Gone in a Flash: Top 10 Vulnerabilities Used by Explo

Posted by **S3** on November 9, 2015 in Cyber Threat Intelligence (https://www.recordedfuture.com/category/analysis/cyber/)

Analysis Summary

- Adobe Flash Player provided eight of the top 10 vulnerabilities used by exploit kits in 2015.

- Vulnerabilities in Microsoft's Internet Explorer and Silverlight are also major targets.
- Angler is currently the most popular exploit kit, regularly tied to malware including Cryptolocker.
- Identifying targeted vulnerabilities can better inform patch management functions within organizations.
- Some security professionals suggest uninstalling Adobe Flash Player. Enabling "Click to Play" is a stop-gap.

Recorded Future threat intelligence analysis of over 100 exploit kits (EKs) and known vulnerabilities identified Adobe Flash Player (https://en.wikipedia.org/wiki/Adobe_Flash_Player) as the most frequently exploited product. While the role of Adobe Flash vulnerabilities as a regular in-road for criminals and malware should come as no surprise to information security professionals, the scale is significant.

According to Web analysis from January 1, 2015 to September 30, 2015, **Adobe Flash Player comprised eight of the top 10 vulnerabilities leveraged by exploit kits**. Other leveraged vulnerabilities affect Microsoft Internet Explorer versions 10 and 11 (CVE-2015-2419) and Microsoft products including Silverlight (CVE-2015-1671).

Background

Exploit kits are crimeware as a service (CaaS) where users pay per install of their malware. Users only need to provide the payload (malware such as Cryptolocker) and a means to distribute the generated URL. This URL can be spread through compromised sites or malicious third-party advertising (malvertising). The teams behind these exploit kits continue to add fresh exploits for software as increased effectiveness in delivering the "customer's" payload will generate more revenue.

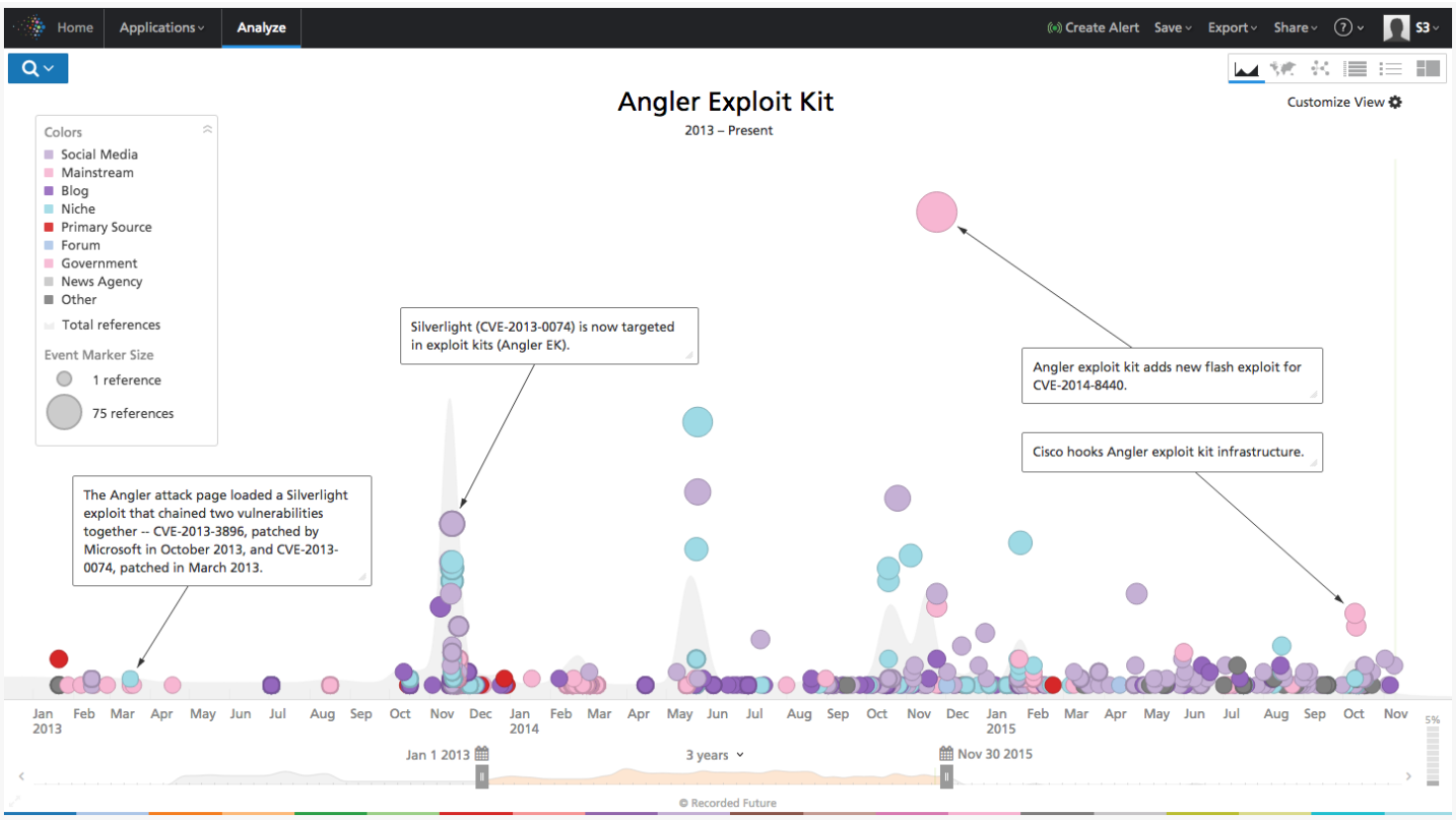
Exploit kit victims load the compromised Web page, malvertisement or unwittingly follow a malicious link to the exploit kit's landing page. Per Sophos (https://blogs.sophos.com/2015/07/21/a-closer-look-at-the-angler-exploit-kit/), "the landing page is the starting point for the exploit kit code." Using a mix of HTML and JavaScript, the EK identifies the visitor's browser and plugins, providing the kit the information necessary to deploy the exploit most likely to result in a drive-by download (https://blogs.mcafee.com/consumer/drive-by-download/).

Understanding what vulnerabilities are targeted by exploit kits can better inform patch management functions within organizations.

Angler Exploit Kit in Focus

Angler is one of the most popular and well-known exploit kits, linked to several high-profile malvertising and ransomware campaigns. First appearing in 2013, it quickly overtook Blackhole (http://blogs.cisco.com/security/talos/angler-domain-shadowing) as a favorite of cyber criminals, likely due to the rapid pace of new exploit adoption and its ability to evade many antivirus products (https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-evolution-of-exploit-kits.pdf).

Recorded Future analysis of Web sources including social media, forums and technical reporting highlighted Angler payloads including Cryptowall, AlphaCrypt, Necurs, and Bedep malware.



(https://www.recordedfuture.com/assets/top-vulnerabilities-2015-1.png)

CLICK IMAGE FOR LARGER VIEW

In October, Cisco claimed to strike a blow to Angler (http://blogs.cisco.com/security/talos/angler-exposed#more-178466) as they found a large batch of Angler proxy servers which accounted for up to 50 percent of the exploit kit's activity. This infrastructure reportedly targeted up to 90,000 victims a day and generated over $30 million a year.

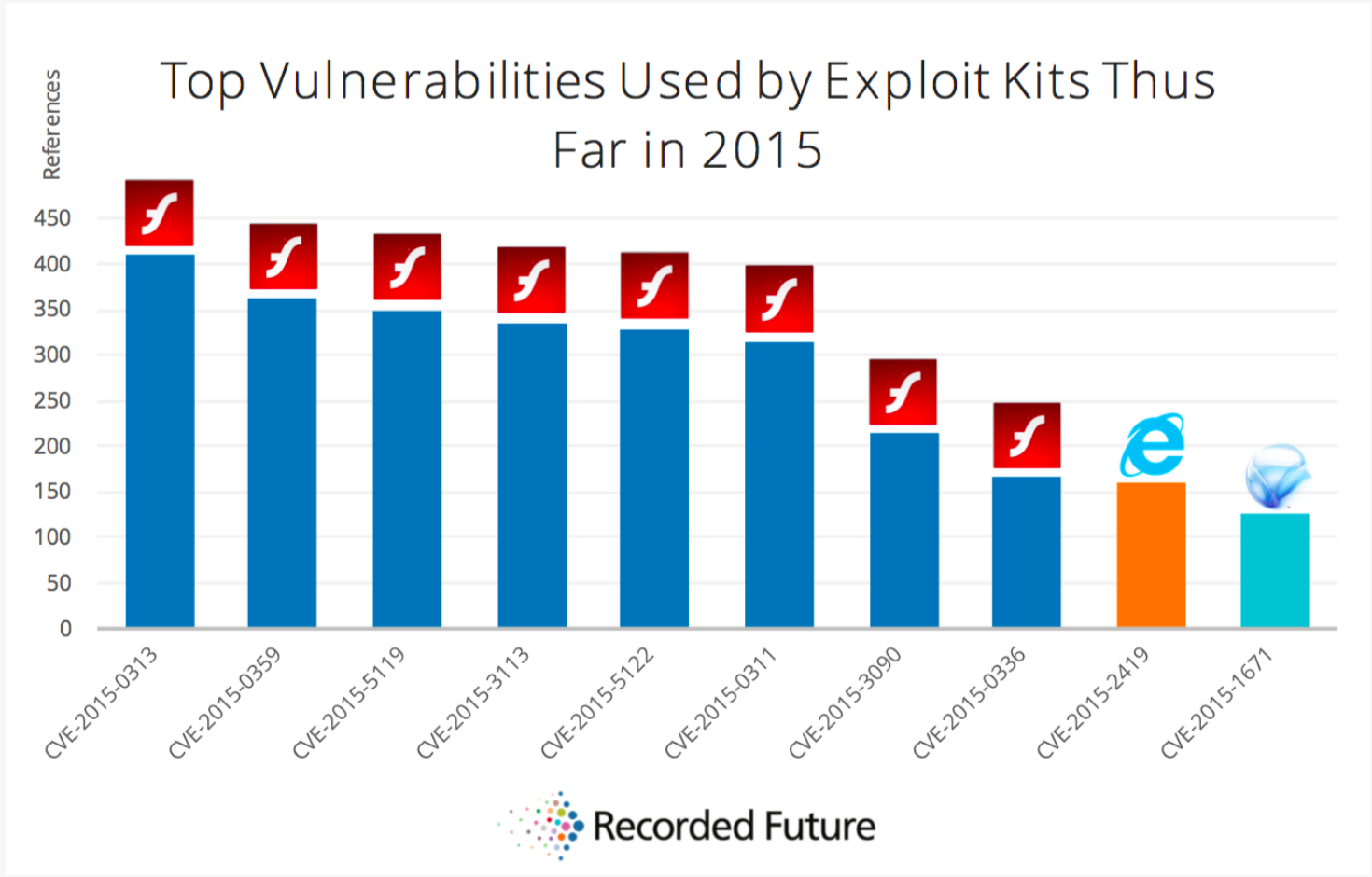
Methodology

Recorded Future analyzed thousands of sources from the Web including .onion site, criminal forums and social media. Analysis focused on exploit kit and vulnerability discussion from January 1, 2015 to September 30, 2015. As part of this research, Recorded Future utilized a list of 108 exploit kits which included well-known EKs such as Angler, Neutrino, Nuclear Pack, etc. Top EK exploited vulnerabilities were ranked by the number of Web references linking them to an exploit kit.

Recorded Future did not reverse engineer any malware mentioned in this analysis and instead performed a meta-analysis of available information from information security blogs, forum postings, etc. Exploits for dozens of other vulnerabilities are currently employed by EKs and this article's intent is to highlight top targets of popular exploit kits.

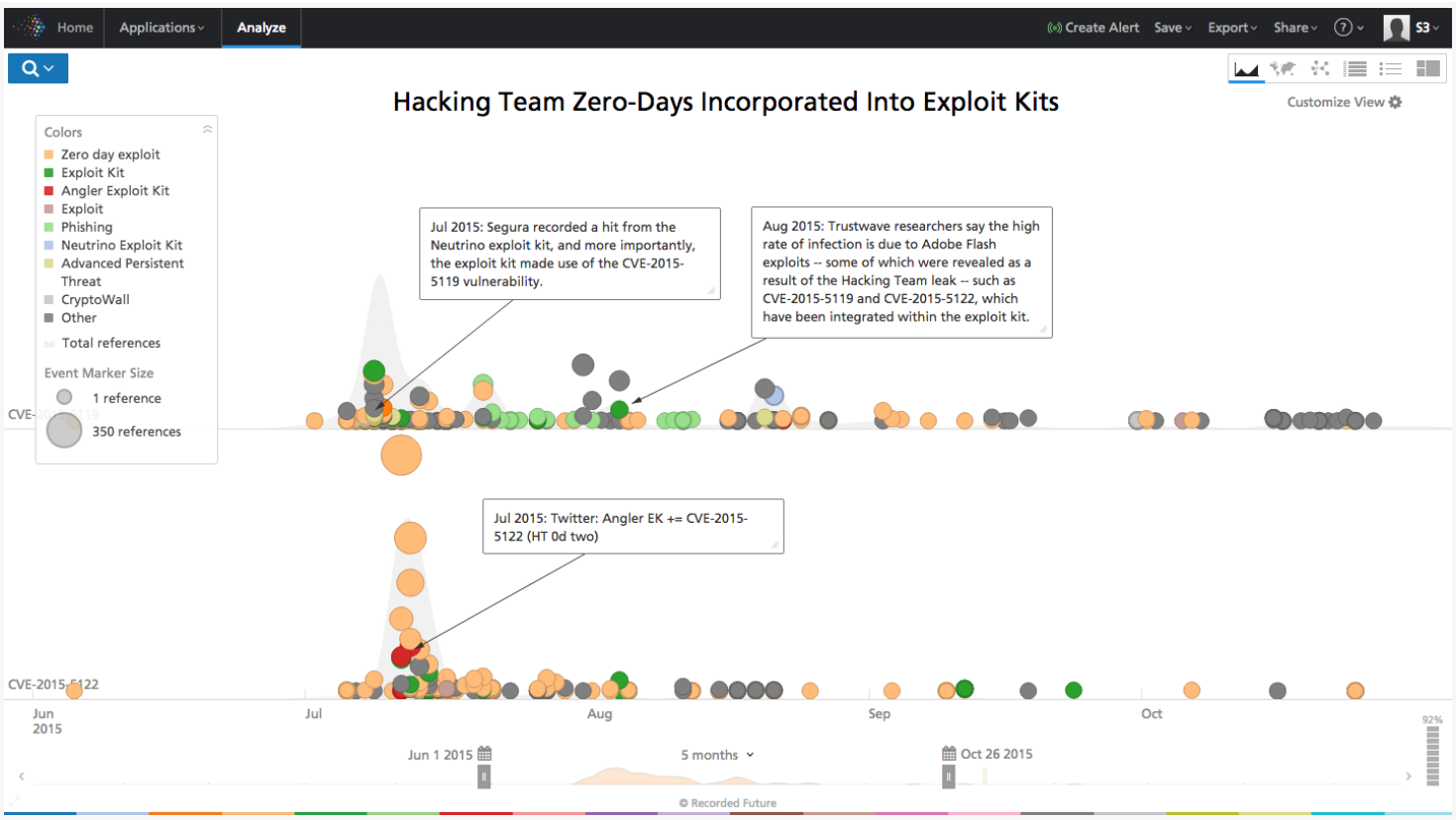
Results

Using this methodology, Recorded Future identified the top vulnerabilities used by exploit kits. Adobe Flash Player vulnerabilities dominated this list with thousands of references.



The top vulnerability CVE 2015-0313 – affecting Flash Player 16.0.0.296 and identified by Adobe as critical – was patched on February 2, 2015 and seen as a zero day exploit as early as December 2014. Recorded Future observed 410 references of CVE-2015-0313 tied to an exploit kit in 2015. This vulnerability has recently been seen in the Hanjuan, Angler and Fiesta EKs.

Exploits tied to the third and fifth most mentioned vulnerabilities (CVE-2015-5119, CVE-2015-5122) were immediately added to EKs including Angler following their disclosure as a Adobe Flash zero-days in the July 2015 Hacking Team leak (http://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-leak-uncovers-another-windows-zero-day-ms-releases-patch/).



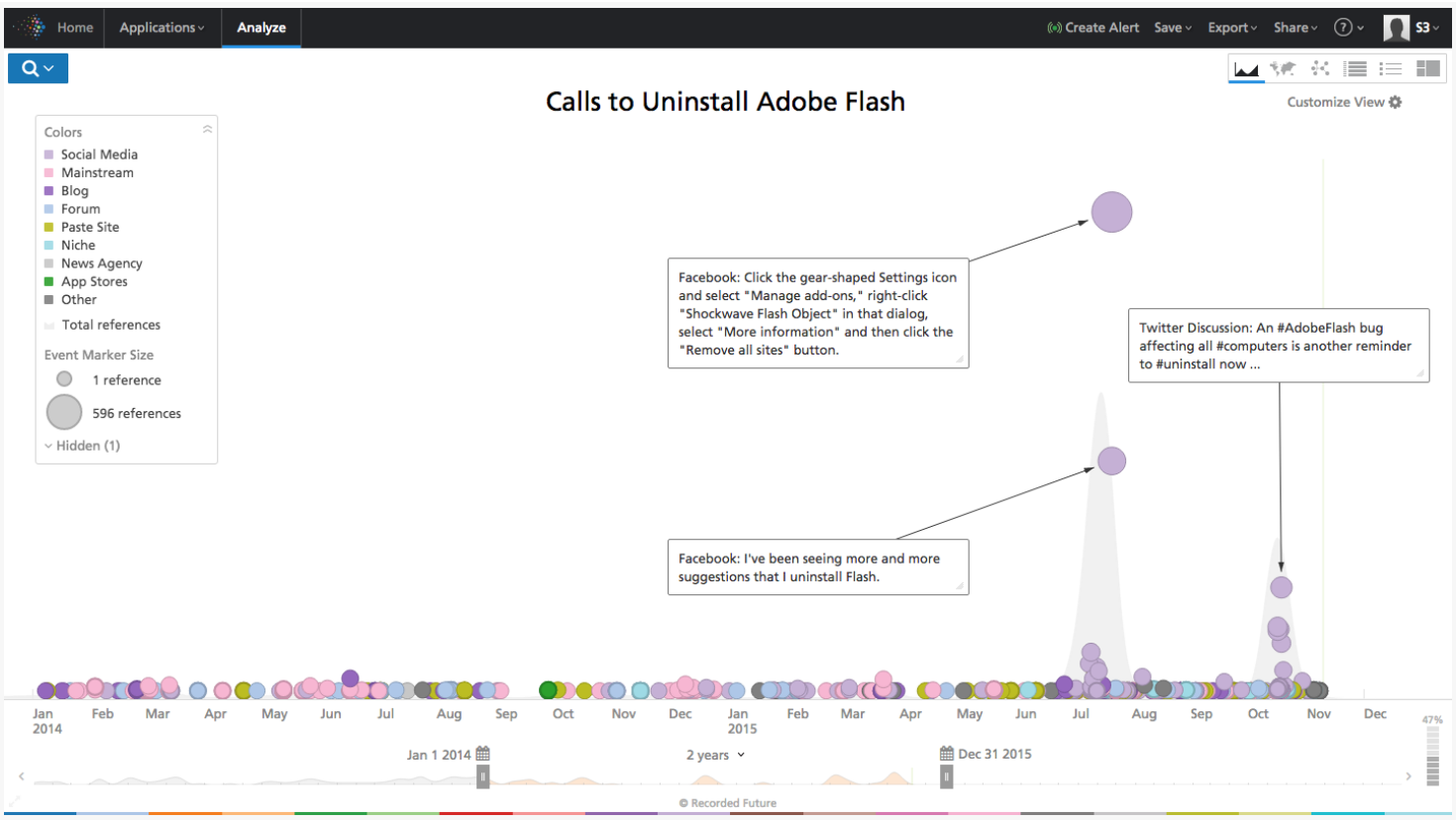
(https://www.recordedfuture.com/assets/top-vulnerabilities-2015-4.png)

CLICK IMAGE FOR LARGER VIEW

Impact

Popular due to compatibility across browsers and operating systems, Adobe Flash Player's recent string of vulnerabilities, and popularity with APT groups such as Pawn Storm, calls into question Flash's place in a secure operating environment.

Flash versions older than 19.0.0.226 (or 18.0.0.255 on older machines) are now actively restricted from running on Apple OS X (http://appleinsider.com/articles/15/10/20/apple-blocks-older-adobe-flash-plug-in-versions-on-os-x). Brian Krebs recently wrote about going a month without Flash (http://krebsonsecurity.com/2015/06/a-month-without-adobe-flash-player/). In July, *WIRED* discussed the Occupy Flash movement and detailed its long line of issues (http://www.wired.com/2015/07/adobe-flash-player-die/).



(https://www.recordedfuture.com/assets/top-vulnerabilities-2015-5.png)

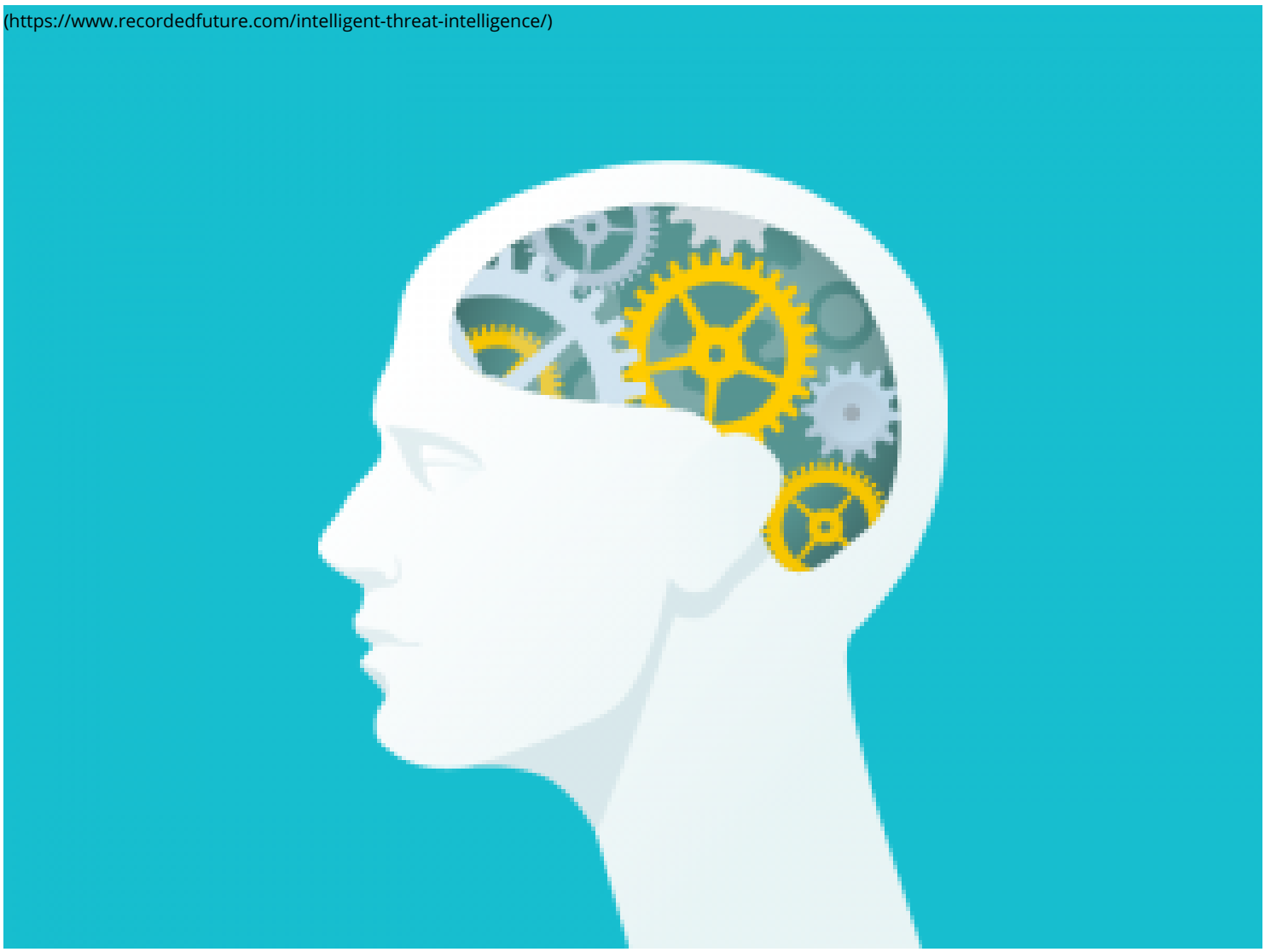
CLICK IMAGE FOR LARGER VIEW

Conclusion

While each organization needs to decide for itself if installing the steady stream of Adobe Flash updates is feasible, steps can be taken as a stop-gap to Adobe exploits. This includes enabling “Click to Play” (http://www.howtogeek.com/188059/how-to-enable-click-to-play-plugins-in-every-web-browser/) which provides a check on use of Adobe Flash Player in an unknown environment.

Related Articles

(https://www.recordedfuture.com/intelligent-threat-intelligence/)



Mind Over Matter: The Importance of Intelligence in Your Threat Program (https://www.recordedfuture.com/intelligent-threat-intelligence/)

Hacker Forum Traffic Analysis: 'Patch Tuesday ... Exploit Wednesday' and Other Patterns (https://www.recordedfuture.com/hacker-forum-traffic/)

The 11-Month Evolution of An0nGhost (https://www.recordedfuture.com/an0nghost-evolution/)

(https://www.recordedfuture.com/opantiisis-cyber-vigilantes/)

Investigating Cyber Vigilantes in #OpAntiISIS (https://www.recordedfuture.com/opantiisis-cyber-vigilantes/)

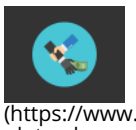
(http://go.recordedfuture.com/cs/c/?cta_guid=49fb5194-0e1d-41bc-a25d-a060183c6ade&placement_guid=a3a005bc-e49a-43b1-a927-bb514f176b59&portal_id=252628&redirect_url=APefjpHJpEPQga7cewHkjNi9KKT0s-E3cXXQuqX4tSY4dw04403tP4Dc7-_ZvoiPkgYYmOUzw-yH5b2Fm9dPVdAVPHXB-TsDpMSCKoNJQ_TU70tZRITZlNjcz0mVGMnhkaK1-8st8jmHQIstXLtvxzJf9qWgYi_H8xP_3HpV2V7qm5vbshFq6siCBB-amLAVwfRxyDg5NJ3IdfGFqYR0DMN29vlJYTmuHjFXEt17RltPxSKO7P5qCSA&hsutk=6997ed892739a5c74c60718a05541277&utm_referrer=https%3A%2vulnerabilities-2015%2F&canon=https%3A%2F%2Fwww.recordedfuture.com%2Ftop-vulnerabilities-2015%2F)

Recent Blog Posts

Gone in a Flash: Top 10 Vulnerabilities Used by Exploit Kits (https://www.recordedfuture.com/top-vulnerabilities-2015/)

By S3 on November 9, 2015


(https://www.recordedfuture.com/top-vulnerabilities-2015/)


Fujitsu UK Tracks Dridex, Using Recorded Future (https://www.recordedfuture.com/fujitsu-uk-tracks-dridex/)

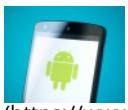
By Nagraj on November 5, 2015

(https://www.recordedfuture.com/fujitsu-uk-tracks-dridex/)


Creating and Delivering Actionable Threat Intelligence (https://www.recordedfuture.com/actionable-threat-intelligence/)

By Greg on November 3, 2015

(https://www.recordedfuture.com/actionable-threat-intelligence/)


Iranian Hackers' Rising Interest in Targeting Android Systems With DroidJack, AndroRAT (https://www.recordedfuture.com/iranian-...

By Rodrigo on October 27, 2015

(https://www.recordedfuture.com/iranian-forums-targeting-android/)

Having Fun (and Learning a Thing or Two) at RFUN 2015 (https://www.recordedfuture.com/rfun-2015/)

By Greg on October 16, 2015

(https://www.recordedfuture.com/rfun-2015/)

Search our blog...

(http://bit.ly/1pV4flS)

(http://feeds.feedblitz.com/recordedfuture) (https://twitter.com/RecordedFuture)

(https://www.facebook.com/RecordedFuture) (https://www.linkedin.com/company/recorded-future)

(http://www.youtube.com/user/RecordedFuture) (https://plus.google.com/+recordedfuture)

See Recorded Future's threat intelligence in action.

RECENT BLOG POSTS (HTTPS://WWW.RECORDEDFUTURE.COM/BLOG/)

Gone in a Flash: Top 10 Vulnerabilities Used by Exploit Kits (https://www.recordedfuture.com/top-vulnerabilities-2015/)

Fujitsu UK Tracks Dridex, Using Recorded Future (https://www.recordedfuture.com/fujitsu-uk-tracks-dridex/)

Creating and Delivering Actionable Threat Intelligence (https://www.recordedfuture.com/actionable-threat-intelligence/)

Iranian Hackers' Rising Interest in Targeting Android Systems With DroidJack, AndroRAT (https://www.recordedfuture.com/iranian-forums-targeting-android/)

@RECORDEDFUTURE (HTTP://WWW.TWITTER.COM/RECORDEDFUTURE/)

#BHEU (http://twitter.com/search?q=%23BHEU) is here! Swing by Booth 401 and hear about real-time threat intelligence. Learn more: https://t.co/UgMLUpjYgJ (https://t.co/UgMLUpjYgJ)

On the right track to a successful threat intelligence program? @robkraus (http://twitter.com/robkraus) of @Solutionary (http://twitter.com/Solutionary) explains how: https://t.co/FZg507ksxm (https://t.co/FZg507ksxm) #InfoSec (http://twitter.com/search?q=%23InfoSec)

Check out Recorded Future in action at #BHEU (http://twitter.com/search?q=%23BHEU). Stop by Booth 401 or schedule a private walkthrough: https://t.co/vANFGCuEYS (https://t.co/vANFGCuEYS) #ThreatIntel (http://twitter.com/search?q=%23ThreatIntel)

RECENT PRESS (HTTPS://WWW.RECORDEDFUTURE.COM/PRESS/)

Critical Fixes for Windows, Adobe Flash Player (http://krebsonsecurity.com/2015/11/critical-fixes-for-windows-adobe-flash-player/)

8 of Top 10 Vulnerabilities Used by Exploit Kits Target Adobe Flash Player (http://www.networkworld.com/article/3003176/security/8-of-top-10-vulnerabilities-used-by-exploit-kits-target-adobe-flash-player.html)

No Surprise Here: Adobe's Flash Is a Hacker's Favorite Target (http://www.pcworld.com/article/3002671/no-surprise-here-adobes-flash-is-a-hackers-favorite-target.html)

Hackers' Threat to Dump 1.2M Stolen TalkTalk Details Online (http://www.thetimes.co.uk/tto/business/industries/telecoms/article4601177.ece)

CUSTOMERS

Login (https://www.recordedfuture.com/live/login/) ›

Support Center (http://support.recordedfuture.com/) ›

Software Status (http://status.recordedfuture.com/) ›

Source Suggestion (https://www.recordedfuture.com/source-suggestion/) ›

Developer Code (https://code.google.com/p/recordedfuture/) ›