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 139/ 25 Marzo de 2008

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

INDICE

FUENTES

- Secunia
- FrSirt
- Per Antivirus
- Alerta Antivirus
- Trend Micro

TROYANO TROJ/SWFPHARM

Troyano se propaga aprovechando la vulnerabilidad "2Wire Routers Cross-Site Request Forgery" que es un dispositivo usado entre muchos proveedores de servicios de alojamiento de bajo costo y usuarios corporativos en todo el mundo, debido a su bajo precio.

- **http://www.2wire.com**

La vulnerabilidad es causada por la interfaz de la administración de sitios web de modelos de este Routeador, la cual permite a los usuarios realizar acciones sensibles via peticiones HTTP sin necesidad de verificar la validez del pedido del usuario.

De este modo se ejecutan determinadas acciones en este dispositivo al ingresar como administrador, logrando obligar al sistema a conectarse a los sitios maliciosamente configurados.

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

Al ingresar a un sistema activa y muestra la siguiente imagen:

y reconfigura el Router redireccionándolo a una lista de direcciones URL con archivos infectados.

Al siguiente inicio del equipo el gusano se conecta a las siguientes URL's desde las cuales intenta descargar archivos infectados con otro troyano.

- http://home/xs[Removido]
- http://gateway.2wire.net/xs[Removido]
- http://192.168.1.254/xs[Removido]
- http://192.168.0.1/xs[Removido]
- http://172.16.0.1/xs[Removido]

MAS INFORMACION:

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

VIRUS BKDR_AGENT.NOZ

El virus abre puertos TCP aleatorios permitiendo a los intrusos el acceso remoto al sistema infectado, haciendo uso de diversos servicios de Internet. Infecta los siguientes sistemas operativos Windows 98/NT/Me/2000/XP y Server 2003.

Al ingresar a un sistema crea la siguiente ruta y carpeta:

- **C:\Documents and Settings\LocalService\Application Data\Microsoft\UPnP Device Host**

Al siguiente inicio del equipo el Backdoor abre puertos TCP aleatorios para permitir que los intrusos se conecten al sistema usando servicios tales como HTTP, Telnet o el IRC (Internet Chat Relay), desde los cuales ejecutará comandos remotos arbitrarios.

MAS INFORMACION:

- **ALERTA ANTIVIRUS**
  http://alerta-antivirus.inteco.es/virus/detalle_virus.html?cod=7648
- **TREND MICRO**
  http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=BKDR_AGENT.NOZ&VSect=P
- **PER ANTIVIRUS**
  http://www.perantivirus.com/sosvirus/virufamo/agentnoz.htm

GUSANO W32/SOCKS.D@MM

Alias:

W32/Socks.D@mm [PerAntivirus], WORM_SOCKS.D [Trend Micro]

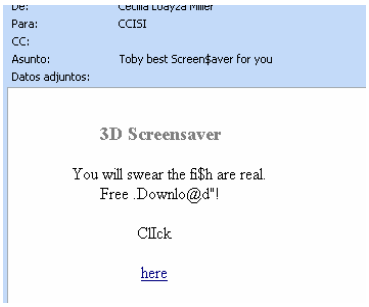
Socks.D es un gusano reportado el 13 de Marzo del 2008 propagado a través de mensajes de Correo con la técnica Spoofing, con un Asunto y un Contenido que tiene un enlace de descarga hacia un sitio web de "salvadores de pantalla" ubicado en Alemania.

Se propaga también en mensajes con el mismo enlace a la Libreta de Contactos del Microsoft Messenger.

Es un PE (Portable Ejecutable) e infecta Windows 98/NT/Me/2000/XP y Server 2003, está desarrollado y compilado en Visual C++, con una extensión de 18KB y comprimido con el utilitario UPX (Ultimate Packer for eXecutables):

http://upx.sourceforge.net

El mensaje tiene las siguientes características:



Al hacer click en el enlace (que dice “here”) dentro del contenido el sistema es dirigido a una dirección URL de Salvadores de Pantallas que contienen un exploit de ejecución automática.

Al siguiente inicio del equipo activa su rutina de envío masivo de correo MultiSPAM.

MAS INFORMACION:

- **TREND MICRO**
  http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_SOCKS.D&VSect=Sn
- **SECUNIA**
  http://secunia.com/virus_information/45572/socks.d/
- **FrSIRT**
  http://www.frsirt.com/english/virus/2008/01567
- **ALERTA ANTIVIRUS**
  http://alerta-antivirus.red.es/virus/busca_virus.html?buscar=Buscar&nombre=&pclave=perantivirus&tipo=0
- **PER ANTIVIRUS**
  http://www.perantivirus.com/sosvirus/virufamo/socksd.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