

Ataques de malware basado en Web

Jorge Mieres

jamieres@gmail.com

Fecha Publicación: 28/02/2009

Disclaimer: las URL que figuran en este artículo son dañinas. Por favor no ingrese a las mismas o hágalo bajo su propia responsabilidad.

Introducción

Internet se ha transformado en una aliada plataforma de ataque para los creadores de malware, quienes a través del empleo de diferentes técnicas tales como Drive-by-Download, Drive-by-Update, scripting, exploit, entre otros, y la combinación de ellos, buscan reclutar todo un ejército de computadoras que respondan sólo a sus instrucciones maliciosas.

Estos ataques, empleando Internet como base para ejecutar cargas dañina de manera directa sobre el sistema víctima, de forma paralela, casi instantánea y transparente a la vista de los usuarios menos experimentado, se ha convertido en un latente y peligroso riesgo de infección por el simple acto de acceder a un sitio web.

En el siguiente documento se expone un ejemplo concreto que recurre a las acciones antes mencionadas para explotar e infectar un sistema víctima, describiendo también varias características extras que potencian el daño del malware.

El proceso de ataque

La situación podría ser la siguiente: como habitualmente lo hace, un usuario accede a su casilla de correo electrónico para chequear sus mensaje; entre ellos, encuentra uno de bajo un atractivo asunto lo insita a abrirlo. El usuario abre el correo en cuestión, y encuentra en el cuerpo del mensaje un enlace incrustado.

El usuario, hace clic sobre dicho enlace para acceder al sitio que se especifica en el cuerpo del mensaje. Cuando el navegador web accede al dominio en cuestión, el usuario sólo visualiza una página en blanco que únicamente contiene “dos líneas”; en consecuencia, cierra el navegador suponiendo que el contenido de la página ya no se encuentra disponible.

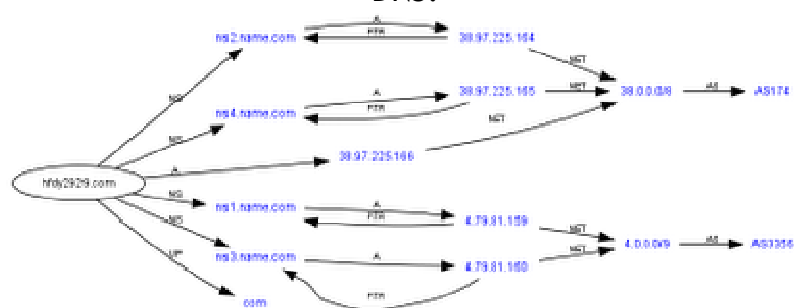
RStray.exe,
DrvAnti.exe,
safeboxTray.exe,
360tray.exe,
360safebox.exe,
360Safe.exe, 360rpt.exe,
adam.exe, AgentSvr.exe,
AntiArp.exe,
AppSvc32.exe,
arswp.exe,
AST.exe,
autoruns.exe,
avconsol.exe,
avgrssvc.exe,
AvMonitor.exe,
avp.com,
avp.exe,
CCenter.exe,
ccSvcHst.exe,
EGHOST.exe,
FileDsty.exe,
filemon.exe,
FTCleanerShell.exe,
FYFireWall.exe,
GFRing3.exe,
GFUpd.exe,
HijackThis.exe,
IceSword.exe,
iparmo.exe,
Iparmor.exe,
isPwdSvc.exe,
kabaload.exe,
KASMain.exe,
ProcessSafe.exe,
rfwProxy.exe,
KPfwSvc.exe,
rfwsrv.exe,
Kregex.exe,
rfwstub.exe,
KRepair.com,
RsAgent.exe,
KsLoader.exe,
Rsaupd.exe,
KvDetect.exe,
rstrui.exe,
KvfwMcl.exe,
runiep.exe,
kvol.exe,
safelive.exe,
kvolself.exe,
scan32.exe,
KVSrvXP.exe,
SelfUpdate.exe,
kvupload.exe,
shcfg32.exe,
kvwsc.exe,
SmartUp.exe,
KvXP.kxp,
SREng.exe,
KWatch.exe,
SuperKiller.exe,
KWatch9x.exe,
symIcsvc.exe,
KWatchX.exe,
SysSafe.exe,
MagicSet.exe,
taskmgr.exe,
mcconsol.exe,
UmxCfg.ex
mmqcj.exe,
TrojanDetector.exe,
mmsk.exe,
TrojDie.exe,
Navapsvc.exe,
UIHost.exe,
Navapw32.exe,
UmxAgent.exe,
NAVSetup.exe,
UmxAttachment.exe,
nod32.exe,
UmxFwHlp.exe.
nod32krn.exe,
nod32kui.exe,
NPFMntor.exe,
PFW.exe,
PFWLiveUpdate.exe,
procexp.exe,
QHSET.exe,
QQDoctor.exe,
QQDoctorMain.exe,

KASTask.exe,	QQKav.exe, Ras.exe,
KAV32.exe,	Rav.exe,
KAVDX.exe,	RavMon.exe,
KAVPF.exe,	RavMonD.exe,
KAVPFW.exe,	RavStub.exe,
KAVSetup.exe,	RavTask.exe,
KAVStart.exe,	RawCopy.exe,
KISLnchr.exe,	RegClean.exe,
KMailMon.exe,	regmon.exe,
KMFilter.exe,	RegTool.exe,
KPFW32.exe,	rwcfcg.exe,
KPFW32X.exe,	rfwmain.exe,

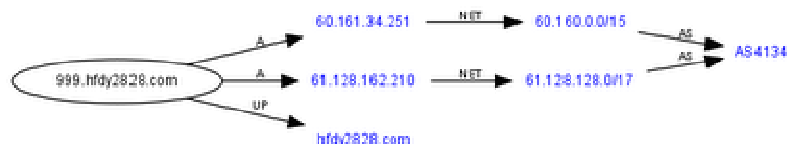
Por otro lado, el malware manipula el registro del sistema eliminando las subclaves contenidas en HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\ y en HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\ para evitar que el sistema pueda ser arrancado en modo seguro (MPF).

Todas estas acciones “defensivas” desplegadas por el malware, tienen como objetivo principal evitar su análisis y posterior detección por parte de las compañías antivirus, prolongando así su ciclo de vida.

Por otro lado, establece una conexión contra la dirección IP **60.161.34.251**, correspondiente al dominio **hfdy2929 .com** (alojada en Beijing, China - Chinanet Yunnan Province Network), y realiza una consulta DNS.



También, a través del protocolo http en el puerto por defecto, establece una conexión contra el dominio **999.hfdy2828 .com**, también alojado en China (Chongqing Chinanet Chongqing Province Network).



Al establecer esta segunda conexión, consulta el archivo **bak.txt** que contiene un listado de malware a descargar, lo que se conoce como Drive-by-Update. El archivo de actualización en cuestión posee la siguiente información:

```
[update]
url=http://www.baidu .com/hun .exe
[file]
isfile=1
count=34
url1=http://999.2005wyt .com/cao/aa1 .exe
url2=http://999.2005wyt .com/cao/aa2 .exe
url3=http://999.2005wyt .com/cao/aa3 .exe
url4=http://www.baidu .com/cao/aa4 .exe
url5=http://www.baidu .com/cao/aa5 .exe
url6=http://999.2005wyt .com/cao/aa6 .exe
url7=http://999.2005wyt .com/cao/aa7 .exe
url8=http://999.2005wyt .com/cao/aa8 .exe
url9=http://www.baidu .com/cao/aa9 .exe
url10=http://www.baidu .com/cao/aa10 .exe
url11=http://999.2005wyt .com/cao/aa11 .exe
url12=http://www.baidu .com/cao/aa12 .exe
url13=http://www.baidu .com/cao/aa13 .exe
url14=http://www.baidu .com/cao/aa14 .exe
url15=http://999.2005wyt .com/cao/aa15 .exe
url16=http://999.2005wyt .com/cao/aa16 .exe
url17=http://999.2005wyt .com/cao/aa17 .exe
url18=http://www.baidu .com/cao/aa18 .exe
url19=http://www.baidu .com/cao/aa19 .exe
url20=http://999.2005wyt .com/cao/aa20 .exe
url21=http://999.2005wyt .com/cao/aa21 .exe
url22=http://www.baidu .com/cao/aa22 .exe
url23=http://999.2005wyt .com/cao/aa23 .exe
url24=http://999.2005wyt .com/cao/aa24 .exe
url25=http://999.2005wyt .com/cao/aa25 .exe
url26=http://999.2005wyt .com/cao/aa26 .exe
url27=http://999.2005wyt .com/cao/aa27 .exe
url28=http://999.2005wyt .com/cao/aa28 .exe
url29=http://999.2005wyt .com/cao/aa29 .exe
url30=http://999.2005wyt .com/cao/aa30 .exe
url31=http://999.2005wyt .com/cao/aa31 .exe
url32=http://www.baidu .com/cao/aa32 .exe
url33=http://999.2005wyt .com/cao/aa33 .exe
url34=http://999.2005wyt .com/cao/aa34 .exe
```

Se trata de un total de 35 archivos binarios (ejecutables) que corresponden a los siguientes códigos maliciosos:

- Win32/TrojanDropper.Agent.NPO
- Win32/PSW.Legendmir.NGG
- Win32/PSW.OnLineGames.NRD
- Win32/PSW.OnLineGames.NRF
- Win32/PSW.OnLineGames.NTM
- Win32/PSW.OnLineGames.NTN
- Win32/PSW.OnLineGames.NTP
- Win32/PSW.WOW.DZI

NOTA: *la nomenclatura empleada como nomenclatura de cada malware corresponde a la establecida por el motor de firmas de ESET NOD32 Antivirus 3.0.672.0.*

En el código script que se muestra en la primera de las imágenes, se aprecia que existen varias etiquetas iframe que mantienen la misma metodología explicada, verificando en el equipo víctima la existencia de vulnerabilidades a través de exploits.

El detalle de los dominios a los que se accede de manera transparente a través de iframes es el siguiente:

La dirección web <http://sss.2010wyt.net/ac.html>, descarga un archivo binario llamado **css.css** que utiliza la misma metodología de engaño empleada por **cina.css**, es decir, simula ser un archivo de estilo, pero a diferencia del primero, explota una vulnerabilidad en Windows Metafile (WMF).

Del mismo modo, un JavaScript explota las vulnerabilidades MS08-067 y MS06-014 a través de <http://sss.2010wyt.net/614.js> descargando el archivo **bak.css** desde <http://xxx.2009wyt.net>.

Por último, desde <http://sss.2010wyt.net/r.js>, <http://sss.2010wyt.net/r.html>, <http://sss.2010wyt.net/fzl.htm> y <http://sss.2010wyt.net/asd.htm>, descargan los archivos **versionie.swf** y **versionff.swf** desde <http://sss.2010wyt.net>. Ambos explotan una vulnerabilidad en Flash Player.

[illegible]

Información útil

<http://www.microsoft.com/latam/technet/seguridad/boletines/2008/ms08-067.msp>

<http://www.microsoft.com/spain/technet/seguiridad/boletines/ms06-014-it.msp>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250>

<http://www.virustotal.com/analysis/f9e0aed93ddfc6077a4c87c6a0437f97>

<http://mipistus.blogspot.com/2009/01/ataque-de-malware-via-drive-by-download.html>

<http://mipistus.blogspot.com/2009/02/drive-by-update-propagacion-de.html>

<http://mipistus.blogspot.com/2009/01/explotacin-masiva-de-vulnerabilidades.html>