Recorded Future

CYBER THREAT ANALYSIS

‘Soft Target: The Top 10 Vulnerabilities Used by Cybercriminals

By Scott Donnelly
Recorded Future

CTA-2018-0327

Executive Summary

Recorded Future's research this year once again highlights the challenges defenders face to make remediation decisions around vulnerabilities without access to all the facts. Official vulnerability databases and even scanning tools cannot arm organizations with one key metric: the overlap between the vulnerabilities in the systems you use and the ones that are being actively exploited by threat actors.

Our analysis of open, deep, and dark web sources identified a shift in preference from Adobe to Microsoft consumer product exploits. Criminal exploit kits and phishing campaigns favored Microsoft products in 2017, with seven of the top 10 vulnerabilities exploited by phishing attacks and exploit kits utilizing Microsoft products, as seen in our rankings (Image 1). This is in stark contrast to our previous rankings (2015, 2016), which saw consistent exploitation of Adobe Flash vulnerabilities.

Analysis of these sources from January 1, 2017 to December 31, 2017 identified Adobe as a still popular but declining avenue of attack, with the remaining three vulnerabilities tied to the aging Flash Player.

Some of this change is due to evolving criminal use of exploited vulnerabilities. Overall, exploit kits are declining as criminal efforts have adapted. This comes as cryptocurrency mining malware popularity rose in the past year. Profiting from cryptocurrency mining has its advantages, including less time spent on collecting victim ransomware payments and the avoidance of rising Bitcoin transaction fees.

Key Judgments

- Microsoft products provided seven of the top 10 vulnerability exploits adopted by exploit kits and phishing campaigns. This is in stark contrast to our previous rankings (2015, 2016) which saw consistent targeting of Adobe Flash exploits.
- For the first time, three vulnerabilities remained on the list. For example, the top exploited vulnerability from 2016, CVE-2016-0189 in Microsoft's Internet Explorer, remained a popular in-road for criminals. Dark web conversations highlighted a lack of new and effective browser exploits.
- In 2017, exploit kits saw a 62 percent decline in development. Only a few exploit kits, including AKBuilder, Disdain, and Terror saw significant activity. Multiple factors, including more specific victim targeting, shifts to more secure browsers, and a rise in cryptocurrency mining malware likely led to the decline.
- Dark web forums and marketplaces continued to offer high and low-quality exploit kit options, with prices ranging from $80 per day for services, to $25,000 for full source-code access.
- Exploit builders for top-ranked Microsoft Office vulnerability CVE-2017-0199 ranged from $400 to $800 in 2017.

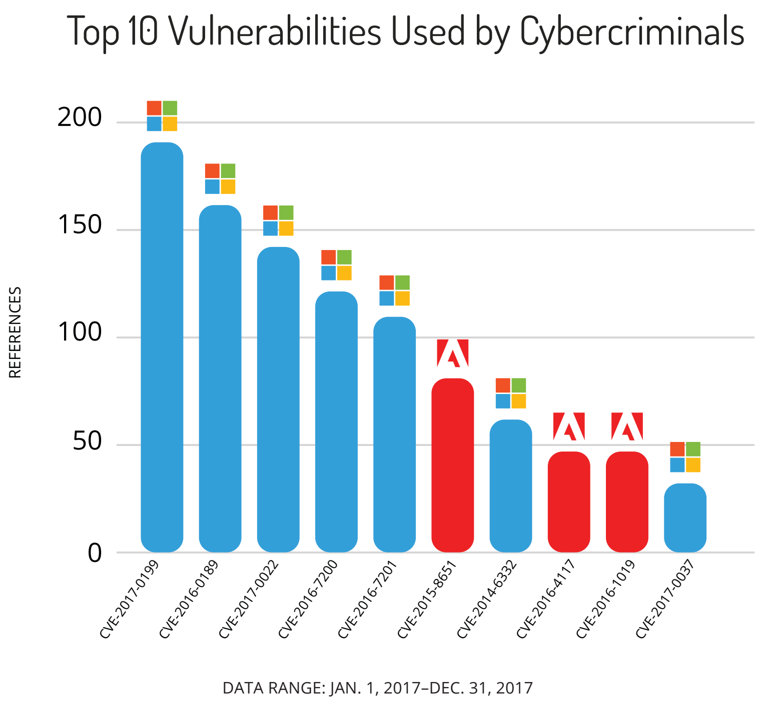


Image 1: References to vulnerability exploitation by exploit kits or phishing.

Background

The goal of this annual list is to provide an account of the most widely adopted vulnerability exploits. Previously, our measurement has focused exclusively on exploit kits, as the criminal market demands continual adoption of exploits for unpatched vulnerabilities. This year, we included phishing attacks and vulnerability co-occurrences to provide a more comprehensive look at criminal attack vectors.

Detailed further in our previous analysis, exploit kits offer a straightforward crimeware-as-a-service channel where users pay per install of their malware. Since the emergence of modern exploit kits in 2006, criminals require less and less personal programming experience, as they only need to provide the payload, such as Matrix ransomware or Dridex banking trojan.

Using a mix of HTML and JavaScript, the exploit kit 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 of the malware.

Our inclusion of phishing attacks this year focuses on email-based campaigns with malicious attachments or links. This includes both targeted campaigns and indirect spam campaigns.

Methodology and Sources

As part of this research, Recorded Future utilized a list of 158 exploit kits. Notably, in 2016, Recorded Future identified 26 new exploit kits. Last year saw a 62 percent drop with only 10 new kits appearing (Image 2). Only a few, including AKBuilder, Disdain, and Terror exploit kits saw significant activity.

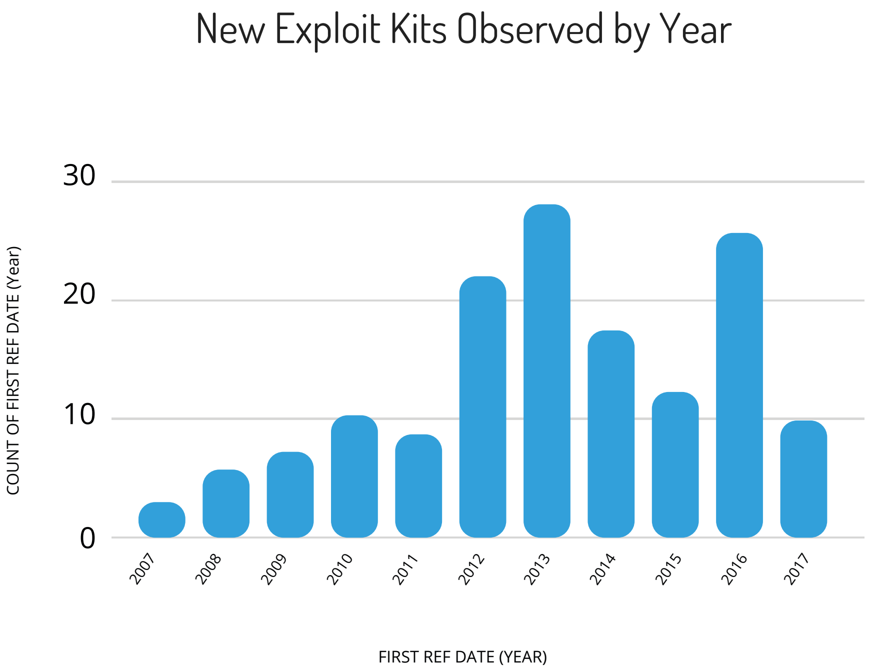


Image 2: Exploit kits observed by year.

Recorded Future did not reverse engineer any malware mentioned in this analysis and instead performed a meta-analysis of available information from the web. Exploits for dozens of other vulnerabilities are currently employed by exploit kits and phishing attacks, and this report's intent is to highlight top criminal exploit targets.

Dozens of major vulnerabilities impacted security operations in 2017, many of which are not included here. This likely includes NSA-sourced Microsoft exploits (MS17-010 linked to WannaCry leaked by Shadow Brokers in April 2017. This vulnerability allowed exploits to self-propagate like a traditional worm and for that reason was not factored into this analysis.

Top Exploits

Our most commonly observed vulnerability was CVE-2017-0199. This weakness affects a slew of Microsoft Office products and allows attackers to download and execute a Visual Basic script containing Powershell commands from a malicious document.

It saw heavy adoption for phishing attacks and we noted a link to 11 distinct pieces of malware during 2017. For instance, exploit builders for CVE-2017-0199 were seen being sold on the dark web for between $400 to $800 at various points in 2017. Purchasing such an exploit builder could support the creation of a payload for a phishing attack.

Our second most frequently cited vulnerability, CVE-2016-0189, also appeared on our 2016 rankings. This Microsoft Internet Explorer vulnerability was a popular avenue for exploit kits in 2017. One example was its adoption by the RIG exploit kit which was known to drop Matrix ransomware in late 2017. This exploit kit and ransomware combination also leveraged Adobe Flash Player's CVE-2015-8651, another returning vulnerability in our rankings.

CVE-2017-0199, CVE-2016-0189, and Adobe Flash Player's CVE-2016-4117 were all associated with 11 different pieces of malware (Image 3). This heavy adoption follows frequent discussion on dark web forums, as all three vulnerabilities had easily obtainable exploit kits, builders, etc.

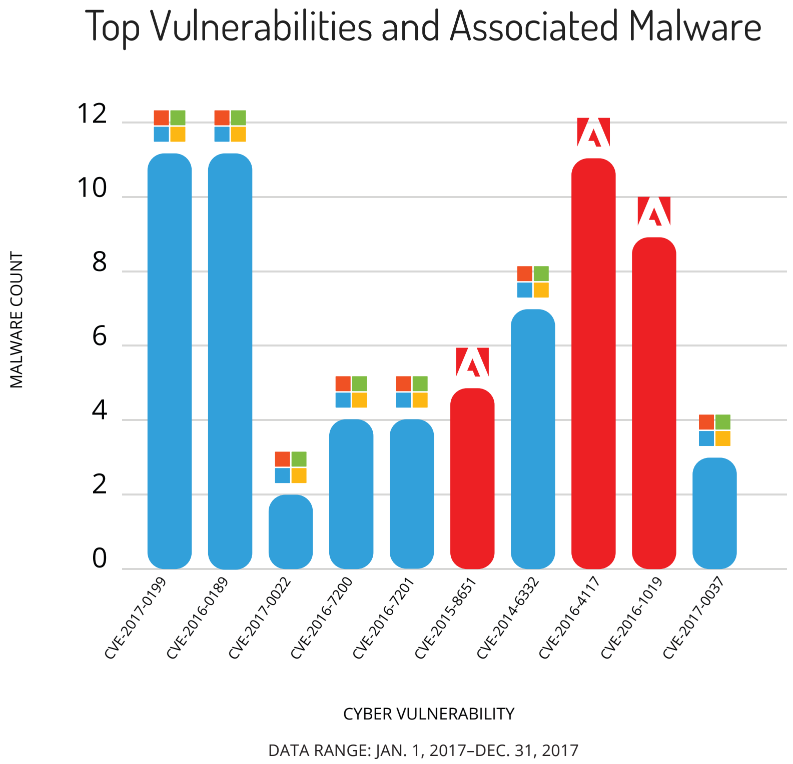


Image 3: Vulnerability with associated malware.

"In the wild" severity does not always correlate with the Common Vulnerability Scoring System (CVSS) score (Image 4). Recorded Future's native risk scoring also takes into consideration criminal adoption, surges in exploit sharing, and links to malware. For example, a Microsoft Windows vulnerability, CVE-2017-0022, was adopted by the Neutrino and Astrum exploit kits, but the vulnerability's CVSS rating is only 4.3 (medium).

CYBER VULNERABILITY	COMPANY	PRODUCT	ASSOCIATED MALWARE	CVSS
CVE-2017-0199	Microsoft	Office	Latentbot Microsoft Word Intruder Hancitor Dridex FinFisher Silent Doc Exploit REMCOS PoohMilk Freenki FreeMilk Cerber	9.3
CVE-2016-0189	Microsoft	Internet Explorer	RIG Exploit Kit Sundown Exploit Kit Magnitude Exploit Kit Terror Exploit Kit Magniber Neutrino Exploit Kit Astrum Exploit Kit Grandsoft Exploit Kit Bleeding Life Exploit Kit Matrix Ransomware Disdain Exploit Kit Kaixin Exploit Kit	7.6
CVE-2017-0022	Microsoft	Windows	Neutrino Exploit Kit Astrum Exploit Kit	4.3
CVE-2016-7200	Microsoft	Edge	Neutrino Exploit Kit Sundown Exploit Kit Kaixin Exploit kit RIG Exploit Kit	7.6
CVE-2016-7201	Microsoft	Edge	Neutrino Exploit Kit Sundown Exploit Kit Kaixin Exploit kit RIG Exploit Kit	7.6
CVE-2015-8651	Adobe	Flash Player	RIG Exploit Kit Astrum Exploit Kit Matrix Ransomware Angler Exploit Kit Ramnit	9.3
CVE-2014-6332	Microsoft	Windows	RIG Exploit Kit Terror Exploit Kit Sundown Exploit Kit Bleeding Life Exploit Kit Astrum Exploit Kit Disdain Exploit Kit Gh0st RAT	9.3
CVE-2016-4117	Adobe	Flash Player	Astrum Exploit Kit Magnitude Exploit Kit Sundown Exploit Kit RIG Exploit Kit Microsoft Word Intruder Neutrino Exploit Kit FinFisher DealersChoice CryptXXX Dridex Kaixin Exploit Kit	10
CVE-2016-1019	Adobe	Flash Player	Magnitude Exploit Kit Astrum Exploit Kit Nuclear Pack Exploit Kit DealersChoice Neutrino Exploit Kit Angler Exploit Kit Pangimop Cerber Locky	10
CVE-2017-0037	Microsoft	Internet Explorer/ Edge	Disdain Exploit Kit Terror Exploit Kit Cerber	7.6

Exploit Kit Development Wanes

A comparative analysis of exploit kit activity between 2015 and 2017 identified a drop in popularity during the last calendar year. In 2017 exploit kits, our previous measure of vulnerability impact saw a significant decline in development. Only 10 new kits appeared in the last year, a 62 percent drop in new exploit kit variants (Image 5).

Multiple factors, including more specific victim targeting, user shifts to more secure browsers, and a rise in cryptocurrency mining malware likely lead to the decline. Late 2017 criminal forum postings suggest a lack of new and effective browser exploits contributes to the decline.

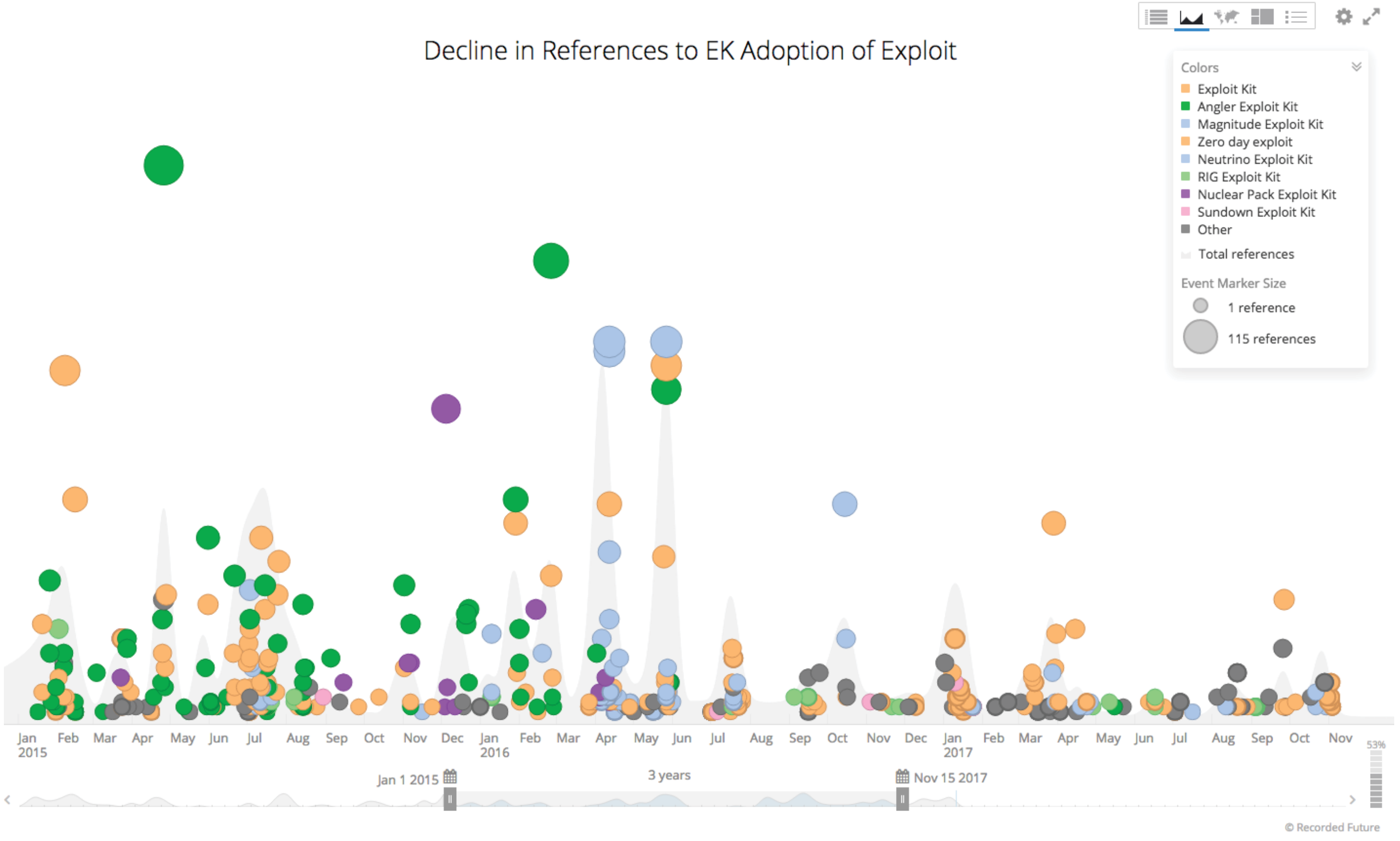
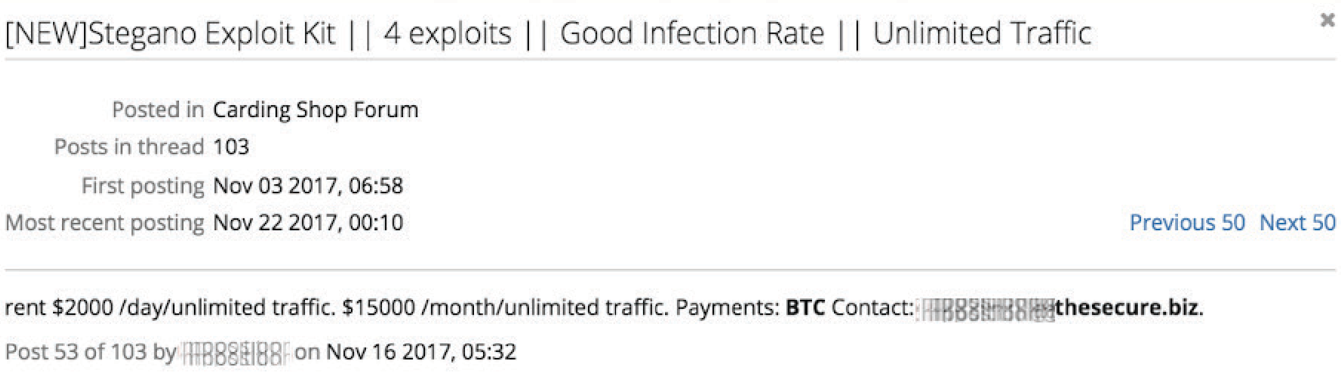


Image 5: 62 percent drop in new exploit kits in 2017.

Down but Not Out

Last year, we profiled RIG and Neutrino exploit kits which filled the void created by Angler exploit kit's June 2016 demise. We saw prices of $200 a week (RIG) to $1,500 a week (Neutrino).

In November 2017, we observed Stegano (Astrum) exploit kit offered for unlimited usage at rates of $2,000 per day or $15,000 per month (Image 6). Stegano leveraged six of the 10 exploits in our report.



[NEW]Stegano Exploit Kit || 4 exploits || Good Infection Rate || Unlimited Traffic

Posted in Carding Shop Forum
Posts in thread 103
First posting Nov 03 2017, 06:58
Most recent posting Nov 22 2017, 00:10

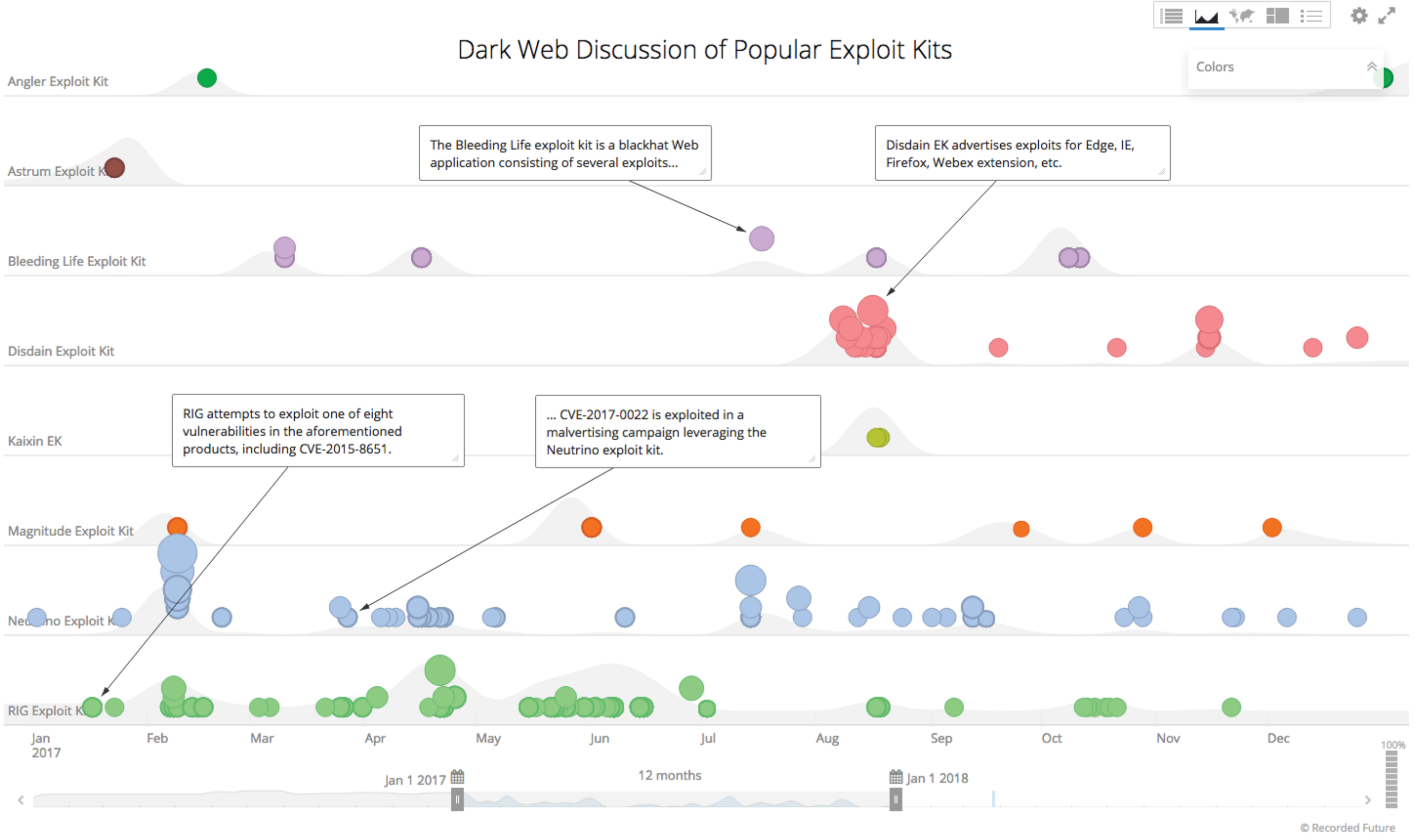
rent $2000 /day/unlimited traffic. $15000 /month/unlimited traffic. Payments: **BTC** Contact: [redacted]**thesecure.biz.**

Post 53 of 103 by [redacted] on Nov 16 2017, 05:32

Image 6: Stegano exploit kit advertisement.

Comparatively, the Disdain exploit kit was offered for $80 per day, $500 per week, $1,400 per month, or $25,000 for the full source code. Forum chatter suggested this was a lower-quality offering.

First appearing in August 2017, Disdain utilized three of the vulnerabilities cited in our report (Microsoft's CVE-2014-6332, CVE-2017-0037, and CVE-2016-0189) and multiple older browser vulnerabilities.



Dark Web Discussion of Popular Exploit Kits

The Bleeding Life exploit kit is a blackhat Web application consisting of several exploits...

Disdain EK advertises exploits for Edge, IE, Firefox, Webex extension, etc.

RIG attempts to exploit one of eight vulnerabilities in the aforementioned products, including CVE-2015-8651.

... CVE-2017-0022 is exploited in a malvertising campaign leveraging the Neutrino exploit kit.

Image 7: Dark web discussions of popular exploit kits.

More Secure Browsing

With Google Chrome usage now nearing 60 percent globally, browsers whose default is “click to play” have taken hold. This secure feature limits the impact of many Adobe Flash Player vulnerabilities used by criminals.

In 2014, 80 percent of desktop Chrome users visited a site with Flash each day, per Google reporting. By July 2017 this number was 17 percent and on the decline. Interestingly, Facebook was the top site with Flash usage by percentage of volume of internet traffic as of late 2017. It was also the top site where users enabled Flash to run.

The drop in overall exploit kit references overlaps with the rapid decline of Flash Player usage. Flash Player exploits, the most popular in-roads for exploit kits in 2015 and 2016, had been plentiful and well packaged due to leaks, including those found in the Hacking Team’s exploit library.

Adobe Flash Player will reach the end of its life in 2020.

Outlook and Recommended Actions

Official vulnerability databases and even scanning tools cannot arm organizations with one key metric: the overlap between the vulnerabilities in the systems you use and the ones that are being actively exploited by threat actors. The goal of this annual list is to provide an account of the most widely adopted vulnerability exploits, in addition to some recommended actions:

- Prioritize patching of all the vulnerabilities identified in this post.
- Remove the affected software if it doesn’t impact key business processes.
- Consider Google Chrome as a primary browser.
- Be aware that Facebook and other social media sites use Flash technology and users frequently enable Flash to run on these sites.
- Utilize browser ad-blockers to prevent exploitation via malvertising.
- Frequently backup systems, particularly those with shared files, which are regular ransomware targets.
- Deliver user training to encourage skepticism of emails requesting additional information or prompting clicks on any links or attachments. Companies will not generally ask customers for personal or financial data, but when in doubt, contact the company directly by phone and confirm if they actually need the information.

Recorded Future

www.recordedfuture.com

@RecordedFuture

About Recorded Future

Recorded Future arms security teams with the only complete threat intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.