Analysis of an attack of web-based malware

Author: Jorge Mieres
E-Mail: jamieres#gmail.com
www.evilfingers.com (febrero de 2009)

White Paper

Introduction

Internet has become an ally platform of attack for malware creators, who through the use of different techniques such as Drive-by-Download, Drive-by-Update, scripting, exploit, among others, and combining them seek to recruit an army of computers that respond only to their malicious instructions.

These attacks, using the Internet as a basis for implementing a direct damaging loads on the victim, in parallel, almost instantaneous and transparent view of the less experienced users, has become a latent and dangerous risk of infection by the simple act of accessing a website.

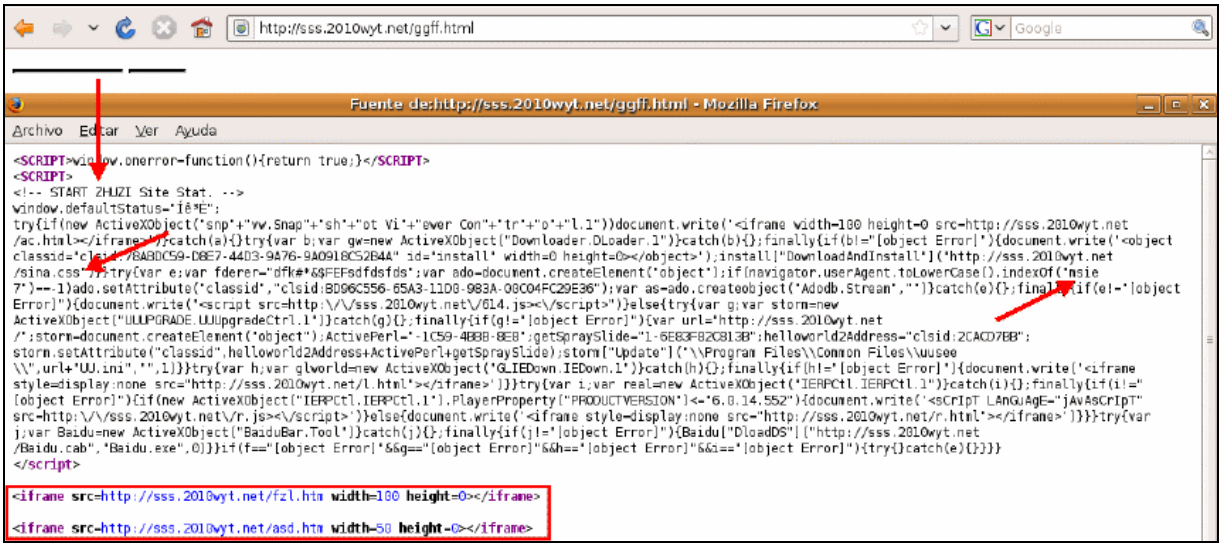
The following document sets out a concrete example that uses the above actions to exploit and infect a victim, describing also several extra features that enhance the damage of malware.

The attack process

The situation could be: as it usually does, a user accesses your email address to check your message, including one located in an attractive case that insite to open it. The user opens the mail in question and found the body of a message embedded link.

The user clicks on the link to access the site as specified in the message body. When the browser accesses the Web domain in question, you only see a blank page that only contains "two lines" and consequently, close the browser if the content of the page is no longer available.

However, far from true that the user means, in the background activities are carried out fully transparent. This page has components that malicious attempt to exploit the victim's machine.



To access the malicious page, a script runs in a transparent *iframe* that allows multiple tags to open in the background of other websites, this technique is known as Drive-by-Download and an exploit designed to exploit a vulnerability in the service Windows server platforms that does not correctly handle a specially created RPC request.

This vulnerability is explained in the bulletin MS08-067, and an interesting fact is that, currently, said the vulnerability is actively being exploited by the worm Downadup, or Conficker, with a very high rate of infection.

In the script, the reference is embedded into a file called **sina.css**. This file isn't what it seems, a cascading style sheet depending on their length, but is an executable file that is responsible for activating the exploit for the vulnerability in question.

Immediately after finding the vulnerability in the victim, the malware injects malicious code into processes *winlogon.exe*, *explorer.exe* and *services.exe*, and a copy of itself in **`C:\DOCUME~1\user\LOCALS~1\Temp\svchost.exe`** under the name of creating their partner.

It also creates the file **Beep.sys** on **C:\WINDOWS\system32\drivers** running as system service and hiding with rootkit capabilities.

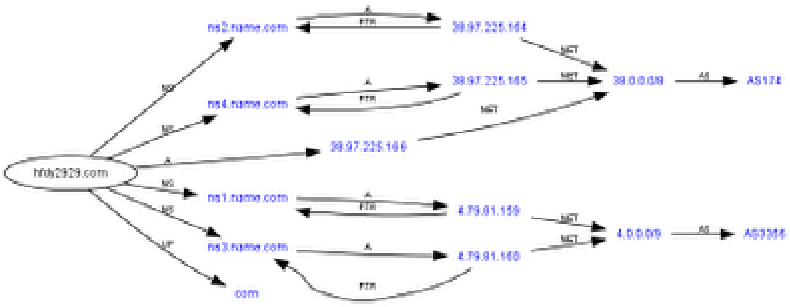
At the same time, manipulate the system registry to prevent the execution of procedures for the following security tools:

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,
KASTask.exe,
KAV32.exe,
KAVDX.exe,
KAVPF.exe,
KAVPFW.exe,
KAVSetup.exe,
KAVStart.exe,
KISLnchr.exe,
KMailMon.exe,
KMFilter.exe,
KPFW32.exe,
KPFW32X.exe,
ProcessSafe.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,
procexp.exe,
QHSET.exe,
QQDoctor.exe,
QQDoctorMain.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,
rstrui.exe,
runiep.exe,
safelive.exe,
scan32.exe,
SelfUpdate.exe,
shcfg32.exe,
SmartUp.exe,
SREng.exe,
SuperKiller.exe,
symlcsvc.exe,
SysSafe.exe,
taskmgr.exe,
UmxCfg.ex
TrojanDetector.exe,
TrojDie.exe,
UIHost.exe,
UmxAgent.exe,
UmxAttachment.exe,
UmxFwHlp.exe.

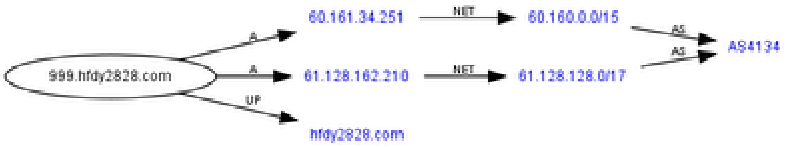
Furthermore, the malware manipulated the system registry by deleting the subkeys contained in `HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\` and in `HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\`. This is to prevent the system can be booted in safe mode (MPF).

All these actions "defensive" deployed by the malware, are intended primarily to avoid detection and subsequent analysis by the antivirus companies, thus extending their life cycle.

On the other hand, establishes a connection to the IP address **60.161.34.251**, corresponding to the domain **hfdy2929.com** (hosted in Beijing, China - Yunnan Province Chinanet Network), and performs a DNS query.



Also, through the http protocol on port by default, a connection to the domain **999.hfdy2828.com**, also hosted in China (Chongqing Chinanet Chongqing Province Network).



By establishing this second connection, see **bak.txt** file containing a list of malware to download, what is known as Drive-by-Update. The update file in question contains the following information:

```
[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
```

This is a total of 35 binaries (executables) that correspond to the following malware:

- 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

NOTE: *The nomenclature used for each classification as malware is set by the engine signature ESET NOD32 Antivirus 3.0.672.0.*

In the script code that is displayed in the first of the images shows that there are several labels iframe that hold the same methodology explained, verifying the existence of the victim computer through vulnerabilities exploits.

The detail of the domains accessed in a transparent manner through iframes is:

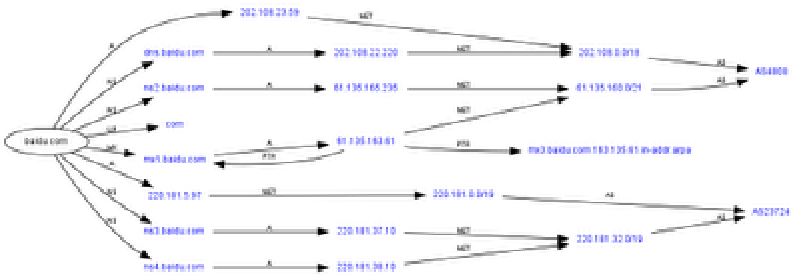
La dirección web **http://sss.2010wyt .net/ac .html**, descarga un archivo binario llamado **css.css** que utiliza la misma metodología de engaño empleada por **cina.css**, es decir, simula ser un archivo de estilo, pero a diferencia del primero, explota una vulnerabilidad en Windows Metafile (WMF).

The web address **http://sss.2010wyt.net/ac.html**, download a binary file called **css.css** using the same method of deception used by **cina.css**, ie pretending to be a style file, but Unlike the first, exploits a vulnerability in Windows Metafile (WMF).

Similarly, a JavaScript exploits vulnerabilities MS08-067 and MS06-014 through **http://sss.2010wyt.net/614.js** downloading file **bak.css** from **http://xxx.2009wyt.net**.

Finally, since **http://sss.2010wyt.net/r.js**, **http://sss.2010wyt.net/r.html**, **http://sss.2010wyt.net/fzl.htm** and **http:// sss.2010wyt.net/asd.htm**, download files **versionie.swf** and **versionff.swf** from **http://sss.2010wyt.net**. Both exploit a vulnerability in Flash Player.

However, not everything ends here, but it appears another domain from which you download some malicious code through Drive-by-Update, discussed above, since the file **bak.txt**. The relationship of this domain with another is as follows:



Attacks by malicious code have become more sophisticated and more common. Herein is a clear reflection of this. The use and combination of different technologies to attack by malicious different methodologies is becoming more complex and difficult to analyze.

Useful Information
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