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 144/ 26 Agosto de 2008

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

INDICE

TROYANO TROJ/FAKEAV.BH

FakeAV.BH es un troyano que se propaga simulando ser un antivirus en línea, al visitar determinadas páginas web o es descargado dentro de otros malwares. Deshabilita funciones y servicios vitales del sistema.

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

Una vez ingresado al sistema, crea la siguiente carpeta:

- *C:\Documents and Settings\{User Name}\Application Data\rhc7pgj0e3ct*

liberando el archivo pphc3pgj0e3ct.exe en la carpeta %System%

Como parte de su instalación realiza lo siguiente:

- Crea diversas llaves.
- Deshabilita el Administrador de Tareas creando una sub-llave.
- Deshabilita el Editor de Registros creando una sub-llave.
- Deshabilita el Comando Prompt, creando una sub-llave.
- Deshabilita la opción de Carpetas del Exlorador de Windows creando una sub-llave

MAS INFORMACION:

- **SOPHOS**
  http://www.sophos.com/security/analyses/viruses-and-spyware/trojfakeavbh.html
- **FrSIRT**
  http://www.frsirt.com/english/virus/2008/04560
- **PER ANTIVIRUS**
  http://www.perantivirus.com/sosvirus/virufamo/fakeavbh.htm
- **Alerta Antivirus**
  http://www.alerta-antivirus.es/virus/detalle_virus.html?cod=8024

TROYANO TROJ/CHEPVIL.RAR

Chepvil.RAR es un que se propaga a través de mensajes de correo MultiSPAM simulando contener un video de la artista Angelina Jolie.

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

Infecta el archivo HOSTS, conecta el sistema a diversos URL desde los cuales descarga archivos malwares que deshabilitan el Firewall de Windows, funciones y servicios del sistema.

FUENTES

- Alerta Antivirus
- Per Antivirus
- Trend Micro
- Sophos
- FrSIRT
- eSecurity Planet.com
- Secunia

El mensaje tiene el siguiente formato, con el icono de los archivos .RAR:

Asunto: Angelina Jolie Free Video
Contenido:"The password on archive anjelina"
Anexado: Angelina_Jolie.rar (10KB) ATT0001.txt (232 bytes)

Al hacer click en el supuesto password el archivo .RAR desempaqueta un archivo .EXE que infectará al archivo HOSTS.

El sistema infectado se conectará a diversos URL con el objeto de descargar los siguientes archivos malwares:

- *exe*
- *php*
- *video-nude-anjelina.avi.exe*

Los mismos que deshabilitan el Firewall de Windows y funciones y servicios del sistema.

MAS INFORMACION:

- **eSecurity Planet.com**
  http://www.esecurityplanet.com/alerts/article.php/3763696

- **Trend Micro**
  http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_CHEPVIL.RAR&VSect=T

TROYANO TROJ/BKDR.QOW

Troj/Bkdr.QOW es un troyano/backdoor, que se propaga a través de servicios de Internet o visitando páginas web que han sido especialmente programadas. Crea un falso servicio con un driver de sistema y a través del puerto TCP 8080 establece una conexión con un servidor HTTP encriptado, desde el cual ejecutará acciones arbitrarias.

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

Al siguiente inicio del equipo el archivo jedoupynna.exe es registrado como un nuevo servicio de driver de sistema con las características:

Nombre mostrado: d77xxfaay4
Descripción: Canon BJ Memory Card Manager
Rutina de ejecución: Automática

Este falso servicio a través del puerto TCP 8080 establece una conexión con un servidor HTTP encriptado, desde el cual podrá ejecutar acciones arbitrarias.

MAS INFORMACION:

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

GUSANO W32/AUTORUN.DAW

Autorun.DAW es un gusano residente en memoria que infecta todas las unidades de disco, físicas, lógicas, removibles y diskettes. Abre la Calculadora de Windows, una ventana oculta del Internet Explorer y descarga malwares.

Al siguiente inicio del equipo, permanece activo en memoria e inyecta su código en los procesos:

- *Calc.exe*
- *IExplorer.exe*

Finalmente el gusano se conecta a un sitio web http://[Bloqueado]2.org para descargar malwares, los cuales causarán daños irreversibles en el sistema

MAS INFORMACION:

- **SECUNIA**
  http://secunia.com/virus_information/49174/autorun.daw/

- **Alerta Antivirus**
  http://alerta-antivirus.inteco.es/virus/detalle_virus.html?cod=8070

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