PRESIDENCIA DEL CONSEJO DE MINISTROS

Oficina Nacional de GOBIERNOELECTRÓNICO e INFORMÁTICA

BOLETÍN DE ALERTA ANTIVIRUS

Centro de Consulta e Investigación sobre Seguridad de la Información

Edición Nº 146/ 31 Octubre de 2008

Visite el Portal del Estado Peruano: www.peru.gob.pe

INDICE

TROYANO TROJ/PWS.AUF

Es un troyano reportado el 13 de Octubre del 2008 que se propaga por diversos servicios de Internet incluyendo MultiSPAM. Infecta los siguientes sistemas operativos: Windows 95/98/Me/NT/2000/XP/ Vista y Server 2003; está desarrollado en Assembler.

El troyano roba contraseñas de juegos de PC y como "keylogger" captura teclas digitadas, en forma aleatoria y las envía a una dirección de correo cifrada.

Al ingresar a un sistema se copia a las siguientes rutas, con las caracterísiticas:
%Windir%\Help\[4_letras _mayúsculas/o_4_dígitos].dll
%Windir%\Help\[4_letras _mayúsculas/o_4_dígitos].exe
Los archivos tienen los atributos de "oculto"y de "sistema"

Al siguiente inicio del equipo el troyano registra su componente .DLL como objeto COM y como Shell, el mismo que captura contraseñas de juegos de PC y teclas digitadas, en forma aleatoria y las envía a una dirección de correo cifrada, perteneciente al autor.

MAS INFORMACION:

- **Alerta Antivirus**
  http://alerta-antivirus.red.es/virus/detalle_virus.html?cod=8224

- **VSAntivirus**
  http://listas.vsantivirus.com/lista/vsantivirus/

- **PER ANTIVIRUS**
  http://www.perantivirus.com/sosvirus/virufamo/pswauf.htm

TROYANO TROJ/ISTBAR.EA

Es un troyano residente en memoria, que se propaga visitando páginas web maliciosamente acondicionadas.

Infecta el archivo HOSTS, altera la funcionabilidad de acceso a Internet y se comunica con servidor remoto a través del puerto TCP 8080 (HTTP), desde el cual descrga malwares.

Infecta a Windows 98/NT/2000/XP/Vista y Server 2003, está desarrollado en Assembler con una extensión variable.
Una vez ingresado al sistema se copia a las siguientes rutas:

- %Desktop%\Cheap Pharmacy Online.url
- %Desktop%\Search Online.url
- %Desktop%\VIP Casino.url
- %Favorites%\Cheap Pharmacy Online.url
- %Favorites%\Search Online.url
- %Favorites%\VIP Casino.url
- %User%\Start Menu\Cheap Pharmacy Online.url
- %User%\Start Menu\Search Online.url
- %User%\Start Menu\VIP Casino.url
- %System%\c.ico
- %System%\lsystipl64.dll
- %System%\m.ico
- %System%\s.ico

FUENTES

- Alerta Antivirus
- Per Antivirus
- Sophos

El archivo lsystipl64.dll es registrado como un objeto COM y Browser Helper Object (BHO) para Internet Explorer, creando los registros:

- *[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects*
- *{1F88A6F5-908C-4C28-9A81-829953C5F5C5}]*
- *[HKCR\CLSID\{1F88A6F5-908C-4C28-9A81-829953C5F5C5}]*
- *[HKCR\Interface\{06360872-0310-49C1-8EDA-953E73941E3E}]*
- *[HKCR\Interface\{419803E0-EBB5-418E-BCDD-8EA63647EC5E}]*
- *[HKCR\TypeLib\{10026069-7A5F-4531-811E-C8DF20643BEE}]*

Al siguiente inicio del equipo, permanece activo en memoria y al haber infectado el archivo HOSTS, monitorea el acceso a sitios web aleatorios y se conecta a un servidor remoto via el puerto TCP 8080 (HTTP), desde el cual descarga malwares y actualizaciones de sí mismo.

MAS INFORMACION:

- **Alerta Antivirus**
  http://alerta-antivirus.red.es/virus/detalle_virus.html?cod=8226
- **PER ANTIVIRUS**
  http://www.perantivirus.com/sosvirus/virufamo/lstbarea.htm

TROYANO TROJ/INFOSTEALER.HIBIK

Hibik es un troyano que se propaga a través de diversos servicios de Internet incluyendo MultiSPAM. Roba infomación crítica del sistema afectado. Finalmente se auto-elimina.

Infecta Windows 95/98/NT/Me/2000/XP/Vista y Server 2003, está programado en Assembler.

Al ingresar a un sistema se copia a la carpeta %System% como:

- *%System%\drivers\HBKernel32.sys*
- *%System%\System.exe*

Libera los siguientes archivos para robar información crítica del sistema:

%System%\HBQQXX.dll	*%CurrentFolder%\HBCONQUER.dll*
%CurrentFolder%\HBmhly.dll	*%CurrentFolder%\HBSOUL.dll*
%CurrentFolder%\HB1000Y.dll	*%CurrentFolder%\HBCHIBI.dll*
%CurrentFolder%\HBWOOOL.dll	*%CurrentFolder%\HBDNF.dll*
%CurrentFolder%\HBXY2.dll	*%CurrentFolder%\HBWARLORDS.dll*
%CurrentFolder%\HBJXSJ.dll	*%CurrentFolder%\HBTL.dll*
%CurrentFolder%\HBSO2.dll	*%CurrentFolder%\HBPICKCHINA.dll*
%CurrentFolder%\HBFS2.dll	*%CurrentFolder%\HBCT.dll*
%CurrentFolder%\HBXY3.dll	*%CurrentFolder%\HBGC.dll*
%CurrentFolder%\HBSHQ.dll	*%CurrentFolder%\HBHM.dll*
%CurrentFolder%\HBFY.dll	*%CurrentFolder%\HBHX2.dll*
%CurrentFolder%\HBWULIN2.dll	*%CurrentFolder%\HBQQHX.dll*
%CurrentFolder%\HBW2I.dll	*%CurrentFolder%\HBTW2.dll*
%CurrentFolder%\BKDXY.dll	*%CurrentFolder%\HBQQSG.dll*
%CurrentFolder%\HBWORLD2.dll	*%CurrentFolder%\HBQQFFO.dll*
%CurrentFolder%\HBASKTAO.dll	*%CurrentFolder%\HBZT.dll*
%CurrentFolder%\HBZHUXIAN.dll	*%CurrentFolder%\HBMIR2.dll*
%CurrentFolder%\HBWOW.dll	*%CurrentFolder%\HBRXJH.dll*
%CurrentFolder%\HBZERO.dll	*%CurrentFolder%\HBYY.dll*
%CurrentFolder%\HBBO.dll	*%CurrentFolder%\HBMXD.dll*
%CurrentFolder%\HBPPBL.dll	*%CurrentFolder%\HBSQ.dll*
%CurrentFolder%\HBXMJ.dll	*%CurrentFolder%\HBTJ.dll*
%CurrentFolder%\HBQJSJ.dll	*%CurrentFolder%\HBFHZL.dll*
%CurrentFolder%\HBLYFX.dll	*%CurrentFolder%\HBWLQX.dll*
%CurrentFolder%\HBR2.dll	*%CurrentFolder%\HBWD.dll*
%CurrentFolder%\HBCHD.dll	*%CurrentFolder%\HBZG.dll*
%CurrentFolder%\HBTZ.dll	*%CurrentFolder%\HBJTLQ.dll*
%CurrentFolder%\HBQQXX.dll	

Seguidamente crea las siguientes sub-llaves:

- *[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY_HBKERNEL32]*
- *[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\HBKernel32]*
- *[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet003\Services\HBKernel32]*
- *[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_HBKERNEL32]*
- *[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HBKernel32]*

Crea una llave de registro para ejecutarse la próxima vez que se re-inice el sistema. Revisa todas las unidades de disco y sus carpetas y substrae información crítica del sistema, la cual envía a una cuenta de correo cifrada.

Finalmente el troyano se auto-elimina.

LISTA DE ANTIVIRUS

NOMBRE DEL ANTIVIRUS	PAGINA WEB
Panda Software	http://www.pandasoftware.es/
Per Antivirus	http://www.perantivirus.com/
The Hacker	http://www.hacksoft.com.pe/
AVAST Antivirus	http://www.antivir.com/support.htm
Zap Antivirus	http://www.zapantivirus.com
Sophos Antivirus	http://esp.sophos.com/
Norton Antivirus (NAV)	http://www.sarc.com/avcenter/download.html
Antiviral Toolkit Pro (AVP)	http://www.kaspersky.com/
ESafe	http://www.esafe.com/download/virusig.html
Antivirus Enterprise Protection	http://www.commandcom.com/html/files.html
InoculateIT	http://support.cai.com/Download/virussig.html
McAfee VirusScan	http://download.mcafee.com/updates/updates.asp
AVG Antivirus	http://www.grisoft.com/us/us_index.php
Symantec	http://www.symantec.com/
TrenMicro	http://www.trendmicro.com/download/pattern.asp
BitDefender	http://www.bitdefender-es.com
Antivirus	http://www.antivirus.com

CUALQUIER CONSULTA ENVIAR UN CORREO AL
CENTRO DE CONSULTA E INVESTIGACION SOBRE SEGURIDAD DE LA INFORMACION - CCISI

ccisi@pcm.gob.pe
Teléfono : 2744356 – 106