



Ethical Hacking Training

OUR STUDENTS HAVE THE HIGHEST EXAM PASS RATE IN THE INDUSTRY!

[View our course](#)

INFOSEC Skills

Outsmart cybercrime with 400+ skill development and certification courses.

[Start your free trial](#)

Which are the weapons in the arsenal of cybercrime gangs? Which are the most exploited vulnerabilities?

To respond to these questions let's analyze the [annual report](#) published by the threat intelligence firm Recorded Future that analyzes Top Ten vulnerabilities used by crooks.

The report is based on the analysis of open, deep, and dark web sources, the analysts observed a significant shift in preference from Adobe to Microsoft exploits.

Seven of the top 10 vulnerabilities exploited by phishing attacks and exploit kits leveraged Microsoft vulnerabilities, an inversion compared with past years which primary saw the exploitation of the Adobe Flash vulnerabilities.

0

0

0

The researchers at Recorded Future monitored the sale of the exploits in the cybercrime underground and [dark web](#), the analysis does not include nation-state activities because third-party suppliers of exploits to a nation-state actor avoid cybercriminal forum.

As anticipated, vulnerabilities in Microsoft software were most exploited by crooks, the researchers observed that Flash exploits had dominated earlier annual reports.

"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," [states the report](#).

"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."

0

Figure 1 - Top 10 Vulnerabilities Used by Cybercriminals 2017 (Recorded Future Report)

The top three vulnerabilities used by cybercriminals are:

- [CVE-2017-0199](#) allows attackers to use a specially-crafted document embedding an OLE2link object to spread malware such as the Dridex banking Trojan.
"While labeled as an Outlook issue, this is actually bug actually stems from an issue within RTF files. According to published reports, the exploit uses an embedded OLE2link object in a specially-crafted document. It should also be noted that these attacks can be thwarted by enabling Office's [Protective View](#) feature. There are updates for both Office and Windows to be applied, and both should be considered necessary for complete protection," reads the [Patch Tuesday analysis by the Zero Day Initiative](#).

The flaw was fixed by Microsoft in April 2017 after [threat actor](#) had been exploiting it in the wild. Hackers leveraged weaponized Rich Text File (RTF) documents exploiting a flaw in Office's Object Linking and Embedding (OLE) interface to deliver malware such as the [Dridex banking Trojan](#). In August 2017, experts from Trend Micro observed crook triggering the flaw to download and execute RATMAN.EXE the command and control (C&C) server. The file used by crooks was a Trojanized version of the legitimate REMCOS remote access tool (RAT). In April security researchers at FireEye discovered that the Microsoft Word CVE-2017-0199 exploit was linked to cyber espionage in Ukraine conflict. In May, Malware researchers at security firm ProofPoint reported the Chinese TA459 APT had exploited the CVE-2017-0199 vulnerability to target Financial firms. These last two cases demonstrated that nation-state attackers also used exploit kits in their campaigns.

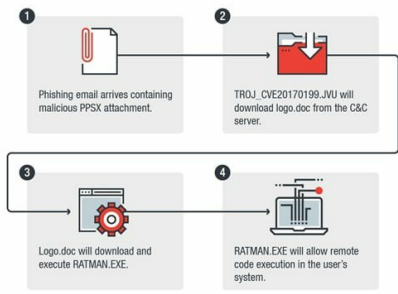


Figure 2 - CVE-2017-0199 attack exploitation (Trend Micro)

- [CVE-2016-0182](#) is an old flaw affecting Internet Explorer that was exploited by attackers to drop malware. We have reported cases in which the flaw was triggered to deliver the [Matrix ransomware](#), to drop [Monero cryptocurrency Miner](#) in Neptune Exploit Kit or [Disdain exploit kit](#) campaigns.
- [CVE-2017-0022](#) is an XML Core Services information disclosure vulnerability that can be exploited by attackers by tricking victims into clicking on a specially crafted link.
"An information vulnerability exists when [Microsoft XML Core Services \(MSXML\)](#) improperly handles objects in memory. Successful exploitation of the vulnerability could allow the attacker to test for the presence of files on disk," reads the [security advisory](#) published by Microsoft.

"To exploit the vulnerability, an attacker could host a specially-crafted website that is designed to invoke MSXML through Internet Explorer. However, an attacker would have no way to force a user to visit such a website. Instead, an attacker would typically have to convince a user to either click a link in an email message or a link in an Instant Messenger request that would then take the user to the website."

The flaw was discovered by a joint investigation conducted by security researchers at [Trend Micro](#) and [ProofPoint](#), it was reported to Microsoft in September 2016.

ETHICAL HACKING TRAINING - RESOURCES (INFOSEC)

Earn your CEH, guaranteed!

Complete the form below to receive course pricing

FIRST NAME

LAST NAME

EMAIL

PHONE

ORGANIZATION

INTERESTED IN STUDENT FINANCING?

WHO WILL FUND YOUR TRAINING?

TRAINING BUDGET

According to the security researchers at Trend Micro, the zero-day vulnerability has been exploited in the [AdCholas](#) malvertising campaign since July 2016. The exploit code of the flaw was added to the [Neutrino exploit kit](#) in September 2016.

"This vulnerability was used in the AdCholas malvertising campaign and later integrated into the Neutrino exploit kit. CVE-2017-0022 likely replaced the similar CVE-2016-3298 and CVE-2016-3351 vulnerabilities from the same campaign, which were addressed by previous patches," reads the [analysis](#) published by TrendMicro.

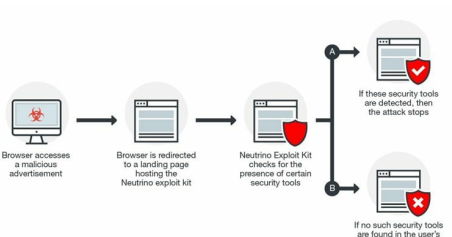


Figure 3 - AdCholas malvertising campaign

"An attacker exploiting CVE-2017-0022 could use phishing attacks to lure potential targets to malicious websites. Successful exploitation of this vulnerability could allow a cybercriminal access to information on the files found in the user's system," explained the experts from TrendMicro. "In particular, the attacker would be able to detect if the system is using specific security solutions—especially ones that analyze malware."

According to Recorded Future's report, in 2017 the researchers have observed a significant drop in the development of new exploit kits.

The experts noticed a 62 percent decline in the development of exploit kits, they observed only a few new EKs in the threat landscape, including AKBuilder, [Disdain](#) and [Terror Ek](#). The experts pointed out that multiple factors have caused the drop, including more specific victim targeting, shifts to more secure browsers, and a rise in cryptocurrency mining malware likely led to the decline.

"Overall, exploit kits are declining as criminal efforts have adapted. This comes as cryptocurrency mining malware popularity rose in the past year," continues the report.

The report states that in 2017 the number of new exploit kits was 10 out of a total list of 158 EKs, experts highlighted that the drop-in exploit kit activity also overlaps with the decline of Flash Player usage, many EKs included the codes to trigger the flaws in Adobe products.

According to the experts, users have shifted to more secure web browsers making hard for attackers the development of new efficient exploit kits.

Another element that influenced the drop of the EK was the spikes in cryptocurrency mining malware that were more profitable for crooks.

The researchers also investigated how the malware exploited the flaws and how crooks used them.

The vulnerability CVE-2017-0199 was heavily used in phishing campaigns: Recorded Future linked it to 11 distinct strain of malware during 2017.

The second most frequently used vulnerability, CVE-2016-0189, was associated with the [RIG exploit kit](#) to deliver ransomware.

Let's close with the analysis of the economic value of exploit codes for top 2017 vulnerabilities. It was quite easy to find high, and low-quality exploit kit in the [Dark web](#) forums and [marketplaces](#), with prices ranging from \$80 per day for services to \$25,000 for full source-code access.

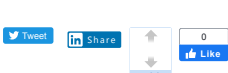
"In November 2017, we observed Stegano (Astrum) exploit kit offered for unlimited usage at rates of \$2,000 per day or \$15,000 per month (Image 6). Stegano leveraged six of the 10 exploits in our report."

It is also interesting to note that Exploit builders for Microsoft Office vulnerability CVE-2017-0199 ranged from \$400 to \$800 in 2017. Purchasing such an exploit builder could support the creation of a payload for a phishing attack.

Now that we know which were the most exploited vulnerabilities in 2017 let's adopt all necessary countermeasures to prevent further attacks in the incoming months.

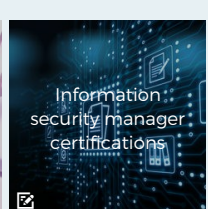
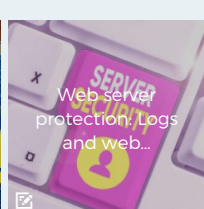
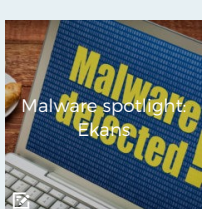
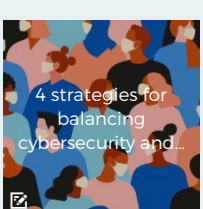
References

- <https://go.recordedfuture.com/hubs/reports/cta-2018-0327.pdf>
- <https://securityaffairs.co/wordpress/62028/cyber-crime/powerpoint-slide-show-exploit.html>
- <http://securityaffairs.co/wordpress/57947/hacking/microsoft-patch-tuesday.html>
- <https://securityaffairs.co/wordpress/57985/cyber-crime/cve-2017-0199-finspy-spyware.html>
- <https://securityaffairs.co/wordpress/58692/malware/ta459-apt-targets-financial-firms.html>
- <https://securityaffairs.co/wordpress/57408/cyber-crime/cve-2017-0022-flaw-adcholas.html>



Pierluigi Paganini

Pierluigi Paganini is CTO at Cybase Enterprise SpA. Pierluigi is member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group, member of Cyber G7 Workgroup of the Italian Ministry of Foreign Affairs and International Cooperation, Professor and Director of the Master in Cyber Security at the Link Campus University. He is also Security Evangelist, Security Analyst and Freelance Writer, Editor-in-Chief at Cyber Defense Magazine". Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTE, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines.



Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

Save my name, email, and website in this browser for the next time I comment.

0 = 18

Post Comment

About Infosec

At Infosec, we believe knowledge is the most powerful tool in the fight against cybercrime. We provide the best certification and skills development training for IT and security professionals, as well as employee security awareness training and phishing simulations. Learn more at [infosecinstitute.com](#)

Connect with us

Stay up to date with [infosec](#)

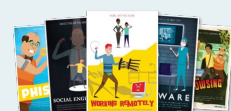
[Like Us](#) [Follow @infoseciq](#)

Join our newsletter

Get the latest news, updates & offers straight to your inbox.

ENTER YOUR EMAIL

SUBSCRIBE



We made security awareness & training easy

Get a 12-month security awareness plan sent directly to your inbox!

Enter your work email here...

Download