telelink

Advanced Security Operations Center
Telelink Business Services
www.telelink.com

Monthly Security Bulletin

August 2018

Contents

1. Just Five File Types Make Up 85% of All Spam Malicious Attachments

Despite a lone report claiming that online piracy is the primary source of malware, spam still reigns supreme as today's main infection vector and the go-to tool of online criminals, according to a report published by Finnish cyber-security firm F-Secure. Experts say that one of the main reasons why spam still works is that users are still failing at recognizing spam. Users are having a hard time picking up spam despite spam being more than a 40-year-old trick. This has led to users clicking on spam emails more than ever.

Spam click rates are up

F-Secure reports that spam email click rates have gone up from the 13.4% recorded in the second half of 2017 to 14.2% recorded in the first half of the year.

With browsers and operating systems getting harder to hack via exploit kits and vulnerabilities, spam has been the safety net on which most cybercriminal operations have fallen on.

"Of the spam samples we've seen over spring of 2018, 46% are dating scams, 23% are emails with malicious attachments, and 31% contain links to malicious websites," said Päivi Tynninen, Threat Intelligence Researcher at F-Secure.

"We've found that just five file types make up 85% of malicious attachments," Päivi added. "They are ZIP, .DOC, .XLS, .PDF, and .7Z."

Spam as inefficient as ever

F-Secure says cybercriminals have not found in spam campaigns a novel and newly efficient infection method. Spam is as inefficient as it ever was, even despite its recently observed increased click rate.

"The technique still relies on spewing out massive numbers of emails in order to snare a tiny number of users," F-Secure said in its report.

But despite the lowly click rate, spam still works better than all alternatives, and criminals are continually refining their tactics to deliver spam with better results.

Wording tricks and proper grammar

F-Secure says that the probability of a recipient opening a spam email increases with 12% if the email claims to come from a known individual.

Having a subject line free from errors also improves a spam campaign's success rate by 4.5%, while phishing emails stating that they are very urgent get less traction than when the urgency is implied, rather than spelled out.

These subtle wordings and email design tricks are now the frontline of the cyber-security industry. With exploit kits beaten to a pulp, spam is all that's left.

"We've reduced criminals to spam, one of the least effective methods of infection," said Sean Sullivan, an F-Secure Security Advisor. "Anti-malware is containing nearly all commoditized, bulk threats. And honestly, I don't see anything coming over the horizon that could lead to another gold rush so criminals are stuck with spam."

Unless users are using a really old browser and OS, they can easily avoid getting infected with malware these days by learning to recognize spam when it slips through spam filters.

Source: https://www.bleepingcomputer.com/news/security/just-five-file-types-make-up-85-percent-of-all-spam-malicious-attachments/

2. On the Hunt for FIN7: Pursuing an Enigmatic and Evasive Global Criminal Operation

On Aug. 1, 2018, the United States District Attorney's Office for the Western District of Washington unsealed indictments and announced the arrests of three individuals within the leadership ranks of a criminal organization that aligns with activity we have tracked since 2015 as FIN7. These malicious actors are members of one of the most prolific financial threat groups of this decade, having carefully crafted attacks targeted at more than 100 organizations. FIN7 is referred to by many vendors as "Carbanak Group," although we do not equate all usage of the CARBANAK backdoor with FIN7. This blog explores the range of FIN7's criminal ventures, the technical innovation and social engineering ingenuity that powered their success, a glimpse into their recent campaigns, their apparent use of a security company as a front for criminal operations, and what their success means for the threat landscape moving forward. With this release, FireEye is also providing technical context, historical indicators, and techniques that organizations can use to hunt for FIN7 behavior enterprise-wide.

FIN7 Does the Crime…

The threat group is characterized by their persistent targeting and large-scale theft of payment card data from victim systems, which it has monetized at least a portion of through a prominent card shop. But FIN7's financial operations were not limited to card data theft. In some instances, when they encountered and could not obtain payment card data from point of sale (POS) systems secured with end-to-end encryption (E2EE) or point-to-point encryption (P2PE), FIN7 pivoted to target finance departments within their victim organizations.

Furthermore, in April 2017, FireEye reported that FIN7 sent spear phishing emails to personnel involved with United States Securities and Exchange Commission (SEC) filings at multiple organizations, providing further insight into FIN7's targeting. These targeted individuals would likely have access to material non-public information that FIN7 actors could use to gain a competitive advantage in stock trading.

Diversification of their monetization tactics has allowed the group to impact a wide range of industries beyond those solely associated with payment card industry. During campaigns that FireEye associates with FIN7, victims within the following sectors have been targeted within the United States and Europe:

- Restaurants
- Hospitality
- Casinos and Gaming
- Energy
- Finance
- High-tech
- Software
- Travel
- Education
- Construction
- Retail
- Telecommunications
- Government
- Business services

Source: *https://www.fireeye.com/blog/threat-research/2018/08/fin7-pursuing-an-enigmatic-and-evasive-global-criminal-operation.html*

3. Massive Coinhive Cryptojacking Campaign Touches Over 200,000 MikroTik Routers

Security researchers have unearthed a massive cryptojacking campaign that targets MikroTik routers and changes their configuration to inject a copy of the Coinhive in-browser cryptocurrency mining script in some parts of users' web traffic.

The campaign appears to have gotten off the ground this week and was, in its first stages, mainly active in Brazil, but later started targeting MikroTik routers all over the world.

The first to spot the attacks was a Brazilian researcher who goes by the name of MalwareHunterBR on Twitter, but as the campaign got bigger and bigger by impacting more and more routers, it also got the attention of Simon Kenin, a security researcher with Trustwave's SpiderLabs division.

In a report Trustwave shared with Bleeping Computer, Kenin says that the hacker (or hackers) behind this campaign appear to have compromised around 72,000 MikroTik routers in Brazil during the first stages of their attack.

Kenin says the attacker uses a zero-day in the Winbox component of MikroTik routers that was discovered in April. MikroTik patched the zero-day in less than a day, back in April, but this didn't necessarily mean that router owners applied the required patch.

Instead, the former zero-day was dissected by security researchers, and public proof-of-concept (PoC) code has appeared in several places on GitHub.

Hacker using April 2018 MikroTik zero-day

According to Kenin, the attacker used one of those PoCs to alter traffic passing through the MikroTik router and inject a copy of the Coinhive library inside all the pages served through the router.

We know it's only one threat actor exploiting this flaw because the attacker used only one Coinhive key for all the Coinhive injections he performed during the past week.

Furthermore, Kenin says that he also identified some cases where non-MikroTik users were also impacted. He says this was happening because some Brazilian ISPs were using MikroTik routers for their main network, and hence the attacker managed to inject the malicious Coinhive code in a massive amount of web traffic.

In addition, Kenin says that because of the way the attack was performed, the injection worked both ways, and not necessarily only for traffic going to the user. For example, if a website was hosted on a local network behind an affected MikroTik router, traffic to that website would also be injected with the Coinhive library.

Hacker became more careful, shrunk operation

But injecting Coinhive in so much traffic is very noisy and tends to annoy users, which could lead to users and ISPs investigating the source of the problem, such as it happened with this user on Reddit.

The attacker also appears to have understood this issue, and Kenin says that in recent attacks, the hacker switched tactics and only injected the Coinhive script in error pages returned by the routers.

But shrinking his attack surface doesn't look to be a downgrade for the attacker. The Trustwave researcher says that in recent days he's seen the attack spreading outside Brazil, and has now more than doubled the initial numbers, having altered configurations and added the Coinhive injection on over 170,000 MikroTik routers.

"Let me emphasize how bad this attack is," Kenin says. "There are hundreds of thousands of these devices around the globe, in use by ISPs and different organizations and businesses, each device serves at least tens if not hundreds of users daily."

"The attacker wisely thought that instead of infecting small sites with few visitors, or finding sophisticated ways to run malware on end user computers, they would go straight to the source; carrier-grade router devices," he added.

"Even if this attack only works on pages that return errors, we're still talking about potentially millions of daily pages for the attacker."

The attack has room to grow

A query on the Shodan IoT search engine reveals that there are over 1.7 million MikroTik routers available online.

Bleeping Computer has reached out to the Coinhive team and inquired if they've taken down this site key, and how much Monero the attacker mined through his scheme.

UPDATE: Shortly after this article's publication, security researcher Troy Mursch told Bleeping Computer he discovered a second Coinhive key being injected in the traffic of MikroTik routers. This campaign has touched over 25,000 routers, bringing the total at over 200,000, as the first Coinhive key was now used on over 175,000 devices. It is unclear if this second campaign is being orchestrated by another hacker, or by the same threat actor who switched to a new key after Trustwave exposed his first operation. Article title was also updated.

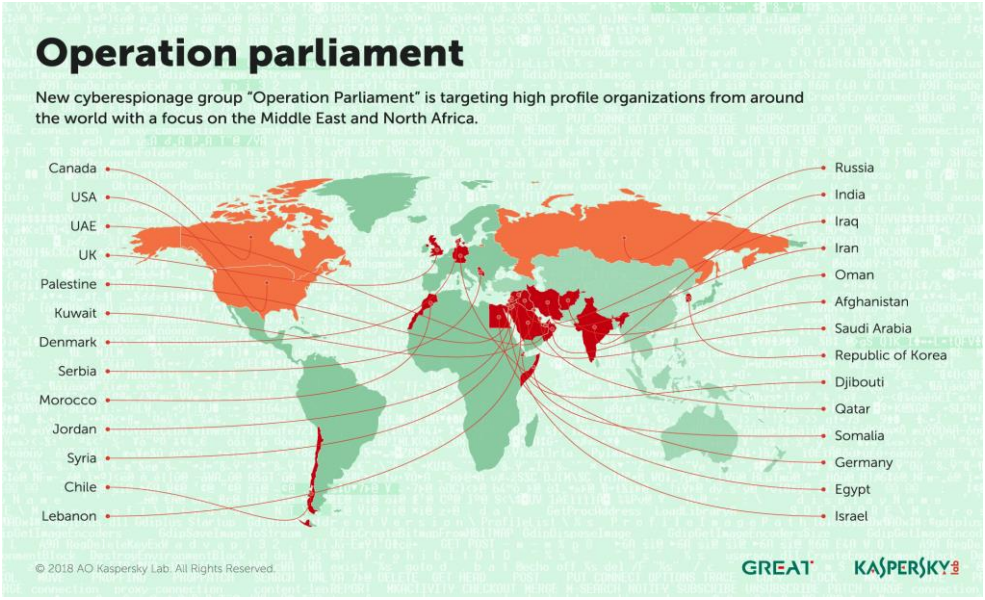
Source: https://www.bleepingcomputer.com/news/security/massive-coinhive-cryptojacking-campaign-touches-over-200-000-mikrotik-routers/

4. IT Threat evolution Q2 2018

Targeted attacks and malware campaigns

Operation Parliament

In April, we reported the workings of Operation Parliament, a cyber-espionage campaign aimed at high-profile legislative, executive and judicial organizations around the world – with its main focus in the MENA (Middle East and North Africa) region, especially Palestine. The attacks, which started early in 2017, target parliaments, senates, top state offices and officials, political science scholars, military and intelligence agencies, ministries, media outlets, research centers, election commissions, Olympic organizations, large trading companies and others.



The attackers have taken great care to stay under the radar, imitating another attack group in the region. The targeting of victims is unlike that of previous campaigns in the Middle East, by Gaza Cybergang or Desert Falcons, and points to an elaborate information-gathering exercise that was carried out prior to the attacks (physical and/or digital). The attackers have been particularly careful to verify victim devices before proceeding with the infection, safeguarding their C2 (Command-and-Control) servers. The attacks seem to have slowed down since the start of 2018, probably after the attackers achieved their objectives.

The malware basically provides a remote CMD/PowerShell terminal for the attackers, enabling them to execute any scripts or commands and receive the result via HTTP requests.

This campaign is a further symptom of escalating tensions in the Middle East.

Read the rest and find out more about other threats, like VPNFilter, LuckyMouse, ZooPark, Olympic Destroyer an the securelists report "IT Threat Evolution Q2 2018".

Source: https://securelist.com/it-threat-evolution-q2-2018/87172/

5. IT threat evolution Q2 2018. Statistics

A Q2 figures

According to KSN:

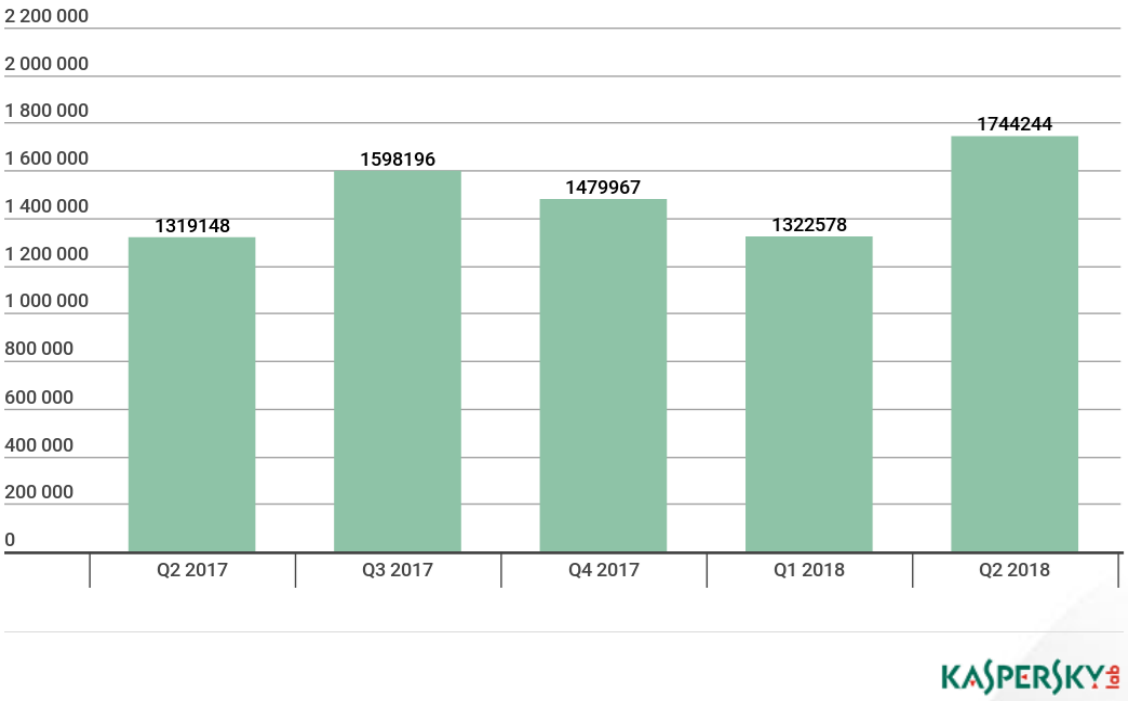
- Kaspersky Lab solutions blocked 962,947,023 attacks launched from online resources located in 187 countries across the globe.
- 351,913,075 unique URLs were recognized as malicious by Web Anti-Virus components.

- Attempted infections by malware designed to steal money via online access to bank accounts were logged on the computers of 215,762 users.
- Ransomware attacks were registered on the computers of 158,921 unique users.
- Our File Anti-Virus logged 192,053,604 unique malicious and potentially unwanted objects.
- Kaspersky Lab products for mobile devices detected:
  - 1,744,244 malicious installation packages
  - 61,045 installation packages for mobile banking Trojans
  - 14,119 installation packages for mobile ransomware Trojans.

Mobile threats

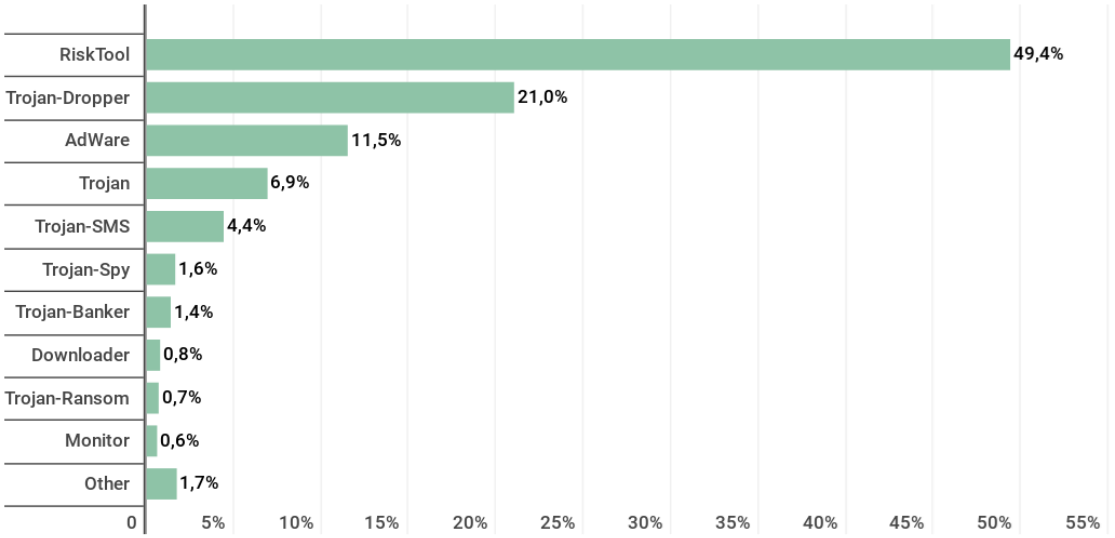
General statistics

In Q2 2018, Kaspersky Lab detected 1,744,244 malicious installation packages, which is 421,666 packages more than in the previous quarter.

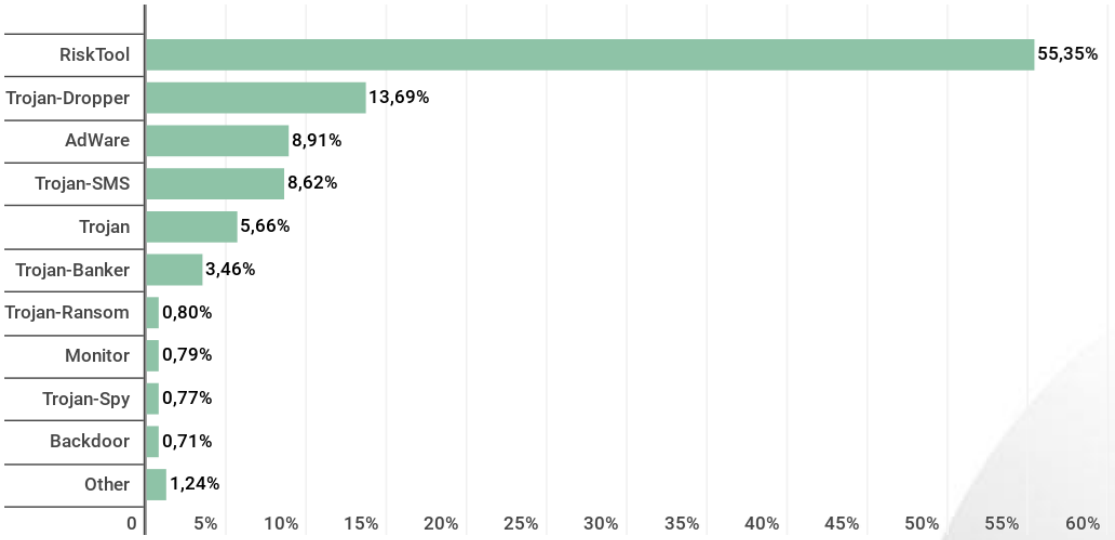


Number of detected malicious installation packages, Q2 2017 – Q2 2018

Distribution of detected mobile apps by type



Distribution of newly detected mobile apps by type, Q1 2018



Distribution of newly detected mobile apps by type, Q2 2018

Among all the threats detected in Q2 2018, the lion's share belonged to potentially unwanted RiskTool apps (55.3%); compared to the previous quarter, their share rose by 6 p.p. Members of the RiskTool.AndroidOS.SMSreg family contributed most to this indicator.

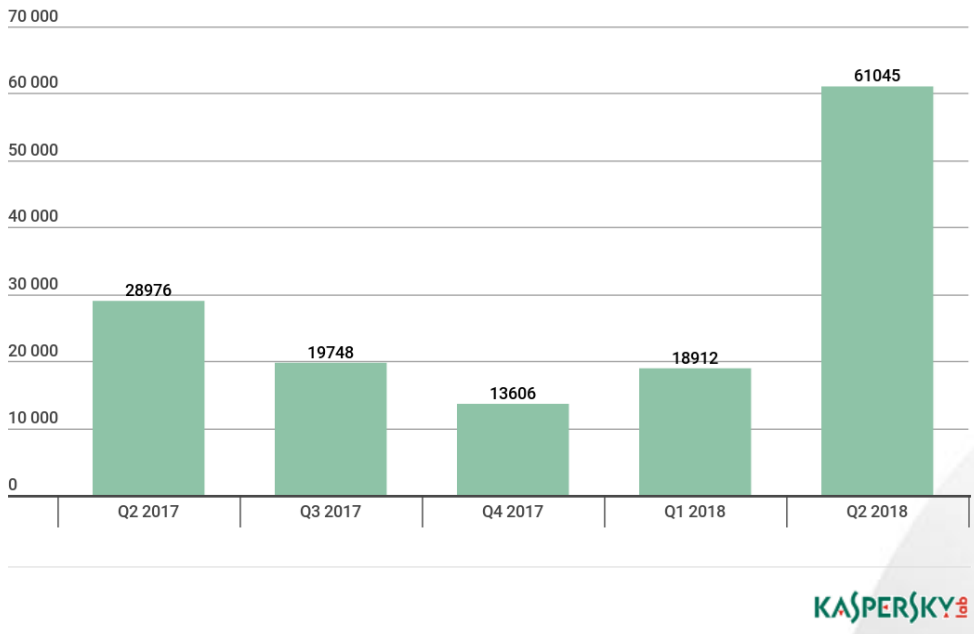
Second place was taken by Trojan-Dropper threats (13%), whose share fell by 7 p.p. Most detected files of this type came from the families Trojan-Dropper.AndroidOS.Piom and Trojan-Dropper.AndroidOS.Hqwar.

The share of advertising apps continued to decreased by 8%, accounting for 9% (against 11%) of all detected threats.

A remarkable development during the reporting period was that SMS Trojans doubled their share up to 8.5% in Q2 from 4.5% in Q1.

Mobile banking Trojans

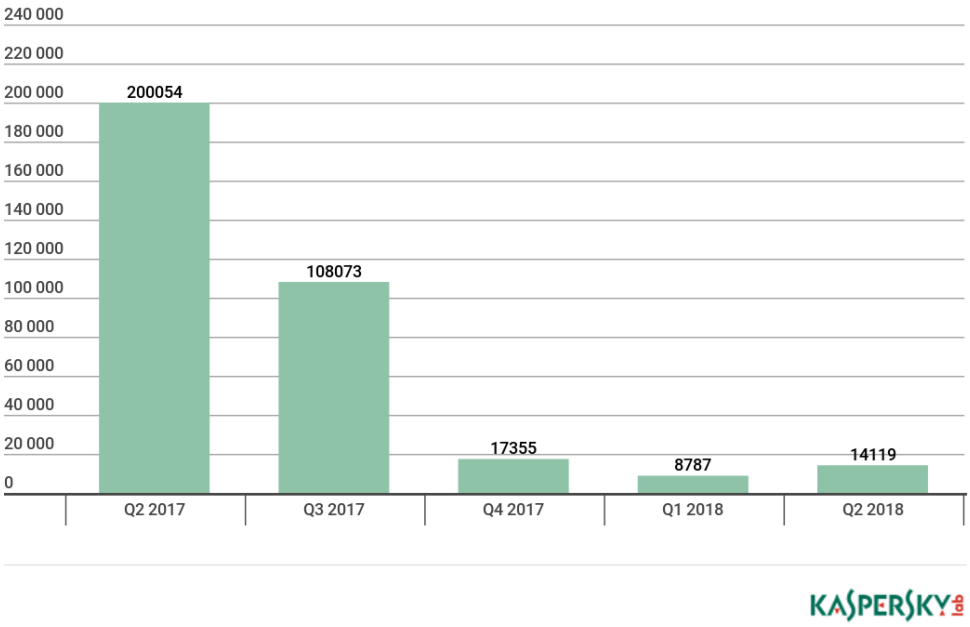
In the reporting period, we detected 61,045 installation packages for mobile banking Trojans, which is 3.2 times more than in Q1 2018. The largest contribution was made by Trojan-Banker.AndroidOS.Hqwar.jck – this verdict was given to nearly half of detected new banking Trojans. Second came Trojan-Banker.AndroidOS.Agent.dq, accounting for about 5,000 installation packages.



Number of installation packages for mobile banking Trojans detected by Kaspersky Lab, Q2 2017 – Q2 2018

Mobile ransomware Trojans

In Q2 2018, we detected 14,119 installation packages for mobile ransomware Trojans, which is larger by half than in Q1.



Number of installation packages for mobile ransomware Trojans detected by Kaspersky Lab, Q2 2017 – Q2 2018

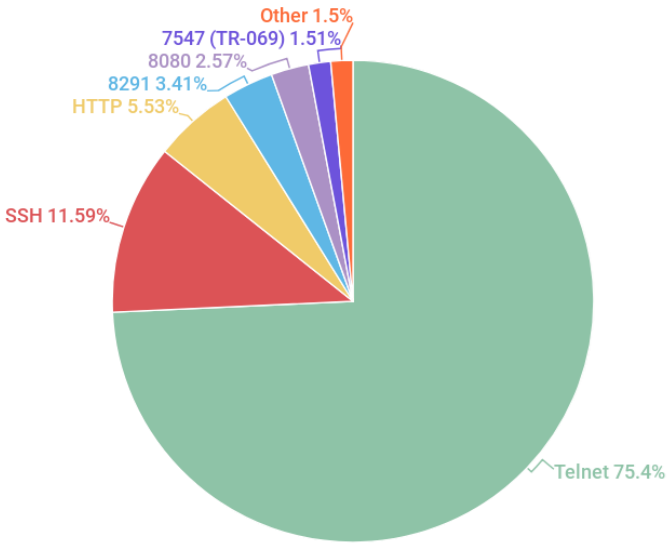
Attacks on IoT devices

Judging by the data from our honeypots, brute forcing Telnet passwords is the most popular method of IoT malware self-propagation. However, recently there has been an increase in the number of attacks against other services, such as control ports. These ports are assigned services for remote control over routers – this feature is in demand e.g. with internet service providers. We have observed attempts to launch attacks on IoT devices via port 8291, which is used by Mikrotik RouterOS control service, and via port 7547 (TR-069), which was used, among other purposes, for managing devices in the Deutsche Telekom network.

In both cases the nature of attacks was much more sophisticated than plain brute force; in particular, they involved exploits. We are inclined to think that the number of such attacks will only grow in the future on the back of the following two factors:

- Brute forcing a Telnet password is a low-efficiency strategy, as there is a strong competition between threat actors. Each few seconds, there are brute force attempts; once successful, the threat actor blocks such the access to Telnet for all other attackers.
- After each restart of the device, the attackers have to re-infect it, thus losing part of the botnet and having to reclaim it in a competitive environment.

On the other hand, the first attacker to exploit a vulnerability will gain access to a large number of device, having spent minimum time.



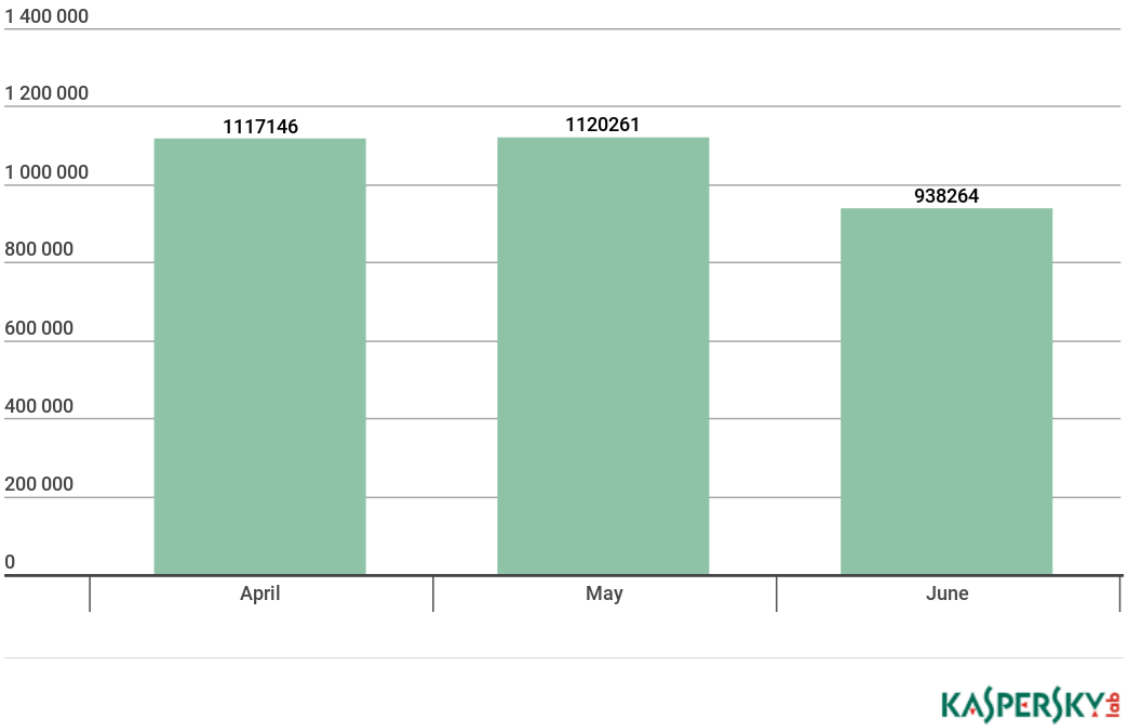
Distribution of attacked services' popularity by number of unique attacking devices, Q2 2018

Cryptominers

As we already reported in Ransomware and malicious cryptominers in 2016-2018, ransomware is shrinking progressively, and cryptocurrency miners is starting to take its place. Therefore, this year we decided to begin to publish quarterly reports on the situation around type of threats. Simultaneously, we began to use a broader range of verdicts as a basis for collecting statistics on miners, so the Q2 statistics may not be consistent with the data from our earlier publications. It includes both stealth miners which we detect as Trojans, and those which are issued the verdict 'Riskware not-a-virus'.

Number of users attacked by cryptominers

In Q2, we detected attacks involving mining programs on the computers of 2,243,581 Kaspersky Lab users around the world.



Number of unique users attacked by cryptominers, Q2 2018

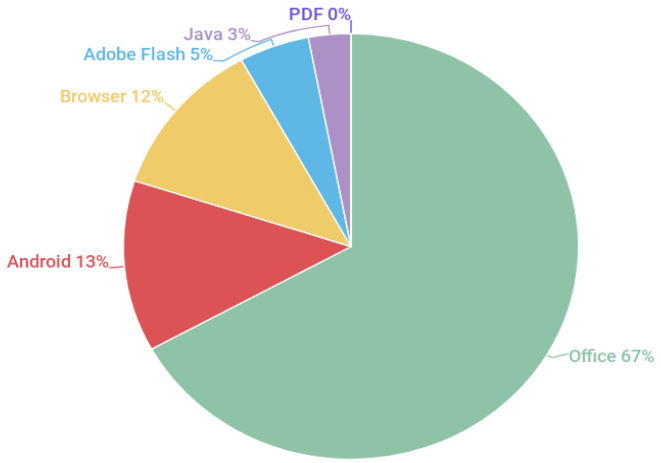
In April and May, the number of attacked users stayed roughly equal, and in June there was a modest decrease in cryptominers' activity.

Vulnerable apps used by cybercriminals

In Q2 2018, we again observed some major changes in the distribution of platforms most often targeted by exploits. The share of Microsoft Office exploits (67%) doubled compared to Q1 (and quadrupled compared with the average for 2017). Such a sharp growth was driven primarily by massive spam messages distributing documents containing an exploit to the vulnerability CVE-2017-11882. This stack overflow-type vulnerability in the old, deprecated Equation Editor component existed in all versions of Microsoft Office released over the last 18 years. The exploit still works stably in all possible combinations of the Microsoft Office package and Microsoft Windows. On the other hand, it allows the use of various obfuscations for bypassing the protection. These two factors made this vulnerability the most popular tool in cybercriminals' hands in Q2. The shares of other Microsoft Office vulnerabilities did no undergo much change since Q1.

Q2 KSN statistics also showed a growing number of Adobe Flash exploits exploited via Microsoft Office. Despite Adobe and Microsoft's efforts to obstruct exploitation of Flash Player, a new 0-day exploit CVE-2018-5002 was discovered in Q2. It propagated in an XLSX file and

used a little-known technique allowing the exploit to be downloaded from a remote source rather than carried in the document body. Shockwave Flash (SWF) files, like many other file formats, are rendered in Microsoft Office documents in the OLE (Object Linking and Embedding) format. In the case of a SWF file, the OLE object contains the actual file and a list of various properties, one of which points to the path to the SWF file. The OLE object in the discovered exploit did not contain an SWF file in it, but only carried a list of properties including a web link to the SWF file, which forced Microsoft Office to download the missing file from the provided link.



KASPERSKY

Distribution of exploits used in cybercriminals' attacks by types of attacked applications, Q2 2018

In late March 2018, a PDF document was detected at VirusTotal that contained two 0-day vulnerabilities: CVE-2018-4990 and CVE-2018-8120. The former allowed for execution of shellcode from JavaScript via exploitation of a software error in JPEG2000 format image processor in Acrobat Reader. The latter existed in the win32k function SetImeInfoEx and was used for further privilege escalation up to SYSTEM level and enabled the PDF viewer to escape the sandbox. Ana analysis of the document and our statistics show that at the moment of uploading to VirusTotal, this exploit was at the development stage and was not used for in-the-wild attacks.

In late April, Kaspersky Lab experts using an in-house sandbox have found the 0-day vulnerability CVE-2018-8174 in Internet Explorer and reported it to Microsoft. An exploit to this vulnerability used a technique associated with CVE-2017-0199 (launching an HTA script from a remote source via a specially crafted OLE object) to exploit a vulnerable Internet Explorer component with the help of Microsoft Office. We are observing that exploit pack creators have

already taken this vulnerability on board and actively distribute exploits to it both via web sites and emails containing malicious documents.

Also in Q2, we observed a growing number of network attacks. There is a growing share of attempts to exploit the vulnerabilities patched with the security update MS17-010; these make up a majority a of the detected network attacks.

Source: https://securelist.com/it-threat-evolution-q2-2018-statistics/87170/

6. New Method Simplifies Cracking WPA/WPA2 Passwords on 802.11 Networks

A new technique has been discovered to easily retrieve the Pairwise Master Key Identifier (PMKID) from a router using WPA/WPA2 security, which can then be used to crack the wireless password of the router. While previous WPA/WPA2 cracking methods required an attacker to wait for a user to login to a wireless network and capture a full authentication handshake, this new method only requires a single frame which the attacker can request from the AP because it is a regular part of the protocol.

This new method was discovered by Jens "atom" Steube, the developer of the popular Hashcat password cracking tool, when looking for new ways to crack the WPA3 wireless security protocol. According to Steube, this method will work against almost all routers utilizing 802.11i/p/q/r networks with roaming enabled.

Previous WPA/WPA2 crackers required an attacker to patiently wait while listening in on a wireless network until a user successfully logged in. They could then capture the four-way handshake in order to crack the key.

"With any previous attacks on WPA an attacker has to be in a physical position that allows them to record the authentication frames from both the access point and the client (the user)," Steube told BleepingComputer. "The attacker also has to wait for a user to login to the network and have a tool running in that exact moment to dump the handshake to disk."

Now an attacker simply has to attempt to authenticate to the wireless network in order to retrieve a single frame in order to get access to the PMKID, which can then be cracked to retrieve the Pre-Shared Key (PSK) of the wireless network.

It should be noted that this method does not make it easier to crack the password for a wireless network. It instead makes the process of acquiring a hash that can can be attacked to get the wireless password much easier.

How long to crack a WPA/WPA2 wireless password?

While Steube's new method makes it much easier to access a hash that contains the pre-shared key that hash still needs to be cracked. This process can still take a long time depending on the complexity of the password.

Unfortunately, many users do not know how to change their wireless password and simply use the PSK generated by their router.

"In fact, many users don't have the technical knowledge to change the PSK on their routers," Steube told BleepingComputer. "They continue to use the manufacturer generated PSK and this makes attacking WPA feasible on a large group of WPA users."

As certain manufacturers create a PSK from a pattern that can easily be determined, it can be fed into a program like Hashcat to make it easier to crack the wireless password.

"Cracking PSKs is made easier by some manufacturers creating PSKs that follow an obvious pattern that can be mapped directly to the make of the routers. In addition, the AP mac address and the pattern of the ESSID allows an attacker to know the AP manufacturer without having physical access to it," Steube continued to tell us via email. "Attackers have collected the pattern used by the manufacturers and have created generators for each of them, which can then be fed into hashcat. Some manufacturers use pattern that are too large to search but others do not. The faster your hardware is, the faster you can search through such a keyspace. A typical manufacturers PSK of length 10 takes 8 days to crack (on a 4 GPU box)."

Protecting your router's password from being cracked

In order to properly protect your wireless network it is important to create your own key rather than using the one generated by the router. Furthermore this key should long and complex by consisting of numbers, lower case letters, upper case letters, and symbols (&%$!).

"There's actually a lot of scientific research on this topic. There's many different ways to create good passwords and to make them memorable," Steube told BleepingComputer when we asked for recommendations on strong wireless passwords. "Personally I use a password manager and let it generate true random passwords of length 20 - 30."

Source: https://www.bleepingcomputer.com/news/security/new-method-simplifies-cracking-wpa-wpa2-passwords-on-80211-networks/

7. Cisco IOS and IOS XE Software Internet Key Exchange Version 1 RSA-Encrypted Nonces Vulnerability

A vulnerability in the implementation of RSA-encrypted nonces in Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to obtain the encrypted nonces of an Internet Key Exchange Version 1 (IKEv1) session.

The vulnerability exists because the affected software responds incorrectly to decryption failures. An attacker could exploit this vulnerability sending crafted ciphertexts to a device configured with IKEv1 that uses RSA-encrypted nonces. A successful exploit could allow the attacker to obtain the encrypted nonces.

There are no workarounds that address this vulnerability.

Source: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180813-rsa-nonce

8. DEF CON 2018: 'Man in the Disk' Attack Surface Affects All Android Phones

Sloppy Android developers not following security guidelines for external storage opens the door to device takeover and more.

A function of the Android storage mechanism opens up an attack surface that affects all Android devices, and allows an attacker to corrupt data, steal sensitive information or even take control of a mobile phone.

Simply put, the issue – dubbed "man in the disk" – allows a bad actor to hijack the communications between privileged apps and the device disk, bypassing sandbox protections to gain access to app functions and potentially wreak havoc.

Source: https://threatpost.com/def-con-2018-man-in-the-disk-attack-surface-affects-all-android-phones/134993/

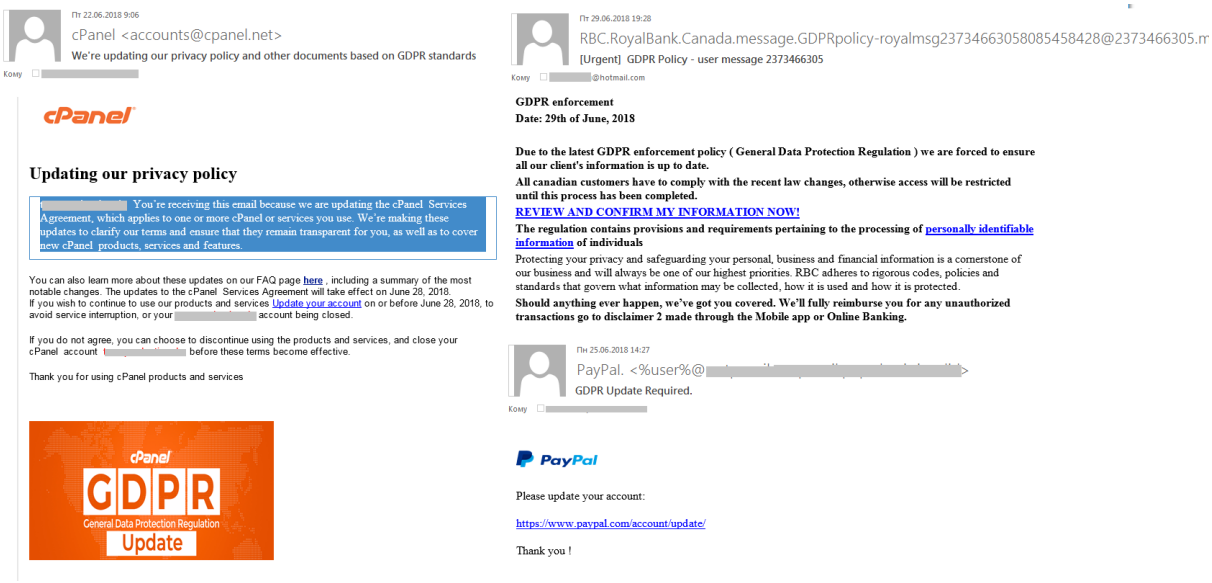
9. Spam and phishing in Q2 2018

Quarterly highlights

GDPR as a phishing opportunity

In the first quarter, we discussed spam designed to exploit GDPR (General Data Protection Regulation), which came into effect on May 25, 2018. Back then spam traffic was limited to invitations to participate in workshops and other educational events and purchase software or databases. We predicted that fraudulent emails were soon to follow. And we found them in the second quarter.

As required by the regulation, companies notified email recipients that they were switching to a new GDPR-compliant policy and asked them to confirm permission to store and process personal information. This was what criminals took advantage of. To gain access to the personal information of well-known companies' customers, criminals sent out phishing emails referencing the GDPR and asking recipients to update their account information. To do this, customers had to click on the link provided and enter the requested data, which immediately fell into the hands of the criminals. It must be noted that the attackers were targeting customers of financial organizations and IT service providers.



Phishing emails exploiting GDPR

Source: *https://securelist.com/spam-and-phishing-in-q2-2018/87368/*

10. Researchers Identify 25 Android Smartphone Models with Severe Vulnerabilities

Speaking at DefCon in Las Vegas last week, Kryptowire researchers said that 25 Android smartphone models contain a slew of vulnerabilities which may expose the user to attack from the time of purchase.

After analyzing Android vendors and carriers from the low-end to flagship, more expensive handsets, the team discovered bugs ranging from minimal risk to critical problems in pre-installed apps and firmware.

As reported by sister site CNET, Kryptowire uncovered a total of 38 different vulnerabilities in pre-loaded applications and the firmware builds of 25 Android handsets, 11 of which are sold in the United States.

The researchers said their research was primarily based in the US but the impact of these bugs is worldwide.

"All of these are vulnerabilities that are prepositioned," Angelos Stavrou, Kryptowire CEO told attendees at the conference. "They come as you get the phone out the box. That's important because consumers think they're only exposed if they download something that's bad."

OEMs and smartphone vendors impacted include ZTE, Sony, Nokia, LG, Essential, and Asus, among others.

Source: *https://www.zdnet.com/article/25-android-smartphone-models-contain-severe-vulnerabilities-off-the-shelf/*

11. Microsoft Cortana Flaw Could Allow Browsing on Locked Systems

Security researchers have shown that having Microsoft Cortana enabled on the Windows lock screen could be a security risk. In such a configuration, users could compromise a system or lead to or impersonate a user using credentials stored in the browser cache.

The Cortana digital assistant is enabled by default on the lock screen and it can answer questions, voiced or typed, even if the user is not authenticated. While in this state, it relies on Edge and a limited version of Internet Explorer 11 to do its job.

Researchers from McAfee detail how this can work to an attacker's advantage if they have physical access to the device. With some effort and by asking the right questions, the experts were able to point Cortana to a domain under their control without unlocking it. As they had control over this domain, they could have have run any javascript they wanted on the visiting computer's browser.

Source: *https://www.bleepingcomputer.com/news/security/microsoft-cortana-flaw-could-allow-browsing-on-locked-systems/*

12. ThreatList: Telecom Sector Plagued with Advanced Malware

Advanced behavior malware threats are targeting telecom services – at a higher level than the global average, researchers found.

Lastline's findings, published today, found that telecom sector threats are "ahead of the curve," based on an analysis of threats to the segment over the past 30 days. In comparing the results to overall global malscape threats in all sectors, the report found that telecom over-indexes in advanced, stealthy malware that may not have been seen before; vague antivirus

flags; and the volume of malicious files being used — all of which is being used to pick off email credentials from the ISP side of the house.

"There were significant differences in the trends seen in telecom services compared to the global trend," said researchers, in the study. "Threats arriving in telecom services organizations are ahead of the curve, essentially a zero-day attack, with very few prior submissions of samples being evidenced on VirusTotal. These malspam attacks represent the tip of emerging campaigns and reflect the inherent criminal value in stolen email credentials."

Source: *https://threatpost.com/threatlist-telecom-sector-plagued-with-advanced-malware/136543/*

13. ThreatList: Almost Half of the World's Top Websites Deemed 'Risky'

Nearly half of the world's most popular websites are risky places to visit, according to a fresh analysis of top Alexa sites. Vulnerable code, the running of active content from risky background sites, and large amounts of code downloads marked a good chunk of the top 50 websites used in all of the countries examined.

According to Menlo Security's annual State of the Web report released Thursday, on a broader level, a full 42 percent of the Alexa Top 100,000 sites globally were deemed "risky," because they either used unpatched server software known to be vulnerable; or, the site had served malware/launched attacks, or suffered a security breach in the past year.

Source: *https://threatpost.com/threatlist-almost-half-of-the-worlds-top-websites-deemed-risky/136636/*

14. Zero-Day In Microsoft's VBScript Engine Used By Darkhotel APT

A vulnerability in the VBScript engine has been used by hackers working for North Korea to compromise systems targeted by the Darkhotel operation.

VBScript is available in the latest versions of Windows and in Internet Explorer 11. In recent versions of Windows, though, Microsoft disabled execution of VBScript in the default configuration of its browser, making it immune to the vulnerability.

Security researchers from Trend Micro noticed a VBScript vulnerability being exploited in the wild a day after Microsoft delivered its regular updates for Windows in July. Now tracked as CVE-2018-8373, the bug has been addressed in this month's patch delivery. It is a use-after-free memory corruption that allows the attacker to run shellcode on the compromised computer.

Source: *https://www.bleepingcomputer.com/news/security/zero-day-in-microsofts-vbscript-engine-used-by-darkhotel-apt/*

15. New “Turning Tables” Technique Bypasses All Windows Kernel Mitigations

Security researchers have discovered a new exploitation technique that they say can bypass the kernel protection measures present in the Windows operating systems.

Discovered by security researchers Omri Misgav and Udi Yavo from enSilo, the technique is named Turning Tables, and exploits Windows' page tables.

Page tables are a data structure common to all operating systems, not just Windows, that are used to store mappings between virtual memory and physical memory.

The Turning Tables technique relies on crafting malicious code that alters these "shared code pages" in a negative way to affect the execution of other processes, some of which have higher privileges.

By doing this, the Turning Tables technique allows attackers to elevate the privileges of their code to higher levels, such as SYSTEM.

Furthermore, since the concept of page tables is also used by Apple and the Linux project, macOS and Linux are, in theory, also vulnerable to this technique, albeit the researchers have not verified such attacks, as of yet.

Source: *https://www.bleepingcomputer.com/news/security/new-turning-tables-technique-bypasses-all-windows-kernel-mitigations/*

16. Turla Outlook Backdoor Uses Clever Tactics for Stealth and Persistence

The Outlook backdoor used by Turla APT group for its espionage operations is an unusual beast built for stealth and persistence, capable to survive in highly restricted networks.

The malware does not connect to a command and control server and can receive updates and instructions via PDF files delivered to the victim’s email address. Its control depends only on an email exchange that can originate from any address the attacker chooses.

Security researchers from ESET analyzed the functionality of the utility and managed to learn how it can exfiltrate data without triggering the alarm.

The Turla group counts on this backdoor since at least 2013 and has developed it from a basic utility that only dumped email content to a tool that can execute PowerShell commands with the help of Empire PSInject open-source kit.

Source: *https://www.bleepingcomputer.com/news/security/turla-outlook-backdoor-uses-clever-tactics-for-stealth-and-persistence/*

17. Apache Struts Remote Code Execution Vulnerability Affecting Cisco Products: August 2018

A vulnerability in Apache Struts could allow an unauthenticated, remote attacker to execute arbitrary code on a targeted system.

The vulnerability exists because the affected software insufficiently validates user-supplied input, allowing the use of results with no namespace value and the use of url tags with no value or action. In cases where upper actions or configurations also have no namespace or a wildcard namespace, an attacker could exploit this vulnerability by sending a request that submits malicious input to the affected application for processing. If successful, the attacker could execute arbitrary code in the security context of the affected application on the targeted system.

Source: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180823-apache-struts

18. Linux and FreeBSD Kernels TCP Reassembly Denial of Service Vulnerabilities Affecting Cisco Products: August 2018

On August 6, 2018, the Vulnerability Coordination team of the National Cyber Security Centre of Finland (NCSC-FI) and the CERT Coordination Center (CERT/CC) disclosed vulnerabilities in the TCP stacks that are used by the Linux and FreeBSD kernels. These vulnerabilities are publicly known as SegmentSmack.

The vulnerabilities could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. An attack could be executed by using low transfer rates of TCP packets, unlike typical distributed denial of service (DDoS) attacks.

The vulnerabilities are due to inefficient TCP reassembly algorithms in the TCP stacks that are used by the affected kernels. Linux Kernel Versions 4.9 and later and all supported versions of the FreeBSD kernel are known to be affected by these vulnerabilities.

An attacker could exploit these vulnerabilities by sending a stream of packets that are designed to trigger the issue in an established TCP session with an affected device. A sustained DoS condition requires the attacker to maintain a continuous stream of malicious traffic. Due to the required use of an established session, an attack cannot be performed using spoofed IP addresses.

Source: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180824-linux-tcp

19. OCR Software Dev Exposes 200,000 Customer Documents

A misconfigured MongoDB server belonging to Abbyy, an optical character recognition software developer, allowed public access to customer files.

Independent security researcher Bob Diachenko discovered the database on August 19 hosted on the Amazon Web Services (AWS) cloud platform. It was 142GB in size and it allowed access without the need to log in.

The sizeable database included scanned documents of the sensitive kind: contracts, non-disclosure agreements, internal letters, and memos. Included were more than 200,000 files from Abbyy customers who scanned the data and kept it at the ready in the cloud.

The duration of the exposure is unclear, but it is not far-fetched to assume that data has already been accessed by unauthorized individuals. Such a finding could be worth a lot of money.

Abbyy's customer portfolio counts high-profile names from various sectors. Volkswagen, Deloitte, PwC, PepsiCo, Sberbank, McDonald's are just a few of Abbyy's clients.

Source: *https://www.bleepingcomputer.com/news/security/ocr-software-dev-exposes-200-000-customer-documents/*

20. Exploit Published for Unpatched Flaw in Windows Task Scheduler

The vulnerability is a "local privilege escalation" issue that allows an attacker to elevate the access of malicious code from a limited USER role to an all-access SYSTEM account.

The vulnerability resides in the Windows Task Scheduler, and more precisely in the Advanced Local Procedure Call (ALPC) interface.

The ALPC interface is a Windows-internal mechanism that works as an inter-process communication system. ALPC enables a client process running within the OS to ask a server process running within the same OS to provide some information or perform some action.

The researcher, who goes online by the name of SandboxEscaper, has released proof-of-concept (PoC) code on GitHub for exploiting the ALPC interface to gain SYSTEM access on a Windows system.

Malware authors will particularly be interested in this PoC, as it allows benign malware to gain admin access on targeted systems using an exploit more reliable than many existing methods.

Source: *https://www.bleepingcomputer.com/news/security/exploit-published-for-unpatched-flaw-in-windows-task-scheduler/*

21. ThreatList: Ransomware Attacks Down, Fileless Malware Up in 2018

The use of fileless malware in attacks continues to grow and now represents 42 out of 1,000 endpoint attacks, according to an analysis of 2018 data by one security firm. The uptick represents a 94 percent increase in the use of fileless-based attacks between January and June 2018.

The study, released Tuesday by SentinelOne, also noted rollercoaster fluctuation in the prevalence of ransomware attacks in the same time period. Ransomware attacks represented just over 10 out of 1,000 attacks in January. In February, 14 out 1,000 attacks were tied to ransomware. As of June, ransomware attacks are at an all-time yearly low of 5.1 per 1,000 attacks.

Source: *https://threatpost.com/threatlist-ransomware-attacks-down-fileless-malware-up-in-2018/136962/*

22. Active Attacks Detected Using Apache Struts Vulnerability CVE-2018-11776

After last week a security researcher revealed a vulnerability in Apache Struts, a piece of very popular enterprise software, active exploitation attempts have started this week.

The vulnerability in question is tracked as CVE-2018-11776, a remote code execution flaw that allows an attacker to gain control over Struts-based web applications.

The vulnerability is not exploitable in default Struts configurations, according to an analysis by Palo Alto Networks, but the flaw is of interest to everyone, mainly because Struts is used by some of the world's largest companies (including Equifax, which suffered a major data breach last year because of a Struts flaw).

Over the course of last week, several security researchers have put together different proof-of-concept (PoC) scripts for CVE-2018-11776, including a step-by-step tutorial.

One of these PoCs has also been embedded into an all-in-one Struts exploitation toolkit that combines previous Struts remote code execution flaws into a hacker's dream.

Source: *https://www.bleepingcomputer.com/news/security/active-attacks-detected-using-apache-struts-vulnerability-cve-2018-11776/*

23. Cisco Data Center Network Manager Path Traversal Vulnerability

A vulnerability in Cisco Data Center Network Manager software could allow an authenticated, remote attacker to conduct directory traversal attacks and gain access to sensitive files on the targeted system.

The vulnerability is due to improper validation of user requests within the management interface. An attacker could exploit this vulnerability by sending malicious requests containing directory traversal character sequences within the management interface. An exploit could allow the attacker to view or create arbitrary files on the targeted system.

Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

Source: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180828-dcnm-traversal

Advanced Security Operations Center
Telelink Business Services
www.telelink.com

If you want to learn more about ASOC and how it can improve your security posture, contact us at: **asoc.sales@telelink.com**