Malwarebytes
RESEARCH BRIEF

An inside view of the rapid weaponization of a leaked zero-day POC

Jean Taggart Security Researcher, Malwarebytes

Overview

From POC (proof of concept) to exploit kit integration, cyber criminals are getting more and more adept at weaponizing zero-days exploits. The speed at which exploit kit makers can take a vulnerability and integrate it is ever increasing.

This paper details a unique case where a security company specializing in offensive technology was compromised, and their trove of zero days was leaked to the Internet, including several for Adobe's Flash Player. As the zero days were previously unknown, but were accompanied by clear and concise instructions to deploy them, we had a keen interest in seeing if our solution, Malwarebytes Anti-Exploit, would effectively block the zero days (which it did), as well as how fast the exploit kit developers would deploy them.

Timeline

This zero-day campaign is notable for the speed demonstrated by exploit kit makers in integrating the exploit into their platforms. This was further facilitated by the helpful readme files provided by Hacking Team, which clearly explained how to deploy the vulnerability. After the announcement of the Hacking Team breach and subsequent leak of the 400GB

Topline Facts

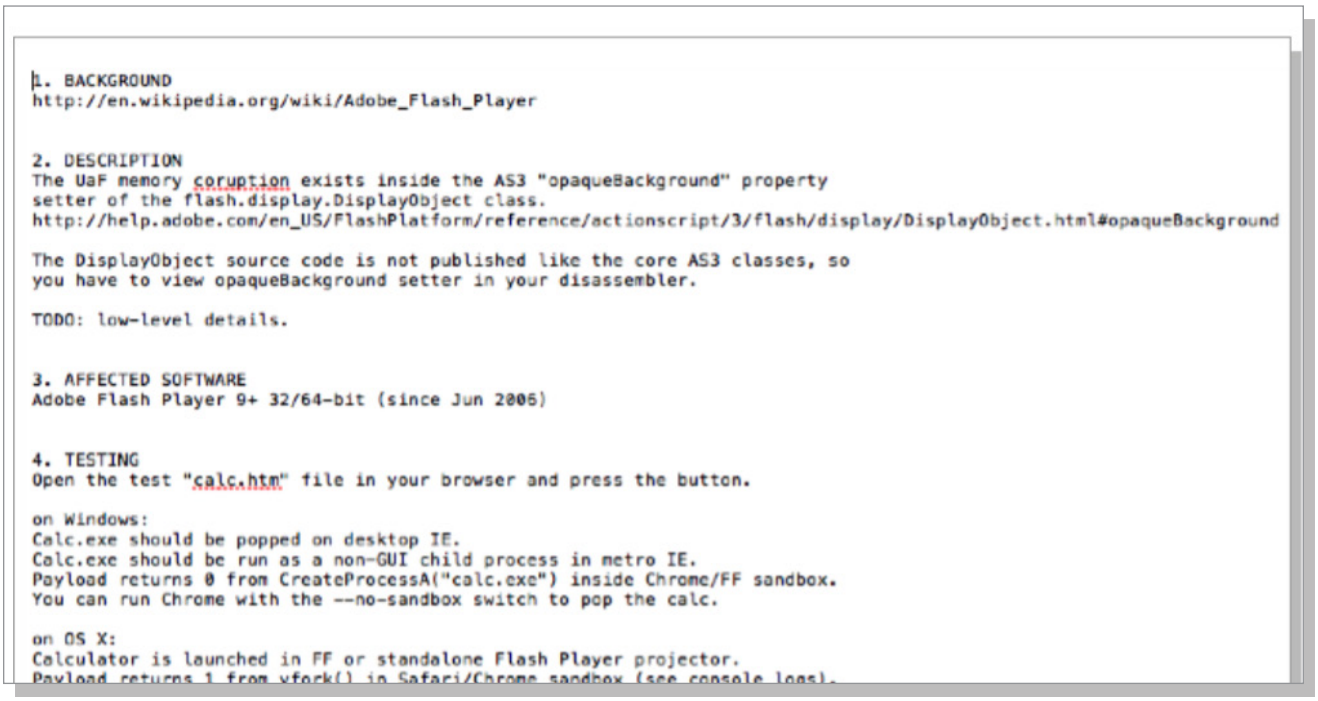
CVE-2015-5119:
Adobe Flash vulnerability, affected 14.x up to 18.0.0.194, fixed with version 18.0.0.203

Integration:
The zero day was discovered in the leaked archive from the Italian offensive security firm Hacking Team. Exploit kit makers integrated it into their digital weapons as fast as possible.

Window of exposure:
July 6 to July 8, 2015

Payload:
- Neutrino drops a proxy Trojan
- Angler drops a password stealer
- Nuclear Pack drops crypto ransomware
- Magnitude drops crypto ransomware
- HanJuan drops ad fraud

archive, there was much speculation in security circles if this leak included previously undocumented zero days. Not surprisingly, it did.



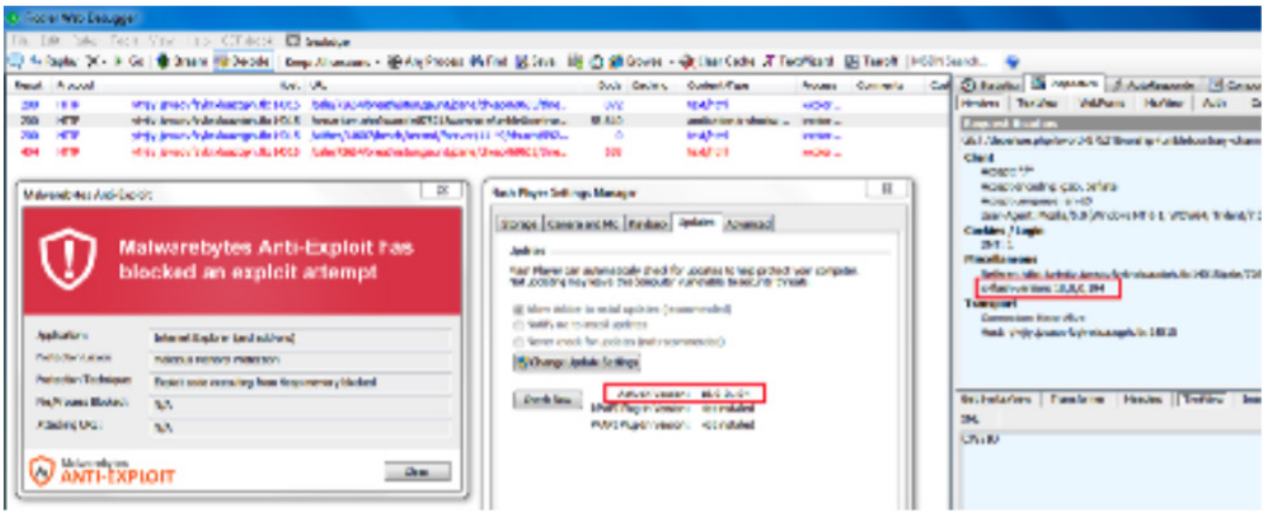
```
1. BACKGROUND
http://en.wikipedia.org/wiki/Adobe_Flash_Player


2. DESCRIPTION
The UaF memory coruption exists inside the AS3 "opaqueBackground" property
setter of the flash.display.DisplayObject class.
http://help.adobe.com/en_US/FlashPlatform/reference/actionscript/3/flash/display/DisplayObject.html#opaqueBackground

The DisplayObject source code is not published like the core AS3 classes, so
you have to view opaqueBackground setter in your disassembler.

TODO: low-level details.


3. AFFECTED SOFTWARE
Adobe Flash Player 9+ 32/64-bit (since Jun 2006)


4. TESTING
Open the test "calc.htm" file in your browser and press the button.

on Windows:
Calc.exe should be popped on desktop IE.
Calc.exe should be run as a non-GUI child process in metro IE.
Payload returns 0 from CreateProcessA("calc.exe") inside Chrome/FF sandbox.
You can run Chrome with the --no-sandbox switch to pop the calc.

on OS X:
Calculator is launched in FF or standalone Flash Player projector.
Payload returns 1 from vfork() in Safari/Chrome sandbox (see console logs).
```

Hacking Team presented this information in the simplest of manners, as their expected target audience was customers that lacked the technical know-how to find and develop their own zero day.

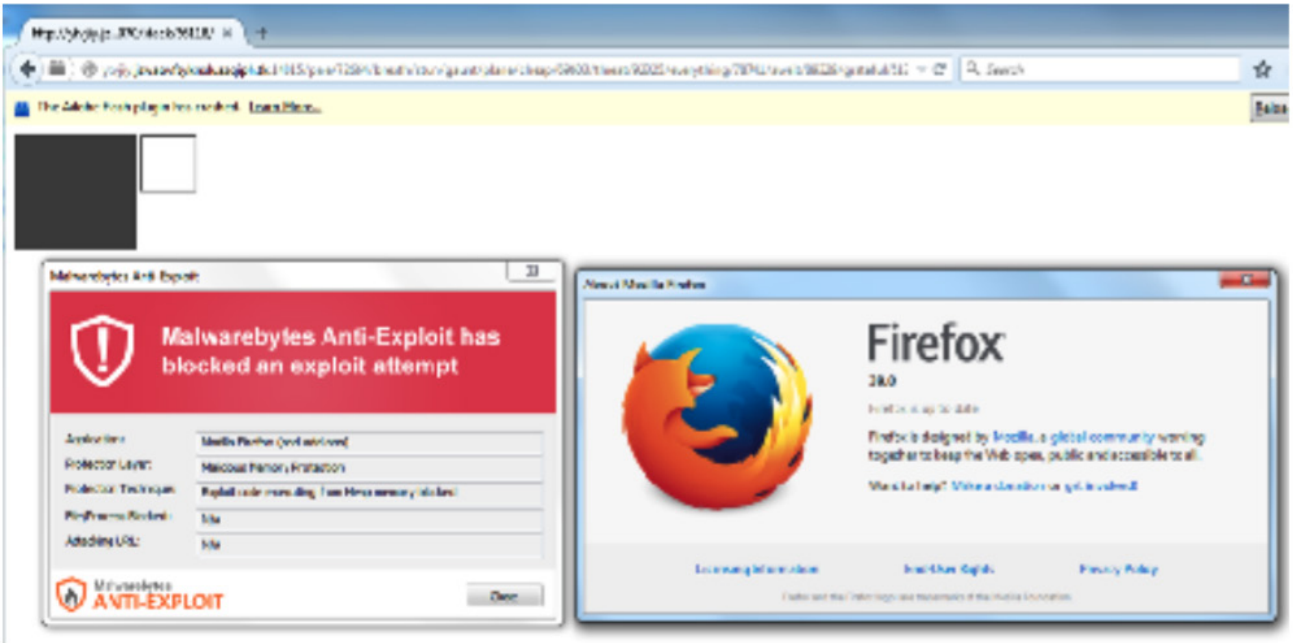
July 6 – Hacking Team breach announced: 400GB archive of documents leaked via Torrent

July 6 – Tweet from security researcher: webDEViL (@w3bd3vil), Tweets the Flash zero day and crib sheet (Tweet has since been deleted)

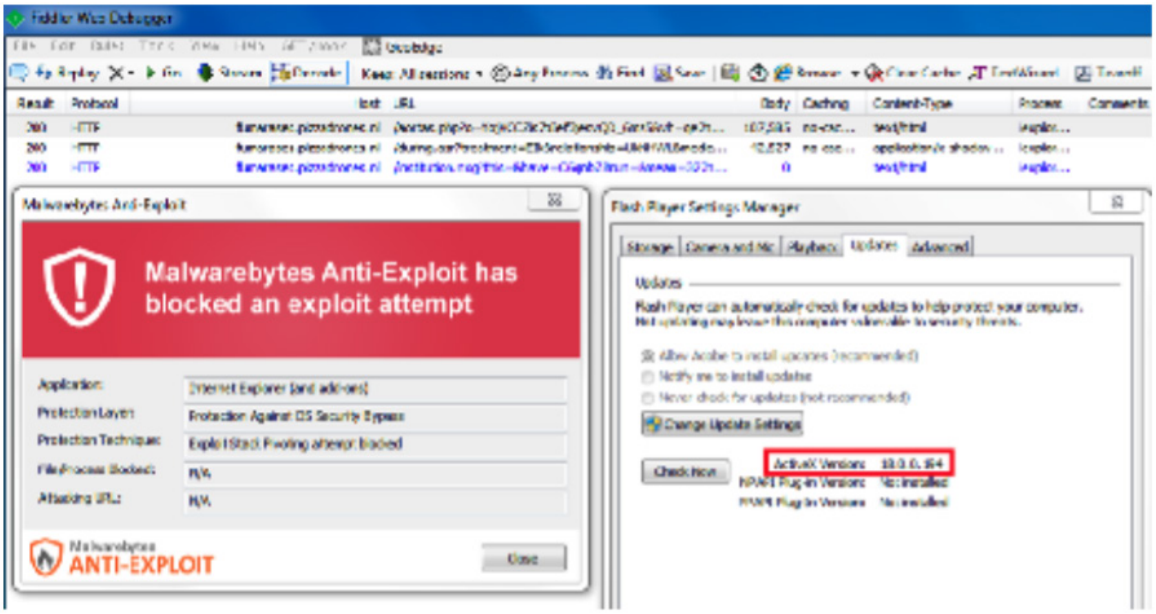
July 7, 3:23PM – First seen: Jerome Segura, senior security researcher at Malwarebytes, identifies that the Neutrino exploit kit has integrated CVE-2015-5119 and is active in the wild*



CVE-2015-5119 fires successfully against Firefox



July 7, 3:40PM – Second EK spotted: Angler deploying CVE-2015-5119**



July 7, 4:20PM – Nuclear deploying CVE-2015-5119

Third EK: Nuclear deploying CVE-2015-5119*

Metasploit module added: CVE-2015-5119 is integrated in the Metasploit framework, the open source component of the most popular computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development.

July 8, 8:59AM – Metasploit framework integration independently confirmed (1)

CVE-2015-5119 Flash 1day Exploit の確認結果。Metasploit Module 使用。Win8.1 x86 / FF 39.0 / Flash 18.0.0.194 / EMET 無し。刺さりました。 http://t.co/6LIGObpQJ0
– Neutral8x9eR (@0x009AD6_810) via Twitter Web Client

July 8, 12:13PM – Adobe update: Adobe pushes an update addressing the vulnerability with Flash Player 18.0.0.203, effectively making all downstream EK integration non zero day***

July 8, 1:07PM – Fourth EK: Magnitude deploying CVE-2015-5119**(2)

July 8, 12:13PM – Adobe update: Adobe pushes an update addressing the vulnerability with Flash Player 18.0.0.203, effectively making all downstream EK integration non zero-day***

July 8, 1:07PM – Fourth EK: Magnitude deploying CVE-2015-5119**

July 9, 11:09AM – Fifth EK: RIG deploying CVE-2015-5119*

July 10, 12:54AM – Sixth EK: HanHuan deploying CVE-2015-5119(This was only confirmed after Adobe addressed CVE-2015-5119. However, HanHuan has always been notoriously difficult to replay and tends to stay under the radar. There is a significant chance that they deployed this zero-day exploit prior to patching, but were better at hiding it** (1)

Targeting

The cyber criminals who develop exploit kits are always on the lookout for additional vulnerabilities to add to their arsenal. Their selection of vulnerabilities directly affects their businesses, their popularity, as well as the prices they can charge malware authors who use their services as a vehicle for delivery. All of this hinges on successful infections, and using zero days yields the highest infection rates possible.

Conclusions

This particular zero day continues to illustrate the trend of shorter and shorter times between publicly available information of the existence of a zero day and integration into exploit kits.

This incident is unique, as zero-day exploits are seldom available at no cost and accompanied with a detailed crib sheet explaining how to deploy them. Our timeline shows the speed at which zero days are weaponized and highlights which exploit kit makers are the most adept at this. It also clearly demonstrates the need for a layered defense that includes addressing the challenges that zero days bring to the table.

We used Malwarebytes Anti-Exploit during all of our tracking of the deployment of CVE-2015-5119 across these major exploit kits. It successfully shielded Flash and prevented its exploitation.

References

*As reported on https://blog.malwarebytes.org/exploits-2/2015/07/neutrino-ek-leverages-latest-flash-0day/ by security researcher Jérôme Segura.

** As reported on http://malware.dontneedcoffee.com/2015/07/hackingteam-flash-0d-cve-2015-xxxx-and.html by security researcher Kafeine.

*** As reported on http://krebsonsecurity.com/tag/cve-2015-5119/ by security journalist Brian Krebs.

(1) https://twitter.com/0x009AD6_810/status/618811693888507908/photo/1

About Malwarebytes

Malwarebytes provides anti-malware and anti-exploit software designed to protect businesses and consumers against zero-day threats that consistently escape detection by traditional antivirus solutions. Malwarebytes Anti-Malware earned an "Outstanding" rating by CNET editors, is a PCMag.com Editor's Choice, and was the only security software to earn a perfect malware remediation score from AV-TEST.org. That's why more than 38,000 SMBs and Enterprise businesses worldwide trust Malwarebytes to protect their data. Founded in 2008, Malwarebytes is headquartered in California, operates offices in Europe, and employs a global team of researchers and experts.