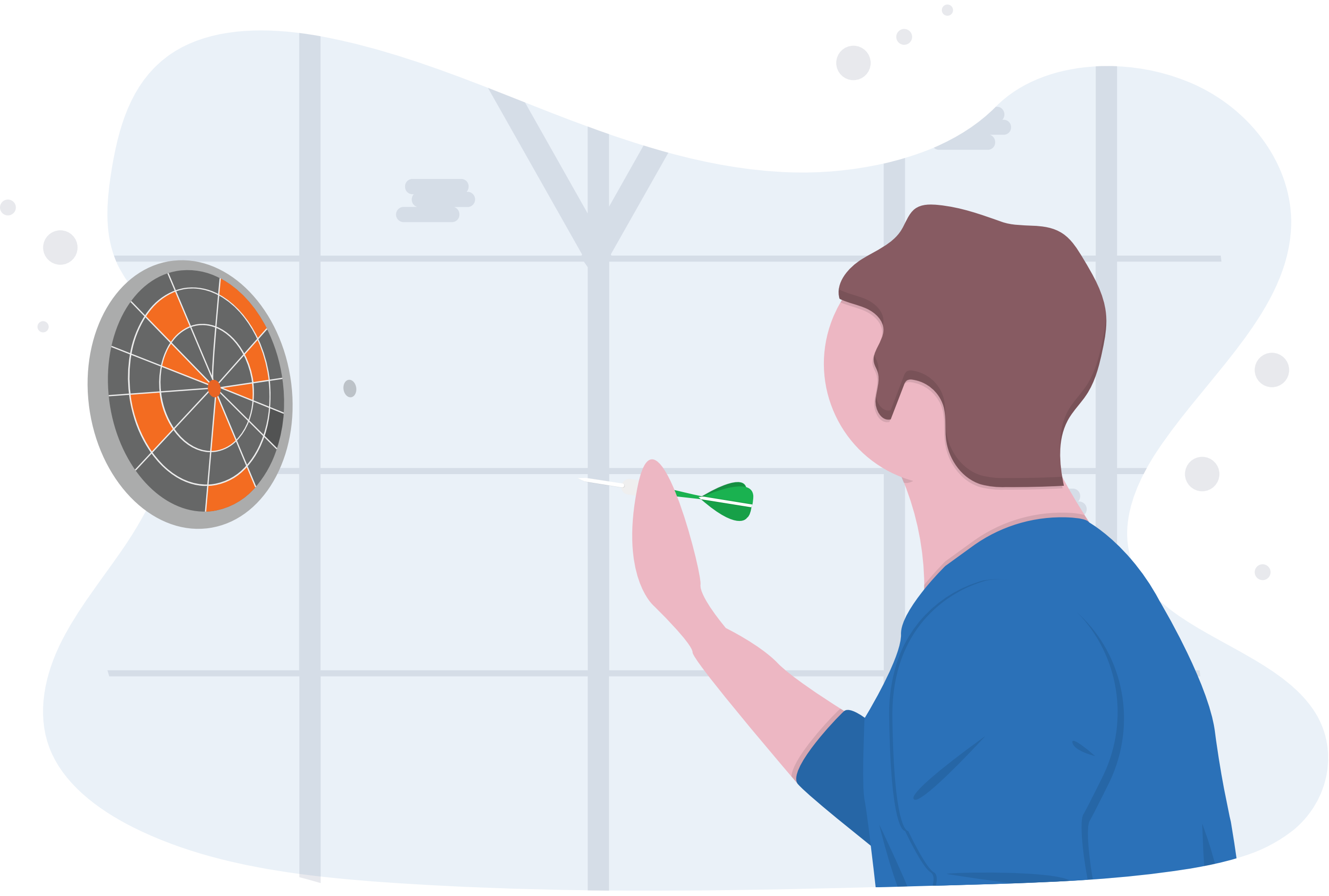
CYBER THREAT ANALYSIS

Criminal Underground Continues to Target Microsoft Products in Top 2019 Exploited Vulnerabilities List

By Kathleen Kuczma and Briana Manalo



CTA-2020-0204

This analysis focuses on exploit kit, phishing attack, or remote access trojan co-occurrences with vulnerabilities from January 1 to December 31, 2019. We analyzed thousands of sources, including code repositories, underground forum postings, and dark web sites. This is a follow-up to our 2018 report, and the intended audience includes information security practitioners, especially those supporting vulnerability risk assessments.

Executive Summary

This report provides insight into which vulnerabilities in 2019, across multiple CVE years, were most exploited on criminal underground sources. As in 2018, Recorded Future observed more exploits targeting Microsoft products than Adobe products in 2019. Eight out of 10 vulnerabilities exploited via phishing attacks, exploit kits, or remote access trojans (RATs) impact Microsoft products. Four of these vulnerabilities impact Internet Explorer. Despite experiencing a drop in browser usage, Internet Explorer is still running in many enterprise environments, making it a top target for threat actors. Only two Adobe Flash vulnerabilities made the top 10, likely due to a combination of better patching and Flash Player's impending demise in 2020.

Many vulnerability and patch management teams face the challenge of keeping up with countless product patch updates without having visibility into which vulnerabilities are actively exploited by cybercriminals. To better illustrate this daunting task, in 2019, there were over 12,000 vulnerabilities reported and classified through CVE. Although this is fewer than previous calendar years (2018 had more than 16,000 vulnerabilities), the U.S. government and the National Vulnerability Database (NVD) have scored over 1,000 of those 12,000 vulnerabilities with a CVSS score of a score of nine or higher and deemed them "critical" to patch.

Official vulnerability databases, and even conventional 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. Insight into weaponization is necessary to adequately prioritize vulnerabilities to patch, as often less than 1% of vulnerabilities have been weaponized within the past month or year. As such, it is imperative that security professionals have knowledge of those vulnerabilities that impact a company's technology stack and are included in exploit kits, used to distribute a RAT, or are currently being used in phishing attacks.

Key Observations

- For a third straight year, Microsoft was the technology most affected by vulnerabilities, with eight of the top 10 vulnerabilities identified targeting its products, the same number as in our 2018 report.
- For the first year, six of the vulnerabilities, all impacting Microsoft, were repeats from the prior year. CVE-2018-8174 dropped one spot from the top exploited vulnerability in 2018 to the second in 2019; CVE-2017-11882 stayed in the third spot, while CVE-2012-0158 dropped from ninth to tenth.
- Only one vulnerability from the 2019 calendar year was ranked in the top 10 that impacted Internet Explorer 10 and 11: CVE-2019-0752. This vulnerability was included in a new exploit kit called Capesand.
- The number of new exploit kits continued to decrease, dropping from five to four in 2019. Capesand was one new exploit kit that targeted vulnerabilities on this list. An underground forum user claimed to stop development on both Capesand and DarkRat in December 2019.
- In 2019, 23 new remote access trojans (RATs) were released compared to 37 in 2018. Only one of these new RATs — BalkanRAT — was associated with a top vulnerability that impacted Microsoft WinRAR ACE: CVE-2018-20250.

Cyber Vulnerability	Company	Product	Associated Malware	CVSS	Recorded Future Risk Score
CVE-2018-15982	Adobe	Flash Player	Fallout Exploit Kit, Spelevo Exploit Kit, ThreadKit, GreenFlash Sundown, Lord Exploit Kit, GandCrab, Capesand Exploit Kit, Maze Ransomware	10	99
CVE-2018-8174	Microsoft	Internet Explorer	SLUB, Fallout Exploit Kit, KaiXin Exploit Kit, LCG Kit Exploit Kit, Magnitude Exploit Kit, RIG Exploit Kit, Trickbot, Underminer Exploit Kit, Capesand Exploit Kit, Dridex, IcedID, Buran Ransomware, Gandcrab	7.6	99
CVE-2017-11882	Microsoft	Office	Agent Tesla Keylogger, Artemis, Formbook, Nanocore, PowerShower, Loki, Heur, Chanitor, Trillium Security MultiSploit Tool, Artemis, Emotet, Silent Doc Exploit, ThreadKit, VenomKit	9.3	99
CVE-2018-4878	Adobe	Flash Player	Gandcrab, Fallout Exploit Kit, RIG Exploit Kit, Spelevo, Capesand Exploit Kit, GreenFlash Exploit Kit, Hermes Ransomware, Sundown Exploit Kit, Threadkit Exploit Kit	7.5	99
CVE-2019-0752	Microsoft	Internet Explorer	SLUB, Capesand Exploit Kit	7.6	99
CVE-2017-0199	Microsoft	Office	njRAT, RevengeRAT, Pony, QuasarRAT, REMCOS RAT, SHUTTERSPEED, Silent Doc Exploit Kit, Threadkit Exploit Kit	9.3	99
CVE-2015-2419	Microsoft	Internet Explorer	Capesand Exploit Kit, Sundown Exploit Kit	9.3	99
CVE-2018-20250	Microsoft	WinRAR	BalkanRAT	6.8	99
CVE-2017-8750	Microsoft	Internet Explorer	ThreadKit Exploit Kit, QuasarRAT	7.6	99
CVE-2012-0158	Microsoft	Office	Silent Doc Exploit	9.3	99

The top 10 vulnerabilities in 2019.

Background

Similar to prior years, the goal of this list is to highlight the vulnerabilities most exploited by the criminal underground. As such, vulnerabilities related to nation-state exploits (such as the ETERNAL vulnerabilities suite) have been removed. As in past years, Recorded Future did not see evidence that tools leaked by groups, such as the Shadow Brokers, were heavily used or included in exploit kits by the criminal underground.

In 2019, Recorded Future observed strong overlap between the top vulnerabilities observed this year and those in 2018, with six of the vulnerabilities repeated from the prior year.

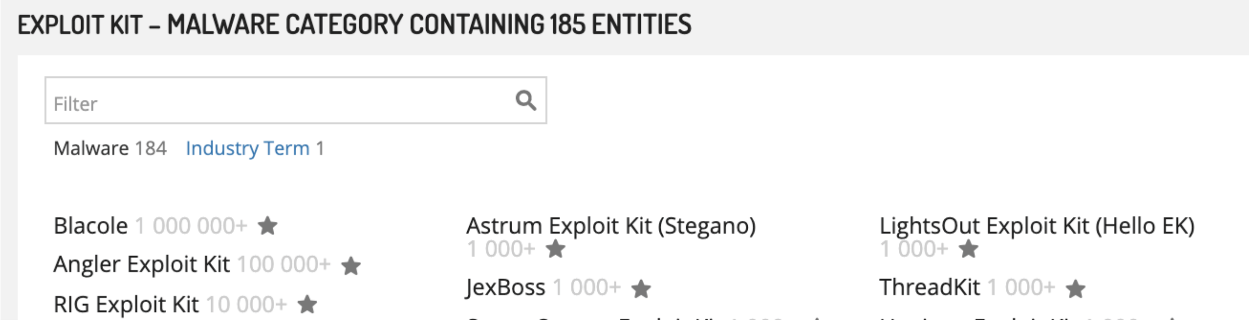
2019	2018	2017	2016
1. CVE-2018-15982	1. CVE-2018-8174	1. CVE-2017-0199	1. CVE-2016-0189
2. CVE-2018-8174	2. CVE-2018-4878	2. CVE-2016-0189	2. CVE-2016-1019
3. CVE-2017-11882	3. CVE-2017-11882	3. CVE-2017-0022	3. CVE-2016-4117
4. CVE-2018-4878	4. CVE-2017-8750	4. CVE-2016-7200	4. CVE-2015-8651
5. CVE-2019-0752	5. CVE-2017-0199	5. CVE-2016-7201	5. CVE-2016-0034
6. CVE-2017-0199	6. CVE-2016-0189	6. CVE-2015-8651	6. CVE-2016-1010
7. CVE-2015-2419	7. CVE-2017-8570	7. CVE-2014-6332	7. CVE-2014-4113
8. CVE-2018-20250	8. CVE-2018-8373	8. CVE-2016-4117	8. CVE-2015-8446
9. CVE-2017-8750	9. CVE-2012-0158	9. CVE-2016-1019	9. CVE-2016-3298
10. CVE-2012-0158	10. CVE-2015-1805	10. CVE-2017-0037	10. CVE-2015-7645

Table of top exploited CVEs between 2016 and 2019 (repeats are noted by color).

One notable observation from the table above is that CVE-2017-0199 was ranked as one of the top exploits over the past three calendar years — this is the second occurrence with this annual report, as CVE-2016-0189 was the first vulnerability to make the top 10 vulnerability list three years in a row in 2018's report. In 2018, CVE-2017-0199 ranked fifth due to its inclusion in the ThreadKit exploit kit and its association with eight different types of malware. CVE-2017-0199 stayed in the top 10 in 2019 as it is still an often-exploited Microsoft vulnerability and still advertised on underground forums for sale with the Silent Doc exploit.

Methodology and Sources

This report continues the trend of analyzing co-occurrences of vulnerabilities with exploit kits and RATs. Recorded Future used a list of 184 exploit kits, using Recorded Future's exploit kit malware category, as one of the parameters to determine the top referenced and exploited vulnerabilities of 2019. Similarly, the ranking of the top exploited vulnerabilities was based on the co-occurrence with 551 RATs, also from Recorded Future's RAT malware category.



EXPLOIT KIT – MALWARE CATEGORY CONTAINING 185 ENTITIES

Filter

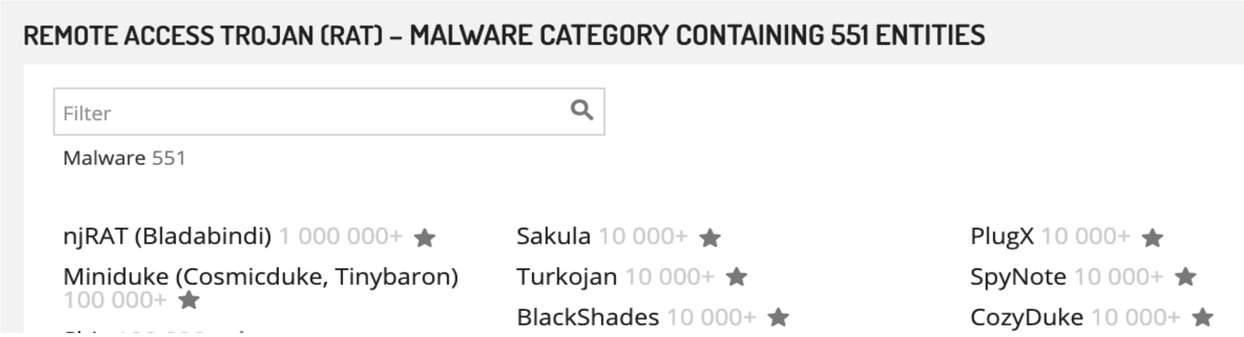
Malware 184 Industry Term 1

Blacole 1 000 000+ ★
Angler Exploit Kit 100 000+ ★
RIG Exploit Kit 10 000+ ★

Astrum Exploit Kit (Stegano) 1 000+ ★
JexBoss 1 000+ ★

LightsOut Exploit Kit (Hello EK) 1 000+ ★
ThreadKit 1 000+ ★

Exploit kit malware category in Recorded Future.



REMOTE ACCESS TROJAN (RAT) – MALWARE CATEGORY CONTAINING 551 ENTITIES

Filter

Malware 551

njRAT (Bladabindi) 1 000 000+ ★
Miniduke (Cosmicduke, Tinybaron) 100 000+ ★

Sakula 10 000+ ★
Turkojan 10 000+ ★
BlackShades 10 000+ ★

PlugX 10 000+ ★
SpyNote 10 000+ ★
CozyDuke 10 000+ ★

RAT malware category in Recorded Future.

Two vulnerabilities, ETERNALBLUE and ETERNALROMANCE, were not included in the top 10 due to adoption by nation-state actors as opposed to being observed on criminal underground sources. The ETERNALBLUE exploit (which relied on MS17-010) and ETERNALROMANCE (which exploited CVE-2017-0143) were not mentioned often by the underground community or offered in exploit kits for sale.

For example, ETERNALROMANCE (CVE-2017-0143) was only briefly mentioned by a few underground forum members. One possible reason for this is that these exploits have been freely available since the Shadow Brokers released them in 2017. Additionally, the exploits are more sophisticated and difficult to use versus typical exploit kits, which were once prolific due to their ease of use. As shown by Recorded Future's previous research on top vulnerabilities, the emergence of new exploit kits continues to decrease, likely due to improved browser security and specific victim targeting.

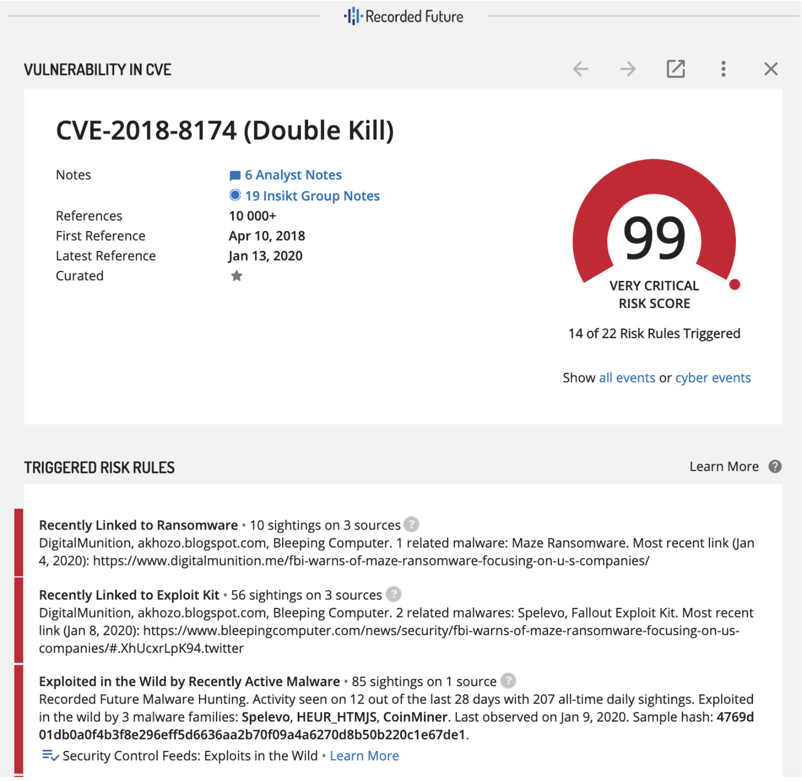
As this annual list is based on both data and metadata analysis of available information from both open and closed source reporting, Recorded Future did not reverse-engineer any malware mentioned in this report. Instead, the aim of this report is to showcase the most exploited vulnerabilities.

Exploitation Risk Score Methodology

This report combined the methodology outlined above with new risk scoring methodology for vulnerabilities. Although Recorded Future's risk score for vulnerabilities has always considered weaponization, Recorded Future formally added "Recorded Future Malware Hunting," a methodology developed by Insikt Group in 2019. This capability analyzes billions of malware samples to identify important samples that have static and behavioral characteristics that make them important to security teams.

The "Exploits in the Wild" data set[1], a subset of Malware Hunting, identifies vulnerabilities where Recorded Future observed recent malware activity in the wild. This data set uses submissions to popular malware repositories as a rough proxy for propagation in the wild, as Recorded Future assesses that the majority of the submission activity to malware repositories is done automatically by security tools and antivirus vendors as samples are discovered on endpoints, in email, or on networks. All of the top 10 exploited vulnerabilities in this report have this risk rule.

[1] To learn more about these data sets, see a previous blog post on Security Control Feeds.



Recorded Future

VULNERABILITY IN CVE

CVE-2018-8174 (Double Kill)

Notes	6 Analyst Notes 19 Insikt Group Notes
References	10 000+
First Reference	Apr 10, 2018
Latest Reference	Jan 13, 2020
Curated	★

14 of 22 Risk Rules Triggered

Show all events or cyber events

TRIGGERED RISK RULES

Learn More ?

Recently Linked to Ransomware • 10 sightings on 3 sources ?
DigitalMunition, akhozo.blogspot.com, Bleeping Computer. 1 related malware: Maze Ransomware. Most recent link (Jan 4, 2020): https://www.digitalmunition.me/fbi-warns-of-maze-ransomware-focusing-on-u-s-companies/

Recently Linked to Exploit Kit • 56 sightings on 3 sources ?
DigitalMunition, akhozo.blogspot.com, Bleeping Computer. 2 related malwares: Spelevo, Fallout Exploit Kit. Most recent link (Jan 8, 2020): https://www.bleepingcomputer.com/news/security/fbi-warns-of-maze-ransomware-focusing-on-us-companies/#.XhUcxrLpK94.twitter

Exploited in the Wild by Recently Active Malware • 85 sightings on 1 source ?
Recorded Future Malware Hunting. Activity seen on 12 out of the last 28 days with 207 all-time daily sightings. Exploited in the wild by 3 malware families: **Spelevo, HEUR_HTMJS, CoinMiner**. Last observed on Jan 9, 2020. Sample hash: **4769d01db0a0f4b3f8e296eff5d6636aa2b70f09a4a6270d8b50b220c1e67de1**.
Security Control Feeds: Exploits in the Wild • Learn More

Vulnerability Intelligence Card for CVE-2018-8174, including the risk rule "Exploited in the Wild by Recently Active Malware."

Top Exploited Vulnerabilities

The top exploited vulnerability on the list is CVE-2018-15982, which did not appear on last year's list. One of two Adobe Flash Player vulnerabilities, CVE-2018-15982, is a use-after-free vulnerability, meaning memory can be accessed after it has been freed. This specific vulnerability allows attackers to execute arbitrary code on a victim system by sending a maliciously crafted Flash object. CVE-2018-15982 was included in at least 10 known exploit kits this year: Fallout, Spelevo, GreenFlash, Sundown, Threadkit, Lord, RIG, UnderMiner, Capesand, and Grandsoft. Recorded Future assesses that this vulnerability is the top exploited one because it was included in multiple well-known exploit kits. This vulnerability was being sold by a user "ExploitCVE" on XSS Forum on March 21, 2019.

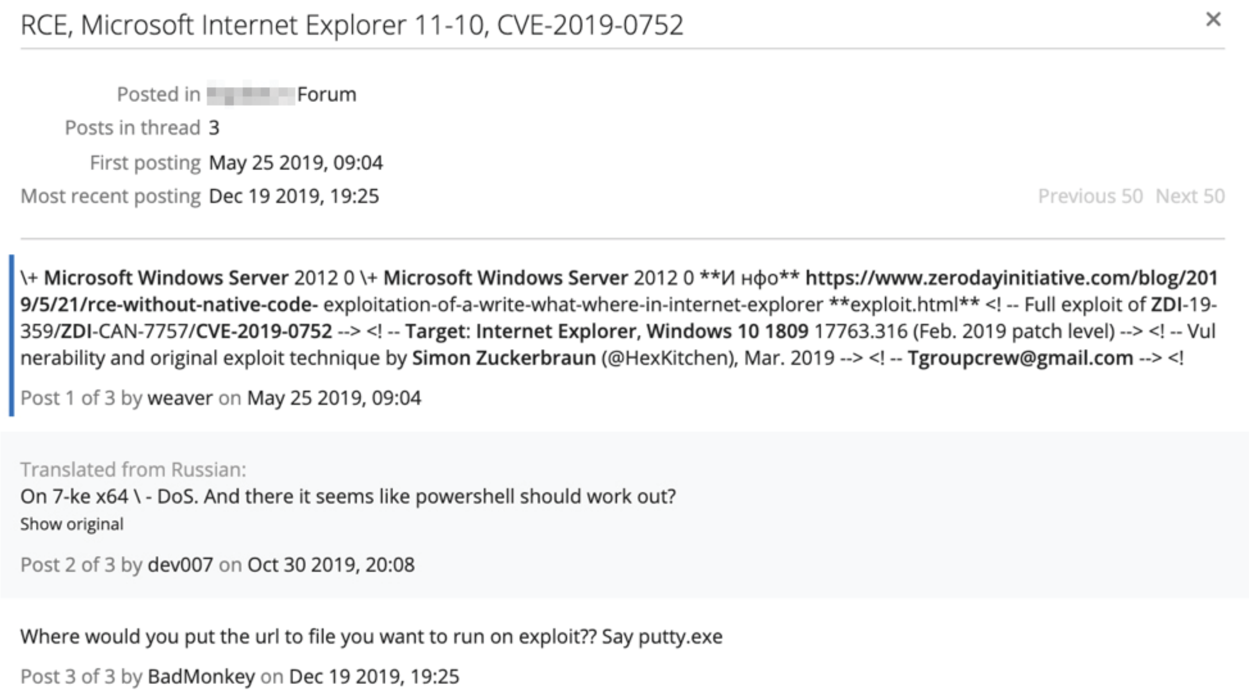
Last year's top vulnerability, CVE-2018-8174, was this year's second most commonly exploited vulnerability. One of eight Microsoft vulnerabilities in the top 10, CVE-2018-8174, or "Double Kill," is a Microsoft Internet Explorer vulnerability that exists in Windows VBScripting engine. Known for active exploitation, CVE-2018-8174 is used in RIG Exploit Kit, Fallout, Spelevo, and Capesand.

Both CVEs are associated with Spelevo, a new exploit kit created this year. Spelevo is an exploit kit that takes advantage of compromised websites and abuses unpatched Internet Explorer and Adobe Flash vulnerabilities, and is most notable for delivering Maze ransomware, IcedID, and Dridex malware. First seen by Recorded Future on March 11, 2019 on a Pastebin post, more analysis and dark web discussion emerged on the exploit kit in mid-2019. A search across our dark web sources reveals minor discussion of Spelevo, but we currently have no information to indicate that the exploit kit is being sold openly across any dark web markets.

Notable CVEs Published in 2019

TThe top exploited vulnerability list for 2019 only includes one vulnerability from the same calendar year: CVE-2019-0752. This is compared to the 2018 and 2017 annual top vulnerability reports, which had three CVEs each from the same calendar year.

CVE-2019-0752, which was patched in April 2019, is a “Scripting Engine Memory Corruption Vulnerability” that impacts Internet Explorer 10 and 11. This vulnerability was incorporated into the Capesand exploit kit, discussed in more detail below. Security researcher Simon Zuckerbraun first detailed a proof of concept for CVE-2019-0752 in May 2019, which was circulated on underground forums such as Exploit.in and XSS.



RCE, Microsoft Internet Explorer 11-10, CVE-2019-0752

Posted in [redacted] Forum
Posts in thread 3
First posting May 25 2019, 09:04
Most recent posting Dec 19 2019, 19:25

+ Microsoft Windows Server 2012 0 \+ Microsoft Windows Server 2012 0 **И нфо** https://www.zerodayinitiative.com/blog/2019/5/21/rce-without-native-code- exploitation-of-a-write-what-where-in-internet-explorer **exploit.html** <! -- Full exploit of ZDI-19-359/ZDI-CAN-7757/CVE-2019-0752 --> <! -- Target: Internet Explorer, Windows 10 1809 17763.316 (Feb. 2019 patch level) --> <! -- Vulnerability and original exploit technique by Simon Zuckerbraun (@HexKitchen), Mar. 2019 --> <! -- Tgroupcrew@gmail.com --> <!

Post 1 of 3 by weaver on May 25 2019, 09:04

Translated from Russian:
On 7-ke x64 \ - DoS. And there it seems like powershell should work out?

Post 2 of 3 by dev007 on Oct 30 2019, 20:08

Where would you put the url to file you want to run on exploit?? Say putty.exe

Post 3 of 3 by BadMonkey on Dec 19 2019, 19:25

Dark web forum member sharing exploit of CVE-2019-0752.

Outside of criminal underground communities, CVE-2019-0752 became associated with the SLUB malware when it was used in a watering hole attack in July 2019. SLUB was first observed in March when it exploited another top 2019 vulnerability: CVE-2018-8174. Researchers from Trend Micro reported that the websites used for the watering hole attacks were pro-North Korean government.

While only one vulnerability from 2019 was ranked high enough for inclusion in the top 10, two other calendar-year vulnerabilities ranked in the top 20: CVE-2019-0841 and CVE-2019-3396.

At the time it was published in May by a user referred to as "Sandbox Escaper[2]" on on Twitter, CVE-2019-0841 was a workaround to a patch that Microsoft issued fixing a Windows AppX Deployment Service error. The workaround, dubbed "ByeBear," allows attackers to gain elevated access to a machine and install malicious content, see data, or change and delete files.

[2] Sandbox Escaper gained notoriety by publishing eight Microsoft zero-day vulnerabilities within a 10-month span between 2018 and 2019. The developer allegedly did not disclose these vulnerabilities to Microsoft before publishing them.

CVE-2019-3396, the other 2019-specific vulnerability in the top 20, is an Atlassian Confluence Server vulnerability first targeted by cybercriminals in April to install cryptojacking malware designed to mine for Monero. However, as recently as December, North Korean state-sponsored threat actors used the vulnerability to gain initial access to systems in order to deploy a new RAT called Dacls. Dacls is modular malware, with Windows and Linux versions that employ the same command and control (C2) that uses TLS and RC4 encryption when communicating with its C2, as well as AES encryption to protect configuration files. A patch is available for this vulnerability.

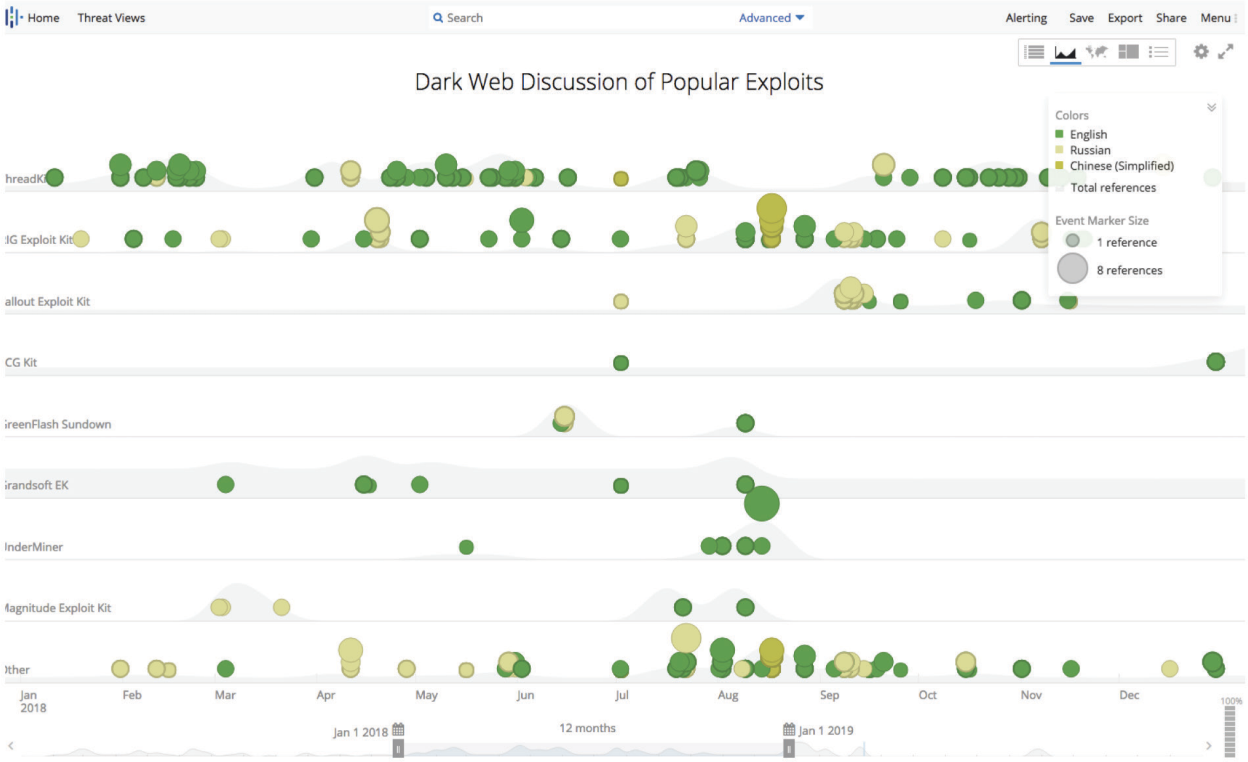
New Exploit Kit Development Continues to Decrease

The development of new exploit kits continued to decrease this year, a trend witnessed in prior reports. In 2019, only four new exploit kits were developed, compared to five in 2018, 10 in 2017, and 62 in 2016. The emergence of exploit kits in 2006 has enabled cybercriminals with less coding experience to infiltrate target systems, making exploit kits one of the more attractive crimeware-as-a-service channels for criminals of all skill levels.

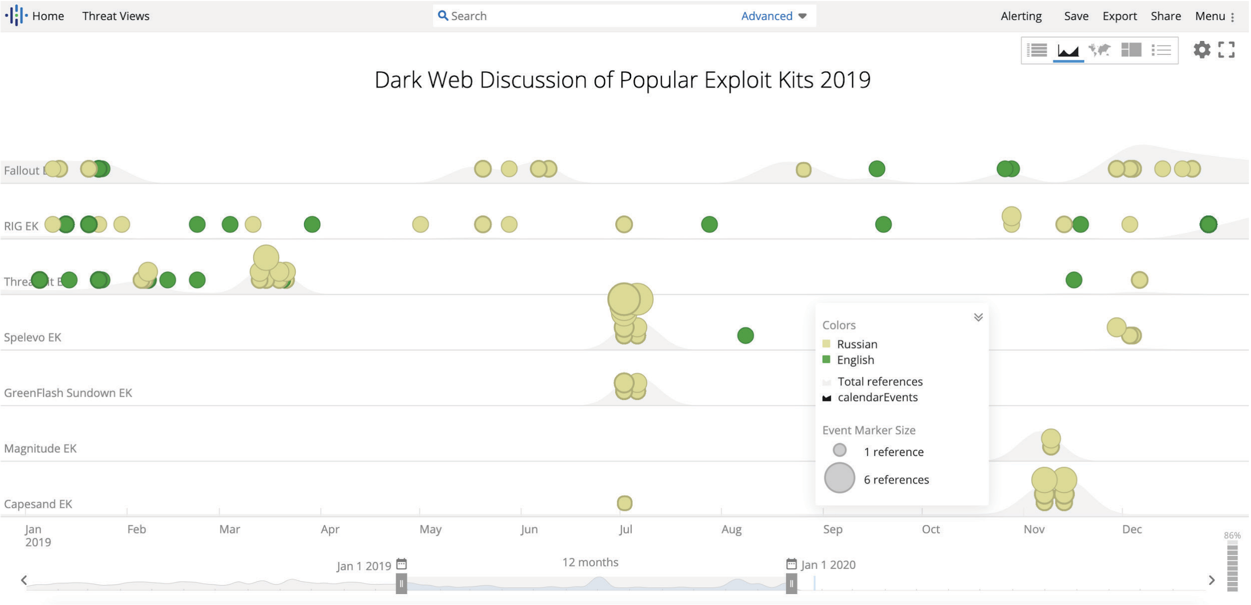
Exploit Kit Name	Technologies Impacted
CapeSand	Microsoft's Internet Explorer (CVE-2015-2419 and CVE-2019-0752); Adobe Flash Player (CVE-2018-4878 and CVE-2018-15982)
Spelevo	Adobe Flash Player (CVE-2018-15928)
Lord Exploit Kit	Adobe Flash Player (CVE-2018-15928)
10KBlaze	SAP NetWeaver

New exploit kits in 2019 and technologies impacted.

In comparison to 2018, dark web discussions of exploit kits have significantly decreased overall. The two most popular exploit kits, Fallout and RIG, also reflected this decrease in discussions. The new Spelevo exploit kit, which first emerged in March 2019, was met with only a surge of chatter in July, while Capesand saw a similar surge of chatter toward the end of the year.



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



Dark web discussion of exploit kits associated with 2019's top vulnerabilities.

The continued use of exploit kits, despite relying on older vulnerabilities and web browsers, and seeing a decline in 2019, indicates that operators can still monetize traffic redirects. We assess that this is largely due to malware authors paying exploit kit actors for their infections and services. Otherwise, exploit kits would have little ability to monetize the browser compromises they create. The use of modern web browsers, such as Edge, Chrome, and Firefox, alleviate the threat from exploit kits; however, Internet Explorer contains many vulnerabilities exploited by these kits.

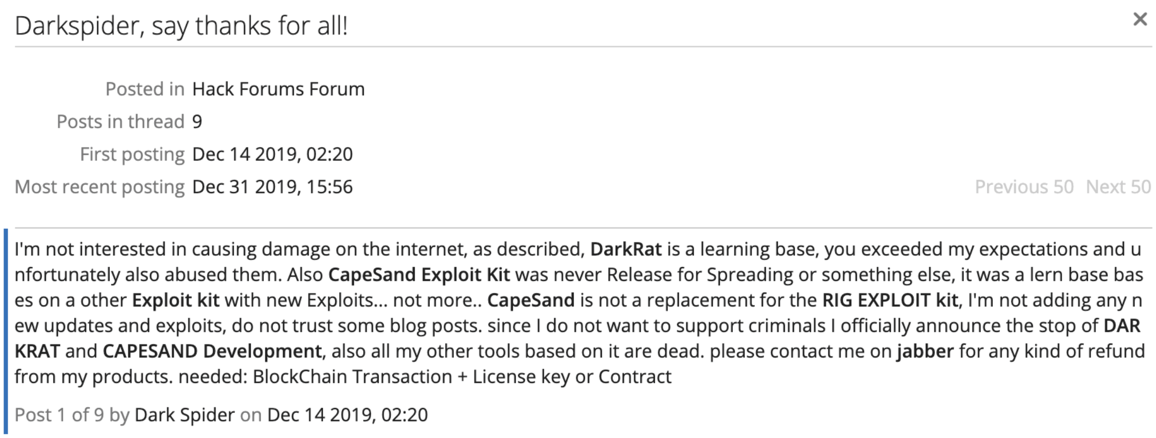
Capesand Exploit Kit

One new exploit kit that was associated with the top exploited vulnerabilities of 2019 was Capesand. Capesand targeted four of the top 10 exploited vulnerabilities: CVE-2015-2419 and CVE-2019-0752 (Microsoft's Internet Explorer), and CVE-2018-4878 and CVE-2018-15982 (Adobe Flash Player).

Researchers at TrendMicro discovered the new exploit kit while analyzing a malvertising campaign using the RIG exploit kit. Capesand's code is unique in that nearly all of its functions are derived from open source code. Based on the front-end source code, researchers believe Capesand may be derived from an old exploit kit, Demon Hunter. (Demon Hunter targeted an array of vulnerabilities impacting Java, Microsoft, and Adobe from 2008, 2010, and 2013.)

Previous reports did not identify the user who created and distributed Capesand initially. Based on searches for references to Capesand on underground forums, a user named "Dark Spider" claimed that they would stop development of Capesand and DarkRat in mid-December 2019. Dark Spider is possibly a German-speaking user, primarily active on Hack Forums.

According to Dark Spider, both Capesand and DarkRat exploit kits were never intended for release; Capesand, specifically, was never intended to replace the RIG exploit kit. Dark Spider claimed refunds would be available via Jabber requests.



Darkspider, say thanks for all!

Posted in Hack Forums Forum
Posts in thread 9
First posting Dec 14 2019, 02:20
Most recent posting Dec 31 2019, 15:56

> I'm not interested in causing damage on the internet, as described, **DarkRat** is a learning base, you exceeded my expectations and u nfortunately also abused them. Also **CapeSand Exploit Kit** was never Release for Spreading or something else, it was a lern base bas es on a other **Exploit kit** with new Exploits... not more.. **CapeSand** is not a replacement for the **RIG EXPLOIT kit**, I'm not adding any n ew updates and exploits, do not trust some blog posts. since I do not want to support criminals I officially announce the stop of **DAR KRAT** and **CAPESAND Development**, also all my other tools based on it are dead. please contact me on **jabber** for any kind of refund from my products. needed: BlockChain Transaction + License key or Contract
>
> Post 1 of 9 by Dark Spider on Dec 14 2019, 02:20

Thread published by the Hack Forums user Dark Spider claiming to stop Capesand development.

New RATs in 2019

Dacls, one of 23 RATs newly published in 2019, was the third most referenced RAT on the list. While not associated with any of the top 10 exploited vulnerabilities, as mentioned above, the RAT was associated with the top 20 exploited vulnerability CVE-2019-3396.

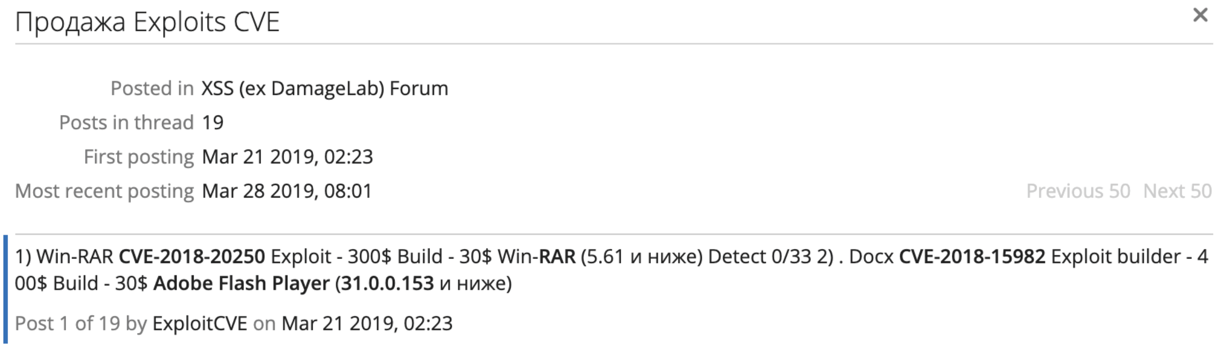
RATs	Cyber Vulnerability Count
QuasarRAT	2
BalkanRAT	1
njRAT	1
RevengeRAT	1
REMCOS RAT	1

RATs associated with the top 10 exploited vulnerabilities.

Only one new RAT was associated with a top exploited vulnerability from 2019: BalkanRAT. This RAT specifically targeted the Microsoft WinRAR ACE vulnerability, CVE-2018-20250, and was one of two new tools used in attacks that targeted entities in Croatia, Bosnia and Herzegovina, Serbia, and Montenegro. A malware variant named BalkanDoor was also used in targeting entities in the aforementioned countries.

BalkanRAT allows attackers to take control of a compromised computer remotely via a graphical interface. The RAT's goal is to deploy a copy of the Remote Utility software on the victim's computer. The RAT is distributed via malicious links in emails mimicking official government websites and email correspondence.

An exploit for CVE-2018-20250 was offered for sale by a user referred to as “ExploitCVE” on the underground forum XSS in March 2019. According to the threat actor, the price for CVE-2018-20250 was either $30 for a single build or $400 for all Win RAR versions up to 5.61.



Продажа Exploits CVE

Posted in XSS (ex DamageLab) Forum
Posts in thread 19
First posting Mar 21 2019, 02:23
Most recent posting Mar 28 2019, 08:01

1) Win-RAR **CVE-2018-20250** Exploit - 300$ Build - 30$ Win-**RAR** (5.61 и ниже) Detect 0/33 2) . Docx **CVE-2018-15982** Exploit builder - 400$ Build - 30$ **Adobe Flash Player** (**31.0.0.153** и ниже)

Post 1 of 19 by ExploitCVE on Mar 21 2019, 02:23

ExploitCVE selling exploits for CVE-2018-20250 and CVE-2018-15982 in March 2019.

Vulnerability-Specific Patches

The chart below provides links to remediation sources for the top 10 exploited vulnerabilities in this report.

CVE	Remediation	Recorded Future Risk Score
CVE-2018-15982	Adobe addressed this vulnerability in Flash Player 32.0.0.101 or later.	99
CVE-2018-8174 (Double Kill)	Microsoft has addressed this vulnerability in a May 2018 security update.	99
CVE-2017-11882	On November 29, 2017 Microsoft released security updates 4011604 for affected editions of Microsoft Office 2007 and 4011618 for affected editions of Microsoft Office 2010. Microsoft recommends that customers running these versions of Office install the updates to be protected from this vulnerability. Customers who have already installed the previously-released updates (4011276 or 2553204) do not need to take any further action.	99
CVE-2018-4878	Adobe addressed this vulnerability in version 28.0.0.161, released on February 6, 2018.	99
CVE-2019-0752	Microsoft has addressed this vulnerability in an April 2019 security update.	89
CVE-2017-0199	Microsoft addressed this vulnerability in an April 2017 security update.	99
CVE-2015-2419	Microsoft addressed this vulnerability in a July 2015 security update (also known as MS15-065).	99
CVE-2018-20250	This is a 19 year old vulnerability. WinRAR has decided to drop support for unpacking ACE archives in WinRAR 5.70 Beta 1. The current beta version is 5.70 Beta 2. WinRAR users are encouraged to upgrade to the latest beta version as soon as possible.	99
CVE-2017-8750	Microsoft addressed this vulnerability in a September 2017 security update.	89
CVE-2012-0158	Microsoft addressed this vulnerability in an April 2012 security update (also known as MS12-027).	99

Remediation table for top 2019 vulnerabilities.

Recommended Actions

The goal of this annual list is to provide an account of the most widely adopted vulnerability exploits by the criminal underground. Security teams can take action on data within this report with any of the following recommended actions:

- Given the outsized number of exploits included in this top exploited list, prioritize the patching of Microsoft products in your technology stack.
- Ensure that Flash Player is automatically disabled in your browser settings. (Sites are increasingly removing this technology as Adobe will end support for Flash Player on December 31, 2020.)
- Prioritize patching of all the vulnerabilities identified in this report.
- Do not forget to patch older vulnerabilities — the average vulnerability stays alive for nearly seven years, according to a 2017 RAND report.
- Remove affected software if it does not impact key business processes.
- Install browser ad-blockers to prevent exploitation via malvertising.
- Frequently back up systems, particularly those with shared files, which are regular ransomware targets.
- Conduct or maintain phishing security awareness to mitigate attacks. This can include 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.
- Vulnerability management teams can use Recorded Future’s technical intelligence to prioritize patching based on which vulnerabilities are actively being exploited in the wild by malware.

About Recorded Future

Recorded Future arms security teams with the only complete security 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.