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 137/ 25 Enero de 2008

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

INDICE

FUENTES

- Per Antivirus
- Symantec
- Alerta Antivirus
- VSANTIVIRUS
- NOD 32

TROYANO TROJ/TANTO.H

El troyano se propaga a través de diversos servicios de Internet, principalmente por mensajes de correo o visitando sitios web con archivos infectados.

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

Al ingresar a un sistema se copia al directorio %Windir% con el nombre de **wscntfy.exe** cuyo archivo registra como un nuevo servicio del sistema con el nombre de "Microsoft wscntfy Service", que muestra el mismo nombre con el atributo de arranque automático al Inicio del equipo.

El troyano activa su componente Backdoor y captura información crítica del sistema, nombres de usuarios, contraseñas, teclas digitadas, etc. y las envía a través de un puerto TCP abierto a determinado URL cifrado.

MAS INFORMACION:

- **ALERTA ANTIVIRUS**
  http://www.alerta-antivirus.es/virus/detalle_virus.html?cod=7484
- **SOPHOS**
  http://esp.sophos.com/security/analyses/trojtantoh.html
- **PER ANTIVIRUS**
  http://www.perantivirus.com/sosvirus/virufamo/tantoh.htm

GUSANO W32/NEKAT

Nekat es un gusano residente en memoria, infecta las unidades de disco removibles.

Deshabilita funciones y servicios vitales del sistema y será necesario reinstalar Windows.

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

También se copia a los discos y medios de almacenamiento removibles, incluyendo dispositivos USB:
Esconde funciones del Panel de Control de Windows.

Al siguiente inicio del equipo el gusano se copia a sí mismo en todas las unidades removibles:

%Unidad_de_disco%\autorun.inf

Las llaves y sub-llaves generadas desahabilitan funciones y servicios dejando al sistema inoperativo. Será necesario re-instalar Windows.

MAS INFORMACION:

- **ALERTA ANTIVIRUS**
  http://www.alerta-antivirus.es/virus/detalle_virus.html?cod=7462

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

GUSANO W32/IRCBOT.SN

Es un gusano residente en memoria que se propaga a través del IRC (Internet Chat Relay), redes con recursos compartidos o visitando páginas web con códigos malignos.

Usando puertos TCP aleatorios, su componente Backdoor se une a uno de dos canales de Chat, desde donde ejecutará acciones arbitrarias en forma remota.

Una vez ingresado a un sistema, el gusano se copia a la carpeta %System% con el nombre de w[xx]svc.exe.

Al siguiente inicio del equipo, haciendo uso de puertos TCP aleatorios, su componente Backdoor se conecta a los canales ##net o ##net-sa de un servidor IRC (Internet Chat Relay) desde los que ejecutará las siguientes acciones:

- Descargar, ejecutar archivos con códigos arbitrarios
- Terminar procesos en ejecución
- Desestabilizar la seguridad del siste ma
- Activar un servidor FTP y/o HTTP
- Unirse o salir de otros canales de Chat
- Ejecutar ataques de Denegación de Servicios (DoS) a redes con recursos compartidos
- Controlar el sistema en forma remota

MAS INFORMACION:

- **VSANTIVIRUS**
  http://www.vsantivirus.com/back-ircbot-sn.htm
- **SOPHOS**
  http://esp.sophos.com/virusinfo/analyses/trojircbots.html

W32/MYDOOM.BD@MM

MyDoom.DB es un gusano reportado propagado a través de mensajes de Correo con Remitentes disfrazados bajo la técnica Spoofing, Asuntos, Contenidos y archivos Anexados elegidos en forma aleatoria.

Inserta su micro-código en el proceso del Explorer.exe que integra con un Shell para activar el gusano al abrir determinados archivos.

Deshabilita el Administrador de Barra de Tareas y el Editor de Registros del sistema.

Posee su propio SMTP (Simple Mail Transfer Protocol) y se envía a los buzones de correo de la Libreta Global de Windows WAB (Windows Address Book), así como de la carpeta temporal de Internet Explorer.

MAS INFORMACION:

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