

CONTENIDO

- ✚ [VIRUS W32/AGOBOT.BQJ](#)
- ✚ [EXPLOIT IFRAME.BoF](#)
- ✚ [VIRUS MYDOOM.AE y MYDOOM.AF](#)
- ✚ [VIRUS GAVIR.A](#)
- ✚ [VIRUS SOBER.I](#)
- ✚ [VIRUS YANZ.A](#)
- ✚ [VIRUS DREW.A](#)
- ✚ [CONSEJOS PARA PROTEGERSE DE LOS VIRUS INFORMATICOS](#)
- ✚ [LISTA DE ANTIVIRUS](#)

INFORMACION DE VIRUS INFORMATICOS

VIRUS W32/AGOBOT.BQJ

Alias:

Troj/Gaobot.BQJ

MÉTODO DE INFECCIÓN

Es un virus que infecta redes con el archivo **bcvsrv32.exe**, cancela los procesos antivirus, firewalls y software de control, bloquea el acceso a diversas direcciones URL, abre un Backdoor que permite controlar los sistemas infectados a través del IRC (Internet Relay Chat).

El virus infecta a los siguientes sistemas operativos: Windows 95/98/NT/Me/2000/XP, incluyendo los servidores NT/2000/Server 2003, está programado en Visual C++.

Una vez que el virus ingresa al sistema se auto-copia a la carpeta %System% el archivo de nombre bcvsrv32.exe y para ejecutares la próxima vez que se re-inicie el sistema crea las siguientes llaves de registro:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
"Bcvsrv32" = "%System%\bcvsrv32.exe"
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices]
"Bcvsrv32" = "%System%\bcvsrv32.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.

Al siguiente inicio del equipo el virus termina los procesos de los siguientes antivirus, firewalls o programas de monitoreo que se encuentren instalados, dejando al sistema vulnerable a los virus y ataques de intrusos:

• **Fuentes**

- Panda Software
- Hispasec
- Per Antivirus
- Hacksoft

_AVP32.EXE	ATRO55EN.EXE	NOD32.EXE	NWTOOL16.EXE
_AVPCC.EXE	ATUPDATER.EXE	NORMIST.EXE	OLLYDBG.EXE
_AVPM.EXE	ATWATCH.EXE	NOTSTART.EXE	ONSRVR.EXE
ACKWIN32.EXE	AU.EXE	NPFMESSENGER.EXE	OPTIMIZE.EXE
ADAWARE.EXE	AUPDATE.EXE	NPROTECT.EXE	OSTRONET.EXE
ADVXDWIN.EXE	AUTODOWN.EXE	NPSCHECK.EXE	OTFIX.EXE
AGENTSVR.EXE	AUTOTRACE.EXE	NPSSVC.EXE	PADMIN.EXE
AGENTW.EXE	AUTOUPDATE.EXE	NSCHED32.EXE	PANIXK.EXE
ALERTSVC.EXE	AVPUPD.EXE	NSSYS32.EXE	PATCH.EXE
ALEVIR.EXE	AVWUPD32.EXE	NSTASK32.EXE	PAVCL.EXE
ALOGSERV.EXE	AVXQUAR.EXE	NSUPDATE.EXE	PAVPROXY.EXE
AMON9X.EXE	CONSOL.EXE	NT.EXE	PAVSCHED.EXE
ANTI-TROJAN.EXE	F-AGOBOT.EXE	NTRTSCAN.EXE	PAVW.EXE
ANTIVIRUS.EXE	HIJACKTHIS.EXE	NTVDM.EXE	PCC2002S902.EXE
ANTS.EXE	NETSCANPRO.EXE	NTXconfig.EXE	PCC2K_76_1436.EXE
APIMONITOR.EXE	NETSPYHUNTER-1.2.EXE	NULXEXE	PCCIOMON.EXE
APLICA32.EXE	NETSTAT.EXE	NVARCH16.EXE	PCCNTMON.EXE
APVXDWIN.EXE	NETUTILS.EXE	NVC95.EXE	PCCWIN97.EXE
ARR.EXE	NISSERV.EXE	NVSV32.EXE	PCCWIN98.EXE
ATCON.EXE	NISUM.EXE	NWINST4.EXE	PCDSETUP.EXE
ATGUARD.EXE	NMAIN.EXE	NWSERVICE.EXE	PENIS.EXE

PERISCOPE.EXE	SMSS32.EXE	VSWIN9XE.EXE
PERSFW.EXE	SOAP.EXE	VSWINNTSE.EXE
PERSWF.EXE	SOFI.EXE	VSWINPERSE.EXE
PF2.EXE	SPERM.EXE	W32DSM89.EXE
PFWADMIN.EXE	SPF.EXE	W9X.EXE
PGMONITR.EXE	SPHINX.EXE	WATCHDOG.EXE
PINGSCAN.EXE	SPOLER.EXE	WEBDAV.EXE
PLATIN.EXE	SPOOLCV.EXE	WEBSCANX.EXE
POP3TRAP.EXE	SPOOLSV32.EXE	WEBTRAP.EXE
POPROXY.EXE	SPYXX.EXE	WFINDV32.EXE
POPCAN.EXE	SREXE.EXE	WGFE95.EXE
PORTMONITOR.EXE	SRNG.EXE	WHOSWATCHINGME.EXE
POWERSCAN.EXE	SS3EDIT.EXE	WIMMUN32.EXE
PPINUPDT.EXE	SSG_4104.EXE	WIN32.EXE
PPTBC.EXE	SSGRATE.EXE	WIN32US.EXE
PPVSTOP.EXE	ST2.EXE	WINACTIVE.EXE
PRIZESURFER.EXE	START.EXE	WIN-BUGSFIX.EXE
PRMT.EXE	SICLOADER.EXE	WINDOW.EXE
PRMVR.EXE	SUPFTRL.EXE	WINDOWS.EXE
PROCDUMP.EXE	SUPPORT.EXE	WININETD.EXE
PROPORT.EXE	SUPPORTER5.EXE	WININIT.EXE
PROTECTX.EXE	SVC.EXE	WININITX.EXE
PSPF.EXE	SVCHOSTC.EXE	WINLOGIN.EXE
PURGE.EXE	SVCHOSTS.EXE	WINMAIN.EXE
PUSSY.EXE	SVSHOST.EXE	WINNET.EXE
PVIEW95.EXE	SWEEP95.EXE	WINPPR32.EXE
QCONSOLE.EXE	SYMPROXYSVC.EXE	WINRECON.EXE
QSERVER.EXE	SYMTRAY.EXE	WINSERVN.EXE
RAPAPP.EXE	SYSEDIT.EXE	WINSK32.EXE
RAV7.EXE	SYSTEM.EXE	WINSTART.EXE
RAV7WIN.EXE	SYSTEM32.EXE	WINSTART001.EXE
RAY.EXE	SYSUPD.EXE	WINTSK32.EXE
RB32.EXE	TASKMG.EXE	WINUPDATE.EXE
RCSYNC.EXE	TASKMO.EXE	WKUFIND.EXE
REALMON.EXE	TASKMON.EXE	WNAD.EXE
REGED.EXE	TAUMON.EXE	WNT.EXE
REGEDIT.EXE	TBSCAN.EXE	WRADMIN.EXE
REGEDT32.EXE	TC.EXE	WRCtrl.EXE
RESCUE.EXE	TCA.EXE	WSBGATE.EXE
RESCUE32.EXE	TCM.EXE	WUPDATER.EXE
RRGUARD.EXE	TDS2-98.EXE	WUPDT.EXE
RHELLL.EXE	TDS2-NT.EXE	XPF202EN.EXE
RTVSCAN.EXE	TDS-3.EXE	ZAPRO.EXE
RTVSCN95.EXE	TEEKIDS.EXE	ZAPSETUP3001.EXE
RULAUNCH.EXE	TFAK.EXE	ZATUTOR.EXE
RUN32DLL.EXE	TFAK5.EXE	ZONALM2601.EXE
RUNDLL.EXE	TGBOB.EXE	ZONEALARM.EXE
RUNDLL16.EXE	TITANIN.EXE	VET32.EXE
RUXDLL32.EXE	TITANINXP.EXE	VET95.EXE
SAFEWEB.EXE	TRACERT.EXE	VETTRAY.EXE
SAHAGENT.EXE	TRICKLER.EXE	VFSETUP.EXE
SAVE.EXE	TRJSCAN.EXE	VIR-HELP.EXE
SAVENOW.EXE	TRJSETUP.EXE	VNLAN300.EXE
SBSERV.EXE	TROJANTRAP3.EXE	VNPC3000.EXE
SC.EXE	TSADBOT.EXE	VPC32.EXE
SCAM32.EXE	TVMD.EXE	VPC42.EXE
SCAN32.EXE	TVTMD.EXE	VPFW30S.EXE
SCAN95.EXE	UNDOBOOT.EXE	VPTRAY.EXE
SCANPM.EXE	UPDAT.EXE	VSCAN40.EXE
SCRSCAN.EXE	UPDATE.EXE	VSCENU6.02D30.EXE
SCRSVR.EXE	UPGRAD.EXE	SMC.EXE
SCVHOST.EXE	UTPOST.EXE	SMS.EXE
SD.EXE	VBCMSERV.EXE	VSCHED.EXE
SERV95.EXE	VBCONS.EXE	VSECOMR.EXE
SERVICE.EXE	VBUST.EXE	VSHWIN32.EXE
SERVLCE.EXE	VBWIN9X.EXE	VSISSETUP.EXE
SERVLCS.EXE	VBWINNTW.EXE	VSMAIN.EXE
SFC.EXE	VCSSETUP.EXE	VSMON.EXE
SGSSFW32.EXE	SH.EXE	
SHN.EXE	VSSTAT.EXE	

EXPLOIT IFRAME.BoF

MÉTODO DE INFECCIÓN

IFRAME.BoF es un exploit (es una técnica o un programa que aprovecha un fallo o hueco de seguridad -una vulnerabilidad- existente en un determinado protocolo de comunicaciones, sistema operativo, o herramienta informática), afecta a la versión 6.0 del navegador Microsoft Internet Explorer.

El exploit puede ser insertado en páginas web maliciosas o en mensajes de correo electrónico en formato HTML, a los que se añade código ejecutable. Éste se ejecutará automáticamente en el momento que se produzca el desbordamiento de búfer. El código ejecutable puede ser de cualquier naturaleza, lo que posibilita la realización de todo tipo de acciones maliciosas.

RECOMENDACIONES

- ✚ Desactivar la ejecución de "Active Scripting" del navegador.
- ✚ Cambiar la configuración del cliente de correo electrónico, de manera que los mensajes sean visualizados en formato de texto plano.

VIRUS MYDOOM.AE y MYDOOM.AF

MÉTODO DE INFECCIÓN

Los virus Mydoom.AE y Mydoom.AF llegan mediante correo electrónico, incluyen un link a archivos que contienen el **exploit IFRAME.BoF** y que se encuentran en otros computadores afectados. En caso de que el usuario que recibe el e-mail pulse sobre dicho enlace y su computador sea vulnerable, el código malicioso se se descargará y ejecutará automáticamente en el sistema.

Además, Mydoom.AE y Mydoom.AF tratan de establecer conexiones con un gran número de servidores de IRC a través del puerto de comunicaciones 6667.

VIRUS GAVIR.A

MÉTODO DE INFECCIÓN

Gavir.A es un virus que se propaga a través de recursos compartidos de red, creando copias de sí mismo en los recursos IPC\$ y ADMIN\$ a los que consigue acceso.

El virus también genera un script (el término script hace referencia a todos aquellos archivos o secciones de código escritas en algún lenguaje de programación, como

Visual Basic Script (VBScript), JavaScript, etc.), en un directorio temporal, cuya función es borrarse a sí mismo una vez que ha terminado su ejecución.

VIRUS SOBER.I

MÉTODO DE INFECCIÓN

Sober.I se envía por correo electrónico, utilizando su propio motor SMTP, en un mensaje escrito en alemán o en inglés, dependiendo del destinatario. Obtiene direcciones de correo del equipo al que afecta y las almacena en archivos. Además, para ejecutarse cada vez que se enciende la computadora, crea varias entradas en el Registro de Windows.

VIRUS YANZ.A

MÉTODO DE INFECCIÓN

Yanz.A es un virus de correo electrónico que se distribuye en mensajes de características muy variables, que muestran direcciones de remitentes falsas. También puede utilizar programas de intercambio de archivos punto a punto (P2P), creando archivos -de nombre variable- con copias de sí mismo en directorios que contengan la cadena de texto "shar". Tanto los mensajes de correo, como los archivos compartidos que crea, hacen referencia a la cantante china Sun Yan Zi.

En el caso de que el archivo que lo contiene sea ejecutado, Yanz.A mostrará una pequeña ventana con el siguiente texto:

"Kernel Hatasi".

Además, abre el puerto TCP 67, a través de dicho puerto intenta descargar archivos conteniendo todo tipo de malware, que el virus se encargará de ejecutar inmediatamente.

VIRUS DREW.A

MÉTODO DE INFECCIÓN

Drew.A se propaga tanto a través de correo electrónico, como de aplicaciones P2P. En el primer caso, utiliza su propio motor SMTP para enviar mensajes de formato variable. Tanto el asunto como el cuerpo de texto, así como el nombre del archivo adjunto, son escogidos de forma aleatoria a partir de una lista de opciones. Para difundirse a través de aplicaciones P2P, Drew.A busca todas las carpetas con la cadena de texto "Share" que se encuentren en el equipo, en las que se copia con nombres que puedan resultar atractivos o interesantes para el usuario, como "Cameron Dias.scr", "Delphi 8 keygen.com" y "DrWeb 4.32 Key.com".

El virus se envía a todas las entradas de la libreta de direcciones y procede al borrado de todos los archivos -que tengan extensión HTM o TXT-, que encuentre en la computadora.

VIRUS ALER.A

MÉTODO DE INFECCIÓN

Es un virus que se propaga a través de mensajes de correo electrónico con el siguiente formato:

Asunto: "Latest News about Arafat !!!",
y adjuntan dos archivos.

Uno de ellos es un archivo de imagen mostrando una escena del funeral del político recientemente fallecido.

Sin embargo, el otro archivo contiene un código diseñado para aprovechar una vulnerabilidad del navegador Internet Explorer. A través de ésta, se instala automáticamente en el equipo el virus.

CONSEJOS PARA PROTEGERSE DE LOS VIRUS INFORMATICOS

Hay muchos virus que se esparcen a mediante la red a nivel mundial y nacional, por lo cual estamos dando unas recomendaciones para que las instituciones

y usuarios en general puedan proteger sus equipos informáticos:

- ◆ Si dispone de herramientas de filtrado, configúrelas para que rechacen los mensajes que cumplan las características de los virus más conocidos.
- ◆ No ejecute archivos adjuntos desconocidos y bórrelos incluso de la carpeta de Elementos Eliminados.
- ◆ Los archivos adjuntos deben ser revisados por un antivirus actualizado.

- ◆ Tener cuidado con los archivos que reciba a través de las aplicaciones de intercambio de archivos punto a punto (P2P).
- ◆ Actualice el antivirus del computador.

□ Se adjunta una lista de páginas webs donde el usuario puede obtener mayor información sobre virus y actualizar el 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/
TrendMicro	http://www.trendmicro.com/download/pattern.asp
BitDefender	http://www.bitdefender-es.com

CUALQUIER CONSULTA ENVIAR UN CORREO AL

**CENTRO DE CONSULTA
E INVESTIGACION SOBRE SEGURIDAD DE LA INFORMACION**

ccisi@pcm.gob.pe