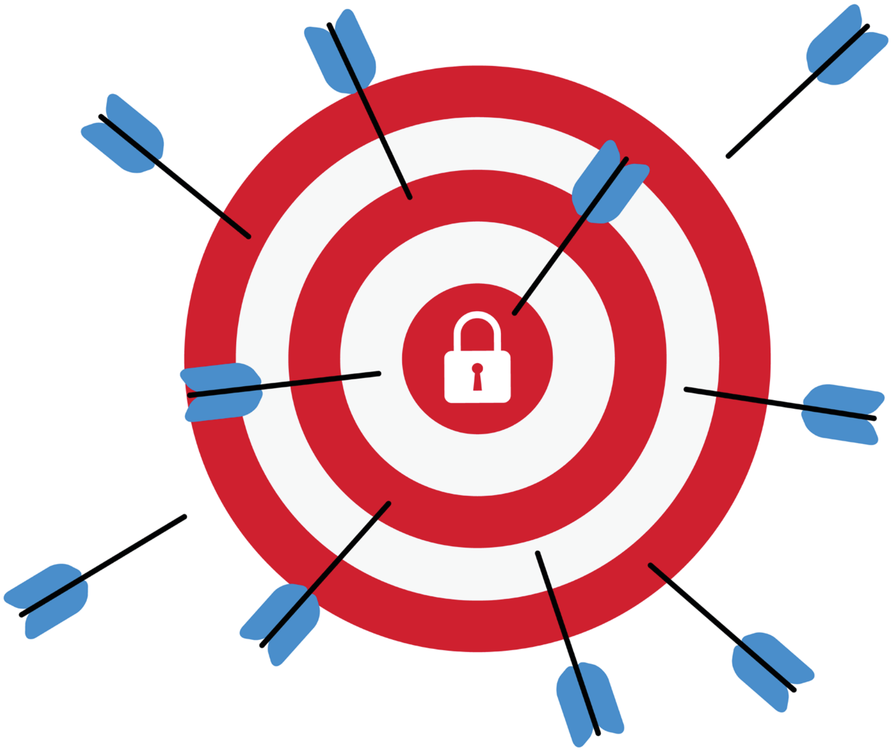
Recorded Future

Microsoft Targeted by 8 of 10 Top Vulnerabilities in 2018

By Kathleen Kuczma



2019-0319

This analysis focuses on an exploit kit, phishing attack, or remote access trojan co-occurrence with a vulnerability from January 1, 2018 to December 31, 2018. We analyzed thousands of sources, including code repositories, deep web forum postings, and dark web sites. This is a follow-up to our 2017 report, and the intended audience includes information security practitioners, especially those supporting vulnerability risk assessments.

Executive Summary

Many vulnerability management practitioners face the daunting task of prioritizing vulnerabilities without adequate insight into which vulnerabilities are actively exploited by cybercriminals. Here, we'll attempt to shed light on this by determining the top 10 vulnerabilities from 2018. It is imperative that security professionals have insight into those vulnerabilities that impact a company's technology stack and are included in exploit kits, used to distribute a remote access trojan (RAT), or are currently being used in phishing attacks.

In 2018, we observed more exploits targeting Microsoft products than Adobe ones. Eight out of 10 vulnerabilities exploited via phishing attacks, exploit kits, or RATs targeted Microsoft products, and only one Adobe Flash vulnerability made the top 10, likely due to a combination of better patching and Flash Player's impending demise in 2020.

Like in past years, the development of new exploit kits has continued to drop amid the shift to more targeted attacks and less availability of zero-day vulnerabilities. Exploit kits in previous years took advantage of Adobe product vulnerabilities, which have continued to dwindle.

Key Judgments

- For the second year in a row, Microsoft was consistently targeted the most, with eight of the top 10 vulnerabilities impacting its products. In 2017, seven of the top 10 vulnerabilities also affected Microsoft. Conversely, the majority of 2016 and 2015's top vulnerabilities targeted Adobe Flash Player.

- Like 2017's report, only a few vulnerabilities from past reports remained in the top exploited vulnerabilities. CVE-2017-0199, last year's top exploited vulnerability, which impacted Microsoft Office, moved to fifth place, with its continued inclusion in the ThreadKit exploit kit. CVE-2016-0189, the top vulnerability in 2016 and ranked second in 2017, was still associated with five different exploit kits. On average, vulnerabilities have an average life expectancy of nearly seven years, per a 2017 RAND report.
- The number of new exploit kits continued to drop in 2018 by 50 percent, with only five new exploit kits, compared to 10 the year before. Two of these exploit kits were associated with 2018's top exploited vulnerabilities: Fallout and LCG Kit. As in previous years, similar trends continue to impact the downward trend of exploit kits, including shifts to more secure browsers and specific victim targeting.
- With this year's inclusion of RATs, 35 new RATs were released in 2018, versus 47 in 2017. Only one of these new RATs, Sisfader, was associated with a top vulnerability: CVE-2017-8750, a Microsoft Office exploit.
- One exploit kit, ThreadKit, stood out for its number of references on the dark web compared to other exploit kits. As of December 31, 2018, ThreadKit contained four of the top 10 vulnerabilities and was last selling on the dark web for $400.

Cyber Vulnerability	References	Company
CVE-2018-8174	567	Microsoft
CVE-2018-4878	387	Adobe
CVE-2017-11882	223	Microsoft
CVE-2017-8750	192	Microsoft
CVE-2017-0199	91	Microsoft
CVE-2016-0189	78	Microsoft
CVE-2017-8570	68	Microsoft
CVE-2018-8373	66	Microsoft
CVE-2012-0158	55	Microsoft
CVE-2015-1805	49	Google Android

Background

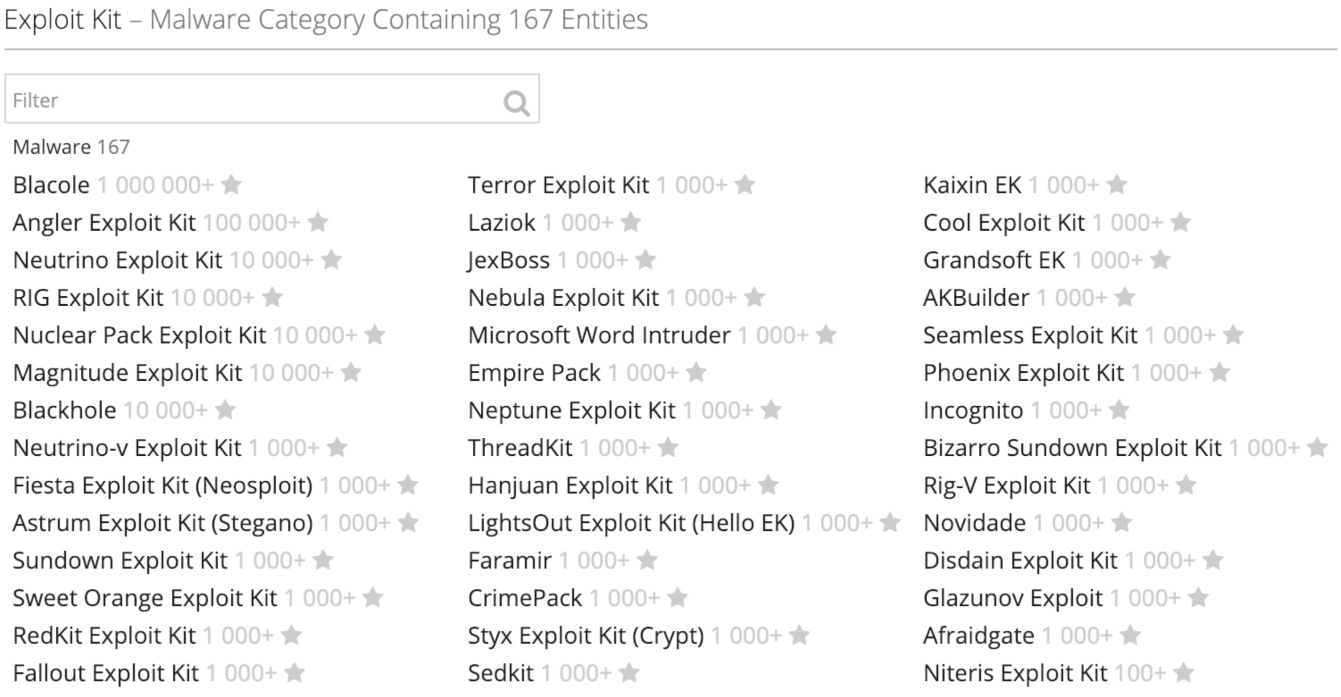
Recorded Future continued to expand the breadth of its annual list of top 10 vulnerabilities by adding RATs, in addition to co-occurrence with exploits or phishing attacks, which were added in 2017. Like other years, the goal of this list is to highlight the vulnerabilities most exploited by the criminal underground. While the leak of nation state-related exploits made headlines in 2018, Recorded Future did not see evidence that these exploits were highly used by the criminal underground and thus are not a focus in this analysis.

The list continued to analyze occurrences of vulnerabilities with exploit kits, as done in the past three years' reports. Since the emergence of exploit kits in 2006, cybercriminals require less coding experience to take advantage of this straightforward crimeware-as-a-service channel.

The inclusion of RATs provides an additional malware category to determine which vulnerabilities were the most frequent in 2018. RATs have been a mainstay for cybercriminals, as they can provide the attacker with complete control over a victim's computer.

Methodology and Sources

Recorded Future utilized a list of 167 exploit kits as one of the parameters to determine the top referenced and exploited vulnerabilities of 2018. Only five new exploit kits were created in 2018, compared to 10 in 2017.



Exploit Kit – Malware Category Containing 167 Entities

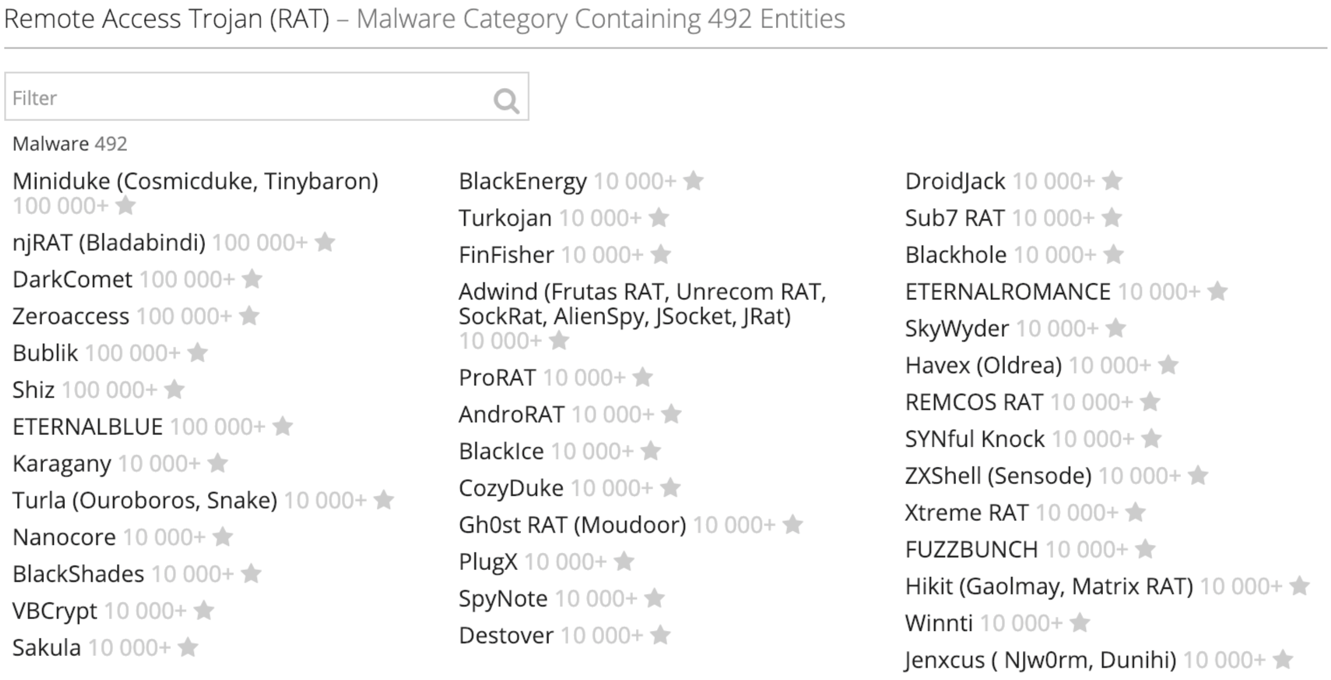
Filter

Malware 167

Blacole	1 000 000+	★
Angler Exploit Kit	100 000+	★
Neutrino Exploit Kit	10 000+	★
RIG Exploit Kit	10 000+	★
Nuclear Pack Exploit Kit	10 000+	★
Magnitude Exploit Kit	10 000+	★
Blackhole	10 000+	★
Neutrino-v Exploit Kit	1 000+	★
Fiesta Exploit Kit (Neosploit)	1 000+	★
Astrum Exploit Kit (Stegano)	1 000+	★
Sundown Exploit Kit	1 000+	★
Sweet Orange Exploit Kit	1 000+	★
RedKit Exploit Kit	1 000+	★
Fallout Exploit Kit	1 000+	★
Terror Exploit Kit	1 000+	★
Laziok	1 000+	★
JexBoss	1 000+	★
Nebula Exploit Kit	1 000+	★
Microsoft Word Intruder	1 000+	★
Empire Pack	1 000+	★
Neptune Exploit Kit	1 000+	★
ThreadKit	1 000+	★
Hanjuan Exploit Kit	1 000+	★
LightsOut Exploit Kit (Hello EK)	1 000+	★
Faramir	1 000+	★
CrimePack	1 000+	★
Styx Exploit Kit (Crypt)	1 000+	★
Sedkit	1 000+	★
Kaixin EK	1 000+	★
Cool Exploit Kit	1 000+	★
Grandsoft EK	1 000+	★
AKBuilder	1 000+	★
Seamless Exploit Kit	1 000+	★
Phoenix Exploit Kit	1 000+	★
Incognito	1 000+	★
Bizarro Sundown Exploit Kit	1 000+	★
Rig-V Exploit Kit	1 000+	★
Novidade	1 000+	★
Disdain Exploit Kit	1 000+	★
Glazunov Exploit	1 000+	★
Afraidgate	1 000+	★
Niteris Exploit Kit	100+	★

Exploit kit category in Recorded Future containing dozens of exploits.

This year's report also included RATs when determining the top exploited vulnerabilities. Recorded Future used its repository of 492 RATs. RATs were added in part because of the increase in their usage due to their role as a multipurpose malware.



Remote Access Trojan (RAT) – Malware Category Containing 492 Entities

Filter

Malware 492

Miniduke (Cosmicduke, Tinybaron)	100 000+	★
njRAT (Bladabindi)	100 000+	★
DarkComet	100 000+	★
Zeroaccess	100 000+	★
Bublik	100 000+	★
Shiz	100 000+	★
ETERNALBLUE	100 000+	★
Karagany	10 000+	★
Turla (Ouroboros, Snake)	10 000+	★
Nanocore	10 000+	★
BlackShades	10 000+	★
VBCrypt	10 000+	★
Sakula	10 000+	★
BlackEnergy	10 000+	★
Turkojan	10 000+	★
FinFisher	10 000+	★
Adwind (Frutas RAT, Unrecom RAT, SockRat, AlienSpy, JSocket, JRat)	10 000+	★
ProRAT	10 000+	★
AndroRAT	10 000+	★
BlackIce	10 000+	★
CozyDuke	10 000+	★
Gh0st RAT (Moudoor)	10 000+	★
PlugX	10 000+	★
SpyNote	10 000+	★
Destover	10 000+	★
DroidJack	10 000+	★
Sub7 RAT	10 000+	★
Blackhole	10 000+	★
ETERNALROMANCE	10 000+	★
SkyWyder	10 000+	★
Havex (Oldrea)	10 000+	★
REMCOS RAT	10 000+	★
SYNful Knock	10 000+	★
ZXShell (Sensode)	10 000+	★
Xtreme RAT	10 000+	★
FUZZBUNCH	10 000+	★
Hikit (Gaolmay, Matrix RAT)	10 000+	★
Winnti	10 000+	★
Jenxcus (NJw0rm, Dunihi)	10 000+	★

RAT malware category in Recorded Future.

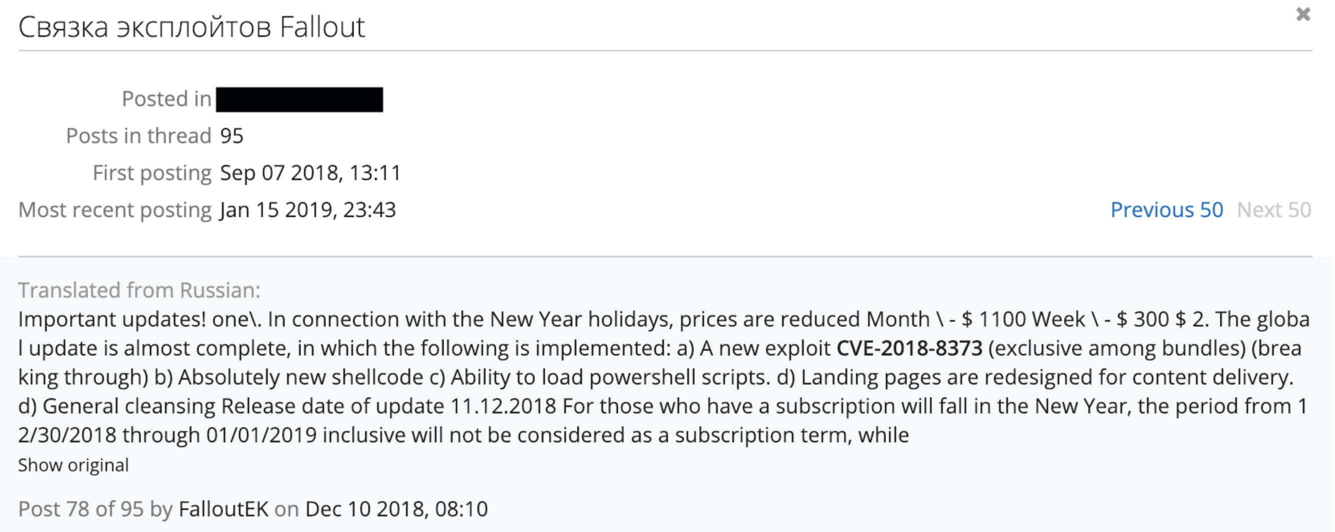
A few vulnerabilities were not included in the top 10 due to adoption by nation-state actors as opposed to use by the criminal underground: ETERNALBLUE and Spectre/Meltdown. The ETERNALBLUE exploit (which used MS17-010), while often mentioned, was not used by the criminal underground or offered for sale as a part of other exploit kits. Spectre, while noted in a few phishing attacks, was also not heavily used by cybercriminals. One possible reason why is that these exploits are more sophisticated and difficult to use versus typical exploit kits, which were once prolific due to their ease of use. However, as shown by Recorded Future's previous research on top vulnerabilities, the emergence of new exploit kits continues to decrease.

As this annual list is based off metadata analysis of available information from open, deep, and dark web sources, Recorded Future did not reverse-engineer any malware mentioned in this piece. Instead, the aim of this report is to showcase the most exploited vulnerabilities.

Last Year's Top Exploited Vulnerabilities

The top exploited vulnerability on the list, CVE-2018-8174, a Microsoft Internet Explorer vulnerability nicknamed "Double Kill," was included in four exploit kits (RIG, Fallout, KaiXin, and Magnitude). Exploit kits associated with this vulnerability were noted to spread the malware Trickbot through phishing attacks. The Magnitude exploit kit delivered Magniber ransomware, which primarily targeted users in Asia where computer default languages were in Korean, Chinese, or Malay.

CVE-2018-4878 was the second most commonly observed vulnerability and is the only Adobe Flash Player vulnerability on this year's top 10. Like CVE-2018-8174, this vulnerability was included in multiple exploit kits, most notably the Fallout exploit kit, which was used to distribute GandCrab ransomware. Fallout took its name and URI patterns from the now defunct Nuclear exploit kit, which had been associated with CVE-2015-7645, one of 2016's top 10 vulnerabilities. In 2018, Fallout was last selling for $300 a week and $1,100 a month, as seen below.



Связка эксплойтов Fallout

Posted in [redacted]
Posts in thread 95
First posting Sep 07 2018, 13:11
Most recent posting Jan 15 2019, 23:43

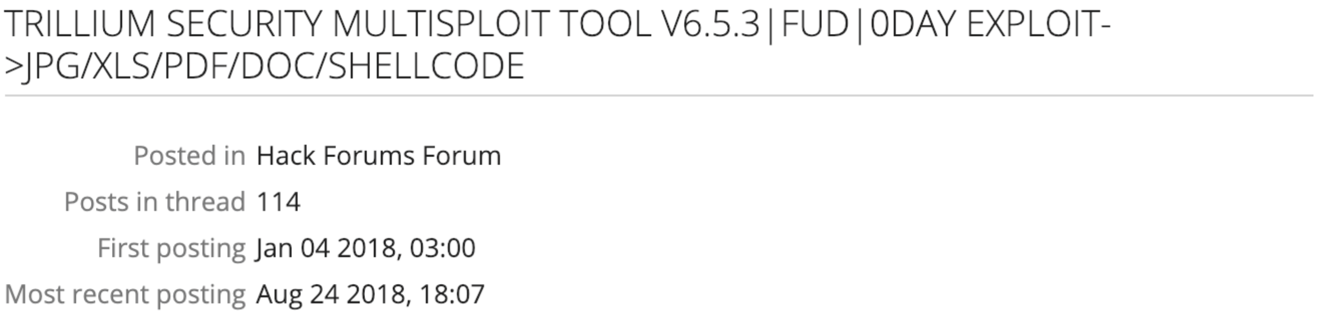
Translated from Russian:
Important updates! one\. In connection with the New Year holidays, prices are reduced Month \ - $ 1100 Week \ - $ 300 $ 2. The global update is almost complete, in which the following is implemented: a) A new exploit **CVE-2018-8373** (exclusive among bundles) (breaking through) b) Absolutely new shellcode c) Ability to load powershell scripts. d) Landing pages are redesigned for content delivery. d) General cleansing Release date of update 11.12.2018 For those who have a subscription will fall in the New Year, the period from 12/30/2018 through 01/01/2019 inclusive will not be considered as a subscription term, while

Post 78 of 95 by FalloutEK on Dec 10 2018, 08:10

Last price update for the Fallout exploit kit by FalloutEK.

For the first time, a vulnerability has made the top 10 vulnerability list three years in a row — CVE-2016-0189. Why has this vulnerability persisted? For starters, CVE-2016-0189 is not dependent on one version of Internet Explorer (it impacts IE 9 through 11), resulting in a more reliable vulnerability to exploit. Because of this versatility, the vulnerability has been successfully incorporated into a variety of various exploit kits over the years, as many as five in 2018 (Underminer, Magnitude, Grandsoft, KaiXin, and RIG). Additionally, there are no mitigating factors available to prevent CVE-2016-0189 — the only workarounds are restricting access to two common dynamic-linked library files: VBScript.dll and JScript.dll.

Two vulnerabilities were associated with numerous pieces of malware: CVE-2017-11882 and CVE-2017-0199. These vulnerabilities were associated with 10 and eight pieces of malware, respectively. Both were used in Trillium's Security Multisploit Tool, which included four of the top 10 vulnerabilities. This tool was heavily discussed and advertised on Hack Forums and Nulled Forum, and received positive reviews. CVE-2017-0199 was notably used by Gorgon Group, a threat group operating out of Pakistan which targeted government organizations in the U.K. and United States, among others, through targeted spearphishing attacks.



TRILLIUM SECURITY MULTISPLOIT TOOL V6.5.3|FUD|0DAY EXPLOIT->JPG/XLS/PDF/DOC/SHELLCODE

Posted in	Hack Forums Forum
Posts in thread	114
First posting	Jan 04 2018, 03:00
Most recent posting	Aug 24 2018, 18:07

Post on Trillium's Security Multisplit Tool as seen on numerous dark web forums.

Cyber Vulnerability	Malware Count
CVE-2018-8174	7
CVE-2018-4878	4
CVE-2017-11882	10
CVE-2017-8750	4
CVE-2017-0199	8
CVE-2016-0189	5
CVE-2017-8570	4
CVE-2018-8373	1
CVE-2012-0158	1
CVE-2015-1805	1

Cyber Vulnerability	Company	Product	Associated Malware	CVSS	Recorded Future Risk Score
CVE-2018-8174	Microsoft	Internet Explorer	Fallout Exploit Kit, KaiXin Exploit Kit, LCG Kit Exploit Kit, Magnitude Exploit Kit, RIG Exploit Kit, Trickbot, Underminer Exploit Kit	7.6	89
CVE-2018-4878	Adobe	Flash Player	Fallout Exploit Kit, GreenFlash Exploit Kit, Hermes Ransomware, Sundown Exploit Kit, Threadkit Exploit Kit	7.5	89
CVE-2017-11882	Microsoft	Office	AgentTesla, Andromeda, BONDUPDATER, HAWKEYE, LCG Kit, Loki, POWRUNNER, QuasarRAT, REMCOS RAT, ThreadKit Exploit Kit	9.3	99
CVE-2017-8750	Microsoft	Office	Formbook, Loki, QuasarRAT	7.6	89
CVE-2017-0199	Microsoft	Office	DMShell++, njRAT, Pony, QuasarRAT, REMCOS RAT, SHUTTERSPEED, Silent Doc Exploit Kit, Threadkit Exploit Kit	9.3	99
CVE-2016-0189	Microsoft	Internet Explorer	Grandsoft Exploit Kit, KaiXin Exploit Kit, Magnitude Exploit Kit, RIG Exploit Kit, Underminer Exploit Kit	7.6	89
CVE-2017-8570	Microsoft	Office	Formbook, QuasarRAT, Sisfader RAT, Threadkit Exploit Kit, Trickbot	9.3	99
CVE-2018-8373	Microsoft	Internet Explorer	Quasar RAT	7.6	89
CVE-2012-0158	Microsoft	Office	Silent Doc Exploit, PlugX	9.3	89
CVE-2015-1805	Google	Android	AndroRAT	7.2	89

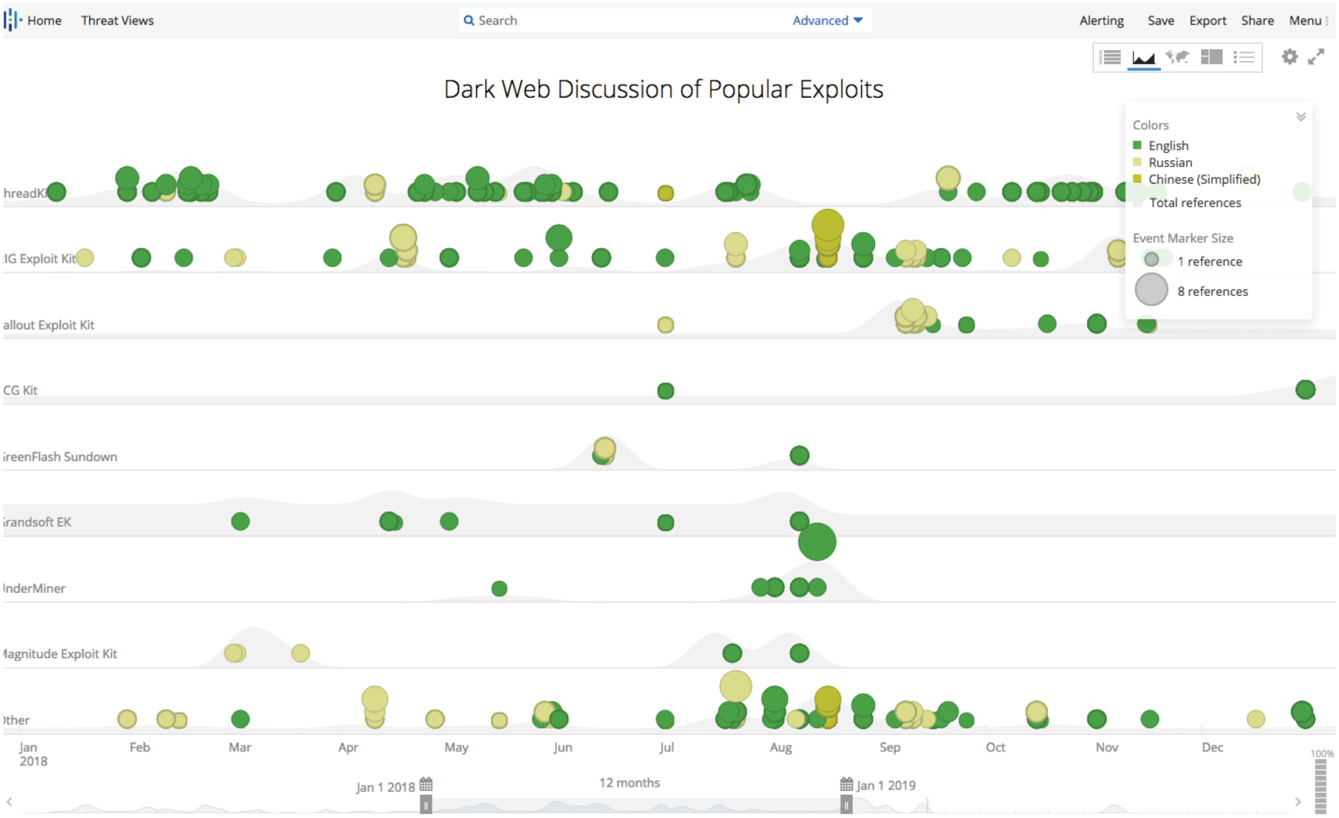
Development of Exploit Kits Continues to Decrease

As observed in prior reports, the development of new exploit kits continued to decrease. Only five new exploit kits emerged in 2018, compared with 10 in 2017, and 62 in 2016. Of those five, two were associated with a top 10 vulnerability: Fallout and LCG Kit. Starting in March, LCG Kit incorporated CVE-2017-11882, but later that year also incorporated 2018's top vulnerability, CVE 2018-8174. Although LCG Kit has been associated with a number of malicious attachments, including the spreading of RATs such as REMCOS and QuasarRAT, there were no direct references to this exploit kit for sale on the dark web in 2018 using the LCG Kit name. New exploit kits developed in 2018 include:

- Best Pack Exploit Kit
- Creep Exploit Kit
- Darknet Angler
- Fallout Exploit Kit
- LCG Kit

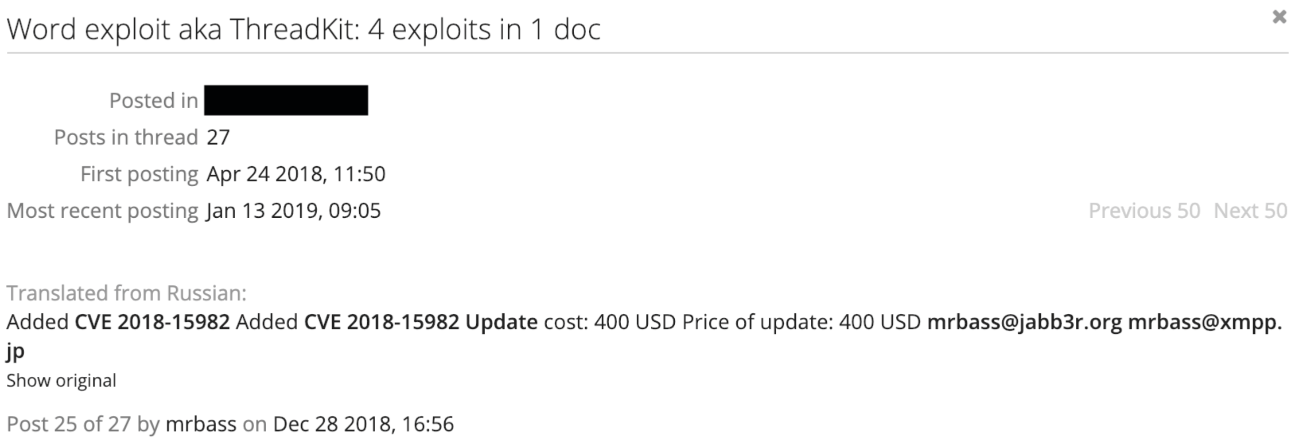
Exploit Kits That Continued to Make Their Mark

Among exploit kits associated with the top vulnerabilities, ThreadKit was the most discussed on dark web sources in 2018. ThreadKit incorporated four of the top 10 vulnerabilities (CVE-2018-4878, CVE-2017-11882, CVE-2017-0199, and CVE-2017-8570). ThreadKit's notoriety increased when the Cobalt Hacking Group (or Cobalt Group) added another stage to the macro exploit by including its signature CobInt trojan. The group typically attacks financial institutions, although the group's activity has lessened due to the arrests of some of its members.



Dark web discussion of exploits associated with 2018's top vulnerabilities.

In 2018, ThreadKit was last updated on December 28 by mrbass, a user on a dark web forum, to include vulnerability CVE-2018-15982 (a more recent Adobe zero-day vulnerability), which continued to be sold for $400, as seen below.



Word exploit aka ThreadKit: 4 exploits in 1 doc ✖

Posted in [redacted]
Posts in thread 27
First posting Apr 24 2018, 11:50
Most recent posting Jan 13 2019, 09:05

Previous 50 Next 50

Translated from Russian:
Added **CVE 2018-15982** Added **CVE 2018-15982 Update** cost: 400 USD Price of update: 400 USD **mrbass@jabb3r.org mrbass@xmpp.jp**
Show original

Post 25 of 27 by mrbass on Dec 28 2018, 16:56

Last update in 2018 for the ThreadKit exploit kit by mrbass on a dark web forum.

UnderMiner, which exploited two of 2018's top vulnerabilities — CVE-2016-0189 and CVE-2018-4878 — made a resurgence in the latter part of 2018. Like ThreadKit, UnderMiner took advantage of, and was the first to exploit, the zero-day vulnerability CVE-2018-15982 in late December 2018.

RATs in Focus

Sisfader is the only RAT that first emerged in 2018 and was associated with a top vulnerability, with its exploit of CVE-2017-8570. The RAT maintains persistence by installing itself as a service when launched from malicious RTF files. According to available sources, there was no evidence of Sisfader for sale.

RATs	Cyber Vulnerability Count
QuasarRAT	5
REMCOS RAT	2
HAWKEYE	1
njRAT	1
PlugX	1
AndroRAT	1

QuasarRAT was associated with the most vulnerabilities, including, most notably, those in Trillium's Security Multisploit Tool. This RAT, which has been active since 2011, continues to show its viability in a variety of attacks, including spearphishing attacks on government organizations.

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.

- Do not forget to patch older vulnerabilities — the average vulnerability stays alive for nearly seven years.
- Remove the affected software if it does not impact key business processes.
- Consider Google Chrome as a primary browser.
- While Flash Player is going away and more sites increasing have removed this technology from its site, continue to heed caution with websites that don't.
- Utilize browser ad-blockers to prevent exploitation via malvertising.
- Frequently back up systems, particularly those with shared files, which are regular ransomware targets.
- Users and organizations should conduct or maintain phishing security awareness to mitigate attacks.
- Companies should 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.