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 143/ 31 Julio de 2008

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

## INDICE



## GUSANO W32/GAEL.B

***Alias:* *WORM_GAEL.B; W32/Gael.B; Gael.B***

W32/GAEL.B es un gusano que infecta la raíz de las unidades lógicas de disco, removibles y floppies. Es un PE (Portable Ejecutable) e infecta los siguientes sistemas operativos Windows 95/98/Me/NT/XP y Server 2003, desarrollado en Assembler.

Al ingresar a un sistema se copia a la carpeta **%System%** usando el nombre del archivo en ejecución actual. Para engañar al usuario, el gusano muestra un falso icono de carpeta de Windows.

Para ejecutarse la próxima vez que se re-inicie el sistema crea la llave de registro:

- *[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]*
- *"RavMont" = "%System%\[nombre del archivo_ejecutado_infectado]"*
  - *%System% es la variable C:\Windows\System para Windows 95/98/Me, C:\Winnt\System32 para Windows NT/2000 y C:\Windows\System32 para Windows XP y Windows Server 2003.*

Para infectar la raíz de las unidades lógicas de disco, removibles y floppies, el gusano crea el siguiente archivo AUTORUN.INF:

- [AutoRun]
- open=[nombre del archivo_ejecutado_infectado]

**MAS INFORMACION:**

- **PER ANTIVIRUS**
  http://www.perantivirus.com/sosvirus/virufamo/gaelb.htm
- **Alerta Antivirus**
  http://alerta-antivirus.inteco.es/virus/detalle_virus.html?cod=7935
- **Trend Micro**
  http://www.trendmicro.com/la/home/enterprise.htm

## TROYANO TROJ/MDROPER.ZT

Es unn troyano que se propaga via HTTP con otros malwares o visitando páginas web sospechosas, expresamente acondicionadas.

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

Al ingresar a un sistema el archivo se copia en las siguientes rutas y con los nombres:

- *%System%\msjava.exe*
- *%System%\dump.exe*
- *%System%\6to4ex.dll*

## FUENTES

- Alerta Antivirus
- Per Antivirus
- Trend Micro

- *%Windows%\spupdsvc.exe*
- *%Windows%\hscancon.dll*
- *%User Temp%\WINWORD.exe*
- *%System% es la variable C:\Windows\System para Windows 95/98/Me, C:\Winnt\System32 para Windows NT/2000 y C:\Windows\System32 para Windows XP y Windows Server 2003.*

- *%Windir% es una variable que corresponde a C:\Windows en Windows 95/98/Me/XP/Server 2003 y C:\Winnt en Windows NT\2000.*
- *%ProgramFiles% es la variable referida a la carpeta de archivos de programa. Por defecto es C:\Program Files.*
- *%User Temp% es la variable que registra la información temporal específica de cada usuario y que define los límites de su entorno de trabajo. Es igual a C:\Documents and Settings\[nombre_de _usuario]\Local Settings\Temp en Windows 2000, XP y Server 2003.*

Al siguiente inicio del equipo el troyano inserta su código viral en los archivos con extensión .DOC, .EXE y .DLL dejándolos inoperativos.

**MAS INFORMACION:**

- **Alerta Antivirus**
  http://alerta-antivirus.inteco.es/virus/detalle_virus.html?cod=7961

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

## TROYANO BKDR/IRCBOT.BGY

El troyano crea una falsa salva-pantallas y fondo de escritorio de Windows con un mensaje en texto ASCII.

Una vez ingresado a un sistema se copia a:

- *%System%\blphc3pgj0e3ct.scr (pantalla azul)*
- *%System%\lphc3pgj0e3ct.exe (copia del troyano)*
- *%System%\phc3pgj0e3ct.bmp (archivo inocuo)*

Para ejecutarse la próxima vez que se re-inicie el sistema crea la llave:

- *[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ Windows\ CurrentVersion\Run]*
- *"lphc3pgj0e3ct" = "%System%\lphc3pgj0e3ct.exe"*

El troyano configura el archivo phc3pgj0e3ct.bmp para crear un falso fondo de escritorio modificando las siguientes entradas:

- *[HKEY_CURRENT_USER\Control Panel\Desktop] Wallpaper = "%System%\phc3pgj0e3ct.bmp"*
- *[HKEY_CURRENT_USER\Control Panel\Desktop] OrigianlWallpaper = "%System%\phc3pgj0e3ct.bmp"*
- *[HKEY_CURRENT_USER\Control Panel\Desktop] ConvertedWallpaper = "%System%\phc3pgj0e3ct.bmp"*

Como consecuencia muestra el siguiente fondo de escritorio:


Finalmente el troyano se conecta a diferentes sitios web para descargar malwares en el sistema infectado.

## 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**