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 145/ 26 Septiembre de 2008

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

INDICE

- GUSANO TROJ/ONLINEG-BC
- GUSANO W32/AUTORUN.BHX
- Lista de Antivirus

FUENTES

- Alerta Antivirus
- Per Antivirus
- Sophos

GUSANO TROJ/ONLINEG-BC

Alias : Vbs/Gedzac.B, OnLineG.BC

Es un gusano de ejecución automática que se propaga por correo MultiSPAM, servicios de compartimiento de archivos Peer to Peer y redes de correo gratuito basadas en la web.

El gusano infecta los siguientes sistemas operativos: Windows 95/98/NT/Me/2000/XP y Server 2003.

Cuando este gusano ingresa a un sistema se copia a la carpeta %System% con los siguientes nombres:

- %System%\AvrilLavigne.jpg (imagen usada como disfraz para atraer a los usuarios incautos)
- %System%\iw.dat (macros)
- %System%\iwn.dat (macros)
- %System%\ix.dat (macros)
- %System%\ixn.dat (macros)
- %System%\pkzip.exe (extractor de archivos)
- %System%\regsrv.exe (deshabilitador de antivirus)
- %System%\sendi.exe (aplicación propietaria de envio de mensajes de correo)

El gusano libera copias de sí mismo en la misma carpeta:
- %System%\File.vbs
- %System%\FILEZIP.ZIP
- System%\GEDZAC.vbs
- %System%\Israfel.vbs
- %System%\Kernel32.win
- %System%\mouse_configurator.win
- %System%\Template.htm
- %System%\winmgd.win

El archivo FILEZIP.ZIP es una copia empaquetada del gusano que es enviada por correo bajo la modalidad MultiSPAM.

Para ejecutarse la próxima vez que se re-inicie el sistema modifica las llaves de registro.
Para afectar el funcionamiento del mouse edita el archivo "win.ini".
Para afectar el sistema de Inicio de Windows edita el archivo "system.ini".
Para cambiar los iconos de Windows al icono de DLL crea un registro.
Para generar plantillas infectadas de Outlook Express crea llaves.
Para disminuir la seguridad de MS Word y Excel crea sub-llaves.
Para propagarse a través de redes Peer to Peer busca en todas las unidades de disco las carpetas con cadenas "share" y "download" copiando a las mismas una extensa lista de archivos con extensión .EXE

Finalmente activa su archivo de envío masivo de correo MultiSPAM.

MAS INFORMACION:

- **SOPHOS**
  http://www.sophos.com/security/analyses/viruses-and-spyware/trojonlinegbc.html

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

- **Alerta Antivirus**
  http://alerta-antivirus.inteco.es/virus/detalle_virus.html?cod=8132

GUSANO W32/AUTORUN.BHX

AutoRun.BHX es un gusano residente en memoria, que se propaga a través de servicios de Internet o redes con recursos compartidos.

Infecta unidades de disco removibles y redes compartidas configuradas con contraseñas débiles. Roba nombres de usuarios y contraseñas de conocidos juegos en línea.

Se conecta a un sito web ubicado en la China y descarga un malware comprimido en formato .rar

Infecta a los siguientes sistemas operativos: Windows 95/98/NT/2000/XP/Vista y Server 2003.

Una vez ingresado al sistema se copia al directorio %Windir% como xadeiect.com que es un "dropper" que libera los siguientes archivos en las rutas:

- %Temp%\n2mmf2qu.dll
- %Windir%\system32\kavo.exe
- %Windir%\system32\kavo0.dll

Modifica los siguientes archivos:

- %Temp%\6itt.sys
- %Windir%\system32\wincab.sys

Para activarse la próxima vez que se re-inicie el sistema, crea la siguiente llave de registro:

[HKEY_CURENT_USER\SoftWare\Microsoft\Windows\CurrentVersion\Run]
"kava" = "%Windir%\System32\kavo.exe

%Windir% es una variable que corresponde a C:\Windows en Windows 95/98/Me/XP/Server 2003 y C:\Winnt en Windows NT\2000.

%Temp% es la variable C:\Windows\Temp en Windows 95/98/Me, C:\Winnt\Temp en Windows NT\2000 y C:\Document and Settings\[nombre_de_usuario]\Local Settings\Temp en Windows XP/Server 2003.

Al siguiente inicio del equipo, infecta la raíz de las unidades de disco removibles.

Engancha las siguientes rutinas SSDT Stealth a los procesos Kernel:

- pntoskrnl.exe!NtOpenProcess
- ntoskrnl.exe!NtEnumerateValueKey
- ntoskrnl.exe!NtEnumerateKey

En la ruta:

- %windir%\system32\wincab.sys

Con el objeto de robar los nombres y contraseñas de los siguientes juegos en línea:

- Dekaron
- MapleStory
- Perfect World
- Ragnarok Online
- Seal Online
- Yulgang
- Zheng Tu Online

También se propaga a través de redes con recursos compartidos, configuradas con contraseñas débiles.

MAS INFORMACION:

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

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