Operation SnowMan: DeputyDog Actor Compromises US Veterans of Foreign Wars Website

On February 11, FireEye identified a zero-day exploit (CVE-2014-0322) being served up from the U.S. Veterans of Foreign Wars' website (vfw[.]org). We believe the attack is a strategic Web compromise targeting American military personnel amid a paralyzing snowstorm at the U.S. Capitol in the days leading up to the Presidents Day holiday weekend. Based on infrastructure overlaps and tradecraft similarities, we believe the actors behind this campaign are associated with two previously identified campaigns (**Operation DeputyDog** and **Operation Ephemeral Hydra**).

This blog post examines the vulnerability and associated attacks, which we have dubbed "Operation SnowMan."

Exploit/Delivery analysis

After compromising the VFW website, the attackers added an iframe into the beginning of the website's HTML code that loads the attacker's page in the background. The attacker's HTML/JavaScript page runs a Flash object, which orchestrates the remainder of the exploit. The exploit includes calling back to the IE 10 vulnerability trigger, which is embedded in the JavaScript. Specifically, visitors to the VFW website were silently redirected through an iframe to the exploit at www.[REDACTED].com/Data/img/img.html.

Mitigation

The exploit targets IE 10 with Adobe Flash. It aborts exploitation if the user is browsing with a different version of IE or has installed Microsoft's Experience Mitigation Toolkit (EMET). So installing EMET or updating to IE 11 prevents this exploit from functioning.

Vulnerability analysis

The vulnerability is a previously unknown use-after-free bug in Microsoft Internet Explorer 10. The vulnerability allows the attacker to modify one byte of memory at an arbitrary address. The attacker uses the vulnerability to do the following:

- Gain access to memory from Flash ActionScript, bypassing address space layout randomization (ASLR)
- Pivot to a return-oriented programing (ROP) exploit technique to bypass data execution prevention (DEP)

EMET detection

The attacker uses the Microsoft.XMLDOM ActiveX control to load a one-line XML string containing a file path to the EMET DLL. Then the exploit code parses the error resulting from the XML load order to determine whether the load failed because the EMET DLL is not present. The exploit proceeds only if this check determines that the EMET DLL is not present.

ASLR bypass

Because the vulnerability allows attackers to modify memory to an arbitrary address, the attacker can use it to bypass ASLR. For example, the attacker corrupts a Flash *Vector* object and then accesses the corrupted object from within Flash to access memory. We have discussed this technique and other ASLR bypass approaches **in our blog**. One minor difference between the previous approaches and this attack is the heap spray address, which was changed to 0x1a1b2000 in this exploit.

Code execution

Once the attacker's code has full memory access through the corrupted Flash *Vector* object, the code searches through loaded libraries gadgets by machine code. The attacker then overwrites the *vftable* pointer of a *flash.Media.Sound()* object in memory to point to the pivot and begin ROP. After successful exploitation, the code repairs the corrupted Flash *Vector* and *flash.Media.Sound* to continue execution.

Shellcode analysis

Subsequently, the malicious Flash code downloads a file containing the dropped malware payload. The beginning of the file is a JPG image; the end of the file (offset 36321) is the payload, encoded with an XOR key of 0×95. The attacker appends the payload to the shellcode before pivoting to code control. Then, when the shellcode is executed, the malware creates files "sqlrenew.txt" and "stream.exe". The tail of the image file is decoded, and written to these files. "sqlrenew.txt" is then executed with the *LoadLibraryA* Windows API call.

ZxShell payload analysis

As documented above, this exploit dropped an XOR (0×95) payload that executed a ZxShell backdoor (MD5: 8455bbb9a210ce603a1b646b0d951bce). The compile date of the payload was 2014-02-11, and the last modified date of the exploit code was also 2014-02-11. This suggests that this instantiation of the exploit was very recent and was deployed for this specific strategic Web compromise of the Veterans of Foreign Wars website. A possible objective in the SnowMan attack is targeting military service members to steal military intelligence. In addition to retirees, active military personnel use the VFW website. It is probably no coincidence that Monday, Feb. 17, is a U.S. holiday, and much of the U.S. Capitol shut down

Thursday amid a severe winter storm.

The ZxShell backdoor is a widely used and publicly available tool used by multiple threat actors linked to cyber espionage operations. This particular variant called back to a command and control server located at newss[.]effers[.]com. This domain currently resolves to 118.99.60.142. The domain info[.]flnet[.]org also resolved to this IP address on 2014-02-12.

Infrastructure analysis

The info[.]flnet[.]org domain overlaps with icybin[.]flnet[.]org and book[.]flnet[.]org via the previous resolutions to the following IP addresses:

- 58.64.200.178
- 58.64.200.179
- 103.20.192.4

First Seen	Last Seen	CnC Domain	IP
2013-08-31	2013-08-31	icybin.flnet[.]org	58.64.200.178
2013-05-02	2013-08-02	info.flnet[.]org	58.64.200.178
2013-08-02	2013-08-02	book.flnet[.]org	58.64.200.178
2013-08-10	2013-08-10	info.flnet[.]org	58.64.200.179
2013-07-15	2013-07-15	icybin.flnet[.]org	58.64.200.179
2014-01-02	2014-01-02	book.flnet[.]org	103.20.192.4
2013-12-03	2014-01-02	info.flnet[.]org	103.20.192.4

We previously observed GhostRat samples with the custom packet flag “HTTPS” calling back to book[.]flnet[.]org and icybin[.]flnet[.]org. The threat actor responsible for **Operation DeputyDog** also used the “HTTPS” version of the **Ghost**. We also observed another “HTTPS” Ghost variant connecting to a related command and control server at me[.]scieron[.]com.

MD5 Hash	CnC Domain
758886e58f9ea2ff22b57cbbb015166e	book.flnet[.]org
0294f9280491f85d898ebe471f0fb58e	icybin.flnet[.]org
9d20566a327076b7152bbf9ed20292c4	me.scieron[.]com

The me[.]scieron[.]com domain previously resolved to 58.64.199.22. The book[.]flnet[.]org domain also resolved to another IP in the same subnet 58.64.199.0/24. Specifically, book[.]flnet[.]org previously resolved to 58.64.199.27.

Others domain seen resolving to this same /24 subnet were dll[.]freshdns[.]org, ali[.]blankchair[.]com, and cht[.]blankchair[.]com. The domain dll[.]freshdns[.]org resolved to 58.64.199.25. Both ali[.]blankchair[.]com and cht[.]blankchair[.]com resolved to 58.64.199.22.

First Seen	Last Seen	CnC Domain	IP

2012-11-12	2012-11-28	me.scieron[.]com	58.64.199.22
2012-04-09	2012-10-24	cht.blankchair[.]com	58.64.199.22
2012-04-09	2012-09-18	ali.blankchair[.]com	58.64.199.22
2012-11-08	2012-11-25	dll.freshdns[.]org	58.64.199.25
2012-11-23	2012-11-27	rt.blankchair[.]com	58.64.199.25
2012-05-29	2012-6-28	book.flnet[.]org	58.64.199.27

A number of other related domains resolve to these IPs and other IPs also in this /24 subnet. For the purposes of this blog, we've chosen to focus on those domains and IP that relate to the previously discussed DeputyDog and Ephemeral Hydra campaigns.

You may recall that dll[.]freshdns[.]org, ali[.]blankchair[.]com and cht[.]blankchair[.]com were all linked to both **Operation DeputyDog** and **Operation Ephemeral Hydra**. Figure 1 illustrates the infrastructure overlaps and connections we observed between the strategic Web compromise campaign leveraging the VFW's website, the DeputyDog, and the Ephemeral Hydra operations.

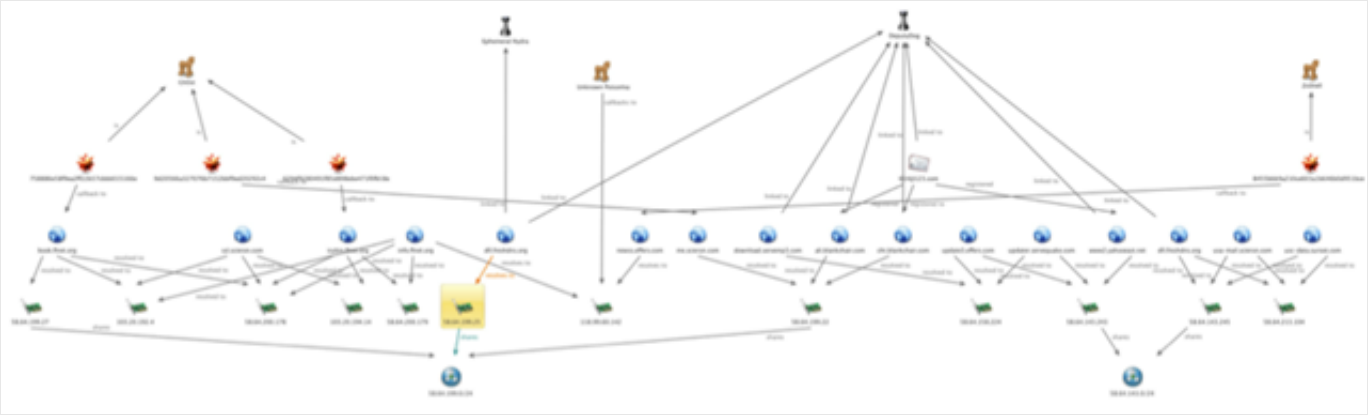

Figure 1: Ties between Operation SnowMan, DeputyDog, and Ephemeral Hydra

Links to DeputyDog and Ephemeral Hydra

Other tradecraft similarities between the actor(s) responsible for this campaign and the actor(s) responsible for the DeputyDog/Ephemeral Hydra campaigns include:

- The use of zero-day exploits to deliver a remote access Trojan (RAT)
- The use of strategic web compromise as a vector to distribute remote access Trojans
- The use of a simple single-byte XOR encoded (0×95) payload obfuscated with a .jpg extension
- The use of GhostRat with the "HTTPS" packet flag
- The use of related command-and-control (CnC) infrastructure during the similar time frames

We observed many similarities from the exploitation side as well. At a high level, this attack and the **CVE-2013-3163** attack both leveraged a Flash file that orchestrated the exploit, and would call back into IE JavaScript to trigger an IE flaw. The code within the Flash files from each attack are extremely similar.

They build ROP chains and shellcode the same way, both choose to corrupt a Flash *Vector* object, have some identical functions with common typos, and even share the same name.

Conclusion

These actors have previously targeted a number of different industries, including:

- U.S. government entities
- Japanese firms
- Defense industrial base (DIB) companies
- Law firms
- Information technology (IT) companies
- Mining companies
- Non-governmental organizations (NGOs)

The proven ability to successfully deploy a number of different private and public RATs using zero-day exploits against high-profile targets likely indicates that this actor(s) will continue to operate in the mid to long-term.

This entry was posted in Advanced Malware, Exploits, Targeted Attack, Threat Research, Vulnerabilities and tagged oday, zero-day by Darien Kindlund, Dan Caselden, Xiaobo Chen, Ned Moran and Mike Scott. Bookmark the permalink.