VOLEXITY

Incident Response & Suppression

Home

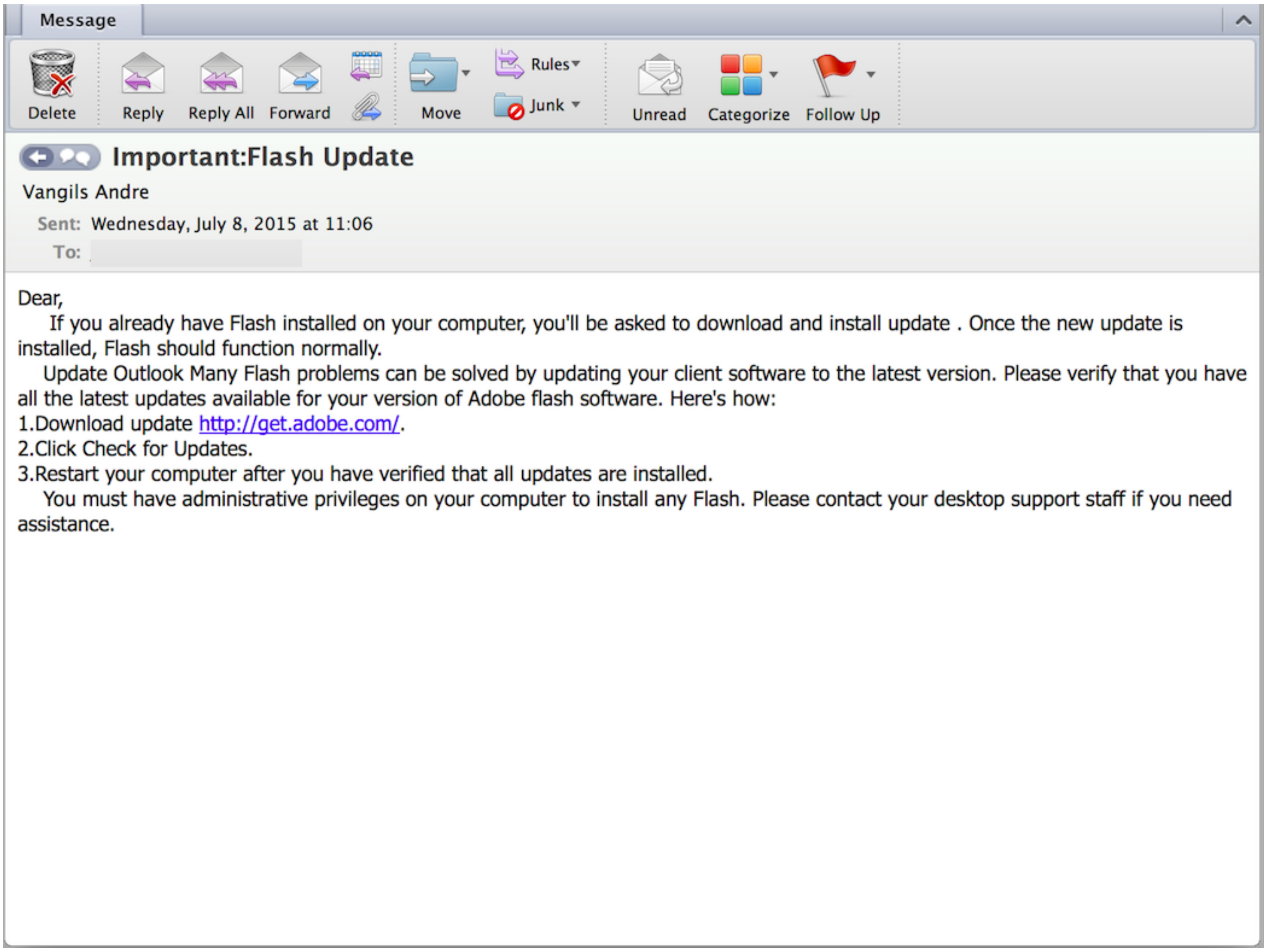
APT Group Wekby Leveraging Adobe Flash Exploit (CVE-2015-5119)

Posted on July 8, 2015 by Steven Adair

As if the recent breach and subsequent public data dump involving the Italian company Hacking Team wasn't bad enough, it all gets just a little bit worse. Emerging from the bowels of Hacking Team data dump was a Flash 0-day exploit (CVE-2015-5119) that was just patched today by Adobe as covered in APSB15-16. The exploit has since been added into the Angler Exploit Kit and integrated into Metasploit. However, not to be out done, APT attackers have also started leveraging the exploit in targeted spear phishing attacks as well. Before we start dishing the details, there is going to be one main takeaway from this blog post: If you haven't already, update/patch your Adobe Flash now.

Spear Phishing

This morning, a well known APT threat group, often referred to as **Wekby,** kicked off a rather ironic spear phishing campaign. The attackers launched spoofed e-mail messages purporting to be from **Adobe**. The e-mail messages references an Adobe Flash update and encourage the recipients to click a link to download and install the update. Take a look at an example of the spear phish e-mail message below.



Important:Flash Update

Vangils Andre

Sent: Wednesday, July 8, 2015 at 11:06

To:

Dear,

If you already have Flash installed on your computer, you'll be asked to download and install update . Once the new update is installed, Flash should function normally.

Update Outlook Many Flash problems can be solved by updating your client software to the latest version. Please verify that you have all the latest updates available for your version of Adobe flash software. Here's how:

1.Download update http://get.adobe.com/.

2.Click Check for Updates.

3.Restart your computer after you have verified that all updates are installed.

You must have administrative privileges on your computer to install any Flash. Please contact your desktop support staff if you need assistance.

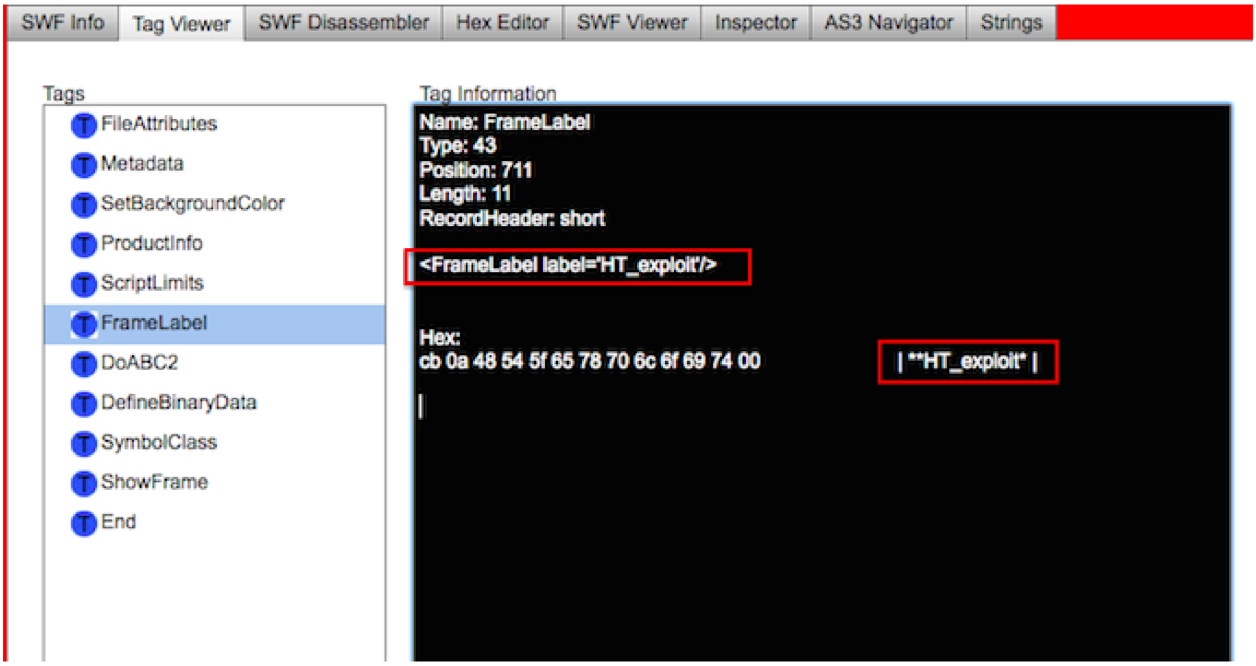
The visible and spoofed source e-mail address for “Andre Vangils” is **avangils@adobe.com**. This is not a particularly advanced spear phish message. However, the visible link http://get.adobe.com, as you have likely guessed, does not actually go to Adobe’s website. Instead it leads to **index.htm** on an IP address belonging to a hosting provider named PEG TECH INC. This page is far less helpful than one would hope. Instead of providing a legitimate Adobe Flash update, the page loads a malicious SWF file instead. The following contents are found from the HTML page from the link:

```
<body>
<div style=”position:fixed; top:50%; left:50%; width:600; height:400; margin-left:-300; margin-top:-200;”>
<object classid=”clsid:D27CDB6E-AE6D-11cf-96B8-444553540000″   id=”swf” width=”600″   height=”400″  >
<param name=”movie” value=”movie.swf” />
<param name=”allowScriptAccess” value=”always” />
<embed src=”movie.swf” width=”600″   height=”400″   allowScriptAccess=”always” type=”application/x-shockwave-flash” />
</object>
</div>
</body>
</html>
```

If you guess this was a Flash exploit, then you are 100% correct.

Exploits and Malware

The aforementioned exploit works on Adobe Flash versions all the way up to **18.0.0.194**. You need to have updated your Flash since this morning to be safe from its grips. The attackers appear to have modified one of the exploits that came from the Hacking Team dump. Unlike most of the other versions we have observed up until this point, this SWF file is LZMA compressed and has the ZWS file header. There are plenty of great tools out there that can be used to look at Flash files. One of our favorites is SWF Investigator from Adobe. Poking around a bit we can see a few interesting labels that appear to reference Hacking Team, such as the one shown below:



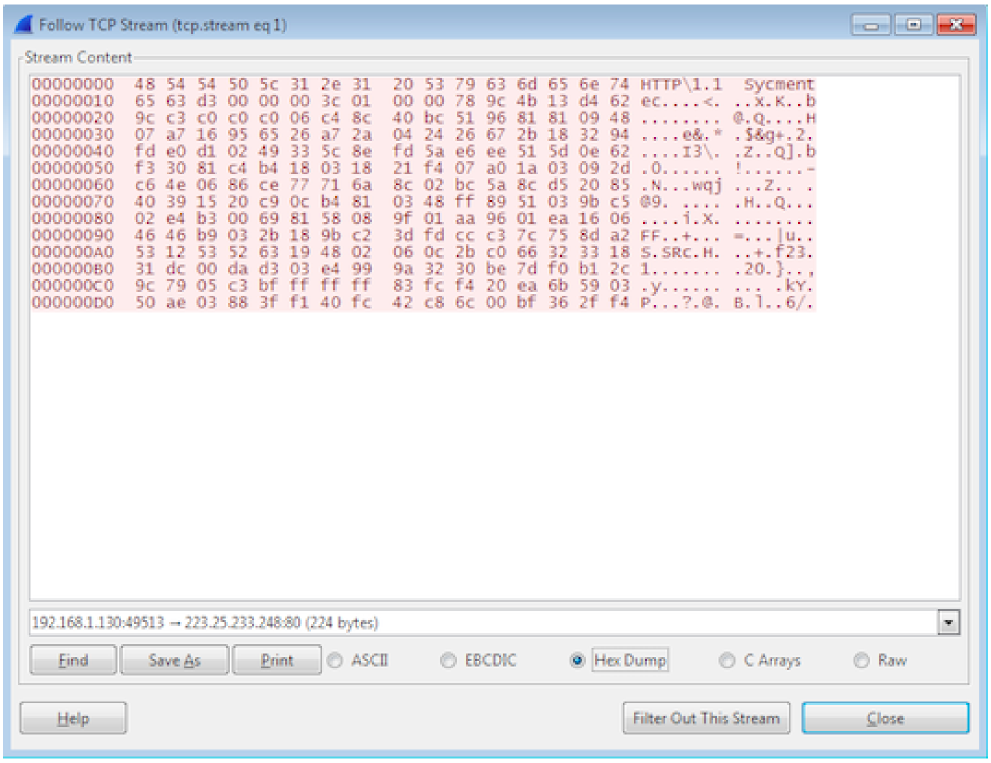
```
Name: FrameLabel
Type: 43
Position: 711
Length: 11
RecordHeader: short

<FrameLabel label='HT_exploit'/>


Hex:
cb 0a 48 54 5f 65 78 70 6c 6f 69 74 00          | **HT_exploit* |
```

Notice the “HT_exploit” label. Further down in the file is a class with the same name. These appear to be not so subtle references to the source of this exploit. We did not see these labels or class names in any of the other files we observed thus far, so we presume these were recently created as part of this new exploit file. At the end of the day, the goal of this attack is to install malware on target systems. If a vulnerable system were to visit the exploit site from the spear phish message, this is exactly what would happen. In this case the flash file would drop an executable into the victim user’s Temp directory similar to the path shown below:

> *C:\Users\$Username\AppData\Local\Temp\Rdws.exe*

The malware would then execute and immediately start beaconing to the Singapore IP address **223.25.233.248** on TCP **port** 80. This is a well known Wekby command and control (C2) IP address that has been used for years. Currently there a few other active DNS names that resolve to IP such as **gmail.bkz88.com** and **info.imly.org.** Any connection involving this IP address or these hostnames should be consider hostile and a likely indicator of compromise.

The 223.25.233.248 IP address has served as a C2 server for a variety of different malware in the past (Poison Ivy, Gh0st, Remote RSS, etc.). However, this go around the malware is a modified version of the Gh0st remote access trojan (RAT). Typically the default version of Gh0st sends a packet flag of “Gh0st” in the first 5-bytes. This has been heavily modified over the years and several custom versions of Gh0st have emerged with dozens and dozens of customer packet flags such as cb1st, Winds, https, and so on. However, the Wekby APT actor last year started using a modified version that has an 18 character packet flag. This version was reused in this attack and an infected system will send a rather peculiar packet flag as seen in the image below:



```
00000000  48 54 54 50 5c 31 2e 31  20 53 79 63 6d 65 6e 74 HTTP\1.1  Sycment
00000010  65 63 d3 00 00 00 3c 01  00 00 78 9c 4b 13 d4 62 ec.....<. ..x.K..b
00000020  9c c3 c0 c0 c0 06 c4 8c  40 bc 51 96 81 81 09 48 ........ @.Q....H
00000030  07 a7 16 95 65 26 a7 2a  04 24 26 67 2b 18 32 94 ....e&.* .$&g+.2.
00000040  fd e0 d1 02 49 33 5c 8e  fd 5a e6 ee 51 5d 0e 62 ....I3\. .Z..Q].b
00000050  f3 30 81 c4 b4 18 03 18  21 f4 07 a0 1a 03 09 2d .0...... !......-
00000060  c6 4e 06 86 ce 77 71 6a  8c 02 bc 5a 8c d5 20 85 .N...wqj ...Z.. .
00000070  40 39 15 20 c9 0c b4 81  03 48 ff 89 51 03 9b c5 @9. .... .H..Q...
00000080  02 e4 b3 00 69 81 58 08  9f 01 aa 96 01 ea 16 06 ....i.X. ........
00000090  46 46 b9 03 2b 18 9b c2  3d fd cc c3 7c 75 8d a2 FF..+... =...|u..
000000A0  53 12 53 52 63 19 48 02  06 0c 2b c0 66 32 33 18 S.SRc.H. ..+.f23.
000000B0  31 dc 00 da d3 03 e4 99  9a 32 30 be 7d f0 b1 2c 1....... .20.}..,
000000C0  9c 79 05 c3 bf ff ff ff  83 fc f4 20 ea 6b 59 03 .y...... ... .kY.
000000D0  50 ae 03 88 3f f1 40 fc  42 c8 6c 00 bf 36 2f f4 P...?.@. B.l..6/.
```

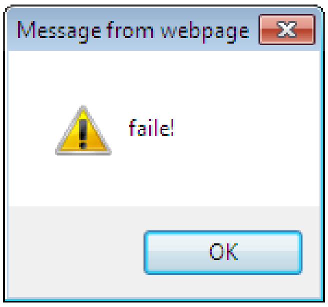
192.168.1.130:49513 → 223.25.233.248:80 (224 bytes)

You are reading that correctly, it’s sending: **HTTP\1.1 Sycmentec.** Presumably this is a poor attempt to blend in as HTTP traffic and appear to be affiliated with Symantec. There are plenty of signatures in the Emerging Threats rulesets to pick up on Gh0st, but you can use the signature below to pickup on this specific instance of Gh0st.

> *alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:”Volexity – Wekby Gh0st Variant [HTTP\1.1 Sycmentec]”; flow:to_server,established; content:”HTTP|5c|1.1 Sycmentec”; depth:18; sid:201507081;)*

You can add in a check for two null bytes followed by zlib header (“|000789c|”) for an additional match. However, chances are a hit on that string by itself is probably bad news and solid enough. Add a rule for the reverse direction to catch the server’s response as well.

Also, pretty interesting and funny is what happens is your version of Flash is up-to-date when you visit the exploit page. Instead of silently failing in the background, it instead results in the rather obvious popup:



faile!

Your eyes are not deceiving you. It says **faile!** right on the screen. It looks like the attackers may have left a debug message from their testing. Not very subtle at all.

File Details and Persistence

Here’s what to look for when it comes to file indicators.

Filename	movie.swf
File size	214976 bytes

MD5	079a440bee0f86d8a59ebc5c4b523a07
SHA1	7389e78cca58de6cb2cbe2b631d2fec259e9cdcc
Notes	Malicious flash file that drops Wekby Gh0st RAT.

Filename	Rdws.exe
File size	138240 bytes
MD5	cfbcb83f8515bd169afd0b22488b4430
SHA1	959638ee177b51bda8701c10258b4956f8b1c367
Notes	HTTP\1.1 Sycmentec packet flag malware.

The malware sets its persistence adding an entry to the HKCU "RUN" key (HKCU\Software\Microsoft\Windows\CurrentVersion\Run):

> *NAME: CSics*
> *DATA: C:\Users\$User\AppData\Local\Rdws.exe*

Conclusion

Volexity is aware of multiple other ongoing APT and non-APT cyber attacks leverage CVE-2015-5119. While it is always important to patch your software and keep it up-to-date, it is **CRITICAL** that you patch your Adobe Flash immediately. The attackers are having a field day with this exploit and will not slow down any time soon. Patching is the most prudent course of action to deal with this exploit that is very much in the wild. Additionally, as always, for Microsoft Windows users, looking at deploying the Enhance Mitigation Experience Toolkit (EMET) would also be advised.

FOLLOW US ON TWITTER @VOLEXITY.

This entry was posted in Adobe Flash, APT, China, Exploits, Vulnerabilities. Bookmark the permalink.

« Afghan Government Compromise: Browser Beware

Virtual Private Keylogging: Cisco Web VPNs Leveraged for Access and Persistence »

Search …

Recent Posts

› Virtual Private Keylogging: Cisco Web VPNs Leveraged for Access and Persistence

› APT Group Wekby Leveraging Adobe Flash

Exploit (CVE-2015-5119)

- Afghan Government Compromise: Browser Beware
- A New Shellshock Worm on the Loose
- Drupal Vulnerability: Mass Scans & Targeted Exploitation

Archives

- October 2015
- July 2015
- June 2015
- April 2015
- October 2014
- September 2014

Categories

- Adobe Flash
- APT
- China
- Digital Surveillance
- Drupal
- Exploits
- Hong Kong
- Japan
- Java
- Scanning
- Vulnerabilities