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 141/ 23 Mayo de 2008

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

INDICE

FUENTES

- Per Antivirus
- Alerta Antivirus
- Symantec

TROYANO TROJAN.W32/SPRYCT

Alias: *Trojan.Spryct ; TROJ/SPRYCT*

Spryct es un troyano reportado que se propaga visitando páginas web expresamente acondicionadas. Infecta los siguientes sistemas operativos: Windows 95/98/Me/NT/2000/XP/Vista y Server 2003, está desarrollado en Assembler.

Roba información del sistema y descarga un archivo de configuración de sistema y aleatoriamente malwares de dos web ubicadas en Dinamarca y una en los Estados Unidos, las cuales han sido "crackeadas". Al ingresar a un sistema se copia a la carpeta %System% como crypts.dll y para ejecutarse la próxima vez que se re-inicie el sistema crea las llaves en el registro.

Al siguiente inicio del equipo el troyano captura la siguiente información:

- Características del CPU
- Dirección IP
- Identificador OEM
- Versión de sistema operativo
- Procesos en ejecución
- Velocidad de Acceso a Internet
- La misma que envía a una dirección de correo cifrada perteneciente al autor.

Luego se conecta a las siguientes URLs, las mismas que han sido crackeadas y desde las cuales intenta descargar un archivo de configuración de sistema:

- http://www.itrysrying.com/[Removido] ubicado en Dinamarca
- http://www.littlesoring.com/[Removido] ubicado en Dinamarca
- http://www.dbafbceefae.com/[Removido] ubicado en USA

Aleatoriamente, el troyano puede descargar archivos malware en los sistemas infectados.

MAS INFORMACION:

- **Alerta Antivirus**
  http://www.alertaantivirus.es/virus/detalle_virus.html?cod=7830

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

GUSANO W32/ZATYUDI

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++.

Al siguiente inicio del equipo el gusano captura las direcciones de correo de los archivos con las extensiones:

exe	eml	shtml
scr	htm	txt
com	html	xml
pif	jsp	js
cmd	msg	xml
wab	php	aspx
asp	shtm	dbx

Activa su rutina MultiSPAM componiendo los mensajes de correo con la direcciones extraídas y asuntos y contenidos existentes en el sistema.

Seguidamente el gusano se copia a las carpetas compartidas y unidades de disco removibles, con los siguiente nombres:

Bank mini Games.exe	Crack Windows vista final release.exe
Apache_server_831.exe	Gorilaz complete album lyrics.exe
Internet Explorer Vista.exe	Bank Mini Games complete 2007.exe
Nation Instinct.exe	New yahoo messenger vista.exe
Winamp Deluxe pro.exe	Update windows media player 10.exe
Nero final version 8.exe	full complete codec pack.exe
PHP nuke hack 3.exe	Hawai Beach screen saver.exe
Guitar XP studio.exe	Britney Screensaver (live).exe
war games.exe	e-Gold auto hack v2.1.exe
Splinter Cell.exe	full AVG update 2007 pack.exe
XP Update.exe	Complete password cracker tool.exe
Defacer tool.exe	Soccer Manager 2007.exe
Trojan removal	DeepFreeze Pro full.exe
eBay userID.exe	Deep_freeze enterprise.exe
eBay password.exe	Games Cheats DataBase.exe
Yahoo! password.exe	GameHouse Collection.exe
Californian Food v3.exe	

El gusano puede crear aleatoriamente los siguientes archivos comprimidos:

- Entertainment.zip
- don't touch this!.zip
- my briefcase.zip
- Photo Album Packed.zip
- Deep_freeze_pro8.zip
- Always in memory.rar
- Billing_13_professional.zip
- AVP_N_license.zip
- XP anti hacker.zip

Los archivos .ZIP contienen una copia del gusano con el nombre de SETUP.EXE, los cuales también son copiados a las carpetas compartidas y unidades de disco removibles.

MAS INFORMACION:

- **PER ANTIVIRUS**
  http://www.perantivirus.com/sosvirus/virufamo/zatyudi.htm
- **Symantec**
  http://www.symantec.com
- **Alerta Antivirus**
  http://www.alertaantivirus.es/virus/detalle_virus.html?cod=7755

TROYANO TROJ/FLATSE

Flatse es un troyano residente en memoria, que se propaga a través de los servicios de Mensajería de Yahoo y AIM (AOL Instant Messenger). Descarga un malware exploit automático.

Inhabilita el Firewall de Windows y ejecuta ataques de Denegación de Servicios (Dos) invocando servicios SYN, UDP y HTTP a las direcciones web contenidas en el cache DNS del sistema infectado.

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

Al ingresar a un sistema se copia al directorio %Windir% con el nombre de smrs.exe y para ejecutarse la próxima vez que se re-inicie el sistema crea una llave de registro.

Al siguiente inicio del equipo, el troyano captura las direcciones de las Libretas de Contactos del Yahoo Messenger y el AIM y envía un mensaje invitándolos a visitar un sitio web, el cual tiene un malware exploit de descarga automática.

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