dat mide 20Kb después de ser atacado por el troyano mide 10Kb. En la siguiente ejecución del antivirus The Hacker notará que el archivo de registro thact.dat está corrupto, emitirá un mensaje de error y no correrá.

El código fuente de las últimas variantes del troyano han sido difundidas en websites de creación de virus por lo que su modificación es inminente, pudiéndose encontrar en el futuro variantes con nuevas características incluso más dañinas, borrado de archivos del usuario, ataque a otros antivirus o programas, etc.

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

Nombre:	**Linux/Bofishy.C** **Alias:** Backdoor.Bofishy.C, tcpdump trojan
Tipo:	Troyano
Tamaño:	N/D
Origen:	Internet
Destructivo:	SI
En la calle (in the wild):	SI
Detección y Eliminación	The Hacker 5.3 Registro de Virus al: 14/11/2002

Descripción

Linux/Bofishy.C, es un troyano que puede infectar servidores linux y Unix:

- El troyano afecta a las rutinas **configure** de los siguientes paquetes **libpcap-0.7.1, tcpdump-3.6.2, tcpdump-3.7.1** y algunas versiones de **libpcap y tcpdump**.
- El troyano descarga el archivo **SERVICES** desde un sitio Web y lo ejecuta, dicho archivo tiene en su rutina crear una puerta trasera en la computadora infectada a través de un programa llamado **conftes.c.**
- Este programa establece comunicación con la dirección IP 212.146.0.34 a través del puerto 1963 y queda en espera de las ordenes del atacante.
- El paquete **libpcap** contiene una versión modificada de la función **pcap_compile()**, en el archivo **gencode.c**, su función es la de crear reglas de filtrado de paquetes, evitando así que los paquetes sean capturados en el puerto 1963. Obteniendose como resultado que sea imposible detectar el tráfico en la red generado por la puerta trasera, porque es imposible de utilizar a **libpcap y tcpdump**, que se encuentran infectadas por el troyano.

Nombre:	**KillBoot.B** **Alias:** Troj/Killboot.B, TROJ_KILLBOOT.B
Tipo:	Troyano
Tamaño:	1,085 bytes
Origen:	Internet
Destructivo:	SI
En la calle (in the wild):	SI
Detección y Eliminación	The Hacker 5.3 y 5.4, Registro de Virus al 29/12/2002

Descripción

KillBoot.B, es un troyano que sobrescribe el **MASTER BOOT RECORD** (MBR) con ceros, como resultado de esta acción es la pérdida de datos y la imposibilidad de iniciar el sistema en el siguiente reinicio.

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

Este troyano utiliza llamadas a la Interrupción 13h del DOS, para lograr sobrescribir el MBR del Disco Duro, Sólo funciona en sistemas que corren bajo DOS o desde una ventana DOS.

Nombre:	**JS/Seeker.J** **Alias:** JS.Seeker.J
Tipo:	Troyano
Tamaño:	N/D
Origen:	Internet
Destructivo:	SI
En la calle (in the wild):	SI
Detección y Eliminación	The Hacker 5.3 y 5.4, Registro de Virus al 10/01/2003

Descripción

JS/Seeker.J, es un troyano que intenta modificar la configuración del Internet Explorer. También cambia las últimas 15 direcciones Web visitadas con la dirección de un sitio web de contenido para adultos.

Seguidamente modifica las siguientes entradas en el registro del sistema:

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Start Page
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\First Home Page
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Default_Page_URL
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Search Page
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\(Default)
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Start Page
HKE_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel\HomePage
HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel\SecChangeSettings
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RegisterOrganization
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RegisterOwner
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\NoRun
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableRegistryTools

Finalmente intentará crear varios enlaces con nombres chinos a diferentes sitios web en las siguientes carpetas:

Carpeta favoritos del usuario
C:\WINDOWS\Menu Inicio
C:\WINDOWS\Escritorio
C:\WINDOWS\Menu Inicio\Programas
C:\WINDOWS\Application Data\Microsoft\Internet Explorer\Quick Launch

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

Nombre:	**JS/Pursue** **Alias:** Pursue
Tipo:	Troyano
Tamaño:	N/D
Origen:	Internet
Destructivo:	SI
En la calle (in the wild):	SI
Detección y Eliminación	The Hacker 5.3 ó 5.4, Registro de Virus al 11/12/2002

Descripción

JS/Pursue, es un troyano que se transmite a través de sitios web infectados, con tan solo abrir el sitio web. No crea ningún archivo en el computador infectado, solo creará y modificará algunas entradas en el registro para causar sus daños.

Cuando el troyano infecta la computadora, crea y modifica algunas entradas en el registro del sistema :

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
"rundll.exe"="rundll.exe user.exe,exitwindows"

Con esto logra que la computadora infectada se apague cada vez que se inicie Windows.

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Polices\System
"DisableRegistryTools"="00000001"

Con este cambio impide que se ingrese al editor del registro (**Regedit**).

Además también oculta la opción de **APAGAR** del menú **INICIO** de Windows

Nombre:	**JS/Offiz** **Alias:** JS/NoClose, JS/NoClose.F, JS.Trojan.Offiz, Trojan.JS.Offiz
Tipo:	Troyano
Tamaño:	2,595 bytes
Origen:	Alemania
Destructivo:	NO
En la calle (in the wild):	SI
Detección y Eliminación	The Hacker 5.3 y 5.4, Registro de Virus al 23/12/2002

Descripción

JS/Offiz, es un troyano escrito en JavaScript, que se encuentra dentro de una página HTML, infecta a las computadoras cuando los usuarios visitan páginas que estan infectadas con este troyano, este impide que se cierren las ventanas abiertas, bloquea las teclas ALT, F4, CTRL y DEL (SUPR)

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

Si el usuario pulsa alguna de las teclas descritas el troyano mostrara el siguiente mensaje :

El troyano no posee rutina destructiva, no hace otros cambios en la configuración de la computadora infectada

Nombre:	**JS/NoClose** **Alias:** js.noclose, JS/NoClose.gen, JS.Trojan.NoClose
Tipo:	Troyano de JavaScript
Tamaño	N/Determinado
Origen:	Internet
Destructivo:	NO
En la calle (in the wild):	SI
Defección/Eliminación:	The Hacker 5.2 Registro de Virus 24/05/2002

Descripción

El JS/NoClose es un troyano de JavaScript. Procede a infectar al computador cuando se esta accesando a una Web infectada, este procedera ha abrir sitios web con publicidad o contenido pornográfico sin el consentimiento del usuario creando ventanas ocultas que son dificiles de cerrar. Tambien minimiza la ventana del Internet Explorer, haciendo que no se pueda maximizar.

Este Troyano no contiene ninguna rutina destructiva y no causa ningun daño en los archivos del sistema y de usuarios.

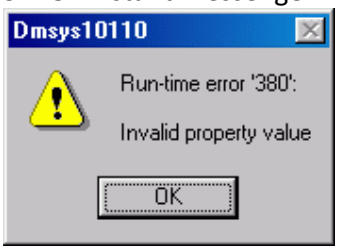
Nombre:	**APSTrojan.sl** **Alias:** Dmsys
Tipo:	Troyano
Tamaño	122,880 bytes
Origen:	Internet
Destructivo:	NO
En la calle (in the wild):	SI
Detención / Eliminación:	The Hacker 5.1 al 06/02/2002

Descripción

APStrojan.sl, es un troyano que intenta robar los usuarios y contraseñas de AOL Instant Messenger; para luego enviar estos datos a una dirección de E-mail en Yahoo.com. Cuando se ejecuta el troyano, este se copia asi mismo en la carpeta:

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

C:\WINDOWS\START MENU\PROGRAMS\STARTUP
Si AOL Instant Messenger no esta instalado, aparece el siguiente mensaje de error:



Todas las teclas pulsadas y titulos de ventanas son registradas en el archivo DAT.LOG en la misma carpeta donde se encuentre el ejecutable del troyano. Luego de capturar esta información el troyano intenta crear el archivo **"C:\PROGRAM FILES\DMSYSMAIL.EML"** y enviar este archivo utilizando las extensiones **MAPI** a it090d@yahoo.com.

Nombre:	**Backdoor.Gspot** **Alias:** Troj/Backdoor.Gspot, Tojan.W32.G-Spot
Tipo:	Troyano
Tamaño:	N/Determinado
Origen:	Internet
Destructivo:	SI
En la calle (in the wild):	SI
Detección/Eliminación:	- The Hacker 5.2 al 03/06/2002

Descripción

Backdoor.Gspot, es un troyano Este necesita de la intervención del usuario para ser ejecutado, esto lo logra atravez de engaños, haciendose pasar como un archivo de utilidad, este puede tener cualquier nombre. Este troyano utiliza un sevidor y un cliente, el servidor se instala en la computadora atacada, permitiendo el acceso remoto a dicho sistema, de esta manera compromete la seguridad y privacidad, ademas busca conexiones ICQ abiertas y posibles HOSTS.

Cuando el troyano es ejecutado, este muestra una imagen, la cual puede ser encontrada en la carpeta de temporales, esta se puede borrar no es un archivo maligno.

C:\WINDOWS\Temp\Temp2.jpg
Además se copia a si mismo en:
C:\WINDOWS\Temp\Temp1.exe
Luego se ejecuta y crea el siguiente archivo en :
C:\WINDOWS\SYSTEM\Msregdrv32.exe
Modifica una entrada en el registro para poder ejecutarse en cada inicio del sistema:
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
"Video Driver" ="C:\WINDOWS\SYSTEM\Msregdrv32.exe"

Nombre:	**Backdoor.Tron** **Alias:** RAT.Tron, Troj/Backdoor.tron
Tipo:	Troyano

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

Tamaño:	481 kb
Origen:	Internet
Destructivo:	SI
En la calle (in the wild):	SI
Detección/Eliminación:	- The Hacker 5.2 al 04/06/2002

Descripción

Backdoor.Tron, es un troyano que intenta eliminar los procesos de los siguientes firewall, ZoneAlarm y Tiny Personal Firewall, que esten instalados en la computadora atacada, y así no ser detectado por el firewall. Este necesita de la intervención del usuario para ser ejecutado, esto lo logra a travez de engaños, haciendose pasar como un archivo de utilidad, este puede tener cualquier nombre (su nombre por defecto es **tron.exe**) pero puede ser renombrado.

Cuando el troyano es ejecutado, este se copia a si mismo en la carpeta de %windows% con los siguientes nombres:

C:\WINDOWS\<nombre aleatorio>.exe
C:\WINDOWS\Grpvinc.cpe
C:\WINDOWS\Tmplnjs.bat

Ademas modifica el archivo **Autoexec.bat** (realiza solo estos cambios en Win 9x)

PATH=C:\WINDOWS\;%PATH%
tmplnjs
cls

modifica una entrada en el registro para poder ejecutarse en cada inicio del sistema:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
"LoadOrderVerification" ="C:\WINDOWS\<nombre aleatorio>.exe"

Ademas este troyano abre los puertos 58008 y 58009 a la espera de una conexión, si llega a realizar una conexión un atacante tomaría el control de la computadora pudiendo llegar a realizar lo siguiente:

-Copiar, mover, borrar, cargar o descargar archivos.
-Visualizar los procesos activos.
-Apagar el sistema.
-Eliminar cualquiera de los procesos activos.
-Abrir o cerrar la bandeja de la unidad de CD.

Nombre:	**Bandung** **Alias:** WM/BANDUNG
Tipo:	Macrovirus, infecta documento de ms-word 6.x/7.x
Tamaño	Numero de Macros 6: AutoExec, AutoOpen, FileSave, FileSaveAs, TooolsMacro, ToolsCustomize(no encriptados) Tamaño de la Macros: 4262 bytes
Origen:	Indonesia/1996
Destructivo:	SI
En la calle (in the wild):	SI

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

Descripción

WM/Bandung infecta la plantilla global cuando un documento infectado es abierto. Los documentos del usuario son infectados por medio de las macros 'FileSave'' y 'FileSaveAs'. WM/Bangung tiene capacidades de STEALTH (ToolsMacro) para hacer más difícil su detección.

WM/Bandung es un virus superdestructivo, cada vez que se ejecuta WORD verifica si el día actual es mayor a 20 y la hora actual es mayor a 11:00am, si esto se cumple muestra el mensaje:

"Reading menu...Please wait !"

y empieza a borrar todos los archivos de la unidad C: excepto los archivos del directorio C:\WINDOWS, C:\WINWORD, C:\WINWORD6.

Inmediatamente crea el archivo C:\PESAN.TXT con el siguiente texto:

Anda rupanya sedang sial, semua file di mesin ini kecuali yang berada di direktori WINDOWS dan WINWORD telah hilang, jangan kaget, ini bukan ulah Anda, tapi ini hasil pekerjaan saya...Barang siapa yang berhasil menemukan cara menangkal virus ini, saya akan memberi listing virus ini untuk Anda!!! Dan tentu saja saya akan terus datang kesini untuk memberi Anda salam dengan virus-virus terbaru dari saya...selamat ! Bandung.

Traducido al español:

" Estas con mala suerte, todos los archivos en esta maquina han sido borrados,"
" excepto los de WINDOWS y WINWORD, no tenga pánico, esta no es una falla suya,"
" es el resultado de mi trabajo&ldots..A cualquiera que sea capaz "
" de encontrar una manera de combatir este virus le daré"
" la lista de mis virus y constantemente regresaré para agradecerte"
"con mi nuevo virus&ldots.buena suerte! Bandung Lunes 28 de Junio de 1996, 13:00pm"

Si el usuario usa el Menú Tools/Macros muestra el mensaje:
Err@#(c)*
Fail on step 29296
y reemplaza todos los caracteres 'a' con '@#' en el documento activo.

Nombre:	**Spanska.4250** **Alias:** Elvira, Spanska_II
Tipo:	-Infector de archivos EXE y COM -Encriptado -Residente -Stealth
Tamaño	4250 bytes
Origen:	España/Internet
Destructivo:	NO
En la calle (in the wild):	SI

Descripción

El virus Spanska.4250 es un virus polimórfico complejo muy reportado a inicios de Enero/98. Es residente en memoria e infecta archivos .EXE y .COM.

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

La primera vez que se ejecuta un archivo infectado con Spanska.4250, el virus se coloca residente en memoria ocupando 8K de memoria convencional, se enlaza a la INT 21h para tener el control total del sistema e inmediatamente procede a infectar el archivo 'C:\WINDOWS\WIN.COM'.

El virus contiene código parecido al virus **Natas.4774**, entre otros:

- No infecta archivos que empiezan con los siguientes nombres: TB*.*, VI*.*, AV*.*, NA*.*, VS*.*, FI*.*, F-*.*, FV*.*, IV*.*, DR*.*, SC*.*.
- Cuando se ejecuta un programa de compresión, empaquetador, backup conocido (PK*.*, AR*.*, RA*.*, LH*.*, BA*.*) el virus deshabilita sus rutinas de stealth para que el programa trabaje con el archivo infectado.

El virus se activa si un archivo infectado es ejecutado en minutos=30 y segundos <= 16, en ese momento procede a mostrar varios mensajes en la pantalla tipo efecto 'Guerra de las galaxias' (Star Wars).

ELVIRA !
Black and White Girl
from Paris
You make me feel alive.
ELVIRA !
Pars. Reviens. Respire.
Puis repars.
J'aime ton mouvement.
ELVIRA !
Bruja con ojos verdes
Eres un grito de vida,
un canto de libertad.

Nombre:	**Sordo** **Alias:** Arequipa.1994
Tipo:	-Infector de MBR, Boot Sector -Encriptado -Residente -Stealth
Tamaño	1944 bytes
Origen:	Arequipa/Perú, Setiembre/1996
Destructivo:	SI
En la calle (in the wild):	SI

Descripción

Sordo.1994 es un virus residente en memoria, encriptable, con stealth, infector de archivos.

La primera vez que se ejecuta un archivo infectado Sordo.1944 se coloca residente en memoria y se apropia de la interrupción 21h, una vez en memoria infectará todos los archivos que sean ejecutados y los archivos .EXE y .COM que sean abiertos. El virus se aloja al final de los archivos infectados ocupando 1994 bytes.

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

Activación:

Sordo.1994 tiene dos formas de activación:

1. Si se ejecuta un archivo entre las 12:00pm - 12:30pm.
2. Si un contador interno llega a registrar 10,010 ejecuciones o aperturas de archivos.

cuando se activa sobreescribe el disco duro con "basura" y muestra el mensaje:
Error, memory 1F8E:07A2 hardware internal
Sordo.1994 no infecta los siguientes programas Anti-Virus: -**SCAN.EXE, TBSCAN.EXE, TBAV.EXE MSAV.EXE**-.

Nombre:	**Ornate** **Alias:**
Tipo:	-Infector de Boot sector -Encriptado -Residente -Stealth
Número de sectores:	1
Origen:	Chile, Enero/1997
Destructivo:	SI
En la calle (in the wild):	SI

Descripción

Ornate es un virus infector de Boot Sector tanto en discos duros y disquetes, el virus está encriptado (instrucción NOT) y maneja técnicas de stealth.
Ornate fue reportado por primera vez en el Perú en Enero/1997.

Método de infección:

La única forma de infectar una computadora con este virus es butear de un disquete infectado. No importa si el disquete tiene sistema DOS o no.

Otros:

Como la mayoría de virus, Ornate tiene algunos errores críticos y en algunos casos el sistema no arrancará después de haber sido contaminado.

Daño causado:

Ornate trata de sobre escribir los primeros 9 sectores del disco duro a partir del Boot Sector (dañando el Boot y 8 sectores de la FAT!!!), afortunadamente esta rutina nunca es ejecutada por un error interno.

Nombre:	**Natas** **Alias:** Satan, Satanas
Tipo:	-Multipropósito (infector de MBR, Boot Sector, archivos EXE, COM) -Encriptado -Polimórfico -Residente -Stealth (avanzado)
Tamaño:	4,744 bytes

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

Origen:	USA/1994
Destructivo:	SI
En la calle (in the wild):	SI

Descripción

Este virus es totalmente polimórfico y fue detectado por primera vez en Lima en Noviembre de 1994.

Natas es originario de USA, pero es muy común en Europa, Asia, México, Sudamérica, etc. Natas infecta el Master Boot Record, Boot Sector y archivos ejecutables. Natas no infecta los archivos de un servidor de Red.

Natas puede infectar un sistema ya sea buteando desde un disquete o ejecutando un programa infectado, en ese momento se coloca residente en memoria y se enlaza a la INT 13h, INT 21h, todo disquete insertado o programa ejecutado será infectado.

Cuando se encuentra activo en la memoria de la PC, utiliza avanzadas técnica de STEALTH para evitar ser detectado por el usuario y otros programas.

Las técnicas de STEALTH dejan de funcionar temporalmente mientras se ejecuta un programa con el siguiente nombre: AR*.*, LH*.*, PK*.*, MODEM*.*, BACK*.*

Este virus utiliza también técnicas de TUNNELING para "saltarse" programas residentes que monitorean las actividades del usuario.

Programas residentes que verifican si se intenta escribir en el MBR (Partición), Boot Sector o si se quiere modificar un archivo ejecutable son burlados fácilmente por el virus NATAS.

NATAS es DAÑINO!!!, cuando se activa FORMATEA!!! casi el 80% de todo el disco duro.

1. Cada vez que se BUTEA la computadora con el virus en el MBR o Boot Sector existe 1 en 512 posibilidades que se active (y formatee).
2. Cada vez que se ejecuta un programa infectado existe 1 en 512 posibilidades que se active (y formatee).
3. El virus se puede activar (y formatear) también si detecta que se está intentando TRAZAR (analizar un programa línea a línea) un programa infectado.

El único texto encontrado en el virus es: Natas

Variantes:

Natas.4740: Infecta archivos ejecutables de un Servidor de RED.

Natas.4746: Casi idéntica al original de 4,746 bytes.

Natas.4800 : Es una variante del virus NATAS, existen muchas diferencias con el virus original debido a que el CODIGO FUENTE de este virus ha sido distribuido por BBS de CRACKERS en EUROPA.

Natas.4988: Infecta archivos ejecutables en un servidor de RED. Sus técnicas de Stealth no producen 'errores de asignación de archivos' cuando se ejecutan utilitarios de disco (scandisk, chkdsk, ndd, disktool, etc).

Nombre:	**Naked** **Alias:** Unashamed

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

Tipo:	-Infector de MBR, Boot Sector -Encriptado -Residente -Stealth
Número de Sectores	1
Origen:	USA
Destructivo:	SI
En la calle (in the wild):	SI

Descripción

El virus NAKED (UNashamed) fue detectado por primera vez en el Perú (Lima) en Mayo de 1995.

Infecta el MBR (Partición) de los discos duros y BOOT SECTOR de disquete. Utiliza técnicas de STEALTH para evitar ser detectado.

Este virus toma control absoluto de las operaciones de DISCO, permitiendo SOLO procesos de lectura/escritura, cualquier otra operación como formateo de discos, verificación de sectores, etc no pueden ser realizadas.

Un síntoma común en una PC infectada con Naked es que el usuario no puede formatear ningún disquete, siempre recibe el mensaje del DOS: 'Pista 0 inválida, disquete inservible'

Algunas partes del virus se encuentran encriptadas.

Cuando se activa, muestra en el centro de la pantalla en formato de 40 columnas (letras grandes) el siguiente mensaje:
the UNashamed Naked!
y cuelga la computadora.

Nombre:	**Monkey** **Alias:**
Tipo:	Infector de MBR y Boot sector -Residente, stealth, Encriptado
Número de sectores	2
Origen:	USA
Destructivo:	SI (Indirectamente)
En la calle (in the wild):	SI

Descripción

Infecta el MBR de los discos duros y el BOOT de los disquetes.

La primera vez que se butea la PC desde un disquete infectado el virus lee el MBR, lo encripta y lo copia al sector 3 del disco duro, inmediatamente se enlaza a la INT 13 e infecta el MBR invalidando la tabla de partición (esta es sobreescrita con el código del

virus). Terminado el proceso el virus lee el sector 7 (MBR original), lo desencripta y le cede el control.
Cuando el DOS o cualquier otro programa tratan de "ver" el MBR actual Monkey filtra la operación (INT 13h), lee el sector 7 (MBR original encriptado), lo desencripta y lo retorna como MBR actual.
El usuario no nota nada raro a menos que butee desde un disquete limpio, donde se dará cuenta que no puede accesar al disco duro porque el DOS no reconoce una partición válida en el MBR, el motivo es que el usuario buteo limpio y el DOS SI "vio" el MBR actual (infectado).
Para eliminar el virus monkey con The Hacker Antivirus:

1. Butee el sistema desde un disquete DOS limpio
2. Ejecuta el programa TH.EXE
3. En el menú detectar seleccione [MBR en disco duro] en vez de la opción usual ([DISCO]) y elija el número de disco duro deseado
4. En el menú detectar elija [Detectar y eliminar]. Bingo! el virus está fuera.
5. Reinice la PC y su disco duro está nuevamente con Ud sin virus.
6. TH revisa y elimina el virus del MBR/Boot aún si el DOS no reconoce el disco duro como unidad C:

Como parte del virus se encuentra su nombre en forma codificada. "Monkey 1992"

Nombre:	**JS/Frist** **Alias:** JS.Frist, JS.Firstpart, JS/Frist.ow.dr
Tipo:	Virus
Tamaño:	1,149 bytes
Origen:	Internet
Destructivo:	SI
En la calle (in the wild):	SI
Detección y Eliminación	The Hacker 5.3 y 5.4, Registro de Virus al 24/12/2002

Descripción
JS/Frist, es un virus escrito en JavaScript, sobrescribe todos los archivo de extensión .js que encuentre en el computador infectado, además tambien crea un **Acceso Directo** en el **ESCRITORIO** de Windows llamado **Editor.lnk** que tiene asociado el icono del **Block de Notas** (NOTEPAD), si se ejecuta este enlace se estara ejecutando el archivo del virus **FIRST.JS**.
Cuando el virus se ejecuta se copia a sí mismo como **FIRST.JS** en el directorio actual, seguidamente crea y ejecuta el archivo **DROP.BAT** en la carpeta actual, este copia el archivo **FIRST.JS** en todos los archivos con extensión **.JS** que encuentre en las siguientes ubicaciones:

- Carpeta actual
- Unidad Raiz del disco duro actual.
- En la carpeta padre de la carpeta actual
- Todos los directorios incluidos en la variable path

- En la carpeta Windows
- En la carpeta %tmp%

Tambien Copia el archivo **First.js** en :
C:\WINDOWS\startm~1\progra~1\autost~1\win.js.
Finalmente el virus se elimina a sí mismo una vez que todas las acciones anteriores han sido realizadas

Nombre:	**JAVA/StrangeBrew** **Alias:**
Tipo:	Infecta Java Applets y Aplicaciones Java
Tamaño	3890 bytes (2826 de código)
Origen:	Internet/1998
Destructivo:	NO
En la calle (in the wild):	NO

Descripción
Este es el primer virus capaz de infectar Java Applets y Aplicaciones Java.
Java/StrangeBrew puede infectar solamente si es ejecutado como una aplicación Java. Si se intenta ejecutar un Java Applet infectado desde un Navegador (Netscape, Internet Explorer, el sistema mostrará un mensaje de error y terminará el Applet.
Dado que el virus no se propaga a través de Java Applets, los usuarios no podrán contagiarse con el virus simplemente navegando en Internet.

Infección
Cuando se ejecuta una aplicación Java infectada el virus busca archivos *.class (Applets y Aplicaciones) en el directorio actual y los infecta. Este virus es multiplataforma, capaz de replicar en cualquier sistema operativo que soporte JAVA.

Nombre:	**JAVA/BeanHive** **Alias:**
Tipo:	Infecta Java Applets y Aplicaciones Java
Tamaño	Variable, cargador de 160 bytes de código aprox.
Origen:	Internet/1998
Destructivo:	NO
En la calle (in the wild):	NO

Descripción
Este es el segundo virus que infecta JAVA Applets y Aplicaciones Java. JAVA/BeanHive fue escrito por "Landing Camel", la misma persona que escribió JAVA/StrangeBrew (el primer virus de Java).
JAVA/BeanHive infecta Java Applets y Aplicaciones Java. El virus puede propagarse solamente si el usuario importa en NetScape o Internet Explorer un certificado directo del creador del virus.
Este certificado permite a los Java Applets acceder a funciones de disco (Abrir, Cerrar, Escribir archivos) sin emitir un mensaje de advertencia por parte del navegador. Sin el

certificado, el Navegador Web emite un mensaje de error y el Applet no podrá ser ejecutado.
Java/BeanHive consta de 2 partes: Un cargador y el código principal.
Las aplicaciones Java infectadas contienen solamente el cargador. El código principal del virus reside en un servidor WWW en Usa propiedad de los creadores del virus.
Cuando se ejecuta una aplicación Java, el cargador se conecta al servidor WWW en Internet, baja el código principal del virus y lo ejecuta.
El código principal del virus se encarga de localizar archivos *.class limpios en el directorio actual y sus subdirectorios y los infecta solamente con el cargador.
Esta modalidad de infección permite a los escritores del virus modificar las características del código principal, léase "actualizarlo" o modificarlo.
Por ejemplo los escritores del virus podrían fácilmente modificar el cuerpo principal del virus de tal forma que obtenga una lista de aplicaciones, configuración del sistema, passwords que el usuario posee y los envíe a su Web.

Nombre:	**WM/Rehenes** **Alias:** Abracadabra o Fuji
Tipo:	Macrovirus, infecta documento de ms-word 6.x/7.x, office 97
Número de macros:	2 : autoOpen, HerramMacro, (no encriptados) tamaño: 4584 bytes
Origen:	Lima/Perú, 23-Mayo-1997
Destructivo:	SI
En la calle (in the wild):	NO

Descripción
WM/Rehenes es un variante del virus **WM/Wazzu** e infecta la plantilla global (normal.dot) cuando un documento infectado es abierto, posteriormente todos los documentos abiertos por el usuario serán infectados.
WM/Rehenes tiene algunas capacidades de stealth (volverse invicible). Si el usuario utiliza la opción del menú Herramientas/Macros el virus filtra la operación y presenta una ventana parecida a la original que no muestra ninguna macro (cuando hay 2: **autoOpen, HerramMacro**).
Cada vez que se abre un documento infectado el virus inserta aleatoriamente en el documento una de las siguientes frases:

- Fujimori al 2005
- libertad! 22 de Abril de 1997
- en memoria de los caídos en la crisis de los rehenes
- Para conseguir el antivirus contactarse con nicolas@amauta.rcp.net.pe y preguntar por el Sr. Lúcar o con el Sr Montesinos a montesinos@colina.sin.mil.pe"
- ¡¡¡La pareja del año: Fujimori y Beatriz Boza!!! Es lo que dice Susana, no se si es por celosa o porque le gusta que Betty sea mi calenta
- fuera clones malignos
- ¿Alumno de una conocida Universidad del Perú, Sr. José Martínez?

Inmediatamente muestra una caja de diálogo similar a:

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

> Mensaje del día: xxxxxxxxxxxxxxxxxxxxxxxxxxxxx
>
> [ACEPTAR]

Donde 'xxxxxxxxxxxx' puede ser aleatoriamente:

- Fujimori al 2005
- Para conseguir el antivirus contactarse con nicolas@amauta.rcp.net.pe y preguntar por el Sr. Lúcar
- Se quedaron Machado y Martinez, no podrán conmigo... Muajaja!!!
- Hip!
- Kenyi, anda preparándome el discurso para el 28 de Julio del 200
- Quiero una jugadora bien piernona pa meterle la yuca hasta Alfonso
- Soy Alberto Fujimori, Presidente Constitucional de la República Peruano-Japonesa del Perú, es decir, colonia de Japón >)
- ¡Susana! Prepárate que en el 2000 me caso con Chuchy Díaz
- Para el 2010 prometo regresar de cachimbo a la Agraria jiji >)
- Montesinos, prepara el grupo Colina, para tomar la Residencia blanquiazul de la Universidad Para Corchos jijajija >)"
- Oye, cabezón (Trelles), que la San Ganazo (SIL) no me ponga las pensiones en dólares pe! porque me afecta la economía
- Oye, en esa Universidad Alas Peruanas... nacieron para huevear
- Que intervengan esa Universidad con nombre de chocolate (Winner)
- Que en la UPC vayan preparando Creatividad Presidencial rumbo al 2000, pero inviten de nuevo a las chicas Coca-Cola"
- En la próxima Creatividad Imperial sólo se presentarán el Emperador Alberto y el Príncipe Kenyi, a ver quien gana... >)
- A esa Susana le falta Nicovita..."
- Mi próximo Ministro de Economía será Orlando Nicolini (...es de la familia)
- Ese Andradre me está quitando la cholidaridad
- Yuki, nueva capital del Perú, año 2050, la Emperatriz Keiko V disolverá los últimos grandes animales prehistóricos (Iglesia Católica, el Poder Judicial y el Seleccionado Nacional de Fútbol)
- Disolver! Disolver el Congreso Peruano, para no tener oposición para el 2000

El autor de este virus es conocido como "Johnny Cracker" y es alumno de una conocida Universidad del Perú.

Nombre:	**Exploit-MIME** **Alias:** Exploit-MIME.gen, Exploit-MIME.gen.b, Exploit-MIME.gen.exe
Tipo:	Virus
Tamaño:	Variable
Origen:	Internet
Destructivo:	SI
En la calle (in the wild):	SI

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

Detección y Eliminación	The Hacker 5.1, Registro de Virus al 21/11/2001

Descripción

Exploit-Mime, es un virus que llega en los mensajes de Email, aprovecha la vulnerabilidad del Microsoft Incorrect MIME Header vulnerability (puntero MIME incorrecto).Esta vulnerabilidad permite que los archivos adjuntos se ejecuten cuando un mensaje es simplemente visualizado.

Algunos de los virus que hacen uso de esta vulnerabilidad son W32/Badtrans@MM, W32/Nimda.gen@MM, y W32/Klez.gen@MM entre otros.

Recomendaciones

Algunas recomendaciones para corregir la vulnerabilidad Incorrect MIME Header, la puede hallar visitando el siguiente enlace :
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-020.asp

Nombre:	**Spanska.4250** **Alias:** Elvira, Spanska_II
Tipo:	-Infector de archivos EXE y COM -Encriptado -Residente -Stealth
Tamaño	4250 bytes
Origen:	España/Internet
Destructivo:	NO
En la calle (in the wild):	SI

Descripción

El virus Spanska.4250 es un virus polimórfico complejo muy reportado a inicios de Enero/98. Es residente en memoria e infecta archivos .EXE y .COM.

La primera vez que se ejecuta un archivo infectado con Spanska.4250, el virus se coloca residente en memoria ocupando 8K de memoria convencional, se enlaza a la INT 21h para tener el control total del sistema e inmediatamente procede a infectar el archivo 'C:\WINDOWS\WIN.COM'.

El virus contiene código parecido al virus **Natas.4774**, entre otros:

- No infecta archivos que empiezan con los siguientes nombres: TB*.*, VI*.*, AV*.*, NA*.*, VS*.*, FI*.*, F-*.*, FV*.*, IV*.*, DR*.*, SC*.*.
- Cuando se ejecuta un programa de compresión, empaquetador, backup conocido (PK*.*, AR*.*, RA*.*, LH*.*, BA*.*) el virus deshabilita sus rutinas de stealth para que el programa trabaje con el archivo infectado.

El virus se activa si un archivo infectado es ejecutado en minutos=30 y segundos <= 16, en ese momento procede a mostrar varios mensajes en la pantalla tipo efecto 'Guerra de las galaxias' (Star Wars).

ELVIRA !

Black and White Girl

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS
from Paris
You make me feel alive.
ELVIRA !
Pars. Reviens. Respire.
Puis repars.
J'aime ton mouvement.
ELVIRA !
Bruja con ojos verdes
Eres un grito de vida,
un canto de libertad.

Nombre:	**Die** **Hard** **Alias:** duro de matar
Tipo:	-Infector de archivos EXE y COM -Encriptado -Residente -Stealth
Tamaño	4000 bytes
Origen:	SudAfrica/1995
Destructivo:	NO
En la calle (in the wild):	SI

Descripción

DIE HARD está en la lista de los 10 virus más comunes en Perú (con WM.Wazzu, AntiExe, etc). Die Hard fue detectado en Perú en Diciembre de 1995.

DIE HARD es un virus residente en memoria que infecta archivos .EXE y .COM aumentándoles de tamaño en 4,000 bytes.

La primera vez que se ejecute un archivo infectado, el virus se coloca residente en memoria infectando todo archivo .EXE y .COM que sea ejecutado y/o abierto. Cuando el virus está en memoria, utiliza técnicas de STEALTH para evitar ser detectado, desinfecta "al vuelo" los programas infectados que intentan ser analizados.

Die Hard tiene varias rutinas de activación:

* Si es Jueves y el día es 3, 11, 15, 18 envía al COM1 la cadena: " SW Error "
* Escribe al comienzo de archivo .PAS o .ASM la siguiente rutina:

En archivos .ASM

```
.model small
.code
org 256
s:
push cs
pop ds
call t
db ''DN$"
pop dx
mov ah, 9
```

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS
int 33
mov ah, 76
int 33
end s
En .PAS:
begin
writeln('DS');
end.
El virus usa técnicas de STEALTH para que el usuario no pueda notar el cambio en sus programas.
Si un contador interno llega al valor 15 o superior y el modo de vídeo actual es 13h (gráfico) displaya un gráfico violeta que dice: " SW "
Como parte del código del virus se pueden encontrar el siguiente texto: SW DIE HARD 2

Nombre:	**Diablo** **Alias:** SM-Boot
Tipo:	Infector de MBR y Boot sector -Residente, stealth
Número de sectores	1
Origen:	España/1995
Destructivo:	SI
En la calle (in the wild):	SI

Descripción
El virus **DIABLO** fue detectado en Lima en Agosto de 1995.
DIABLO es un simple virus que infecta el MBR de los discos duros y Boot Sector de disquete. Es residente en memoria y utiliza algunas técnicas de STEALTH para engañar a otros programas que el MBR o BOOT no ha sido modificado.
DIABLO es **DAÑINO!!!**. Debido a un error de programación en el virus, **DIABLO** puede perder algunas entradas de directorio y generar 'cluster perdidos' o 'unidades de asignación cruzadas'.
El error se produce aleatoriamente cuando se graba información en las entradas de directorio.
Como parte del virus se puede encontrar lo siguiente: DIABLO

Nombre:	**Coruna4** **Alias:**
Tipo:	Infector de MBR y Boot sector -Residente
Número de sectores	1
Origen:	?, Aislado en Perú en Setiembre/97

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

Destructivo:	SI
En la calle (in the wild):	SI

Descripción

Coruna4 es un nuevo virus de Boot que ha empezado a ser reportado en setiembre de 1997 en Lima y Provincias (Iquitos, Trujillo, Ica).

Coruna4 es un virus infector de MBR en discos duros y Boot Sector en disquetes. La única forma de infectar el disco duro es buteando desde un disquete infectado en la unidad A, en ese momento el virus se ejecuta y procede a infectar el primer disco duro.

Coruna4 no salva el MBR o Boot original en ninguna parte del disco, simplemente sobreescribe el MBR o boot con el código del virus. Coruna4 asume que la Boot activa que carga al sistema operativo se encuentra en la pista=0, cara=1, sector=1.

Coruna4 es dañino, un mes después de la infección del disco duro sobreescribe con basura casi la totalidad del disco.

Coruna4 fue reportado "in the wild" por primera vez en el Perú en Setiembre/1997.

Dentro del código del virus se puede encontrar:

"HDKiller By Rasek.¡0UT Meilán!"

Nombre:	**WM/Concept** **Alias:** Word Prank Macro, WW6Macro
Tipo:	Macrovirus, infecta documento de ms-word 6.x/7.x/8.x, Numero de Macros: 4 : AutoOpen, AAAZAO, AAAZFS (FileSaveAs), PayLoad (no encriptados)
Tamaño	1968 bytes
Origen:	USA, Julio/1995
Destructivo:	NO
En la calle (in the wild):	SI

Descripción

Es un macro virus que ha sido escrito utilizando el macro lenguaje WordBasic de Microsoft Word v6.x, este virus es capaz de moverse a través de archivos de documentos en las siguiente plataformas:

Microsoft para Windows v6.x y v7.x, Word para Macintosh v6.x, Word para Windows95 y en ambiente Windows NT.

Este virus se ejecuta cada vez que un documento infectado es abierto (AutoOpen), antes de la infección, Concept revisa si la plantilla global ya está infectada, si no se encuentran las macros ''PayLoad" o "FileSaveAs" asume que no está, copia sus macros (la macro AAAZFS es copiada como FileSaveAs).

Después de la infección añade la variable WW6I=1 al archivo Win.ini y displaya la siguiente caja de diálogo:

Una vez que la plantilla global ha sido infectada, todos los documentos que son creados con el comando 'FileSaveAs' serán infectados.
Como todos los Macrovirus, cuando un documento es infectado, internamente se convierte en una plantilla.
El virus Concept fue el primer Macro virus encontrado en la calle (infectando a los usuarios).

Nombre:	**BOZA** **Alias:** Win95.Boza, Bizatch, V32
Tipo:	-Infector de archivos .EXE (PE/32bits)
Tamaño	2704 - 2887 bytes
Origen:	Australia, Febrero/1997
Destructivo:	NO
En la calle (in the wild):	NO

Descripción
Este es el primer virus que ha sido diseñado específicamente para infectar bajo el sistema operativo Windows 95, fue detectado por primera vez en Febrero de 1996 en el mundo y ha generado mucha atención. Boza utiliza rutinas del Kernel32 de Windows 95 para infectar archivos .EXE de 32 bits (archivos PE de Windows 95 y Windows NT).
Si un archivo infectado es ejecutado en Windows NT el virus no se activará.
Cuando un archivo infectado es ejecutado, el virus busca 3 archivos .EXE 'limpios' en el directorio actual y los infecta, si no existen archivos 'limpios' en el directorio actual el virus continua buscando en el directorio anterior (directorio '..').
Este virus no tiene rutinas destructivas pero contiene algunos errores de programación lo que ocasionará en algunos casos que un archivo infectado aumente de tamaño en varios megabytes.
Boza se activa el día 31 de cualquier mes mostrando la siguiente caja de diálogo:
"The taste of fame just got tastier!"
"VLAD Australia does it again with the world's first Win95 Virus."

- From the old school to the new.
  Metabolis
  Qark
  Darkman
  Automag
  Antigen
  RhinceWind
  Quantum
  Absolute Overload
  Coke

Otros textos son:
Please note the name of this virus is [Bizatch] written by Quantum of Vlad Bizatch by Quantum / VLAD.

Nombre:	**Byway** **Alias:** WaiChan, Venezolano, Chavez, Dir.Byway

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

Tipo:	-Infector de archivos .EXE .COM -Residente -Stealth total -Polimorfico
Tamaño	2048 bytes
Origen:	Venezuela/1995
Destructivo:	SI (indirectamente)
En la calle (in the wild):	SI

Descripción

El virus ByWay (Alias: **Wai-Chan**) fue detectado por primera vez en Perú en Enero de 1996.

Este virus al parecer fue creado por un profesor de la Universidad Central de Venezuela llamado Wailang Chang en Agosto de 1994.

ByWay es residente en memoria, polimórfico y utiliza avanzadas técnicas de STEALTH.

La primera vez que se ejecuta un archivo infectado en una maquina limpia, el virus crea un archivo oculto en el directorio raíz llamado "CHKLISTx.MSx" ('x' es un blanco ficticio Alt-255) donde coloca su código, el tamaño del archivo es 2,048 bytes.

El autor del virus utiliza el nombre "CHKLISTx.MSx" para inducir al usuario a pensar que se trata de un archivo creado por el Anti-Virus MSAV que viene con el DOS. (Los archivos creados por MSAV se llaman CHKLIST.MS, tiene cualquier tamaño y pueden estar en más de 1 directorio).

Byway es un virus de CLUSTER o DIRECTORIO.

La forma de infección en el virus Byway es diferente a los demás virus, cuando el virus infecta un archivo reemplaza solamente el número del primer cluster que el archivo tiene asignado; el nuevo número apunta al cuerpo del virus (archivo CHKLISTx.MSx), el virus no modifica el contenido o tamaño del archivo infectado. Solamente existe una copia del virus en todo el disco. Es importante que el usuario no borre o altere el archivo "CHKLISTx.MSx", de lo contrario todos los archivos infectados serán dañados.

La versión original de este virus infecta sólo archivos .COM en disco duro y archivos .COM/.EXE en disquetes. Otras versiones pueden infectar archivos .COM y .EXE en discos duros.

La rapidez con la que Byway infecta un disco es asombrosa, un simple DIR resultará en todos los archivos *.COM *.EXE infectados. BYWAY es DAÑINO!!!. Por su forma de infección, todos los archivos infectados tienen unidades de asignación cruzadas y clusters perdidos.

NO intente utilizar diagnosticadores de disco (CHKDSK, NDD, DISKFIX, SCANDISK) en un disco contaminado, porque todos los programas infectados serán dañados en vez de ser corregidos.

Byway contiene una bomba lógica que se activa a partir del año 1996 los siguientes días: 4-enero, 6-febrero, 8-marzo, 10-abril...etc (incremento de dos días por mes).

En estas fechas, después de un momento de haber trabajado con la PC aparece un mensaje girando en la primera línea de la pantalla que dice:

TRABAJEMOS TODOS POR VENEZUELA !!! y las notas del Himno Nacional de Venezuela.

Como parte del virus se puede encontrar los siguientes textos (algunos encriptados):

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS
Versión Byway.a:
<by:Wai-Chan,Aug94,UCV>
The-HndV
CHKLIST MS
Versión Byway.b:
By:W.Chan
The-HndV

Nombre:	**CACO** **Alias:** GENE-101, AFM, RAFAEL
Tipo:	Infector de archivos .EXE, .COM, Residente, Stealth
Tamaño	2675 bytes
Origen:	Perú, Julio/1994
Destructivo:	NO
En la calle (in the wild):	SI

Descripción
Fue detectado por primera vez en el Perú en Julio de 1994 en la ciudad de Lima. Es una variante del virus **SVC.** Infecta archivos ejecutables **EXE** y **COM**, puede infectar el **COMMAND.COM.** Es residente en memoria y utiliza técnicas de STEALTH para evitar ser detectado mientras está en memoria.
Muchas partes del virus original SVC han sido modificadas. Este virus puede dañar al momento de la infección archivos que manejan overlays internos. Se activa a partir de noviembre de 1994, mostrando en la primera línea de la pantalla el siguiente mensaje en forma permanente:
CACO VIRUS GENE-101.COCO, ALDO, CHINO, OTTO DOOM-TEAM &CREADORES DE VIRUS&
Este mensaje es mostrado en la primera variante conocida, pero se conocen otras Variantes:
A&F&M&: Casi idéntico al supuesto original, con la diferencia que los mensajes están encriptados, contiene: A&F&M&T&l&f:2&7&-6&9&9&1 (?)
RAFAEL: Esta variante muestra el mensaje "TIENES EL VIRUS RAFAEL LLÁMAME PARA ELIMINACIÓN TLF:27-????" en el centro de la pantalla después de 2 horas de haber ejecutado un programa infectado.
Existen algunas "variantes" donde sólo se ha modificado el mensaje de CACO ..., por otros mensajes, por lo demás el virus es idéntico al original o variantes.

Nombre:	**W32/PrettyPark.worm** **Alias:** Pretty Worm, PrettyPark, Trojan.PSW,CHV
Tipo:	Gusano
Tamaño	37Kb (original), 60Kb (Variante .unp)
Origen:	Francia
Destructivo:	NO

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

En la calle (in the wild):	SI
Variantes conocidas:	W32/Prettypark.worm (06/Julio/1999, The Hacker 4.5 y posterior) - W32/Prettypark.worm.unp (01/03/2000, The Hacker 4.8 y posterior)

Descripción

W32/PrettyPark es un gusano que llega por E-mail en el archivo "Pretty Park.EXE" con un icono de un muñeco de la serie "SouthPark".

Al abrir el archivo infectado PrettyPark.Exe el gusano se copia al folder Windows\System como FILES32.VXD y modifica una llave en el registro para ejecutarse en forma automática cada vez que se abre una aplicación tipo .Exe, todas las aplicaciones .Exe se vuelven dependientes del archivo files32.Vxd y dejarán de funcionar si este archivo es borrado del disco.

Llave del registro modificada: HKEY_LOCAL_MACHINE\Software\CLASSES\exefile\shell\open\command

Una vez activo el gusano, se envía automáticamente a todas las direcciones del Libro de direcciones Internet cada 30 minutos.

El gusano tiene backdoors, se conecta a varios servidores IRC y se une a un canal "avisando" que la PC está disponible. Hipotéticamente el autor del gusano vía el IRC puede obtener información de nuestra PC como password, archivos, etc.

ACTUALIZACION

01/03/2000: A finales de febrero del 2000 se detectó una variante descomprimida conocida como W32/PrettPark.worm.unp, esta variante ha sido alterada para evitar ser detectada por todos los antivirus del mercado, por lo demás la funcionalidad de este gusano es idéntica al original.

LIMPIANDO W32/PrettyPark.worm y W32/PrettyPark.worm.unp DE UNA PC

Como se indicó anteriormente el gusano reside en el archivo files32.vxd. Para limpiar el gusano de la PC el archivo files32.vxd debe ser borrado del disco duro pero antes se debe corregir la llave en el registro que hace dependiente las aplicaciones .Exe de este archivo.

Aquí los pasos para limpiar el gusano:

1- Si no tiene el archivo pretty.reg bajelo desde http://www.hacksoft.com.pe/pretty.reg , este archivo contiene los pasos necesarios para eliminar la llave en el registro modificada por el gusano.

2- Abra el archivo pretty.reg con el explorador de Windows, cuando el Explorador de Windows pregunte si desea actualizar el registro indique que SI.

Este paso recupera la llave del registro modificada por el virus.

3- Borre el archivo files32.vxd que se encuentra en Windows\System.

El archivo puede ser borrado con el Explorador de Windows, vía MS-DOS o con The Hacker indicando en la acción "Detectar y Borrar"

4- El virus está fuera!

Nota: El archivo pretty.reg puede ser creado con un editor de texto como NOTEPAD.EXE y debe tener el siguiente contenido:

```
REGEDIT4
[HKEY_LOCAL_MACHINE\Software\CLASSES\exefile\shell\open\command]
@="\"%1\" %*"
```

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

Nombre:	**W32/Cholera.Worm** **Alias:** I-Worm.Cholera
Tipo:	Gusano, crea el archivo rpcsvr.exe y modifica WIN.INI
Tamaño	47 Kbytes aprox.
Origen:	España, Setiembre/1999
Destructivo:	NO
En la calle (in the wild):	NO

Descripción

W32/Cholera.worm y W32/CTX son las nuevas creaciones de Griyo del grupo Español 29A, este grupo es responsable de la mayoría de los virus para plataforma Windows existentes hoy en día, incluyendo Win32/Cabanas, Win95/Marburg, Win95/HPS.

W32/Cholera.worm es un gusano típico de Internet que utiliza el e-mail para autoenviarse, viaja en el archivo SETUP.EXE, no hay ningún mensaje en el e-mail excepto un carita sonriente ";-)".

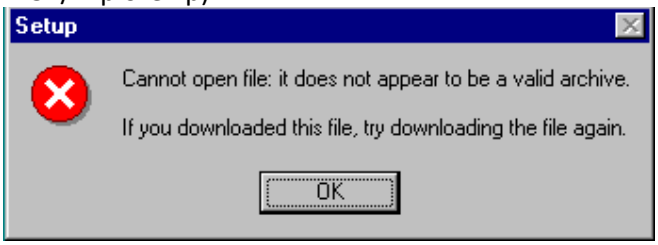
W32/CTX es un virus polimórfico de 32bits, cada vez que un archivo infectado es ejecutado el virus infecta hasta 5 archivos en el folder actual, Windows y Windows\System.

Aunque ambos especímenes son diferentes y funcionan en forma separada (Cholera es un gusano y CTX un virus) , Griyo (el autor del virus) ha propagado sus creaciones en lo que él llama el "Proyecto Simbiosis", el cual consiste en propagar copias del archivo SETUP.EXE (utilizado por Cholera) infectado con el virus CTX.

W32/CHOLERA.WORM - INSTALACION

El gusano llega por E-mail en un attachment como Setup.exe, si el usuario abre (ejecuta) este archivo se activa el worm, lo primero que hace es crear el archivo RPCSRV.EXE en el folder de Windows y añade la entrada run=rpcsrv.exe en el archivo WIN.INI para que el gusano se ejecute automáticamente cada vez que se inicia Windows, después de esto el gusano comienza a buscar otras instalaciones de Windows en directorios \WINDOWS, \WIN95, \WIN98, \WIN, \WINNT, si ubica alguno, modifica el archivo win.ini de este directorio añadiendo el comando run=rpcsrv.exe

Terminada su instalación muestra un mensaje para engañar al usuario que el archivo setup.exe está dañado (este truco es similar al empleado por el gusano W32/ExploreZip)



W32/CHOLERA.WORM - PROPAGACION

La siguiente vez que se inicia Windows se ejecuta el gusano desde el archivo RPCSRV.EXE, en esta ocasión el gusano no muestra ningún mensaje y crea 2 procesos simultáneos corriendo en background:

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

1- En el primer proceso al igual que en la instalación original el gusano busca instalaciones de Windows pero esta vez en UNIDADES de RED, si encuentra alguna instalación de windows, copia el archivo RPCSRV.EXE y modifica el archivo win.ini del disco de la red.

2- El segundo proceso envia archivos infectados por E-Mail, el gusano no trabaja con ningún lector de correo específico como OutLook, Exchange ó Eudora sino que tiene su propio manejador SMTP.

Para saber a que víctimas enviar el archivo setup.exe, el gusano busca archivos .HTM, .TXT, .EML, .DBX, .MBX, .NCH, .IDX y extrae todas las direcciones E-mail que encuentre.

NOTAS:

-El archivo SETUP.EXE propagado originalmente por Griyo/29A está infectado con el virus W32/CTX, con lo que al abrir el archivo setup.exe el usuario también será infectado con este virus (mas información en W32/CTX).

- El gusano no necesita del virus W32/CTX para propagarse por e-mail. Es posible encontrar en el futuro copias de SETUP.EXE sin Win32/CTX.

Nombre:	**W32/Fix.worm** **Alias:** I-Worm.Fix2001
Tipo:	Gusano
Tamaño	12 Kbytes
Origen:	Internet, Octubre/1999
Destructivo:	SI
En la calle (in the wild):	SI
Detectado desde:	The Hacker 4.6 registro al 29/10/1999 y superiores.

Descripción

W32/Fix es un gusano que se propaga automáticamente vía E-Mail en sistemas con Windows 95/98, el gusano no funciona con Windows NT/2000.

El gusano viaja en un mensaje que se supone es un parche para el error del año 2000, adjunto al mensaje viene el archivo "FIX2001.EXE" infectado.

Sujeto: Internet problem year 2000
De: "Admin__"
Estimado Cliente:
Rogamos actualizar y/o verificar su Sistema Operativo para el correcto funcionamiento de Internet a partir del A_o 2000. Si Ud. es usuario de Windows 95 / 98 puede hacerlo mediante el Software provisto por Microsoft (C) llamado -Fix2001- que se encuentra adjunto en este E-Mail o bien puede ser descargado del sitio WEB de Microsoft (C) HTTP://WWW.MICROSOFT.COM
Si Ud. es usuario de otros Sistemas Operativos, por favor, no deje de consultar con sus respectivos soportes tecnicos.
Muchas Gracias.
Administrador.
Internet Customer:

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

We will be glad if you verify your Operative System(s) before Year 2000 to avoid problems with your Internet Connections.
If you are a Windows 95 / 98 user, you can check your system using the Fix2001 application that is attached to this E-Mail or downloading it from Microsoft (C) WEB Site: HTTP://WWW.MICROSOFT.COM
If you are using another Operative System, please don't wait until Year 2000, ask your OS Technical Support.
Thanks.
Administrator"

Si el usuario ejecuta el archivo adjunto FIX2001.EXE se muestra el mensaje:
Your Internet Connection is already Y2K, you don't need to upgrade it,
en forma oculta el gusano se instala en el sistema y propaga de la siguiente forma:
Instalación
El gusano copia el archivo FIX2001.EXE al folder WINDOWS\SYSTEM y modifica el registro ("Run=") para ejecutarse en cada inicio de Windows.
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
"Fix2001" = "FIX2001.EXE"

Propagación

Al siguiente inicio de Windows se ejecuta el archivo FIX2001.EXE que busca el archivo WSOCK32.DLL en memoria y parcha 2 de sus rutinas (Send y Connect), si el usuario envía un mensaje vía E-mail, el gusano extrae el recipiente y le envia el mensaje del supuesto parche del año 2000 con el archivo infectado FIX2001.EXE djunto.

Rutina de Activación

W32/Fix es DAÑINO, si el archivo FIX2001.EXE es alterado de alguna forma el gusano sobreescribe el archivo "C:\COMMAND.COM" con un troyano. Al siguiente inicio del sistema el troyano borrará toda la información del disco duro.

Recomendaciones para sistemas infectados

- Al ser W32/Fix.worm un gusano que trabaja bajo windows tiene que ser eliminado en modo DOS debido a que los archivos infectados están en uso por windows y no pueden ser alterados.

Nombre:	**HLL.Irok.worm** **Alias:**
Tipo:	Gusano/Virus, infecta archivos EXE y COM, se envía por E-mail/mIRC
Tamaño	2 Variantes: 10,001 y 7,877 bytes
Origen:	Internet, Abril/2000
Destructivo:	SI
En la calle (in the wild):	NO
Detectado desde:	The Hacker 4.8 registro al 05/04/2000 y posteriores

Descripción

HLL.Irok.worm es un gusano que se propaga por E-mail y clientes mIRC. Vía E-mail el gusano llega en un mensaje con el attachment IROK.EXE

Caracteristicas del Mensaje de Email:

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

Sujeto: I thought you might like to see this.

Cuerpo: Body I thought you might like this. I got it from paramount pictures website. It's a startrek screen saver.

Si el usuario ejecuta el attachment, se muestra una ventana con efectos tipo galaxia. En forma oculta el gusano infecta todos los archivos *.exe, *.com del fólder actual y todos los indicados en la variable Path del autoexec.bat, el virus tiene muchos errores y los archivos infectados casi siempre dejan de funcionar. Finalizado la infección de archivos, el gusano se copia al fólder **c:\windows\system** y crea IROKRUN.VBS en el fólder **C:\Windows\StartMenu\Startup** para ejecutarse automáticamente en cada inicio de windows.
Inmediatamente el gusano envía por E-mail el archivo infectado "Irok.exe " a los 60 primeros contactos del libro de direcciones del outlook.
El gusano también se propaga vía el mIRC, modifica el script.ini para enviar (DCC) en forma automática el archivo Irok.exe a todos los usuarios conectados en el mismo canal que el usuario "infectado".

HLL.Irok es dañino, al azar borra el contenido del disco duro.

Nombre:	**JS/CoolNow.A** **Alias:** Js/Messenger-Exploit, JS/CoolNow, JS_MENGER.GEN, MENGER.GEN, JScript/CoolNow.Worm, Menger, JS/Menger.Worm.
Tipo:	Gusano de JavaScript
Tamaño	N/Determinado
Origen:	Internet
Destructivo:	NO
En la calle (in the wild):	SI
Defección/Eliminación:	The Hacker 5.1 al 14/02/2002.

Descripción

El JS/CoolNow.A es un gusano de JavaScript que utiliza una vulnerabilidad del Internet Explorer que afecta al MSN Messenger. El gusano utiliza esta vulnerabilidad para enviar mensajes a todos los contactos del MSN Messenger.
El gusano envía un mensaje a todos los contactos del MSN Messenger pidiendo que visiten una página web la cual se encuentra infectada con un código en Javascript. Si el usuario visita la página web se mostrará en el título de la ventana el mensaje "Please Wait...", además este mismo mensaje aparecerá dentro de la Pagina Web. Al activarse el código Script el gusano comenzará a enviar mensajes a los usuarios de la libreta de contactos del MSN Messenger.
Los textos de los mensajes pueden ser:
"Hey Go to http://www.geocities.com /.../teztx1.htm plz"
"URGENT - Go to http://www.rjde.. /cool Now"
"ATTeNT!oN - Go to: http://www.geocities.com/... /teztx1.htm"
Luego envía un e-mail al supuesto autor del gusano con la información obtenida sobre todos los contactos del MSN Messenger.

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

Se recomienda instalar el parche de Microsoft contra esta vulnerabilidad, parche disponible en: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-005.asp

Nombre:	**JS/Gigger.a@MM** **Alias:** JS_GIGGER.A, JS.Gigger.A, VBS_GIGGER.A, IRC_GIGGER.A, JS.Gigger.A@mm, GIGGER.A
Tipo:	Gusano
Tamaño	8,556 bytes
Origen:	Internet
Destructivo:	SI
En la calle (in the wild):	SI
Defección/Eliminación:	The Hacker 5.1 al 12/01/2002

Descripción

JS/Gigger.a@MM es un gusano que se transmite vía E-mail en un archivo **"Mmsn_offline.htm"** enviándose a todos los contactos en la libreta de direcciones de Windows. El gusano también utiliza el mIRC para enviarse.

Características del mensaje de E-mail:

Asunto: Outlook Express Update
Cuerpo: MSNSofware Co.
Archivo Adjunto: Mmsn_offline.htm

Al ser ejecutado el gusano, crea los siguientes archivos:
C:\BLA.HTA
C:\B.HTM
C:\T.TXT
C:\WINDOWS\HELP\MMSN_OFFLINE.HTM
C:\WINDOWS\SAMPLES\WSH\CHARTS.JS
C:\WINDOWS\SAMPLES\WSH\CHARTS.VBS

Ademas si la Pc infectada utiliza el mIRC, el gusano crea un archivo SCRIPT.INI; este archivo sobreescribe a todos los archivos script.ini que se encuentra en la computadora. El script.ini envia una copia del gusano a todos los usuarios del mIRC que en ese momento se encuentren conectados a la Pc infectada.

El gusano modifica el archivo Autoexec.Bat con la intención de formatear la computadora en en siguiente reinicio de Windows:
Echo y|format c:

El gusano se añade al registro para autoejecutarse en cada inicio de Windows:
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
"NAV DefAlert"="C:\Windows\Help\mmsn_offline.htm"

También modifica otros registros del sistema:
HKEY_CURRENT_USER\Software\Microsoft\Windows Scripting Host\Settings\Timeout
HKEY_CURRENT_USER\Software\TheGrave\badUsers\v2.0

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

Si la computadora esta conectada a red, el gusano se copiara a todas las unidades que se encuentren conectadas a la PC: %[unidad de red]%\Windows\Start Menu\Programs\StartUp\msoe.hta
Todos los archivos ASP, HTM y HTML son sobreescritos con el codigo del virus. El contenido de todos los archivos de la PC son borrados los 1,5,10,15,20 de cada mes, dejando 0 bytes de información en cada uno de ellos.

Nombre:	**JS/IEStart** **Alias:** JS/Coolsite@MM, JS.Coolsite@mm, JS/Coolsite.A@mm, Coolsite.A@mm, EML/Coolsite-mm, JS_Exception.Gen, JS/Coolsite.A, JS.Exception.Exploit, UNK/Coolsite@MM, Coolsite, Cool site, Celebxx
Tipo:	Gusano
Tamaño:	N/D
Origen:	Internet
Destructivo:	SI
En la calle (in the wild):	SI
Detección y Eliminación	The Hacker 5.1, Registro de Virus al 18/12/2001

Descripción
JS/IEStart, es un gusano capaz de enviarse en forma masiva a todas las direcciones de email de los mensajes existentes en la carpeta de **"Elementos enviados"** del Outlook. Este esta escrito en Java Script.
Caracteristicas del mensaje de email:
Asunto: Hi!!
Cuerpo: Hi. I found cool site! http://celexxx.cjb.net It's really cool!

Si el usuario ingresa al enlace que se indica, se ejecutará el código del gusano oculto en la página, el cuál se aprovecha de una vulnerabilidad del Internet Explorer que permite la ejecución automática de determinado contenido.
Seguidamente se abriran multiples ventanas con contenido pornográfico. Algunas de estas ventanas contienen otros troyanos (scripts), como **JS/NoClose** y **JS/Coolsite**
Además el gusano modifica una entrada en el registro para cambiar la página de inicio del Internet Explorer,
HKCU\Software\Microsoft\Internet Explorer\Main\Start Page "Start Page"="http://[XXXXX].com/~mic124/sex.htm"

Soluciones

Instalar el parche de seguridad que corrige esta vulnerabilidad en la Máquina Virtual Java (Microsoft VM). Esta vulnerabilidad permite la ejecución de cualquier código en nuestra computadora, con tan sólo visitar una página web o leer un mensaje de correo HTML. La Máquina Virtual Java, es el componente que permite la ejecución de aplicaciones Java, y a la vez, los controla, para impedir que ejecuten acciones no deseadas. Microsoft publicó en octubre de 2000, un parche para acabar con dicha vulnerabilidad, la cuál afecta a todos los sistemas que tengan instalado el Internet Explorer 4.x o 5.x (IE 5.0 y anteriores ya no son soportados por Microsoft).

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

http://www.microsoft.com/technet/security/bulletin/MS00-075.asp

Para eliminar la página de inicio que coloca el gusano realizar lo siguiente

1- Abra su explorador de Internet Explorer
2- Luego desde Herramientas, Opciones de Internet,
3- clic en la pestaña General, Página de inicio, cámbiela por una de su elección o elija usar página en blanco.

Nombre:	**JS/Veren.A** **Alias:** JS_Veren@mm, JS_Never@mm, JS_VEREN.A
Tipo:	Gusano
Tamaño:	3,691 bytes
Origen:	Internet
Destructivo:	SI
En la calle (in the wild):	SI
Detección y Eliminación	The Hacker 5.3, Registro de Virus al 08/12/2002

Descripción

JS/Veren, es un gusano que se transmite a través de E-mail y recursos compartidos, para ello utiliza aplicaciones MAPI (Mail Application Program Interface).

Características del mensaje de E-mail:

Asunto: [puede ser cualquiera de la siguiente lista]

Hello [dirección de email]!
Hey [dirección de email]!
Fwd: Hey You!
Fwd: Check this!
Fwd: Just Look
Fwd: Take a look!
[dirección de email]!
Fwd: Loop at this!
Fwd: Check this out!
Fwd: It's Free!
Fwd: Look!
Fwd: Free Mp3s!
Fwd: Here you go!
Fwd: Have a look!
Look [dirección de email]!"
Fwd: Read This!

Cuerpo :

Hello!
Check out this great list of mp3 sites that I included in the attachments!
I can get any Mp3 file that I want from these sites, and its free! And please don't be greedy!

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

forward this email to all the people that you consider friends, and Let them benefit from these Mp3 sites aswell!
Enjoy!
Archivo Adjunto: [puede ser uno de la siguiente lista]
Free_Mp3s.js
Fwd_Mp3s.js
Fwd-Mp3s.js
Fwd-Sites.js
Mp3_List.js
Mp3_Pages.js
Mp3_Sites.js
Mp3_Web.js
Mp3-Fwd.js
Mp3-Sites.js
Web_Mp3s.js

Cuando el gusano se ejecuta busca todas las unidades compartidas de la red que esten conectadas al computador infectado para copiarse así mismo como **TEMPORARY.JS** y proseguir con su rutina de infección.
Cuando el gusano se instala crea las siguientes copias de si mismo en :
C:\WINDOWS\SYSTEM\CmdWsh32.js
C:\WINDOWS\Menú Inicio\Programas\Inicio\StartUp.js
Además crea las siguientes entradas en el registro para poder ejecutarse en el siguiente reinicio del sistema
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
"JSCmd32"="Wscript.exe C:\WINDOWS\SYSTEM\CmdWsh32.js %1"
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
"JSCmd32"="Wscript.exe C:\WINDOWS\SYSTEM\CmdWsh32.js %1"
También modifica las siguientes entradas para que se infecte un archivo **.TXT, .JS** o **.SCR** cada vez que se ejecute uno de estos.
HKEY_CLASSES_ROOT\txtfile\shell\open\command
"predeterminado"="Wscript.exe C:\WINDOWS\SYSTEM\CmdWsh32.js %1"
HKEY_CLASSES_ROOT\JSFile\Shell\Open\Command
"predeterminado"="Wscript.exe C:\WINDOWS\SYSTEM\CmdWsh32.js %1"
HKEY_CLASSES_ROOT\scrfile\shell\open\command
"predeterminado"="Wscript.exe C:\WINDOWS\SYSTEM\CmdWsh32.js %1"
HKEY_LOCAL_MACHINE\SOFTWARE\CLASSES\txtfile\shell\open\command
"predeterminado"="Wscript.exe C:\WINDOWS\SYSTEM\CmdWsh32.js %1"
HKEY_LOCAL_MACHINE\SOFTWARE\CLASSES\JSFile\Shell\Open\Command
"predeterminado"="Wscript.exe C:\WINDOWS\SYSTEM\CmdWsh32.js %1"
HKEY_LOCAL_MACHINE\SOFTWARE\CLASSES\scrfile\shell\open\command
"predeterminado"="Wscript.exe C:\WINDOWS\SYSTEM\CmdWsh32.js %1"
Finalmente también crea las siguientes entradas con información del autor:
HKEY_CURRENT_USER\Software\Never
"@"="Never by Zed/[rRlf]"

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

HKEY_USERS\.DEFAULT\Software\Never
"@"="Never by Zed/[rRlf]"

Nombre:	**JS/Yama** **Alias:** Worm/Yama, JS.Disturbed.A@m, I-Worm.Yama, JS/Yama.gen@M
Tipo:	Gusano
Tamaño	N/A
Origen:	Perú
Destructivo:	NO
En la calle (in the wild):	SI
Defección/Eliminación:	**Variante .A** - The Hacker 4.10 Dat=28/03/2001, Engine=N/A - The Hacker 5.0 Dat=28/03/2001, Engine=N/A **Variante .B** - The Hacker 4.10 Dat=20/04/2001, Engine=N/A - The Hacker 5.0 Dat=20/04/2001, Engine=N/A

Descripción

JS/Yama es un gusano similar a "JS/KAK" que se propaga vía E-mail en formato Javascript en Windows 95/98/NT/2000/ME, el gusano explota una vulnerabilidad en Internet Explorer 4.0 y 5.0 llamado scriptlet.typelib/eyedog,este fallo permite activar el virus con solo visualizar el mensaje y sin necesidad de abrir ningún archivo adjunto.

PRIMERA PARTE:

Al leer un mensaje infectado se activa el script del gusano y conecta el navegador a: http://orbita.starmedia.com/~yamaperu/yama.gif

Yama.gif no es un archivo GIF sino un archivo .HTA (HTML Application) renombrado que contiene la tercera parte del gusano y será utilizado al reiniciar el sistema.

Inmediatamente el gusano crea un archivo "yama1.hta" en la carpeta de Inicio de Windows (C:\Windows\Menú Inicio\Programas\Inicio o C:\Windows\StartMenu\Programs\Startup).

JS/Yama.A solamente trabaja si Windows está instalado en C:\WINDOWS, si no es el caso el gusano no puede crear el archivo "yama1.hta" y termina su ejecución.

SEGUNDA PARTE:

Al reiniciar el sistema se ejecuta automáticamente el archivo "yama1.hta" desde INICIO o STARTUP y copia el archivo Yama.gif (ver primera parte) como:

C:\WINDOWS\Yama.hta

C:\WINDOWS\Menú Inicio\Programas\Inicio\Yama.hta

TERCERA PARTE:

Nuevamente al reiniciar el sistema, se ejecuta esta vez el archivo "Yama.hta" que contiene el código real del gusano y realiza las siguiente acciones:

Copia el archivo "yama.hta" desde INICIO / STARTUP hacia C:\Windows y lo añade al registro para ejecutarse en cada Inicio del sistema: "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\yama"="C:\Windows\Yama.hta"

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

Borra los archivos "yama1.hta" y "yama.hta" de INICIO / STARTUP
Modifica la página de Inicio de Internet Explorer a "http://orbita.starmedia.com/~yamaperu"
Crea un archivo "C:\WINDOWS\Alan.htm" y lo coloca como imagen de fondo en Internet Explorer vía el registro.
Crea un archivo "C:\WINDOWS\Alan.reg" que modifica la interface del Explorer.
Crea los archivos:
- C:\WINDOWS\Yamalauncher.html (código del gusano)
- C:\WINDOWS\Yamalauncher.rtf (contiene un link al URL del gusano)
- C:\WINDOWS\Yamalauncher.txt (contiene un link al URL del gusano)

Para propagarse a otros equipos JS/Yama no se envía automáticamente a la libreta de direcciones sino que crea una Firma (signature) para "Microsoft Outlook" o "Outlook Express". La firma es creada de tal forma que se incluya el archivo "C:\WINDOWS\yamalauncher.html" a todos los mensajes de salida en código HTML.

VARIANTES:

JS/Yama.B: Detectada con el registro del 20/04/2001, la diferencia más significativa con la variante original .A es que no necesita "C:\WINDOWS" para funcionar, esta variante opera en cualquier instalación de Windows, asimismo el gusano se encuentra encriptado.

DETECCION / ELIMINACION:

Para detectar y eliminar JS/Yama.A utilice The Hacker con registro de virus al 28/03/2001, para la variante .B registro al 20/04/2001.
Se recomienda instalar los parches para este y otros fallos de seguridad en los productos Microsoft para evitar que otro virus con características similares se pueda activar con solo leer el mensaje y sin abrir ningún archivo adjunto.
Parches de Microsoft para vulnerabilidad scriptlet.typelib/eyedog: http://www.microsoft.com/msdownload/iebuild/scriptlet/en/scriptlet.htm
Boletines y parches de seguridad para otras vulnerabilidades:
http://www.microsoft.com/security/bulletins/current.asp (boletines de seguridad)
http://www.microsoft.com/technet/security/bulletin/ms99-032.asp (parche para fallo en scriptlet.typelib/Eyedog)
http://www.microsoft.com/technet/security/bulletin/MS00-043.asp (parche para cabeceras en formato MIME)
http://officeupdate.microsoft.com/2000/downloadDetails/Out2ksec.htm (parche para Outlook attachments)

Nombre:	**VBS/Bimorph@MM** **Alias: VBS_BIMORPH.A, VBS/Bimorph.A**
Tipo:	Gusano de E-mail
Tamaño:	4,400 o 4,714 bytes
Origen:	Internet
Destructivo:	SI
En la calle (in the wild):	SI
Eliminación	The Hacker 5.2 al 07/02/2002

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

Descripción

VBS/Bimorph.A es un gusano que se transmite vía E-mail. Tiene la caracteristica de ser polimorfico. Cuando el gusano se ejecuta se envia a todos los contactos de la libreta de direcciones de Outlook.

Características del mensaje de E-mail:

Asunto: Check this out
Archivo Adjunto: Snoopy shagging Woodstock y Snoopy smoking weed.

Una vez que el gusano se ejecuta, utiliza una clave que tiene guardada en su código para desencriptar el codigo de otro virus encriptado, a su vez tambien genera una nueva clave para encriptarse a si mismo.

Ademas el gusano borra su propio archivo **C:\PASS.ON** el cual es un archivo de texto, luego revisa todas las unidades y carpetas del computador infectado en busca de archivos con extensión **.VBS** y **.VBE**, si los encuentra los sobreescribe copiando su propio codigo. Luego el último archivo **TXT** que encuentre con la palabra **"PASSWORD"** se copia a **C:\PASS.ON.**

El codigo del virus contiene lo siguiente:

'vbs.janis by alcopaul/[rRlf]
'may 02, 2002
a friend with weed is a friend indeed..

el otro virus contiene lo siguiente en su codigo:

'vbs.snoopy by alcopaul/[rRlf]
'05/02/2K2
'warning: morphic, steals info, employs new algorithm....
'greets to disk0rdia, dr.g0nZo, El DudErin0, philet0ast3r, ppacket, rastafarie,
'petik, energy

Cuando los archivos infectados se ejecutan estos realizan lo descrito anteriormente y se envian asi mismo a todos los contactos de la libreta de direcciones del Outook.

Los archivos **.VBE** y **.VBS** que fueron sobrescritos ya no pueden ser recuperados, debiendo ser reemplazados por alguna copia backup o reinstalarlos nuevamente.

Nombre:	**VBS/BubbleBoy** **Alias: 2 variantes A, B (Encriptada)**
Tipo:	Gusano de E-mail
Tamaño:	N/Determinado
Origen:	Internet / Argentina
Destructivo:	NO
En la calle (in the wild):	NO
Eliminación	The Hacker 4.6 al 11/11/1999

Descripción

VBS/BubbleBoy en un gusano que se propaga por e-mail, trabaja con Microsoft OutLook que viene con Internet Explorer 5 (incluyendo OutLook Express), el gusano solo funciona si está instalado el Windows Scripting Host que viene con Windows 98 y Windows 2000 por defecto.

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

Caracteristicas del Mensaje de Email:

Asunto: BubbleBoy is back!

The BubbleBoy incident, pictures and sounds *http://www.towns.com/dorms/tom/bblboy.htm

Si el usuario abre el mensaje el gusano será ejecutado en forma automática, el gusano NO trabaja con attachment sino que viene incluido como código Script en el cuerpo del mensaje y explota un agujero de seguridad en Internet Explorer 5.

Inmediatamente trata de crear el archivo **"UPDATE.HTA"** en el fólder de inicio de Windows para ejecutarse en forma automática la siguiente vez que se inicie Windows. El gusano trata de crear el archivo en 2 rutas fijas (folder de inicio de Windows en Inglés y Español)::

C:\WINDOWS\START MENU\PROGRAMS\STARTUP

C:\WINDOWS\MENÚ INICIO\PROGRAMAS\INICIO

Si Windows está instalado en otro directorio o se está trabajando en un idioma diferente el gusano no trabajará

Al siguiente inicio de Windows se ejecuta el archivo infectado **UPDATE.HTA** y empieza la propagación del gusano, se conecta en forma oculta al OutLook y procede a enviarse por e-mail a todos los destinatarios encontrados en la libreta de direcciones. Terminado este proceso el gusano marca su acción en el registro de Windows para no realizar el proceso una segunda vez.

Marca en el registro:

Variante: VBS/Bubbleboy.A

HKEY_LOCAL_MACHIN\Software\OUTLOOK.BubbleBoy\ = OUTLOOK.Bubbleboy 1.0 by Zulu

Variante: VBS/Bubbleboy.B

HKEY_LOCAL_MACHIN\Software\OUTLOOK.BubbleBoy\ = OUTLOOK.Bubbleboy 1.1 by Zulu

En este punto el gusano modifica algunas opciones del registro de Windows como,

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RegisteredOwner =Bubbleboy

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RegisteredOrganization

= Vandelay Industries

VBS/BubbleBoy ha sido creado por Zulu, un escritor de Virus Argentino avocado a los virus de Visual Basic Script. Zulu es autor de **VBS/FreeLink** el primer virus de Scripts en llegar a estar en el wild (calle).

Importante:

A la fecha el gusano no es considerado en el Wild (calle) pero de seguro que estará por eso hay que tomar todas las precauciones del caso para evitar ser atacados.

Recomendaciones:

1) Es ABSOLUTAMENTE NECESARIO que instale el parche que Microsoft tiene para este agujero de seguridad, con esto Ud. estará libre de VBS/BubbleBoy y todos los virus / gusanos que empleen la misma modalidad de infección.

Parche específico: http://support.microsoft.com/support/kb/articles/Q240/3/08.ASP

Información acerca de agujeros de seguridad en general y parches: http://www.microsoft.com/Security/Bulletins/ms99-032.asp

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS
2) Si es necesario active el nivel de Seguridad de Internet Explorer a "Alta"
3) No abra ningún mensaje cuyo asunto indique "BubbleBoy is back!"
4) Si no se trabaja con archivos .HTA desactívelo vía el explorador de Windows:
- Abra el icono "Mi PC" en el escritorio de Windows
- Ir al menú "Ver", opción "Opciones (de carpeta)".
- Elegir el Tab "Tipos de archivo".
- En "Tipos de archivo registrados" buscar "HTML Application"
- Borrarlo vía "Quitar"

Nombre:	**VBS/Celeron** **Alias:** VBS.Celeron.Worm
Tipo:	Gusano
Tamaño:	2,037 bytes
Origen:	Internet
Destructivo:	SI
En la calle (in the wild):	SI
Detección y Eliminación	The Hacker 5.3 y 5.4 Registro de Virus al: 24/12/2002

Descripción
VBS/Celeron, es un gusano que se propaga a través de la aplicación de intercambio de archivos KaZaa. Si se encuentra el archivo **CELERON_VIVE.txt** es una prueba de que el gusano ya infecto la computadora. Además este gusano tambien elimina el archivo **AUTOEXEC.BAT.**
Cuando el gusano se ejecuta abre una ventana del explorador, con el siguiente mensaje :
Seguidamente se copia a sí mismo en las siguientes ubicaciones:
C:\WINDOWS\System32\Ken32.vbs
C:\WindowsS\System\Scrip.txt.vbs
C:\WindowsS\Prueba.vbs
C:\Program Files\Kazaa\My Shared Folder\Cristina.jpg.vbs
C:\Program Files\Kazaa\My Shared Folder\Lesbianas.jpg.vbs
C:\Program Files\Kazaa\My Shared Folder\Sexo.jpg.vbs
C:\Program Files\Kazaa\My Shared Folder\Video porno.jpg.vbs
C:\Program Files\Kazaa\My Shared Folder\Anal.jpg.vbs
C:\Program Files\Kazaa\My Shared Folder\Britney.jpg.vbs
De esta manera los archivos mencionados anteriormente quedan disponible para los usuarios que utilizan KaZaa.
Además crea las siguientes entradas en el registro del sistema para poder ejecutarse en cada reinicio del sistema :
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
"Run"="C:\WINDOWS\system32\Ken32.vbs"
"Windll"="C:\WINDOWS\system\Scrip.txt.vbs"
También crea los siguientes archivos en:

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

C:\Documents and Settings\Owner\Desktop\CELERON_VIVE.txt
C:\CELERON_VIVE.txt

En ambos archivos se encontro el siguiente texto :

Celeron. DOLOMEDES 1.0
YO SOY UNA FORMA DE VIDA

Si la fecha del sistema es **24** de cualquier mes el gusano procedera a borrar el **AUTOEXEC.BAT** y tratará de conectarse a un sitio Web para descargar y ejecutar el archivo **Fotos.html**

Nombre:	**VBS/HappyTime@mm** **Alias:** VBS.HappyTime.A, VBS/Help, VBS_Haptime.A, VBS/Helper
Tipo:	Gusano E-mail
Tamaño:	varia
Origen:	Internet
Destructivo:	SI (borra archivos con extensión .EXE y .DLL)
En la calle (in the wild):	SI
Eliminación	The Hacker 5.0 al 09/05/2001

Descripción

VBS/HappyTime es un Virus que se propaga por e-mail en código Script (formato HTML).

En Microsoft Outlook y Outlook express el virus explota un fallo de seguridad en Interner Explorer 4.0 y 5.0 llamado scriptlet.typelib/EyeDog, este fallo permite activar el virus con solo visualizar el mensaje y sin necesidad de abrir ningún archivo adjunto

Infección:

Al recibir un mensaje infectado en Microsoft Outlook o Outlook Express el virus se activa con solo leer el mensaje, en ese momento busca archivos con extensión HTML, VBS, HTM y ASP en el disco duro y añade su código al final.

El virus crea los archivos HELP.HTA y HELP.VBS en el primer directorio de la unidad C: que encuentre, además crea los archivos HELP.HTM y UNTITLED.HTM en la carpeta WINDOWS (por defecto C:\Windows)

Para activar su código en cada inicio del sistema el virus añade una referencia en el registro:

HKEY_CURRENT_USER\Control Panel\Desktop\WallPaper=c:\windows\help.htm

El virus infecta todos los archivos con extensión .HTT en la carpeta WINDOWS\WEB, el virus será activado cada vez que el usuario abra una carpeta del disco duro con el Explorador de Windows o Interner Explorer.

Para propagarse a otros equipos **VBS/HappyTime** no se envía automáticamente a la libreta de direcciones sino que crea una Firma (signature) para "Outlook Express". La firma es creada de tal forma que se incluya el archivo "C:\WINDOWS\Untitled.htm" a todos los mensajes de salida en código HTML.

Activación (daño):

El virus verifica si el día actual más el mes actual es 13 (dia+mes=13?), de ser así:

- Borra todos los archivos EXE y DLL en todas las unidades accesibles.

- Se envía en forma automática a todos los contactos en la libreta de direcciones del Outlook
- Activa nuevamente al gusano 366 veces. En este momento aparecen muchas ventanas con el titulo "WSCRIPT.EXE" y el sistema se vuelve lento.

DETECCION / ELIMINACION:

Para detectar y eliminar **VBS/HappyTime** utilice The Hacker con registro de virus al 09/05/2001.

Se recomienda instalar los parches para este y otros fallos de seguridad en los productos Microsoft para evitar que otro virus con características similares se pueda activar con solo leer el mensaje y sin abrir ningún archivo adjunto.

Parches de Microsoft para vulnerabilidad scriptlet.typelib/eyedog: http://www.microsoft.com/msdownload/iebuild/scriptlet/en/scriptlet.htm

Boletines y parches de seguridad para otras vulnerabilidades:

http://www.microsoft.com/security/bulletins/current.asp (boletines de seguridad)

http://www.microsoft.com/technet/security/bulletin/ms99-032.asp (parche para fallo en scriptlet.typelib/Eyedog)

http://www.microsoft.com/technet/security/bulletin/MS00-043.asp (parche para cabeceras en formato MIME)

http://officeupdate.microsoft.com/2000/downloadDetails/Out2ksec.htm (parche para Outlook attachments)

Nombre:	**VBS/Hola** **Alias:** VBS/Hercobolus
Tipo:	Gusano E-mail
Tamaño:	Variante A: 7585 bytes Variante B: 5249 bytes
Origen:	Perú
Destructivo:	SI
En la calle (in the wild):	NO
Eliminación	The Hacker 5.0 al 03/09/2001

Descripción

VBS/Hola@MM es un gusano de E-mail que se propaga utilizando Microsoft Outlook, el virus se envía a todos los contactos en la libreta de direcciones de Outlook.

Características del mensaje de Email:

Asunto: Hola

Cuerpo: Un recuerdo para tí en en Archivo Adjunto
Solo para tí el mensaje del Archivo Adjunto

Archivo Adjunto: Hola.vbs

Si se abre el archivo adjunto **"Hola.vbs"** el gusano realiza las siguientes acciones:

1- El gusano se copia a la carpeta %windows% (Ej. C:\Windows) como "THWIN.vbs", "MiFoto.vbs"

2- Se envía automáticamente a los 70 primeros contactos de la libreta de direcciones de Microsoft Outlook, las características del mensaje se indican arriba.

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

3- El gusano selecciona al azar solamente una de las extensiones entre xls, dbf, wav, dwg, mp3, bak, wav, bmp, htm, hlp, chm, jpg, gif, scr, cdr, ttf y borra todos los archivos del disco duro con esa extensión, los nombres de los archivos borrados son salvados en el archivo "ListWin.txt" de la carpeta %windows%.

4- Si la fecha del sistema es mayor al 27 de Mayo del 2001 el gusano crea el archivo "c:\hercolubus.txt" y lo copia al archivo "C:\autoexec.bat".

El nuevo archivo autoexec.bat contiene intrucciones para borrar todos los *.SYS, *.DLL, *.OCX de la carpeta C:\Windows\System y formatear el disco duro "C:" al siguiente inicio del sistema.

5- El virus se registra en el sistema vía: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "THWIN"="%windows%\system\THWIN.vbs"

6- Muestra el mensaje:

Hola.. Quisiera tener una linda amistad contigo, no sé si recuerdas la vez que platicamos en el chat
yo solo recordaba tu e-mail y la verdad me agradó tu plática y me pareces una buena persona
Quisiera comunicarme continuamente contigo.
Estaré esperando tu respuesta, escríbeme.
HASTA PRONTO.

7- Se conecta en forma oculta a Microsoft Word e infecta la plantilla "normal.dot", el gusano agrega una macro "Hercolubus" que infecta disquetes "A:" cada vez que se inicia Microsoft Word, el virus crea el archivo "A:\Hola.vbs"

VARIANTES

VBS/Hola.B:

- El archivo "C:\autoexec.bat" es sobreescrito para formatear el disco duro en cualquier fecha
- En la lista de extensiones que el gusano borra se ha modificado ".dbf" por ".doc"
- Se propaga a disquetes utilizando el archivo "A:\Mi Foto.vbs"
- Muestra un mensaje adicional:

YA DEBES SABER QUE SE APROXIMA HERCOLUBUS A LA TIERRA, ES UN PLANETA GIGANTE
NO HABRA ESCAPATORIA

- No se conecta a Microsoft Word

Nombre:	**VBS/Homepage@MM** **Alias:** I-Worm.Homepage, VBS.VBSWG2.D@mm, VBS/VBSWG-X, VBS_HomePage.A, VBSWG.X, VBSWG.X@MM
Tipo:	Gusano E-mail
Tamaño:	2,436 bytes
Origen:	Internet
Destructivo:	NO
En la calle (in the wild):	SI
Eliminación	The Hacker 5.0 al 09/05/2001

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

Descripción

VBS/Homepage es un gusano simple que se propaga vía E-mail en un archivo adjunto **"homepage.HTML.vbs"**

Caracteristicas del Mensaje de Email:

Asunto: Homepage

Cuerpo: Hi!
You've got to see this page! It's really cool ;O)

Archivo Adjunto: homepage.HTML.vbs

Al abrir el archivo adjunto el gusano se envía automáticamente a todos los contactos en la libreta de direcciones de Microsoft Outlook

Después de enviarse vía E-mail el gusano abre al azar una de las siguientes páginas en Internet Explorer:

http://hardcore.pornbillboard.net/shannon/1.htm
http://members.nbci.com/_XMCM/prinzje/1.htm
http://www2.sexcropolis.com/amateur/sheila/1.htm
http://sheila.issexy.tv/1.htm

VBS/Homepage borra de la carpeta "Elementos Enviados" o "Sent Items" los mensajes que tengan en el sujeto la palabra "Homepage", al parecer esto lo hace a fin de evitar su detección.

Nombre:	**VBS/Hypoth@MM** **Alias:** VBS.Hypoth@mm
Tipo:	Gusano de Email
Tamaño:	8,499 bytes, 19,692 bytes
Origen:	Internet
Destructivo:	SI
En la calle (in the wild):	SI
Detección y eliminación:	The Hacker 5.3 al 26/11/2002.

Descripción:

VBS/Hypoth@MM, es un gusano que llega a través de emails, este es capaz de enviarse así mismo a todos los contactos de la libreta de direcciones del Outlook, infecta todos los archivos con extensiones .vbs y vbe que encuentre en el computador, dichos archivos los renombra como archivos de Video.

Caracteristicas del Mensaje de Email :

Asunto: Hey <Nombre del receptor>!

Cuerpo :

<Nombre del receptor>! Get free mp3s from the web site that i go to! I can get almost any music that I want, just look at all the cool sites that I went to in the attachments. Bye

Archivo Adjunto : Sitelist.vbs

Asunto: Hello <Nombre del receptor>!

Cuerpo:

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

Have fun with these great jokes!
<Nombre del remitente>
Archivo Adjunto : Jokes.vbs
Asunto: Here is that file you wanted, <Nombre del receptor>.
Cuerpo :
This is the file you wanted - don't let anyone else see it!
<Nombre del remitente>
Archivo adjunto: Confidential.vbs
Asunto: Check this out, <Nombre del receptor>!
Cuerpo:
Hello <Nombre del receptor>, check out these pictures of my last holiday! Don't get jealous!
<Nombre del remitente>
Archivo Adjunto: Holidaypics.vbs
Asunto: Urgent Update!
Cuerpo :
<Nombre del receptor>,
Your computer will need this update to protect your computer from new email viruses. I installed this update and it works fine.
Thanks.
Archivo Adjunto: SecurityUpdate.vbs, Update.vbs, UpdateSecurity.vbs, UpdateInstaller.vbs, UpdateSetup.vbs, or Readme.vbs

---

Cuando este se ejecuta se copia así mismo en la carpeta SYSTEM de Windows como uno o mas de los siguientes nombres
C:\WINDOWS\SYSTEM\Runmsdsk32.vbs
C:\WINDOWS\SYSTEM\Sitelist.vbs
C:\WINDOWS\SYSTEM\Winnt32.vbs
C:\WINDOWS\SYSTEM\Jokes.vbs
C:\WINDOWS\SYSTEM\Confidential.vbs
C:\WINDOWS\SYSTEM\Runmnt32.vbs
C:\WINDOWS\SYSTEM\Holidaypics.vbs
C:\WINDOWS\SYSTEM\Securityupdate.vbs
C:\WINDOWS\SYSTEM\Update.vbs
C:\WINDOWS\SYSTEM\Updatesecurity.vbs
C:\WINDOWS\SYSTEM\Updateinstaller.vbs
C:\WINDOWS\SYSTEM\Updatesetup.vbs
C:\WINDOWS\SYSTEM\Readme.vbs
C:\WINDOWS\SYSTEM\<caracteres aleatorios>.vbs
También modifica la siguiente entrada en el registro para poder ejecutarse en cada reinicio del sistema adicionando uno de los siguientes valores con un archivo de la lista anterior:
Runxpdsk32
Winnt32
Runmnt32
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

Seguidamente el gusano se envia a todos los contactos de la libreta de direcciones de Outlook y Outlook Express, para saber si ya se envio a una de las direcciones de correo, el gusano almacena la dirección de email en la siguiente entrada del registro
HKEY_CURRENT_USER\Software\Theory\Theory\RecordContacts\
Despues de enviarse, busca archivos con la extensión **VBS** y **VBE** en todo el computador infectado, finalmente el gusano adiciona la extensión .vbs a todos los archivos **.mp3, .mp2, .mpg, .mpe, .mpeg, .avi, y .mov** que encuentre en el computador

Nombre:	**W32/ExploreZip** **Alias:** I-Worm.ExploreZip
Tipo:	Gusano
Tamaño:	210,432 bytes
Origen:	Internet
Destructivo:	SI (trunca archivos con extensión .doc, .xls, .ppt, .h, .c, .cpp, .asm a 0 bytes)
En la calle (in the wild):	SI
Detección y eliminación:	The Hacker 4.5 con registro de virus al 10/06/99 o superior.

Descripción
W32/ExploreZip es un gusano DAÑINO reportado el 10 de Junio de 1999 que se propaga por E-Mail utilizando comandos MAPI y clientes Microsoft OutLook, Exchange, etc en Windows 95/98/NT.
El gusano viaja con el attachment **"zipped_files.exe"** en el mensaje similar a:
Hi {nombre del destinatario!}
I received your email and I shall send you a reply ASAP.
Till then, take a look at the attached zipped docs.
bye
<zipped_files.exe>
para engañar el usuario el archivo exe tiene un ícono .ZIP asociado, por lo que aparenta ser un archivo zipeado. Si el usuario abre (ejecuta) el archivo infectado el gusano muestra un mensaje de error indicando que el archivo .ZIP está corrupto:
"Cannot open file: it does not appear to be a valid archive. If this file is"
"part of a ZIP format backup set, insert the last disk of the backup set"
" and try again. Please press F1 for help."
el gusano se copia como c:\windows\system\explore.exe o c:\windows_setup.exe y modifica el archivo WIN.INI para que se ejecute cada vez que se inicia Windows y se autoenvie automáticamente. (run=c:\windows\system\explore.exe o run=_setup.exe)
W32/ExploreZip es DAÑINO, cuando el archivo zipped_files.exe es ejecutado el gusano trunca archivos con extensión .DOC, .XLS, .PPT, .H, .C, .CPP, .ASM a 0 bytes quedando estos irrecuperables. El gusano busca estos archivos en las unidades 'A'...'Z'
Eliminando el virus en forma manual : aquí los pasos (asumiendo que windows está instalado en c:\windows):

1. Reinicie el sistema en modo **MS-DOS**

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

2. En el prompt del DOS digite:
   CD C:\WINDOWS\SYSTEM [pulse enter]
3. Borre el archivo EXPLORE.EXE
   DEL EXPLORE.EXE [pulse enter]
4. En el prompt del DOS digite:
   CD C:\WINDOWS [pulse enter]
5. Borre el archivo _SETUP.EXE
   DEL _SETUP.EXE [pulse enter]
6. Edite el archivo WIN.INI y borre la línea
   "run=C:\windows\system\explore.exe" o **"run=_setup.exe"**

Nombre:	**W32/Horo** **Alias:** W32.Horo@mm, W32/Horo@MM, WORM_WCONN.B
Tipo:	Gusano
Tamaño:	14,736 bytes
Origen:	Internet
Destructivo:	SI
En la calle (in the wild):	SI
Detección y Eliminación	The Hacker 5.3 y 5.4, Registro de Virus al 14/01/2003

Descripción

W32/Horo, es un gusano que llega a través de E-mail. Se envía así mismo a todos los contactos de la libreta de direcciones de Outlook, esta escrito en Visual Basic y comprimido con la utilidad FSG.

Características del mensaje de Email:

Asunto: Today's free horoscope

Cuerpo:

Open this screen saver file to see today's horoscope. No registrions. No fees. And No ugly lady in front of you! ABSOLUTE FREE!!!!!!!!!!!!!!!

Archivo Adjunto: Horoscope.scr

Cuando se ejecuta se copia a sí mismo en:

C:\WINDOWS\Escritorio\Horoscope.scr

Además hace multiples copias de si mismo en:

C:\WINDOWS\Active Setup logtxt.exe
C:\WINDOWS\Active Setup logtxtexe.exe
C:\WINDOWS\Active Setup logtxtexeexe.exe
C:\WINDOWS\Active Setup logtxtexeexeexe.exe

Modifica algunas entradas del registro para poder ejecutarse en el siguiente reinicio del sistema:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
[parte de la ruta] horoscope.scr
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
"[Nombre del archivo.exe]"="[Nombre del archivo de la carpeta de Windows].exe"

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

Nombre:	**X97M/Papa**
Tipo:	Gusano, se propaga por E-Mail vía Excel 97
En la calle (in the wild):	NO

Descripción:
Reportado el 30/03/99. Este gusano se propaga por E-Mail en el archivo **"xpass.xls",** está basado en el código de **W97M/Melissa.**
Al abrir el archivo **XPASS.XLS** el gusano se conecta al OutLook y se envia a las 60 primeras direcciones de la **"libreta de direcciones del OutLook".**
X97M/Papa no infecta otros documentos de Excel 97 ni los envía por E-Mail.
Caracteristicas del Mensaje de Email:
De: [usuario infectado]
Asunto: Fwd: Workbook from all.net and Fred Cohen
Cuerpo:
Urgent info inside. Disregard macro warning.
Archivo Adjunto: XPASS.XLS

Nombre:	**X97M/Oblivion (Alias: X97M/Killer)**
Tipo:	Macrovirus, infecta documentos de Excel 97 y 2000
Origen:	Inglaterra
Módulos:	1 - "Killer"
En la calle (in the wild):	SI.(Según se reportó en REVS)
Destructivo	no

Descripción:
Este es un macrovirus simple que infecta documentos de **Excel 97/2000.**
Hacksoft no ha recibido reportes de infecciones en Perú, el virus ha sido reportado en la calle ("in the wild") en varios países de Europa a través del sistema REVS.
El virus toma el control al abrir un documento infectado y crea un archivo **"ACF.XLS"** infectado en la carpeta de Inicio de Office, este archivo será cargado en forma automática cada vez que Excel inicie, de esta forma el virus infectará todos los documentos que sean abiertos.
Para eliminar este virus utilice The Hacker 4.9 con registro al 23/08/2000 o superior.

Nombre:	**WYX**
Tipo:	Infector de MBR y Boot sector, Encriptado, Residente
Número de Sectores:	2
Origen:	España
Destructivo:	NO
En la calle (in the wild):	SI

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

Detección y eliminación:	The Hacker 4.8, registro de virus al 09/Marzo/2000 o superior

WYX fue reportado por primera vez en Marzo del 2000, a mayo del 2000 el virus se encuentra bastante propagado en Perú, Chile, España.
WYX en forma sorpresiva se encuentra a mayo del 2000 en los TOP-10-PERU virus más reportados en Perú, el hecho es sorpresivo porque WYX es un virus de Boot que se propaga vía disquetes.
La única forma de infectar una computadora es cuando se intenta butear desde un disquete infectado en la unidad A:, la mayoría de veces la infección se produce cuando el usuario olvida un disquete en A: y reinicia la computadora. En ese momento el virus toma el control desde el Boot del disquete y procede a infectar el MBR y Boot Sector del disco duro, después de coloca residente en memoria para infectar cualquier disquete sin protección que se inserte en la unidad A: o B:
WYX es un virus inusual debido a que infecta tanto el MBR y Boot en discos duros, esto hace del virus un poco complicado de eliminar cuando no se butea desde un disquete de sistema limpio en la unidad A:.
WYX no es dañino intencionalmente, es decir, no tiene una bomba lógica (PayLoad) que detona en una fecha o evento específico.
El virus no muestra mensajes. Dentro del código se puede encontrar "31/03/98 WYX"

NOTAS PARA ELIMINACION:
IMPORTANTE:
1- Si lo que está infectado es el MBR o el Boot del disco duro es IMPORTANTE que se elimine el virus buteando en DOS desde un disco de sistema LIMPIO en A:, una vez que aparece el prompt del DOS ejecutar el programa TH.EXE desde el disquete "1 de 2" de The Hacker 4.8
Si lo que está infectado es el Boot de un disquete puede eliminar el virus desde el mismo Windows, asegúrarse que el disquete se encuentre desprotegido, está es una recomendación un poco tonta pero no está demás recordarlo, muchas veces uno asume cosas obvias. También se puede utilizar la opción "Reparar Boot" del menú
2- Para eliminar un virus (cualquiera) es OBLIGATORIO que el antivirus tenga el último registro de virus (TH.DAT) y MUY IMPORTANTE tenga el último Virus Scanner Engine
A la fecha estamos en el registro de virus del 27/05/2000 y Virus Scanner Engine del (24/05/2000) para actualizar su disquete de The Hacker "1 de 2" baje la actualización para DOS en la sección actualizaciones (archivo th48dos.zip)
El virus WXY es un simple virus de MBR y Boot por lo no hay especiales requerimientos para eliminarlo excepto:
1- Butear el sistema desde un disquete limpio en la unidad A:
2- El registro de virus y Virus Scanner Engine (muy importante) deben tener por lo menos fecha a Mayo del 2000.
Realice lo siguiente:
1- Reiniciar la computadora desde un disquete de inicio limpio en la unidad A:
2- A la aparición del prompt del DOS inserte el disquete "1 de 2" de The Hacker y ejecute el programa TH.EXE
3- VERIFICAR que la fecha de registro de virus y Virus Scanner Engine esten a Mayo del 2000, Ir al menú "Información / Acerca de"

DAVID MARTÍNEZ PEÑA
ICO 9
DISEÑO DE SISTEMAS

4- Para eliminar el virus ir "Detectar", en disco seleccionar la unidad C: y "detectar y eliminar"

Nombre:	**Win95/Punch**
Tipo:	Infector PE (32 bits) residente
Tamaño:	9262 bytes
Origen:	Australia
Destructivo:	NO
En la calle (in the wild):	NO
Detección y eliminación:	

Descripción:

Win95.Punch es el primer virus residente que infecta archivos PE EXE de Windows 95. Win95.Punch emplea una nueva modalidad para permanecer residente en memoria y tener el control total de Windows 95: El uso de VxDs.

La primera vez que se ejecuta un archivo infectado el virus crea el archivo **VVFS.VXD** y lo registra en el archivo system.ini. La siguiente vez que windows 95 inicia carga en memoria el archivo **VVFS** y el cede el control, **VVFS** se enlaza al manejador del sistema de archivos de Windows 95 (IFS API Hook) y continua la carga de Windows 95.

VVFS una vez enlazado al IFS API Hook será capaz de infectar practicamente cualquier archivo PE EXE de Windows 95. Los archivos infectados presentan una nueva sección.