Operation GreedyWonk: Multiple Economic and Foreign Policy Sites Compromised, Serving Up Flash Zero-Day Exploit

Less than a week after uncovering **Operation SnowMan**, the FireEye Dynamic Threat Intelligence cloud has identified another targeted attack campaign — this one exploiting a zero-day vulnerability in Flash. We are collaborating with Adobe security on this issue. Adobe has assigned the CVE identifier CVE-2014-0502 to this vulnerability and released a **security bulletin**.

As of this blog post, visitors to at least three nonprofit institutions — two of which focus on matters of national security and public policy — were redirected to an exploit server hosting the zero-day exploit. We're dubbing this attack "Operation GreedyWonk."

We believe GreedyWonk may be related to **a May 2012 campaign outlined by ShadowServer**, based on consistencies in tradecraft (particularly with the websites chosen for this strategic Web compromise), attack infrastructure, and malware configuration properties.

The group behind this campaign appears to have sufficient resources (such as access to zero-day exploits) and a determination to infect visitors to foreign and public policy websites. The threat actors likely sought to infect users to these sites for follow-on data theft, including information related to defense and public policy matters.

Discovery

On Feb. 13, FireEye identified a zero-day Adobe Flash exploit that affects the latest version of the Flash Player (12.0.0.4 and 11.7.700.261). Visitors to the Peter G. Peterson Institute for International Economics (www.piie[.]com) were redirected to an exploit server hosting this Flash zero-day through a hidden iframe.

We subsequently found that the American Research Center in Egypt (www.arce[.]org) and the Smith Richardson Foundation (www.srf[.]org) also redirected visitors the exploit server. All three organizations are nonprofit institutions; the Peterson Institute and Smith Richardson Foundation engage in national security and public policy issues.

Mitigation

To bypass Windows' Address Space Layout Randomization (ASLR) protections, this exploit targets computers with any of the following configurations:

- Windows XP
- Windows 7 and Java 1.6

- Windows 7 and an out-of-date version of Microsoft Office 2007 or 2010

Users can mitigate the threat by **upgrading from Windows XP** and updating Java and Office. If you have Java 1.6, update Java to the latest 1.7 version. If you are using an out-of-date Microsoft Office 2007 or 2010, update Microsoft Office to the latest version.

These mitigations do not patch the underlying vulnerability. But by breaking the exploit's ASLR-bypass measures, they do prevent the current in-the-wild exploit from functioning.

Vulnerability analysis

GreedyWonk targets a previously unknown vulnerability in Adobe Flash. The vulnerability permits an attacker to overwrite the *vftable* pointer of a Flash object to redirect code execution.

ASLR bypass

The attack uses only known ASLR bypasses. Details of these techniques are available from **our previous blog post** on the subject (in the "Non-ASLR modules" section).

For Windows XP, the attackers build a return-oriented programming (ROP) chain of MSVCRT (Visual C runtime) gadgets with hard-coded base addresses for English ("en") and Chinese ("zh-cn" and "zh-tw").

On Windows 7, the attackers use a hard-coded ROP chain for MSVCR71.dll (Visual C++ runtime) if the user has Java 1.6, and a hard-coded ROP chain for HXDS.dll (Help Data Services Module) if the user has Microsoft Office 2007 or 2010.

Java 1.6 is no longer supported and does not receive security updates. In addition to the MSVCR71.dll ASLR bypass, a variety of widely exploited code-execution vulnerabilities exist in Java 1.6. That's why FireEye strongly recommends upgrading to Java 1.7.

The Microsoft Office HXDS.dll ASLR bypass was patched at the end of 2013. More details about this bypass are addressed by Microsoft's **Security Bulletin MS13-106** and an accompanying **blog entry**. FireEye strongly recommends updating Microsoft Office 2007 and 2010 with the latest patches.

Shellcode analysis

The shellcode is downloaded in ActionScript as a GIF image. Once ROP marks the shellcode as executable using Windows' *VirtualProtect* function, it downloads an executable via the *InternetOpenURLA* and *InternetReadFile* functions. Then it writes the file to disk with *CreateFileA* and *WriteFile* functions. Finally, it runs the file using the *WinExec* function.

PlugX/Kaba payload analysis

Once the exploit succeeds, a PlugX/Kaba remote access tool (RAT) payload with the MD5 hash 507aed81e3106da8c50efb3a045c5e2b is installed on the compromised endpoint. This PlugX sample was compiled on Feb. 12, one day before we first observed it, indicating that it was deployed specifically for this campaign.

This PlugX payload was configured with the following command-and-control (CnC) domains:

- java.ns1[.]name
- adservice.no-ip[.]org
- wmi.ns01[.]us

Sample callback traffic was as follows:

```
POST /D28419029043311C6F8BF9F5 HTTP/1.1
Accept: */*
HHV1: 0
HHV2: 0
HHV3: 61456
HHV4: 1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;
InfoPath.2; .NET CLR 2.0.50727; SV1)
Host: java.ns1.name
Content-Length: 0
Connection: Keep-Alive
Cache-Control: no-cache
```

Campaign analysis

Both java.ns1[.]name and adservice.no-ip[.]org resolved to 74.126.177.68 on Feb. 18, 2014. Passive DNS analysis reveals that the domain wmi.ns01.us previously resolved to 103.246.246.103 between July 4, 2013 and July 15, 2013 and 192.74.246.219 on Feb. 17, 2014. java.ns1[.]name also resolved to 192.74.246.219 on February 18.

Domain	First Seen	Last Seen	IP Address
adservice.no-ip[.]org	2014-02-18	2014-02-19	74.126.177.68
java.ns1[.]name	2014-02-18	2014-02-19	74.126.177.68
java.ns1[.]name	2014-02-18	2014-02-18	192.74.246.219
wmi.ns01[.]us	2014-02-17	2014-02-17	192.74.246.219
proxy.ddns[.]info	2013-05-02	2014-02-18	103.246.246.103

updatedns.ns02[.]us	2013-09-06	2013-09-06	103.246.246.103
updatedns.ns01[.]us	2013-09-06	2013-09-06	103.246.246.103
wmi.ns01[.]us	2013-07-04	2013-07-15	103.246.246.103

Further research uncovered a number of older malware samples connecting to the same domain wmi.ns01[.]us.

MD5	Family	Compile Time	Alternate C2s
7995a9a6a889b914e208eb924e459ebc	PlugX	2012-06-09	fuckchina.govnb[.]com
bf60b8d26bc0c94dda2e3471de6ec977	PlugX	2010-03-15	microsafes.no-ip[.]org
fd69793bd63c44bbb22f9c4d46873252	Poison Ivy	2013-03-07	N/A
88b375e3b5c50a3e6c881bc96c926928	Poison Ivy	2012-06-11	N/A
cd07a9e49b1f909e1bd9e39a7a6e56b4	Poison Ivy	2012-06-11	N/A

Domain	First Seen	Last Seen	IP Address
fuckchina.govnb[.]com	2013-12-11	2013-12-11	204.200.222.136
microsafes.no-ip[.]org	2014-02-12	2014-02-12	74.126.177.70
microsafes.no-ip[.]org	2013-12-04	2013-12-04	74.126.177.241

The Poison Ivy variants that connected to the domain wmi.ns01[.]us had the following unique configuration properties:

MD5	Password	Mutex
fd69793bd63c44bbb22f9c4d46873252	java7	NBCD*&^FE
88b375e3b5c50a3e6c881bc96c926928	admin	ytf^&^333
cd07a9e49b1f909e1bd9e39a7a6e56b4	admin	ytf^&^333

We found a related Poison Ivy sample (MD5 8936c87a08ffa56d19fdb87588e35952) with the same "java7" password, which was dropped by an Adobe Flash exploit (CVE-2012-0779). In this previous incident, visitors to the Center for Defense Information website (www.cdi[.]org — also an organization involved in defense matters — were redirected to an exploit server at 159.54.62.92.

This exploit server hosted a Flash exploit file named BrightBalls.swf (MD5 1ec5141051776ec9092db92050192758). This exploit, in turn, dropped the Poison Ivy **variant**. In addition to using the same password "java7," this variant was configured with the mutex with the similar pattern of "YFds*&^ff" and connected to a CnC server at windows.ddns[.]us.

Using passive DNS analysis, we see the domains windows.ddns[.]us and wmi.ns01[.]us both resolved to 76.73.80.188 in mid-2012.

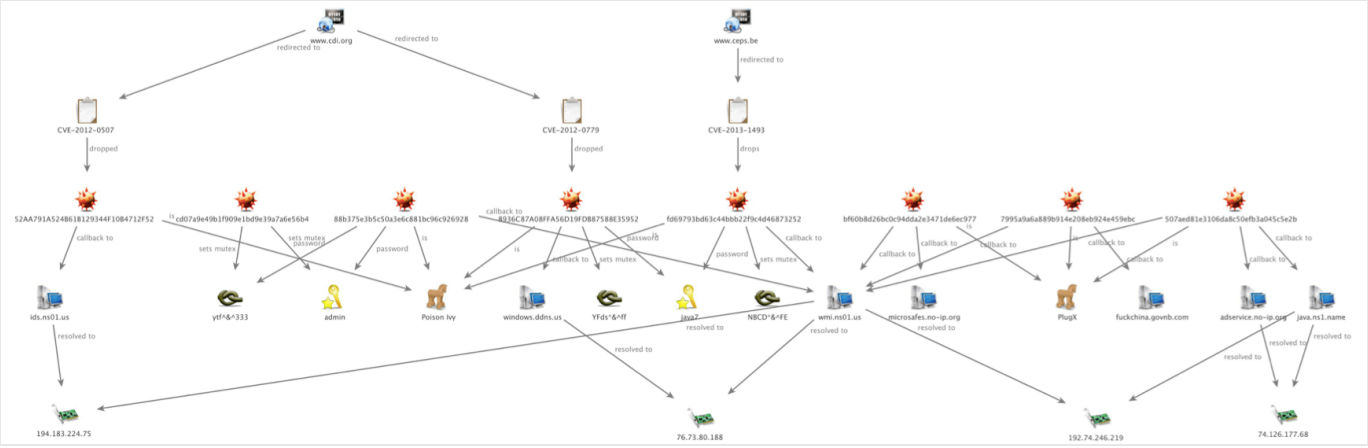
Domain	First Seen	Last Seen	IP Address
wmi.ns01.us	2012-07-07	2012-09-19	76.73.80.188
windows.ddns.us	2012-05-23	2012-06-10	76.73.80.188

During another earlier compromise of the same www.cdi.org website, visitors were redirected to a Java exploit test.jar (MD5 7d810e3564c4eb95bcb3d11ce191208e). This jar file exploited CVE-2012-0507 and dropped a Poison Ivy payload with the hash (MD5 52aa791a524b61b129344f10b4712f52). This Poison Ivy variant connected to a CnC server at ids.ns01[.]us. The domain ids.ns01[.]us also overlaps with the domain wmi.ns01[.]us on the IP 194.183.224.75.

Domain	First Seen	Last Seen	IP Address
wmi.ns01[.]us	2012-07-03	2012-07-04	194.183.224.75
ids.ns01[.]us	2012-04-23	2012-05-18	194.183.224.75

The Poison Ivy sample referenced above (MD5 fd69793bd63c44bbb22f9c4d46873252) was delivered via an exploit chain that began with a redirect from the Center for European Policy Studies (www.ceps[.]be). In this case, visitors were redirected from www.ceps[.]be to a Java exploit hosted on shop.fujifilm[.]be.

In what is certainly not a coincidence, we also observed www.arce[.]org (one of the sites redirecting to the current Flash exploit) also redirect visitors to the Java exploit on shop.fujifilm[.]be in 2013.



Conclusion

This threat actor clearly seeks out and compromises websites of organizations related to international security policy, defense topics, and other non-profit sociocultural issues. The actor either maintains persistence on these sites for extended periods of time or is able to re-compromise them periodically.

This actor also has early access to a number of zero-day exploits, including Flash and Java, and deploys a variety of malware families on compromised systems. Based on these and other observations, we conclude that this actor has the tradecraft abilities and resources to remain a credible threat in at least the mid-term.