MalwareIntelligence

Análisis de un ataque de malware basado en web

Jorge Mieres | MalwareIntelligence | jamieres@malwareint.com

Contenido

IMPORTANTE: el presente documento es de índole técnico y posee información relacionada a direcciones web, direcciones IP, rutas de descarga de binarios, entre otros; que guardan relación directa con las estrategias de infección y los procesos delictivos llevados a cabo por delincuentes informáticos.

Por lo tanto, se recomienda el uso responsable de la información proporcionada en el presente, quedando bajo la exclusiva y única responsabilidad del lector cualquier inconveniente que pueda surgir en función de la manipulación inadecuada y mala utilización de los datos expuestos.

Asimismo, el documento posee información exacta de los resultados arrojados del estudio realizado. Por lo tanto, y por la misma naturaleza del proceso de investigación, no se ha proporcionado el 100% de los datos recabados; sin embargo, más datos se encuentran disponibles enviando la solicitud al autor del informe.

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 ejercito 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.

The document can be downloaded from:

English version
http://www.malwareint.com/docs/myloader-oficla-analysis-en.pdf

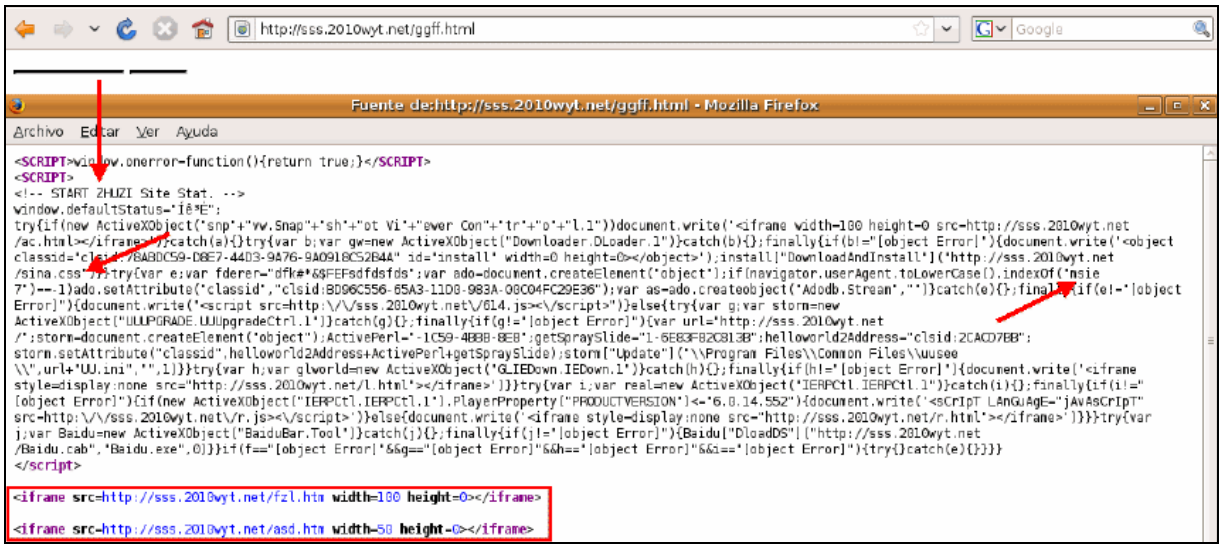
Spanish version
http://www.malwareint.com/docs/myloader-oficla-analysis-es.pdf

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.

Sin embargo, lejos de suceder lo que el usuario supone, en segundo plano se llevan a cabo actividades totalmente transparentes. La página posee componentes maliciosos que intentaran explotar en el equipo de la víctima.



Al acceder a la página maliciosa, un script ejecuta de manera transparente varias etiquetas iframes que posibilita la apertura en segundo plano de otros sitios web, esta técnica es conocida como Drive-by-Download; y un exploit diseñado para aprovechar una vulnerabilidad en el servicio de servidor de plataformas Windows que no trata correctamente una petición RPC especialmente creada.

Dicha vulnerabilidad es explicada en el boletín MS08-067, y un dato interesante radica en que, actualmente, la vulnerabilidad mencionada es activamente explotada por el gusano Downadup/Conficker con una tasa de infección muy alta.

En el script, se encuentra embebida la referencia hacia un archivo llamado **sina.css**. Este archivo no es lo que parecería ser, una hoja de estilo encascada según su extensión, sino que se trata de un archivo ejecutable que es el encargado de activar el exploit para la vulnerabilidad mencionada.

Inmediatamente después de encontrar la vulnerabilidad en el sistema víctima, el malware inyecta código dañino en los procesos **winlogon.exe**, **explorer.exe** y **services.exe**, y realiza una copia de si mismo en `C:\DOCUME~1\user\LOCALS~1\Temp\` bajo el nombre **svchost.exe** creando su proceso asociado.

Además, también crea el archivo **Beep.sys** en `C:\WINDOWS\system32\drivers\` ejecutándolo como servicio del sistema, y ocultándose con las capacidades propias de rootkit.

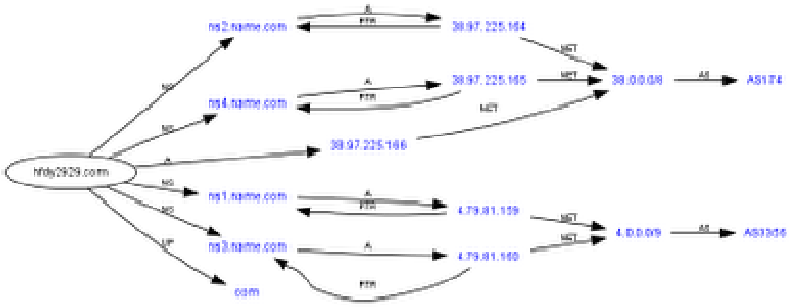
Al mismo tiempo, manipula el registro del sistema para evitar la ejecución de las siguientes procesos correspondientes a herramientas de seguridad:

360tray.exe	adam.exe	AgentSvr.exe
360rpt.exe	360safebox.exe	360Safe.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
DrvAnti.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
KASTask.exe	KAV32.exe	KAVDX.exe
QQDoctorMain.exe	KAVDX.exe	KAVPF.exe
KAVPFW.exe	KAVSetup.exe	KAVStart.exe
KISLnchr.exe	KMailMon.exe	KMFilter.exe
KPFW32.exe	KPFW32X.exe	KPfwSvc.exe
Kregex.exe	KRepair.com	KsLoader.exe
KvDetect.exe	KvfwMcl.exe	kvol.exe
kvolself.exe	KVSrvXP.exe	kvupload.exe
kvwsc.exe	KvXP.kxp	KWatch.exe
KWatch9x.exe	KWatchX.exe	MagicSet.exe
mcconsol.exe	mmqczj.exe	mmsk.exe
Navapsvc.exe	Navapw32.exe	NAVSetup.exe
nod32.exe	nod32krn.exe	nod32kui.exe
NPFMntor.exe	PFW.exe	PFWLiveUpdate.exe
ProcessSafe.exe	procexp.exe	QHSET.exe
QQDoctor.exe	QQKav.exe	Ras.exe
Rav.exe	RavMon.exe	RavMonD.exe
RavStub.exe	RavTask.exe	RawCopy.exe
RegClean.exe	regmon.exe	RegTool.exe
rfwcfg.exe	rfwmain.exe	rfwProxy.exe
rfwsrv.exe	rfwstub.exe	RsAgent.exe
Rsaupd.exe	RStray.exe	rstrui.exe
runiep.exe	safeboxTray.exe	safelive.exe
scan32.exe	SelfUpdate.exe	shcfg32.exe
SmartUp.exe	SREng.exe	SuperKiller.exe
symlcsvc.exe	SysSafe.exe	taskmgr.exe
TrojanDetector.exe	TrojDie.exe	UIHost.exe
UmxAgent.exe	UmxAttachment.exe	UmxCfg.ex

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.

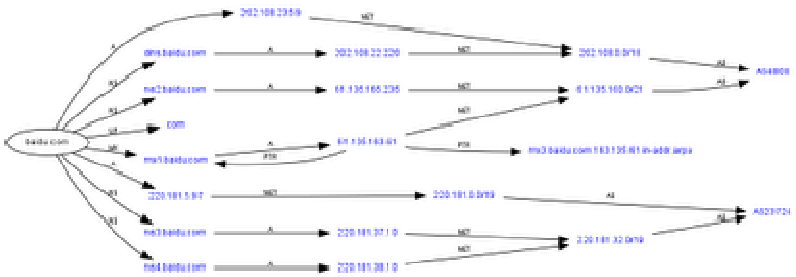
El detalle de los dominios a los que se accede de manera transparente a través de iframes es el siguiente:

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.

Sin embargo, no todo termina aquí mismo, sino que aparece otro dominio desde el cual se descargan algunos de los códigos maliciosos a través de Drive-by-Update, comentado líneas arriba, desde el archivo **bak.txt**. La relación de este dominio con otros es la siguiente:



Los ataques a través de códigos maliciosos se han vuelto más sofisticados y más habituales. Lo expuesto en este documento es un claro reflejo de ello. El empleo y combinación de diferentes tecnologías para atacar a través de diferentes metodologías maliciosas es cada vez más complejo y difícil de analizar.

Referencias

Security Bulletin MS08-067
http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx
Security Bulletin MS06-014
http://www.microsoft.com/technet/security/bulletin/ms06-014.mspx
CVE-2008-4250
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
Detection rate of binary css.css
http://www.virustotal.com/analisis/f9e0aed93ddfc6077a4c87c6a0437f97
Ataque de malware vía Drive-by-Download
http://mipistus.blogspot.com/2009/01/ataque-de-malware-va-drive-by-download.html
Drive-by-Update para propagación de malware
http://mipistus.blogspot.com/2009/02/drive-by-update-para-propagacion-de.html
Explotación masiva de vulnerabilidades a través de servidores fantasmas
http://mipistus.blogspot.com/2009/01/explotacin-masiva-de-vulnerabilidades.html

Sobre Malware Intelligence
Malware Intelligence es un sitio dedicado a la investigación de todo lo relacionado con la seguridad antimalware, crimeware y seguridad de la información en general, desde una perspectiva estrechamente relacionada con el ámbito de inteligencia.

http://www.malwareint.com

http://mipistus.blogspot.com · Versión en Español
http://malwareint.blogspot.com · Versión en Inglés

Sobre Malware Disasters Team
Malware Disasters Team es una división de Malware Intelligence de reciente creación, en el cual se plasma información relacionada a las actividades que realizan determinados códigos maliciosos, ofreciendo también las contramedidas necesarias para contrarrestar las acciones maliciosas en cuestión.

http://malwaredisasters.blogspot.com

Sobre Security Intelligence
Security Intelligence es una división de Malware Intelligence donde se exponen temáticas puramente relacionadas con SGSI. Actualmente se encuentra en su etapa inicial de construcción.

http://securityint.blogspot.com