Ataque a sitios web. Técnicas de exploits alternas

Martín Cano Contreras, Antonio Gordillo Sosa, Joel Quintanilla Domínguez, Jesús Adrián Ramírez López

M. Cano, A. Gordillo, .J. Quintanilla, J. Ramírez.
Universidad de Guanajuato, San Fernando 42, 36000 Guanajuato
mcano_cco@utsoe.edu.mx

M. Ramos.,V.Aguilera.,(eds.). Ciencias de la Ingeniería y Tecnología, Handbook -©ECORFAN- Valle de Santiago, Guanajuato, 2013.

Abstract

In the present article demonstrates and documents a concrete example that uses the actions of techniques Drive-by-Download, Drive-by-Update, scripting, and the use of exploits to operate and infect a victim system, describing also several extra features that expose an attack by such actions and the damage malware can have. This type of attack is classified according to the timing vulnerabilities introduced in the software life cycle.

Classically, are raised six phases and are recognition, Feasibility study, Requirements, Design, Implementation, Integration and Testing. Initially it was considered the operation and maintenance as additional phase.

8 Introducción

Los ataques que se producen en Internet, a razón de varios ataques por minuto en cada equipo conectado, se lanzan automáticamente desde equipos infectados, ya sea por virus, troyanos, gusanos, etc., sin que el propietario sepa lo que está ocurriendo.

Internet se ha transformado en una plataforma aliada de ataque para los creadores de malware, quienes son los verdaderos crackers (o los hackers de sombrero negro, dejando muy atrás a aquellos quienes experimentan con las herramientas creadas por los primeros) a través del empleo de diferentes técnicas tales como Drive-by-Download, Drive-by- Update, scripting, exploits, buscando reclutar todo un ejército de computadoras (algunos las tildan de computadoras zombies) que respondan sólo a sus instrucciones. Quizás alguno de los lectores habrá leído en el canal de IRC (Internet Relay Chat) la puesta en marcha de ataques contra algún objetivo. (Como ejemplo, la llamada "Operación Payback" a fines del 2010 cuyo objetivo fue mastercard). Y todo esto por el simple acto de acceder a un sitio web que ha sido mal planificado. [1]

El escenario planteado ante un ataque de este tipo puede ser el siguiente: como habitualmente lo hace, un usuario accede a su navegador web de correo electrónico para ver sus mensajes; entre ellos, encuentra uno con un atractivo asunto que lo invita a abrir tal mensaje.

El usuario abre el correo en cuestión, y encuentra en el cuerpo del mensaje un enlace incrustado a un sitio web del que no se tiene idea de su contenido y que es muy común los mensajes tipo "Actualiza tu navegador", "Carga la página para continuar", etc.. Al momento de hacer este trabajo, recibo un correo de un colega, con el siguiente formato:

Figura 8 Ejemplo de correo como posible ataque

Como es lógico suponer y que además es una reacción casi natural, 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 ve generalmente una página prácticamente en blanco y con una leyenda que únicamente contiene “dos o tres líneas”; ante esta situación poco atractiva, el usuario en consecuencia cierra el navegador suponiendo que el contenido de la página ya no se encuentra disponible. Típica situación y de todos los días. Un usuario avezado se preguntaría algunos aspectos al recibir este mensaje: por qué recibo este mensaje si no tengo cuenta de webmail? Según las características del servidor webmail, la capacidad de almacenamiento es prácticamente ilimitado… entre otros puntos a cuestionarse antes de hacer clic en tal enlace.[2] y [3]

Sin embargo, nada fuera de la normalidad para el usuario pero muy lejos de suceder, es lo que el usuario supone; en segundo plano se llevan a cabo actividades totalmente transparentes pero ocultas para el usuario. La página posee componentes maliciosos que intentarán explotar el equipo de la víctima de una manera u otra, con un claro beneficio de quien le ha enviado dicho mensaje.

8.1 Método

Cuando por mala fortuna el usuario cae en el ardid descrito en la introducción, y al momento mismo de aceptar el enlace, se desencadena uno o varios scripts, ejecutando 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. Como se sabe, el servidor invocará el procedimiento indicado en nombre del cliente, entregando el valor de retorno, si hay alguno.

Dicha vulnerabilidad es explicada en el boletín MS08-067, en donde se especifica que en los sistemas Microsoft Windows 2000, Windows XP y Windows Server 2003, un atacante podría aprovechar esta vulnerabilidad sin autenticación para ejecutar código arbitrario. Es posible que esta vulnerabilidad se pueda usar en el diseño de un gusano [4], y un dato interesante radica en que, actualmente, la vulnerabilidad descrita es activamente explotada por el gusano Downadup/Conficker con una tasa de infección muy alta. [5]

En este momento, en el script ejecutado se encuentra la referencia hacia un archivo llamado sina.css. Para aquellos que están familiarizados con las hojas de estilo, la primera impresión es obligatoriamente pensar en que se trata de una hoja de estilos según la extensión, pero en realidad se trata de un archivo ejecutable que es el encargado de iniciar el exploit para la vulnerabilidad descrita en tal boletín. [5]

Una vez que se ha hallado y determinado la vulnerabilidad de acuerdo al sistema operativo de la víctima, el malware inyecta código dañino en los procesos winlogon.exe, el cual se encarga de validar la identidad de un usuario en el sistema. Es un proceso esencial y no debería ser terminado. Otro de los procesos afectados es el explorer.exe, el cual es un proceso genérico de los sistemas operativos Windows NT/2000/XP. Este proceso administra la interfaz del usuario y también la interfaz gráfica de Windows. Y por último, el proceso services.exe, el cual es un proceso genérico de Windows NT/2000/XP, que se utiliza para reconocer e implementar cambios en el sistema sin necesidad de que intervenga el usuario, punto en extremo importante pues es crucial para el ataque, y que realiza una copia de sí mismo en C:\DOCUME~1\user\LO-CALS~1\Temp\ bajo el nombre svchost.exe creando su proceso asociado; si el usuario ve este proceso, lo encuentra natural por ser parte de los procesos del sistema. Se inicia a la vez la creación del archivo Beep.sys en C:\WINDOWS\system32\drivers\ ejecutándolo como un servicio más del sistema, y ocultándose con las capacidades propias de rootkit, haciendo con esto casi indetectable para los antivirus actuales. [7], [8]

Para mejorar el entorno de ataque, de manera simultánea se manipula el registro del sistema para evitar la ejecución de los siguientes procesos correspondientes a herramientas de seguridad del propio sistema:

RStray.exe, ProcessSafe.exe, rfwProxy.exe; DrvAnti.exe, KPfwSvc.exe,rfwsrv.exe;

safeboxTray.exe, Kregex.exe, rfwstub.exe; 360tray.exe, KRepair.com;

RsAgent.exe, 360safebox.exe, KsLoader.exe, Rsaupd.exe;

360Safe.exe, 360rpt.exe, KvDetect.exe, rstrui.exe;

adam.exe, AgentSvr.exe, KvfwMcl.exe, runiep.exe;

AntiArp.exe, kvol.exe, safelive.exe;

AppSvc32.exe, kvolself.exe, scan32.exe;

arswp.exe,KVSrvXP.exe, SelfUpdate.exe;

AST.exe, kvupload.exe, shcfg32.exe;

autoruns.exe, kvwsc.exe, SmartUp.exe; avconsol.exe, KvXP.kxp, SREng.exe;

avgrssvc.exe, KWatch.exe, SuperKiller.exe;

AvMonitor.exe, KWatch9x.exe, symlcsvc.exe;

avp.com, KWatchX.exe, SysSafe.exe; avp.exe, MagicSet.exe, taskmgr.exe;

CCenter.exe, mcconsol.exe, UmxCfg.exe;

ccSvcHst.exe, mmqczj.exe, TrojanDetector.exe;

EGHOST.exe, mmsk.exe, TrojDie.exe;

FileDsty.exe, Navapsvc.exe, UIHost.exe;

filemon.exe, Navapw32.exe, UmxAgent.exe;

FTCleanerShell.exe, NAVSetup.exe, UmxAttachment.exe;

FYFireWall.exe, nod32.exe, UmxFwHlp.exe;

GFRing3.exe, nod32krn.exe;

GFUpd.exe, nod32kui.exe;

HijackThis.exe, NPFMntor.exe; IceSword.exe, PFW.exe;

iparmo.exe, PFWLiveUpdate.exe;

Iparmor.exe, procexp.exe;

isPwdSvc.exe, QHSET.exe;

kabaload.exe, QQDoctor.exe;

KASMain.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,

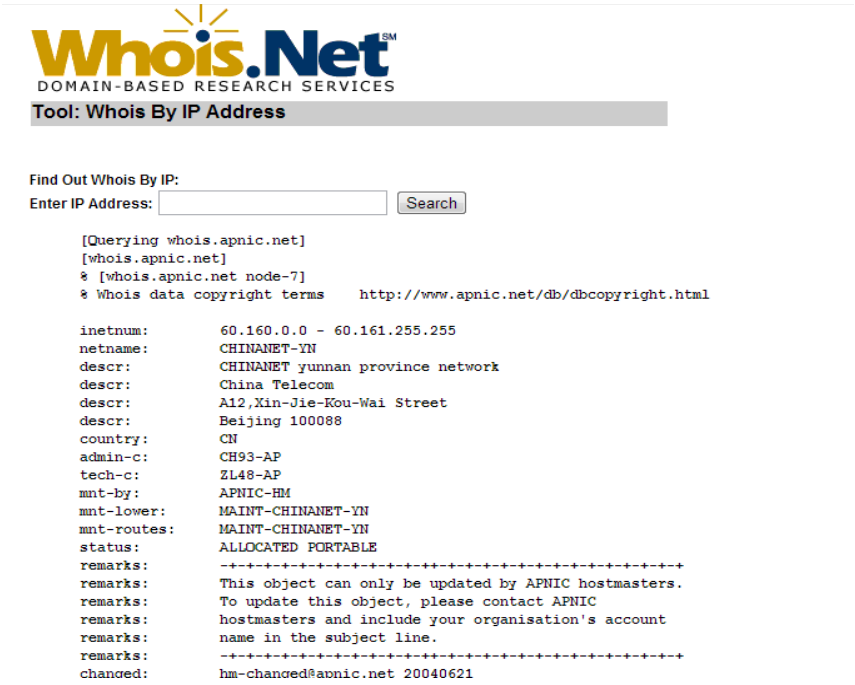
RegClean.exe, KMailMon.exe, regmon.exe, KMFilter.exe, RegTool.exe, KPFW32.exe, rfwcfg.exe, KPFW32X.exe, rfwmain.exe.

Como se puede apreciar, esto desactiva las herramientas de seguridad ofrecidas por los principales antivirus que el usuario pudiese tener instalado en su computadora. 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. [9]

Estas precauciones tomadas en el ataque 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, definido en [3].

Con el uso de este exploit, se establece una conexión hacia 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 [10] [11]. Ver la referencia de www.whois.net como se puede apreciar en las estadísticas arrojadas al consultar dicho sitio con la dirección indicada y que está inserta en el exploit:

Figura 8.1 Consulta del sitio cuya dirección IP es 60.161.34.251 insertada en el exploit ejecutado



Además, al realizar el ataque con este exploit, a través del protocolo http en el puerto por defecto, se establece una conexión contra el dominio 999.hfdy2828.com, también alojado en China (Chongqing Chinanet Chongqing Province Network).

Al establecer esta segunda conexión, se consulta el archivo bak.txt que contiene un listado de malware a descargar, lo que se conoce como Drive-by-Update. [12]. 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;
url3=http://999.2005wyt.com/cao/aa3.exe;
url5=http://www.baidu.com/cao/aa5.exe;
url7=http://999.2005wyt.com/cao/aa7.exe;
url9=http://www.baidu.com/cao/aa9.exe;
url11=http://999.2005wyt.com/cao/aa11.exe;
url13=http://www.baidu.com/cao/aa13.exe;
url15=http://999.2005wyt.com/cao/aa15.exe;
url17=http://999.2005wyt.com/cao/aa17.exe;
url19=http://www.baidu.com/cao/aa19.exe;
url21=http://999.2005wyt.com/cao/aa21.exe;
url23=http://999.2005wyt.com/cao/aa23.exe;
url25=http://999.2005wyt.com/cao/aa25.exe;
url27=http://999.2005wyt.com/cao/aa27.exe;
url29=http://999.2005wyt.com/cao/aa29.exe;
```

```
url3=http://999.2005wyt.com/cao/aa3.exe;
url5=http://www.baidu.com/cao/aa5.exe;
url7=http://999.2005wyt.com/cao/aa7.exe;
url9=http://www.baidu.com/cao/aa9.exe;
url11=http://999.2005wyt.com/cao/aa11.exe;
url13=http://www.baidu.com/cao/aa13.exe;
url15=http://999.2005wyt.com/cao/aa15.exe;
url17=http://999.2005wyt.com/cao/aa17.exe;
url19=http://www.baidu.com/cao/aa19.exe;
url21=http://999.2005wyt.com/cao/aa21.exe;
url23=http://999.2005wyt.com/cao/aa23.exe;
url25=http://999.2005wyt.com/cao/aa25.exe;
url27=http://999.2005wyt.com/cao/aa27.exe;
url29=http://999.2005wyt.com/cao/aa29.exe;
url31=http://999.2005wyt.com/cao/aa31.exe;
url33=http://999.2005wyt.com/cao/aa33.exe;
```

Se trat a de un total de 34 archivos ejecutables que corresponden a los siguientes códigos maliciosos:

Win32/TrojanDropper.Agent.NPO
Win32/PSW.OnLineGames.NRD
Win32/PSW.OnLineGames.NTM
Win32/PSW.OnLineGames.NTP

Win32/PSW.Legendmir.NGG
Win32/PSW.OnLineGames.NRF
Win32/PSW.WOW.DZI
Win32/PSW.OnLineGames.NTN

8.2 Resultados

En el código script que se muestra en la primera línea, 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, se descargan los archivos versionie.swf y versionff.swf desde http://sss.2010wyt.net. Ambos explotan una vulnerabilidad en Flash Player.Entre otras de las vulnerabilidades determinadas en el sistema de Windows en sus variadas versiones, se pueden citar: MS09-069, MS09-070, MS09-071, MS09-072, MS09-073, MS09-074, etc. [5]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. Como puede suponerse, el bloquear mediante un firewall ya sea físico o basado en software, la página solicitada es de poca utilidad al requerirse otros archivos de la misma página.

8.3 Discusión

El mantener un antivirus con su base de datos de los diversos códigos malignos en cualquiera de sus manifestaciones, es un buen método para evitar los ataques aquí descritos pero no es suficiente. Quizás la mejor manera de mantener un sistema operativo seguro, es estar al tanto de las actualizaciones del mismo por parte de Microsoft, recordando que este sistema operativo es por excelencia el objetivo de los ataques; éstos se hacen cada día más eficientes y discretos 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.

8.4 Conclusiones

Prácticamente es imposible definir un sitio web seguro pero se puede mitigar las probabilidades de sufrir un ataque si se mantienen actualizados los parches del sistema y utilizar siempre la versión más actual del navegador. Otra parte que ayuda es desactivar las funciones no necesarias, tales como los códigos ActiveX, permitiendo sólo la ejecución vigilada. Otra recomendación es la de no abrir aquellos mensajes cuyo contenido no sea familiar, y por último, se recomienda instalar aplicaciones que examinen los accesos web en tiempo real.

8.5 Referencias

Garcia-Moran, J.P., Fernández, H. Y., Martínez S. R. Ochoa M. A. R. Hacking y Seguridad En Internet. Edición 2011. Ra-Ma Editorial.

Pacheco, F. G., Jara, H. Ed. Fox Andina (2012). Ethical Hacking 2.0.

Dowd, M, McDonald, J and Schuh, J (2006) The Art of Software Security. Assessment: Identifying and Preventing Software Vulnerabilities. Boston, MA. Addison Wesley Professional.

Boletín de seguridad MS08-067. http://www.microsoft.com/latam/technet/seguridad/boletines/2008/ms08-067.mspx

Microsoft Exploitability Index. http://technet.microsoft.com/en-us/security/cc99-8259.aspx.

Boletín de seguridad MS06-014 http://www.microsoft.com/spain/technet/seguridad/boletines/ms06-014-it.mspx

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

Tasa de detección de los ejecutables css.css y sina.css. http://www.virusto-tal.com/analisis/

Ataque de malware vía Drive-by-Download http://mipistus.blogs-pot.com/2009/01/ataque-de-malware-va-drive-by-download.html

Drive-by-Update para propagación de malware http://mipistus.blog-spot.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