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 138/ 22 Febrero de 2008

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

INDICE

FUENTES

- Per Antivirus
- Symantec
- Alerta Antivirus
- VSANTIVIRUS
- Ciber News

GUSANO W32/ONLINEG.DSO

Es un gusano residente en memoria, se propaga a través de diversos servicios de Internet. Infecta todas las unidades de disco fijos y removibles.

Infecta Windows 95/98/Me/NT/2000/XP y Server 2003, desarrollado en Visual C++, con una extensión de 105KB, está encriptado con rutinas propias.

Al siguiente inicio del equipo el gusano amvo.exe se auto-destruye. Su componente espía extrae información del sistema, nombres de usuarios y contraseñas, las cuales envía a una dirección de correo cifrada.

Luego se copia a todas las unidades de disco fijas o removibles.

El gusano intenta descargar archivos conteniendo la última versión de sí mismo de un portal ubicado en Korea:

http://www.[Censurado].com/mf2/help.exe
http://www.[Censurado].com/mf2/help.rar

Si logra descargarlos los auto-ejecuta y desestabiliza el sistema.

MAS INFORMACION:

- **ALERTA ANTIVIRUS**
  http://www.alerta-antivirus.es/virus/detalle_virus.html?cod=7519
- **CIBER NEWS**
  http://cibernews.info/article.php?story=20080205173109523
- **PER ANTIVIRUS**
  http://www.perantivirus.com/sosvirus/virufamo/onlinegdso.htm

GUSANO W32/AUTOOK

Autook es un gusano residente en memoria que se propaga a través de servicios de Internet principalmente visitando páginas web exprofesamente infectadas.

Infecta todas las unidades de disco fijos, lógicas y removibles, incluyendo dispositivos de almacenamiento USB.

El gusano descarga un archivo que cambia la configuración del sistema desde un portal ubicado en Beijing, China:

http://ddos.fuckunion.com

El cual auto-ejecuta y conecta a otras direciones URL ubicadas en China que descargan archivos con códigos arbitrarios

Infecta Windows 95/98/Me/NT/2000/XP/Vista y Server 2003, desarrollado en Visual C++, con una extensión de 89KB y no está encriptado.

MAS INFORMACION:

- **ALERTA ANTIVIRUS**
  http://www.alerta-antivirus.es/virus/detalle_virus.html?cod=7551

- **SYMANTEC**
  http://www.symantec.com/

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

GUSANO W32/IMAUT.CN

Imaut.CN es un que se propaga vía Yahoo Instant Messenger y redes con recursos compartidos.

Descarca archivos de un portal de Rusia los cuales cambian la configuración del sistema. Se activa cronológicamente todos los días a las 09:00 AM e infecta la raíz de todas las unidades de disco.

Es un PE (Portable Ejecutable) e infecta Windows 98/NT/Me/2000/XP/Vista y Server 2003, está desarrollado en Visual C++.

Luego intenta descargar una actualización de configuraión de sistema desde un sitio web ubicado en Rusia:

- http://crackspider.net/setting.exe
- http://crackspider.net/setting.dll

Al descargarlos crea los siguientes archivos para almacenar la información de configuración:

%System%\settings.ini
%Windir%\winhelp.ini

La nueva configuración contiene instrucciones para acceder a direcciones web con códigos malignos.

El gusano cierra cualquier ventana que tenga una de las siguientes cadenas en su título:

- Bkav2006
- Registry
- System Configuration
- Windows mask

Periódicamente termina los procesos que contengan las cadenas:

- game_y.exe
- cmder.exe

El gusano envía a la lista de contactos del Yahoo Instant Messenger el siguiente mensaje:

Happy sankranti/pongal
http://crackspider.net[Removido]

MAS INFORMACION:

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

- **ALERTA ANTIVIRUS**
  http://www.alerta-antivirus.es/virus/detalle_virus.html?cod=7559

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