CYBER THREAT ANALYSIS

Recorded Future®

By Insikt Group®

CTA-2020-1210

EXPLOIT KITS, THOUGH IN DECLINE, REMAIN POWERFUL TOOL FOR DELIVERING MALWARE

Recorded Future analyzed current data from the Recorded Future® Platform, dark web, information security reporting, and other open source intelligence (OSINT) sources to identify the use and prevalence of exploit kits that facilitate threat actor campaigns. This report expands upon findings addressed in the report "Automation and Commoditization in the Underground Economy," following reports on database breaches, checkers and brute forcers, loaders and crypters, credit card sniffers, and banking web injects. This report will be of most interest to network defenders, security researchers, and executives charged with security risk management and mitigation.

Executive Summary

Exploit kits (hereafter referred to as EKs), also known as exploit packs, remain relevant despite the fact that there are fewer publicly viewable discussions on online forums than in the past. Some criminals have changed their targeting methods, partly due to the securing of browsers and software that EKs have historically used within their arsenal, while other threat actors have ceased operations altogether. However, the decline of public references to EKs does not necessarily mean that they aren't still used by criminals to gain initial access to networks. Insikt Group identified that EKs are still being discussed, albeit at a lower rate, on dark web forums, and also observed references to private sales of niche EKs to high-ranking cybercriminal groups and threat actors. Additionally, the partnership between the operators of EKs and other criminal groups, such as ransomware gangs, has led to an increase in private use of EKs in the last couple years. Ultimately, the overall decline of public EKs is likely due to the ease with which cybercriminals groups can purchase direct access to victim organizations without having to probe targeted organizations for vulnerabilities.

Key Judgments

- Private sales of EKs continue on dark web forums, albeit at a lower rate than at the height of their prominence from 2010 to 2017, with sales being discussed among high-ranking threat actors and criminal groups.
- Active EKs are continuing to be updated to include new vulnerabilities for products such as Microsoft and Adobe. Adobe Flash Player vulnerabilities are frequently used in EKs and there is a high likelihood of continued use of Adobe exploits even though Adobe Flash Player will be phased out on December 31, 2020.
- Commodity malware delivery has shifted targeting tactics from a broader, unselective approach to a strategy that is more focused on the targeting of specific victims. There has been a stable increase in the sale of access to compromised networks of government, business, educational, healthcare, and other sectors on the dark web.
- Over the last two years, operators of EKs have increasingly modified their kits to include first-stage malware that is being used to deploy ransomware, such as the case of the Fallout EK and Maze Locker ransomware operators.

What Exploit Kits Are

EKs, first seen in 2006, are a one-stop shop of automated malware kits that can be used by threat actors to scan and exploit victim systems for various vulnerabilities, allowing for the delivery of an exploit corresponding to a vulnerability found on the victim computer. These EKs often contain publicly identified vulnerabilities for popular products such as Microsoft or Adobe products, taking advantage of an unpatched computer. Having multiple exploits allows malicious threat actors better success rates of gaining access to vulnerable systems or applications.

Threat actors that control EKs are still very much on the hunt for new and unpatched exploits. The collection of multiple vulnerabilities into one package allows threat actors to compromise victim devices without having to put in work to do the initial system scanning and reconnaissance for vulnerable browsers or software. Once an EK has successfully compromised the victim's system, threat actors can then use that initial access to infect the machine with malware, with a popular use being the implementation of cryptocurrency mining software. As vulnerabilities are patched by the software manufacturer, each EK has a limited window of opportunity; however, the steady stream of vulnerabilities identified for popular tools such as Microsoft and Adobe products, and the reality that relatively few organizations remediate vulnerabilities in a timely manner, allow for the continued use of and updates to old EKs to include these newly identified vulnerabilities.

There has been an overall decrease in the number of publicly available references to and use of EKs in the last several years as criminal efforts have had to adapt their tactics and techniques. This decrease is likely due the shift to other infection techniques, such as the rise in popularity of cryptocurrency mining malware, as well as the arrest of EK developers and operators, such as the 2016 arrest of 50 Russians who were thought to be associated with the Angler EK, and the arrest of "Paunch," a developer of Blackhole EK. The threat of EKs is still relevant today as they continue to offer an easy way for lower tier threat actors to enter into the criminal sphere.

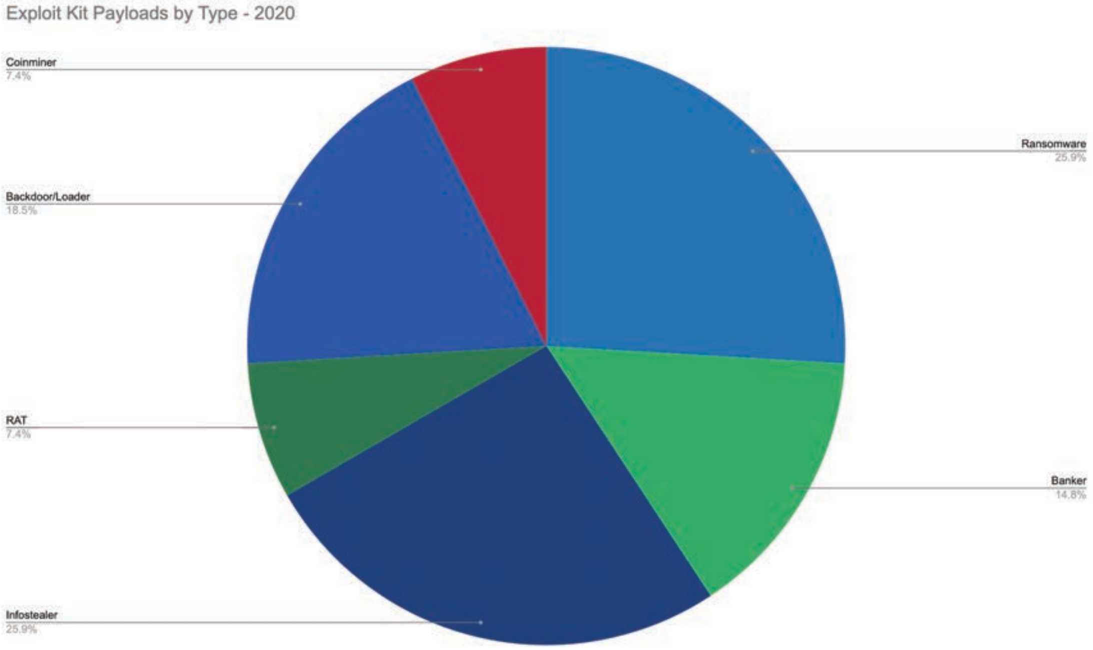


Figure 1: Final payloads delivered by popular exploit kits, 2020 (Source: Recorded Future)

Some EKs are sold and used privately, leaving little to no publicly available discussion about them in underground forums. The majority of EKs that are still active are not publicly advertised on the dark web but are being shared via private communication channels among closed groups. This shift to private channels and groups is likely due to security concerns. The private EKs are purportedly of better quality than public versions that are readily available on the dark web because they include exploits of less well-known vulnerabilities. A large volume of criminal malware continues to be aimed at any target of opportunity and widespread in distribution; EKs can excel at this type of delivery.

EKs deliver many kinds of malware, including ransomware, and as they can be used to target specific countries, operating systems, and more, they are still a practical delivery method with some targeting capabilities. The following chart, based off of information collected by Recorded Future on exploit kit payloads, illustrates the popularity of exploit kit delivery for ransomware, among other malware types.

How Exploit Kits Function

The primary function of an EK is to compromise systems visiting malicious websites using vulnerabilities in browsers, operating systems, or other software. The EK process begins with attracting visitors to a location where they can be analyzed and filtered for potential compromise. The EK analyzes the targeted victim's systems for vulnerabilities; if it detects one that the kit is capable of exploiting, it attempts to do so.

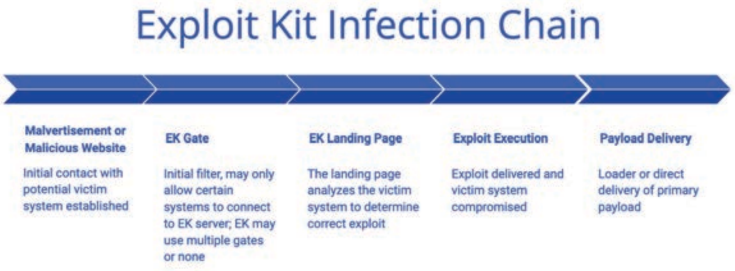

Exploit Kit Infection Chain
Malvertisement or Malicious Website
Initial contact with potential victim system established
EK Gate
Initial filter, may only allow certain systems to connect to EK server; EK may use multiple gates or none
EK Landing Page
The landing page analyzes the victim system to determine correct exploit
Exploit Execution
Exploit delivered and victim system compromised
Payload Delivery
Loader or direct delivery of primary payload

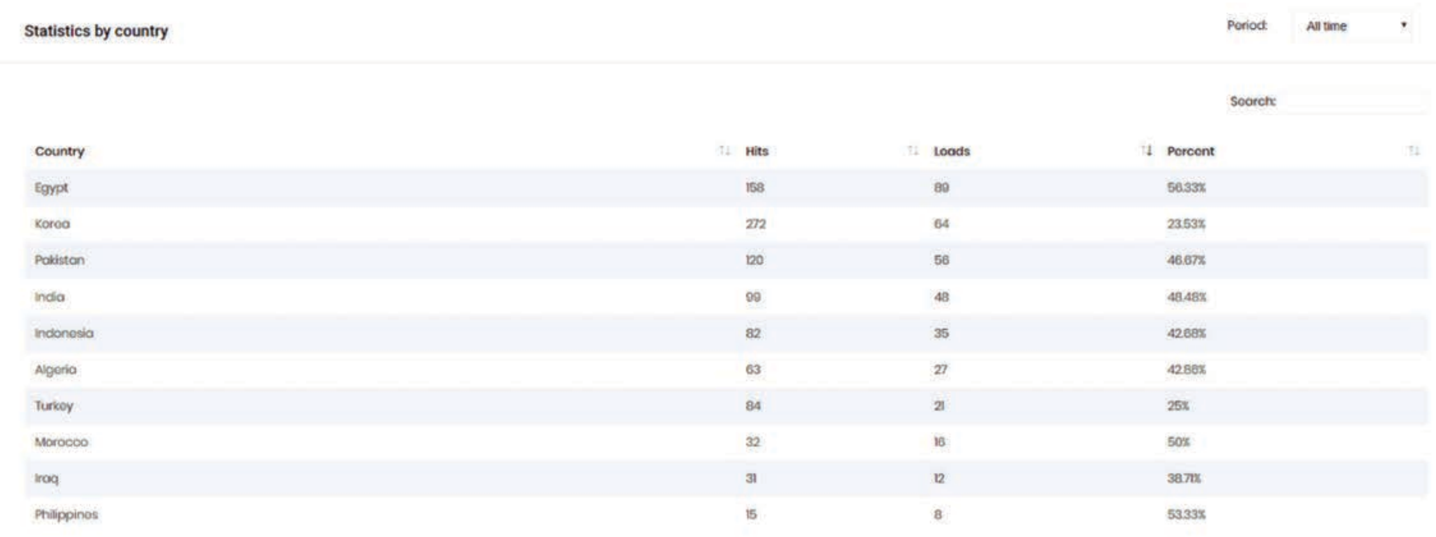
Figure 2: Exploit kit infection process (Source: Recorded Future)

Exploits for internet-connected systems used by EKs can vary widely. While exploits for vulnerabilities in Adobe Flash Player, Internet Explorer, and Microsoft Office have remained consistently popular, as Adobe Flash and Internet Explorer are replaced by other software, their targeting by EKs will decrease.

Analysis of the activities of Fallout EK RIG EK and ThreadEK on the dark web indicates that a peak of their activities happened in 2017 to 2018. A true reason for the decrease is unknown, but since EKs rely on clients paying for their services, a reduction in clientele is a likely cause. Considering that a certain number of new private EKs have appeared, it is probable that the demand on publicly promoted EKs have decreased as users have become more inclined to use private EKs or other infection vectors such as RDP access.

The model of malware delivery by criminals has been trending away from the broad, unselective "spray and pray" strategy, and toward a more focused targeting of victims. This is most clearly observed in the increase of the "big game" hunting strategy of specifically targeting large organizations becoming much more common in recent years, particularly among ransomware operators. This shift in attack vectors is likely another factor in the decline in the popularity of EKs. This trend is mitigated somewhat by the evolution of ransomware affiliate programs, which has increased the infection vectors of any such malware significantly, as the affiliates distribute the malware independent of the program's operators in most cases. EKs are among the tactics used by such affiliates.

Affiliates of EK programs cooperate with other cybercriminals who provide web traffic to deliver their landing pages. As a rule, developers of EKs operate based on a software-as-a-service (SaaS) model, offering daily, weekly, and monthly subscriptions and providing malware updates and regular technical support. The number of EK clients is usually limited from 25 to 30 due to security reasons. The developers perform a serious background check on potential affiliates, in terms of their technical skills, reputation on the dark web, and the ability to provide technical support. If an affiliate breaks the terms and conditions of the agreement with the developer, their subscription will be canceled and a subsequent ban on the forum will likely occur.



Statistics by country

Period: All time

Search:

Country	Hits	Loads	Percent
Egypt	158	89	56.33%
Korea	272	64	23.53%
Pakistan	120	56	46.67%
India	99	48	48.48%
Indonesia	82	35	42.68%
Algeria	63	27	42.86%
Turkey	84	21	25%
Morocco	32	16	50%
Iraq	31	12	38.71%
Philippines	15	8	53.33%

Figure 3: Most-targeted countries by FalloutEK (Source: Exploit Forum)

Frequently Observed Exploit Kit Vulnerabilities

As EKs traditionally relied on the exploitation of browser-based vulnerabilities, the improvements in browser security makes it more difficult for EKs to successfully compromise targeted machines. A September 2020 article by Malwarebytes identified a cyber criminal group, Malsmoke, using adult-themed websites to redirect victims to the Fallout EK malvertising campaign. The exploited vulnerabilities used in this campaign, identified as CVE-2019-0752 and CVE-2018-15982 targeted Internet Explorer and Flash Player, respectively, both of which already have had patches released. The use of these vulnerabilities within the EK indicates that cybercriminals are not actively updating their EKs to include new vulnerabilities, but rather relying on unpatched software targeting those whose browsers are not up to date.

As a rule, EKs provide a control panel with a list of vulnerabilities targeting applications, websites, or software. Within EKs, Microsoft vulnerabilities continued to be the most exploited as seen in Recorded Future research in 2018 on Microsoft vulnerabilities and the 2019 Vulnerability Report. The top exploited vulnerability in 2018 was CVE-2018-8174 a Microsoft Internet Explorer vulnerability nicknamed “Double Kill,” which was included in four EKs (RIG, Fallout, KaiXin, and Magnitude). Unlike our observations in 2017, analysts only observed one vulnerability tied to Adobe Flash Player on this year’s list. Tracked as CVE-2018-8174, exploits for this vulnerability were included in multiple exploit kits, most notably the Fallout Exploit Kit, which was used to distribute GandCrab ransomware. The top exploited vulnerability in 2019, CVE-2018-15982, a use-after-free vulnerability found within Adobe Flash Player, was also used in at least 10 known EKs: Fallout, Spelevo, GreenFlash, Sundown, Thread Kit, Lord, RIG, UnderMiner, CapeSand, and Grandsoft.

Threat Actors Associated With EK Creation and Sales

While publicly advertised EKs have seen a decline since their peak in 2017 to 2018, many cybercriminals who develop and operate different types of malware purchase EKs privately and actively cooperate with EK developers. The following is a list of the more prominent of the recently active EKs and the threat actors behind them.

Fallout Exploit Kit

“FalloutEK,” a member of the Russian-language forum Exploit released the Fallout EK on September 7, 2018. The Fallout EK (FEK) is advertised exclusively on the forum Exploit and has received positive community feedback. FalloutEK is known to work with partners that advertise the sales of the FEK, such as “A. Server” and “GandGrab,” both of whom have touted their successful use of FEK. The website 123crypt[.]tk is a malware crypting service used by FEK.

FEK comes with a variety of standard features among successful EKs, such as the ability to identify and prevent access from honeypots, frequently re-obfuscating exploits to avoid detection, and allowing payloads to be delivered in both EXE and DLL formats. Initially, the kit could be rented for $50 per day, $250 per week, or $900 per month. More recently, the prices to rent the EK were raised to $400 per week or $1,300 per month, and paid tests were made available for reputable members. However, the operator often provides discounts that change prices drastically. FalloutEK limits their clients to 25 in total at any given time, and gives each client an instance of FEK on a separate server with a unique, individualized shellcode as an extra layer of security for monitoring the activities of the affiliates. If a user of FEK targets users in a blacklisted country (usually, the Commonwealth of the Independent States), FalloutEK will cancel their subscriptions, which usually results in them also being banned from Exploit forum.

FEK was a common delivery method for the KPOT Stealer and has also been associated with a number of the ransomware operators:

- Stop
- GandCrab v.5
- Kraken Cryptor
- GandCrab
- Maze Locker
- Fake Globe
- Minotaur
- Matrix
- Sodinokibi/REvil

Analysis of web traffic indicates that attackers primarily target the following countries: Egypt, Japan, South Korea, Pakistan, India, the Philippines, Morocco, Algeria, Indonesia, Turkey, and Iraq.

On Exploit, FalloutEK last posted on May 29, 2020. Many forum members have since posted on the thread requesting FalloutEK to respond to their interest in renting FEK.

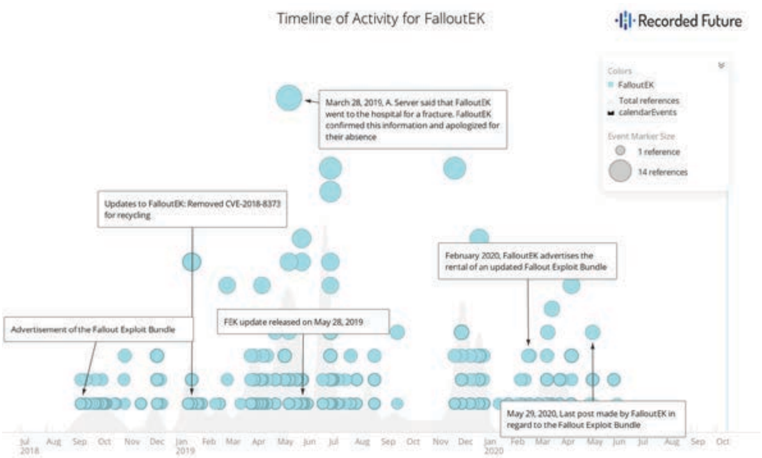


Figure 4: Timeline of activities for FalloutEK threat actor (Source: Recorded Future)

RIG Exploit Kit

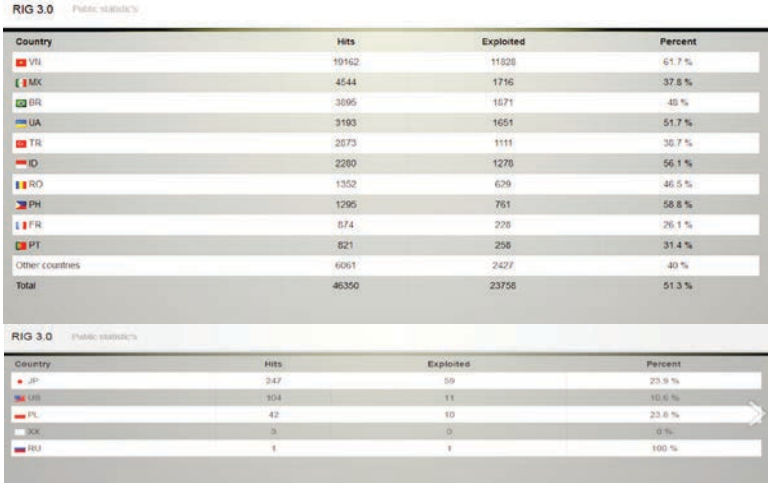
“TakeThat” is a longstanding Russian-speaking member of various dark web forums such as Exploit, Verified and Club2CRD. The first registration of the threat actor on Exploit Forum occurred on June 18, 2014. On the same day, the threat actor created a sales thread for the RIG EK, allowing English-speaking forum members to rent the EK. The threat actor stated that the EK has significant technical features, such as the ability to target all Windows versions (32/64-bit), bypass User Account Control (UAC), and has API functionality for automated link generation. According to the threat actor, the RIG EK variant “RIG EK 3.0” could be rented for $50 per day, $200 per week, or $700 per month.

The RIG EK has been associated with a number of the ransomware operators:

- CryptFIle2
- ASN1
- Sage
- NEMTY
- CryptoShield
- CrypMIC
- Mobef
- Paradise
- GandCrab
- CryptoMix Revenge
- BartCrypt
- Spora
- Erebus
- Mole
- Cry
- FessLeak
- Sodinokibi/REvil
- Matrix
- Cerber
- Philadelphia
- CryptoWall
- Locky
- Alma Locker
- Princess Locker
- FakeGlobe
- BandarChor
- YafunnLocker
- ERIS
- Goopic
- Radamant
- CryptoMix
- GetCrypt
- AnteFrigus
- Buran

Among the most-targeted countries were the United States, Japan, Poland, France, Turkey, Romania, Portugal, Brazil, Mexico, Indonesia, the Philippines, Vietnam, Russia, and Ukraine.

On December4, 2019, TakeThat was advertising the sale of a newly released version of the RIG EK, dubbed RIG EK v.4.0 on the forums Club2CRD and Proxy Base. In these advertisements, the threat actor stated that the new version of the EK had enhanced capabilities, such as the ability to target all Windows versions (32/64-bit), bypass UAC, API functionality, and automated link generation. TakeThat claimed that the average successful infection rate was approximately 10 percent to 15 percent. The threat actor stated that they had been in this business since 2015. According to the threat actor, RIG EK 4.0 could be rented for $100 per day, $400 per week, or $1,200 per month.


RIG 3.0 Public statistics

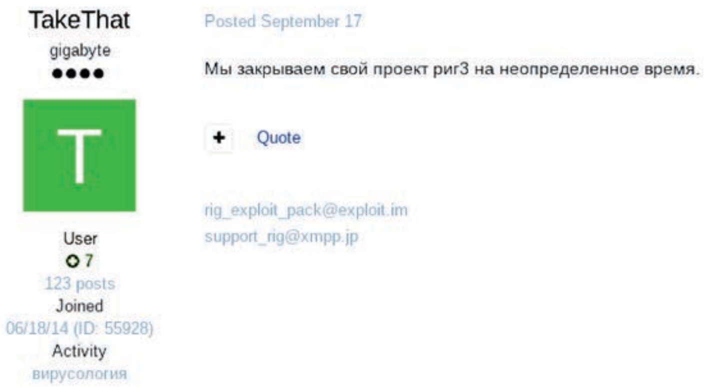
Country	Hits	Exploited	Percent
VN	19162	11828	61.7 %
MX	4544	1716	37.8 %
BR	3895	1871	48 %
UA	3193	1651	51.7 %
TR	2873	1111	38.7 %
ID	2280	1278	56.1 %
RO	1352	629	46.5 %
PH	1295	761	58.8 %
FR	874	228	26.1 %
PT	821	258	31.4 %
Other countries	6061	2427	40 %
Total	46350	23758	51.3 %

RIG 3.0 Public statistics

Country	Hits	Exploited	Percent
JP	247	59	23.9 %
US	104	11	10.6 %
PL	42	10	23.8 %
XX	3	0	0 %
RU	1	1	100 %

Figure 5: RIG EK control panel shows most targeted countries by RIG EK 3.0 (Source: Exploit Forum)

On September 17, 2020, TakeThat announced on the forum Exploit that the project had been put on an indefinite hiatus. It should be noted that the thread on the forum was already temporarily closed by the forum’s administrators in January 2019. Additionally, Recorded Future analysts observed that TakeThat had started deleting their posts on the forums Exploit and Verified, likely for security reasons.


TakeThat
gigabyte
●●●●

User
○ 7
123 posts
Joined
06/18/14 (ID: 55928)
Activity
вирусология

Posted September 17

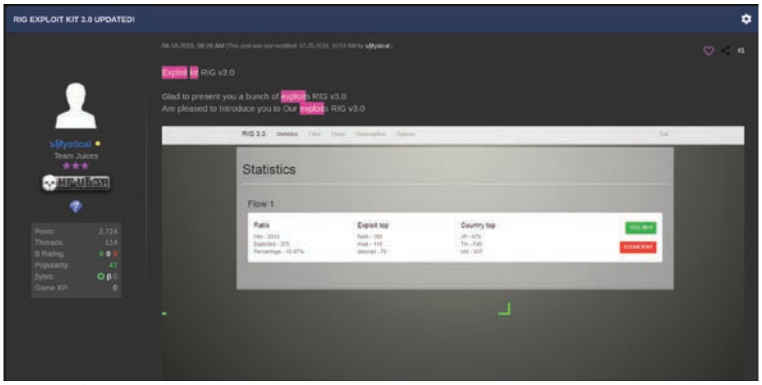
Мы закрываем свой проект риг3 на неопределенное время.

+ Quote

rig_exploit_pack@exploit.im
support_rig@xmpp.jp

Figure 6: TakeThat announcing the end of RIG EK 3.0 (Source: Exploit Forum)

Recorded Future found the threat actor “Mystical” a partner of TakeThat, had been been advertising the sales of RIG EK 3.0 on the English-speaking forum Hack Forums from April 2015 to August 2017. At the time of writing, this threat actor has not had any recent activity.


RIG EXPLOIT KIT 3.0 UPDATED!

Mystical
Team Juices

Posts: 2,724
Threads: 114
Popularity: 47
Game XP: 0

Exploit kit RIG v3.0

Glad to present you a bunch of exploits RIG v3.0
Are pleased to Introduce you to Our exploits RIG v3.0

RIG 3.0

Statistics

Flow 1

Ratio
Exploit top
Country top

Figure 7: Mystical announcing RIG EK 3.0 (Source: Hack Forums)

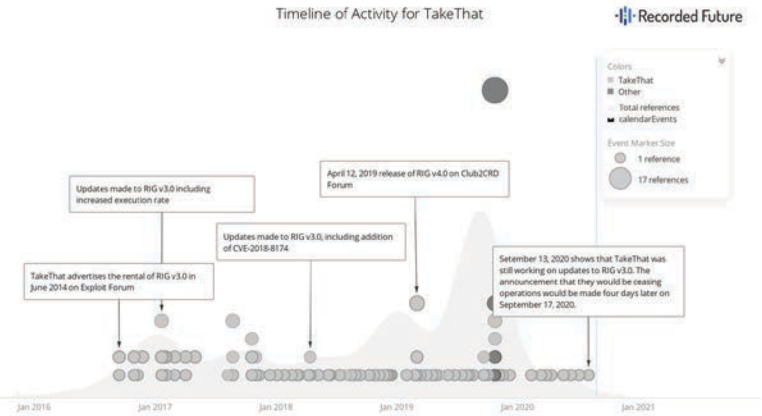
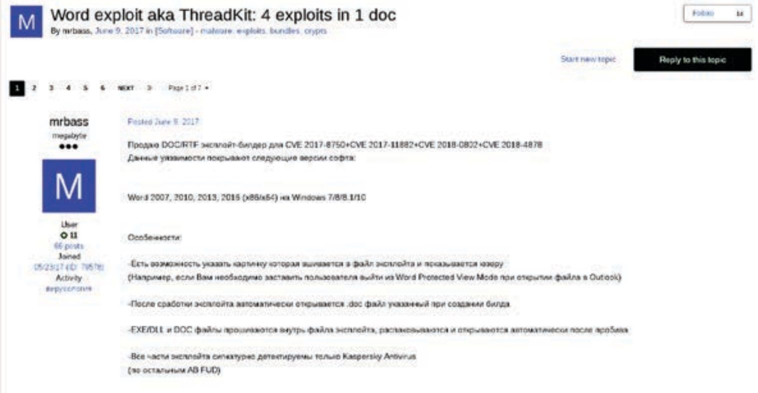


Figure 8: Timeline of activities for TakeThat (Source: Recorded Future)

ThreadKit Exploit Kit

The threat actor "mrbass" a member of the forums Exploit, Verified, and Hack Forums, began advertising the ThreadKit EK, also known as a Word (RTF/DOC) exploit, on June 9, 2017. It targets Microsoft Office Word 2007, 2010, 2013, 2016 (x86/x64) on Windows OS 7, 8, 8.1, and 10. ThreadKit is not a classic exploit kit, but rather is an exploit builder, which only creates weaponized files combined with exploits; it does not assist in distributing the exploits like RIG EK or FEK. The threat actor claimed that the EK can include up to five exploits into a single weaponized Microsoft Word document. The threat actor also stated that the EK was detectable only by Kaspersky Antivirus. On June 18, 2017, the threat actor confirmed on the forum Exploit that they were also the author of "RTF/DOC/XLS/PPT" — an exploit-builder for CVE-2017-0199.

Initially, ThreadKit could be purchased for $1,150. However, the price was later decreased to $800. The price for the ThreadKit update for existing customers was $400 and $150 for anti-detection cleaning.



Word exploit aka ThreadKit: 4 exploits in 1 doc

By mrbass, June 9, 2017 in [Software] - malware, exploits, bundles, crypts

mrbass
megabyte
User
11
66 posts
Joined 05/23/17 (ID: 79578)
Activity вирусология

Posted June 9, 2017

Продаю DOC/RTF эксплойт-билдер для CVE 2017-8750+CVE 2017-11882+CVE 2018-0802+CVE 2018-4878
Данные уязвимости покрывают следующие версии софта:

Word 2007, 2010, 2013, 2016 (x86/x64) на Windows 7/8/8.1/10

Особенности:

-Есть возможность указать картинку которая вшивается в файл эксплойта и показывается юзеру
(Например, если Вам необходимо заставить пользователя выйти из Word Protected View Mode при открытии файла в Outlook)

-После сработки эксплойта автоматически открывается .doc файл указанный при создании билда

-EXE/DLL и DOC файлы прошиваются внутрь файла эксплойта, распаковываются и открываются автоматически после пробива

-Все части эксплойта сигнатурно детектируемы только Kaspersky Antivirus
(по остальным АВ FUD)

Figure 9: mrbass listed ThreadKit Exploit Kit on the dark web (Source: Exploit Forum)

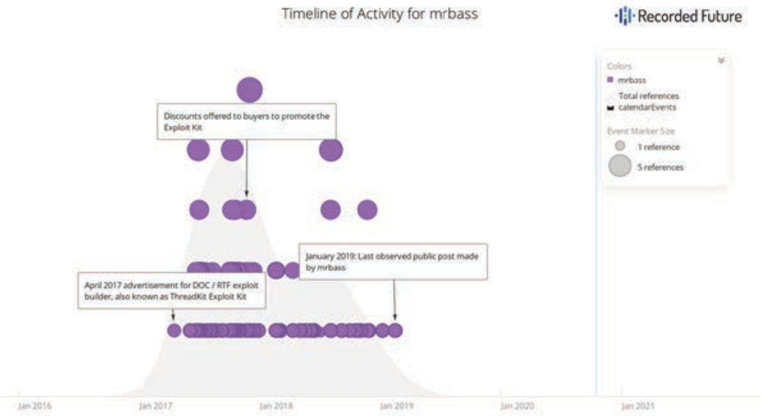


Figure 10: Timeline of Activities for mrbass (Source: Recorded Future)

Capesand Exploit Kit

Capesand EK is one of the newest EKs, first observed in the wild in October 2019, exploiting vulnerabilities in Adobe Flash Player and Microsoft Internet Explorer (IE). At the time of writing, there are no known developers and sellers publicly active on dark web sources. However, there is an English-speaking threat actor, "robinhood" who, on July 20, 2020, advertised Capesand EK for rent on Exploit forum. The actor stated that they were interested in cooperating with those who could provide web traffic for Capesand EK and Raccoon Stealer. The actor first registered on the forum on December 6, 2018 and is also known as a seller of Raccoon Stealer logs and cryptocurrency-related databases.

A search in the Recorded Future Platform for robinhood's listed Jabber account, "cbt@xmpp[.]jp", found that this contact was used by another English-speaking threat actor with the username "La Vida Loca" on Hack Forums, where they were looking for a partner. La Vida Loca also used the Telegram @bitcoin_baron and Discord @shadowdaemon#6124. La Vida Loca is either another alias of robinhood or works as their accomplice.

Trend Analysis

While the overall trend of EK creation has declined in the last few years, existing EKs continue to be modified to include exploits for newly identified vulnerabilities. Furthermore, the operators of these EKs are increasingly partnering with other cybercriminal groups, such as ransomware operators, to repackage these kits. For example, over the last two years, there has been an increase in EK operators modifying their kits to include first-stage malware used specifically for deploying ransomware. Notably, this was identified with the Maze Locker ransomware, which was being delivered by two EK families: FEK and Spelevo EK.

From 2016 to 2017, Angler EK and RIG EK were the most frequently referenced kits on the Recorded Future Platform's dark web sources. Recorded Future's timeline analysis showed an overall decline of Angler EK and RIG EKs starting in late 2017, which correlates with the 2016 arrest of 50 Russian individuals suspected to have been behind Angler EK's development and maintenance. The arrests also included actors involved with the Pseudo-Darkleech and EITest campaigns, who favored using Rig EK in their operations.

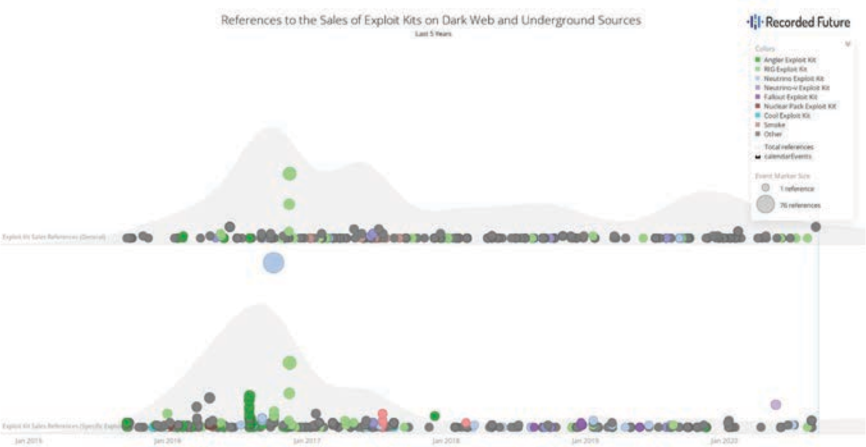


Figure 11: References to the sales of exploit kits from 2015 to 2020 (Source: Recorded Future)

New Exploit Kits Observed Despite Downward Trend of References

Analysts observed an overall lower number of references to general discussions or the sales of EKs on dark web and underground forums within the last two years. Additionally, the last two years have given rise to new EK variants, such as ThreadKit and Capesand, while still maintaining a smaller number of references to historically popular EKs, such as advertisements pertaining to revamped versions of RIG EK.

In 2018, the number of new EKs dropped by approximately 50 percent, with five new EKs released, compared to 10 EKs observed in the year before. Despite this, two of the EKs observed in 2018 were associated with 2018's top exploited vulnerability: CVE-2018-8174. The EKs identified as having exploited this vulnerability include RIG, Fallout, KaiXin, and Magnitude and LCG Kit. Similar to our observed trends for the last two years, the operators of these EKs were seen teaming up with other malware operators to facilitate attacks. These EKs were being used in conjunction with different malware groups, such as Fallout EK being used to distribute GandCrab ransomware and Magnitude being used to deliver Magniber ransomware. In 2018, CVE-2016-0189 which has been on Recorded Future's top 10 vulnerability list for three years in a row, was persistently exploited by five EKs: Underminer, Magnitude, Grandsoft, KaiXin, and RIG.

In 2019, four new EK variants were released: Capesand, Spelevo, Lord EK, and 10KBlaze. Of these four new EKs, Capesand and Spelevo had the most discussions among cybercriminals, likely because Capesand appears to be under development and Spelevo has been used as a dropper for Maze Locker ransomware. Both EKs include vulnerabilities that target compromised websites and abuse unpatched Internet Explorer and Adobe Flash Player vulnerabilities, tracked as CVE-2018-15982 and CVE-2018-8174, respectively.

Furthermore, EK developers have been identified by researchers as having created code for zero-day vulnerabilities and other malware variants. In October 2020, Checkpoint researchers were able to connect the exploit developer Volodya also known as BuggiCorp, to multiple zero-day exploits and malware variants by identifying unique characteristics in the author's code and using that to search for other items that were authored by Volodya throughout the years. The identification of an author's unique fingerprints can help security researchers identify which EK developers are still in operation, as well as to determine if they have been involved in the creation of other zero-days or malware variants.

Shifting Trends

In the last few years, Recorded Futures analysts identified a shift in preference among cybercriminals from these EKs targeting Adobe Flash Player vulnerabilities to Microsoft consumer product exploits. Since 2017, analysts have observed threat actors using EKs and phishing campaigns favored attack vectors towards Microsoft products, with seven of the top 10 vulnerabilities exploited by phishing attacks and EKs using Microsoft products. This is in stark contrast to our previous rankings (2015, 2016), which saw consistent exploitation of Adobe Flash Player vulnerabilities.

There has been a consistent increase in the sales of access to compromised networks of governments, businesses, educational institutions, healthcare providers, and other entities on the dark web. Cybercriminals obtain access to networks using different methods such as compromised third-party software (Citrix, TaxSlayer, or LexisNexis software), virtual private networks (VPN), and remote desktop protocol (RDP). Buying network access is more direct for cybercriminals as opposed to using an EK. Furthermore, successful ransomware operators who do choose to use EKs can do so by directly, employing a developer for their specific ransomware. This could increase the success rate of their attacks and improve their operational security, as there would be no public discussion and therefore no evidence of a relationship between EK developer and the ransomware operator on dark web forums.

Outlook and Mitigation Strategies

While public EKs are, on the surface, declining, private sales of the EKs are still a significant part of the underground economy. However, the rise in ransomware operators purchasing already compromised network access from cybercriminals could potentially lead to a further decline of EKs. Historically, EK operators used several of the top identified vulnerabilities within their arsenal to update the EKs as vulnerabilities are announced. Although the large majority of these vulnerabilities have been issued patches, this does not mean the patches have been applied. Furthermore, vulnerabilities associated with Adobe Flash Player were frequently identified. Considering that Adobe is discontinuing support for Flash on December 31, 2020, many organizations may be using vulnerable software once new vulnerabilities are identified.

To mitigate the risk posed by EKs, we recommend the following:

- Ensure that Adobe Flash Player is automatically disabled in the browser settings. Additionally, install browser ad-blockers to prevent malvertising attacks.
- Identify and prioritize the patching of vulnerabilities that have a “high” or “critical” risk score and/or are actively being exploited by threat actors.
- Patch older vulnerabilities. According to a 2017 RAND report, the average vulnerability stays active for approximately seven years. The identified EKs in this report used vulnerabilities that were identified one to two years ago, if not earlier.
- Maintain a security awareness program to educate employees about phishing campaigns and watering-hole attacks that are commonly used by EK operators.

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.