RECUPERACIÓN DATOS: VIRUS OPASERV

"Su capacidad para distribuirse a través de redes lo convierte en un código malicioso especialmente peligroso para entornos corporativos".

¿Qué es?

Familia de gusanos W32/OPASERV, W32/OPASOFT, I.worm.Opaserv
Desde el mes de Septiembre del 2002 a la fecha, una familia de gusanos viene amenazando en Internet y ha causado confusión entre algunos desarrolladores de antivirus, que obviamente le han asignado el mismo nombre, pero con diferentes extensiones. Al parecer a la fecha ya habría llegado a su versión M o N.
Es importante destacar que un virus tiene una estructura de programación definida y si su autor crea variantes, éstas tienen ligeras modificaciones en su payload o simplemente el nombre o la extensión del archivo infector es cambiada.
En caso contrario, se trataría de un nuevo virus o gusano en particular.
Esta familia está totalmente controlada, pues es suficiente desarrollar una rutina Heurística, específica, para su estructura viral ampliamente conocida. Debido a ello mencionamos sus variantes más notables, sin extendernos en tecnicismos que a la mayoría de usuarios les resulta irrelevantes.

¿Qué clases hay?

OPASERV.E es una variante que al ejecutarse desencripta su código y se auto-copia a **%Windows%** con los nombres de **BRASIL.PIF** o **BRASIL.EXE**.
Para ejecutarse la próxima vez que se inicie el sistema crea las siguientes llaves de registro:
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
Brasil=%Windows%\BRASIL.PIF
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
Brasil=%Windows%\BRASIL.EXE
El gusano propaga los archivos infectados BRASIL.PIF o BRASIL.EXE y los ejecuta como un proceso que no se muestra en la Barra de Tareas de Windows.
Infecta a través de las unidades que comparten C:\ buscando los equipos que tengan completo acceso a la red, para lo cual aprovecha la vulnerabilidad de Share Level Password de Windows (Nivel compartido de Passwords), la cual permite que un intruso, en forma remota, pueda acceder a los sistemas sin necesidad de conocer los Passwords de acceso.
El parche de seguridad para esta vulnerabilidad puede ser descargado desde:
http://www.microsoft.com/technet/security/bulletin/ms00-072.asp

OPASERV.G es un gusano reportado el 30 de Octubre del 2002, miembro de la misma familia y variante del gusano **Opasoft**, descubierto en Septiembre del 2002, creado por el mismo autor, y que a partir de su primera versión empezó a propagar sub-siguientes variantes, con diferentes nombres de archivos de extensiones **.EXE**, **PIF**, **SCR**, etc., pero todos con la misma estructura viral.
Esta última tiene 28 KB de extensión y posee una rutina de ingreso furtivo, conocida como backdoor, la cual se propaga a través de redes locales y compartidas usando los servicios del **NETBIOS** de MS Windows.
Es un **PE** (Portable Ejecutable) e infecta todos los sistemas operativos.
Windows95/98/NT/Me/2000/XP, incluyendo los servidores **NT/2000**.
El gusano se auto-instala en el directorio de Windows con el nombre **scrsvr.exe** y lo agrega a la llave de registro para ejecutarse la próxima vez que se inicie el sistema:

[HKLM\Software\Microsoft\Windows\CurrentVersion\Run]
ScrSvr="%nombre_del_gusano%"
Este gusano rastrea las sub-nets por el **puerto 137** de Servicio del NETBIOS y busca determinadas direcciones IP dentro de unidades de redes y si encuentra que el o los equipos tienen abierto el servicio "**File and Print Sharing**", empieza su proceso de infección, tomando control de los mismos en forma remota.

OPASERV.F se propaga en los equipos que comparten la unidad **C:** con completo acceso en la red donde se produce la infección, para lo cual emplea el comando **SMB** (Server Message Block Protocol) para acceder a las unidades compartidas.
Este gusano envía información a un sitio en la web, actualmente deshabilitado, desde el cual descarga los archivos infectados **mane!!.dat** y **FDP!!!!.dat** y los instala en el directorio raíz C:\ los mismos que son usados para el intercambio de información con el portal ubicado en Brasil.
En los equipos remotos el gusano crea el archivo **GAY.INI** en **C:** y lo sobre-escribe en **%Windows%\win.ini** y para ejecutarse la próxima vez que se inicie el sistema crea la siguiente llave de registro:
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
cronos = "%Windows%\MARCO!.SCR"
%Windows%, es una variable que por defecto es **C:\Windows** para Windows 95/98/Me/XP y **C:\Winnt** para NT/2000.

OPASERV.H se propaga en las unidades que comparten la unidad **C:** y se autocopia al directorio %Windows% con el nombre de **MSTASK.EXE**, e igualmente lo sobre-escribe en: **%Windows%\win.ini** y para ejecutarse la próxima vez que se inicie el sistema crea la siguiente llave de registro:
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
Mstask = "%Windows%\MSTASK.EXE"

OPASERV.I se propaga en las unidades que comparten la unidad **C:** y se autocopia al directorio %Windows% con el nombre de **MQBKUP.EXE**, e igualmente lo sobre-escribe en **%Windows%\win.ini** y para ejecutarse la próxima vez que se inicie el sistema crea la siguiente llave de registro:
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
Mqbkup = "%Windows%\MQBKUP.EXE"
El gusano se activa en fechas igual o posteriores al 24 de Diciembre de 2002 y muestra un mensaje dentro de una ventana de MS-DOS y a continuación borra el contenido de la CMOS y del disco duro:

NOTICE:
Illegal Microsoft Windows license detected!
You are in violation of the Digital Millennium Copyright Act
Your unauthorized license has been revoked
For more information, please call us at:
NOPIRACY
If you are outside the USA, please look up the correct contact information on our website, at:
www.bsa.org
Business Software Alliance
Promoting a safe & legal online world

OPASERV.J (algunos antivirus lo nombran como **Opaserv L/M/N**), reportado a partir del 27 de Diciembre del 2002, se propaga en las unidades que comparten la unidad **C:** y se autocopia al directorio %Windows% con el nombre de **MSTASK.EXE**, e igualmente lo sobre-escribe en **%Windows%\win.ini** y para ejecutarse la próxima vez que se inicie el sistema crea la siguiente llave de registro:
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
Mstask = "%Windows%\MSTASK.EXE"
También infecta a través de las unidades compartidas de **C:** buscando los equipos que tengan completo acceso a la red, para lo cual aprovecha la vulnerabilidad de **Share Level Password** de Windows.
El parche de seguridad para esta vulnerabilidad puede ser descargado desde:
http://www.microsoft.com/technet/security/bulletin/ms00-072.asp
Del mismo modo, muestra el mismo mensaje del **Opaserv.I** y re-inicia el sistema.

NOTICE:
Illegal Microsoft Windows license detected!
You are in violation of the Digital Millennium Copyright Act
Your unauthorized license has been revoked
For more information, please call us at:
1-888-NOPIRACY
If you are outside the USA, please look up the correct contact information on our website, at:
www.bsa.org
Business Software Alliance
Promoting a safe & legal online world

El único cambio del mensaje es el número telefónico.

¿Cómo funciona?

Opaserv y sus variantes se introducen en los equipos a través de Internet, empleando para ello los puertos de comunicaciones 137 y 139 que normalmente, por defecto, se encuentran abiertos. Si el equipo afectado comparte archivos o recursos con otros ordenadores, el código malicioso se transmitirá a éstos últimos aprovechando una vulnerabilidad de Windows 9x y Me denominada "Share Level Password". Por tal motivo, puede infectar rápidamente la totalidad de los equipos conectados a una red.
En relación a Opaserv y a sus variantes Luis Corrons, director del Laboratorio de Investigación de Virus de Panda Software, también destaca el hecho de que "estos gusanos están propiciando el resurgimiento de otros códigos maliciosos más veteranos, como W95/CIH o W32/Funlove. Ello se debe", explica, "a que Opaserv se copia en los equipos a los que afecta. Si dichos ordenadores se encuentran contaminados por un virus, el archivo que contiene Opaserv quedará también contaminado, y llevará la infección donde se propague".
F-Secure Corporation anuncia la aparición in the wild del código malicioso Opaserv, alias Opasoft, que combina características de gusano de red con capacidades troyanas diseñadas para obtener acceso remoto no autorizado de los equipos infectados.

Opaserv se extiende a través de unidades compartidas de red y se copia como ScrSvr.exe en la carpeta de sistemas Windows 9x, quedando residente en el equipo al que afecta. Además, con el objetivo de ejecutarse cada vez que se reinicie el ordenador, genera una entrada en el registro de Windows.
El componente troyano de Opaserv está diseñado para obtener el control remoto no autorizado de las máquinas que infecta. El gusano intenta conectarse a una dirección de Internet (ahora inactiva),

http://www.opasoft.com, para descargar versiones del código malicioso actualizadas si las hubiera y lanzar sobre los sistemas cadenas script maliciosas.
En relación con su acción directa sobre los discos duros, señalamos que el virus realiza una sobre-escritura en los dos primeros tercios del disco, por lo que resulta irrecuperable. De las versiones a las que hemos accedido hasta el momento, constatamos que los dos primeros tercios se rescriben con códigos de manera geométrica, lo que hace que este tipo de escritura sea muy rápida.

¿Cómo eliminarlo?

BitDefender le ofrece una imprescindible herramienta de desinfección del virus Win32.Worm.Opaserv.A, diseñada para detectar y eliminar virus que han infectado su sistema. Esta aplicacion son también de un valor añadido gracias a su tamaño, ya que se descargan fácilmente incluso con una débil conexión de Internet. Asimismo se pueden transferir por e-mail a clientes, amigos o socios.
Si sospecha que su sistema puede estar infectado con el Win32.Worm.Opaserv.A descargelo y ejecutelo en su ordenador. **AntiOpaserv.exe**
Los servicios de Soporte Técnico de Panda Software han puesto gratuitamente a disposición de todos los usuarios que lo deseen, la aplicación PQREMOVE que detecta y elimina eficazmente este nuevo gusano de los ordenadores afectados.
PER ANTIVIRUS® versión 7.8 con registro de virus al 30 de Diciembre del 2002 detecta y elimina eficientemente este gusano y todas sus variantes existentes y por crearse.