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 142/ 30 Junio de 2008

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

INDICE

FUENTES

- Per Antivirus
- Alerta Antivirus
- Symantec

TROYANO TROJ/SWIZZOR.NX

Swizzor.NX es un troyano que se propaga dentro de publicidad no deseada (Adware) insertadas dentro de algunos software gratuitos (Freeware) o copias de Evaluación (Shareware).

El troyano infecta a los siguientes sistemas operativos Windows 95/98/NT/2000/XP/Vista y Server 2003, está desarrollado en Assembler.

Deshabilita la mayoría de funciones del Explorador de Windows y será necesario restaurar el sistema.

Una vez ingresado a un sistema se copia a:

- *%User%\Application Data\Web Okay Five 01*
- *%User%\Application Data\Web Okay Five 01\Media Flap.exe*
- *%User%\Application Data\Web Okay Five 01\Dash Wma.exe*
- *%User%\Application Data\forkmesswin*
- *%User%\Application Data\forkmesswin\cdrom upload file.exe*
- *%User%\Application Data\forkmesswin\joy download acid.exe*
- *%User%\Application Data\forkmesswin\leapzbbq.exe*
- *%Program Files%\forkmesswin*
- *%Program Files%\NetPumper\ZM\minime.exe*

Para ejeucutarse la próxima vez que se instale el sistema crea un llave.

Al siguiente inicio del equipo, el troyano inserta en forma oculta, su código viral en cada instancia ejecutada del Explorador de Windows, hasta dejarlo inoperativo. Será necesario restaurar el sistema.

MAS INFORMACION:

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

GUSANO W32/ZATYUDI.A

Alias: *Worm.W32/Zatyudi@US; W32.Zatyudi.A*

Zatyudi es un gusano que se propaga a través de servicios de Internet visitando páginas web con archivos infectados. Se autocopia a carpetas compartidas y unidades de disco removibles con diferentes nombres de archivos, con extensiones .EXE y .ZIP, descarga imágenes de diversas direcciones web.Termina todos los procesos y servicios en ejecución del sistema infectado y notifica a dos direcciones IP del estado de su progreso infeccioso.

Infecta a los siguientes sistemas operativos: Windows 98/98/Me/NT/2000/XP/Vista y Server 2003, desarrollado en C++.

TROYANO TROJ/BLUSOD

Troyano residente en memoria, propagado por diversos servicios de Internet.

El troyano infecta los siguientes sistemas operativos Windows 95/98/NT/2000/XP/Vista y Server 2003, está desarrollado en Assembler.

Crea un falso salva-pantallas y fondo de escritorio de Windows con un mensaje en texto ASCII. Deshabilita algunas funciones del sistema.

Se conecta a dos sitios web ubicados en Suiza y Finlandia, respetivamente, desde los cuales descarga malwares.

Crea el siguiente mensaje en formato ASCII con colores básicos:

Warning!
Spyware detected on your computer!
Install an antivirus or spyware remover to clean your computer.

Finalmente el troyano se conecta a los siguientes sitios web para descargar malwares en el sistema infectado:

- *www.youpornztube.com (ubicado en Suiza)*
- *www.antivirusxp2008.com (ubicado en Finlandia*)

MAS INFORMACION:

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

TROYANO BKDR/IRCBOT.BGY

Es un troyano/backdoor residente en memoria, que se propaga a través de otros malwares o visitando páginas web maliciosamente acondicionadas.
Abre puertos TCP aleatorios, se conecta a un servidor HTTP y ejecuta comandos arbitrarios en forma remota.

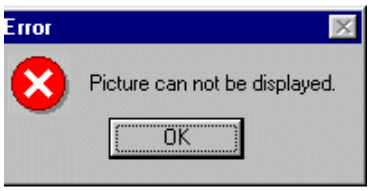
Infecta los siguientes sistemas operativos Windows 98/NT/2000/XP y Server 2003, está desarrollado en Assembler.

Una vez ingresado al sistema se copia a:

- *%Windir%\wksvcsc.exe*

Para activarse cada vez que se re-inicie el sistema, crea varias llaves de registro.

Al siguiente inicio del equipo muestra la siguiente falsa caja de diálogo:



Luego su componente Backdoor abre un puerto aleatorio que se encuentre abierto y se conecta a un servidor HTTP desde el cual el autor podrá ejecutar, entre otras, las siguientes acciones arbitrarias:

- *Descargar o extraer y subir archivos*
- *Ejecutar comandos arbitrarios*
- *Ejecutar o terminar procesos o hilos.*
- *Removerse a sí mismo*
- *Actualizarse a sí mismo*

MAS INFORMACION:

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

LISTA DE ANTIVIRUS

NOMBRE DEL ANTIVIRUS	PAGINA WEB
Panda Software	http://www.pandasoftware.es/
Per Antivirus	http://www.persystems.net/
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