THREAT REPORT Q1 2020

WeLiveSecurity.com
@ESETresearch
ESET GitHub

ENJOY SAFER TECHNOLOGY™

Contents

Foreword

Welcome to the first quarterly ESET Threat Report!

The first quarter of 2020 was, without a doubt, defined by the outbreak of COVID-19 – now a pandemic that has put much of the world under lockdown, disrupting peoples' lives in unprecedented ways.

In the face of these developments, many businesses were forced to swiftly adopt work-from-home policies, thereby facing numerous new challenges. Soaring demand for remote access and videoconferencing applications attracted cybercriminals who quickly adjusted their attack strategies to profit from the shift.

Cybercriminals also haven't hesitated to exploit public concerns surrounding the pandemic. In March 2020, we saw a surge in scam and malware campaigns using the coronavirus pandemic as a lure, trying to capitalize on people's fears and hunger for information.

Even under lockdown, our analysts, detection engineers and security specialists continued to keep a close eye on this quarter's developments. Some threat types – such as cryptominers or Android malware – saw a decrease in detections compared with the previous quarter; others – such as web threats and stalkerware – were on the rise. Web threats in particular have seen the largest increase in terms of overall numbers of detections, a possible side effect of coronavirus lockdowns.

ESET Research Labs also did not stop investigating threats – Q1 2020 saw them dissect obfuscation techniques in Stantinko's new cryptomining module; detail the workings of advanced Brazil-targeting banking trojan Guildma; uncover new campaigns by the infamous Winnti Group and Turla; and uncover Kr00k, a previously unknown vulnerability affecting the encryption of over a billion Wi-Fi devices.

Before lockdowns became the new normal, experts from ESET Research Labs were sharing their insights at security conferences and events around the world. In February, they unveiled the Kr00k vulnerability research and led a workshop for hunting Linux malware at RSA Conference 2020, and presented two talks at BlueHat IL.

*While seeing our researchers on stage might not be possible for a while, you can still follow their findings on our blog, **WeLiveSecurity**, and the **ESETresearch Twitter** feed. And, don't forget, in these Threat Reports!*

Happy reading, stay safe – and healthy!

Roman Kováč, Chief Research Officer

FEATURED STORY

Kr00k: Serious vulnerability affected encryption of billion+ Wi-Fi devices

Miloš Čermák and Robert Lipovský

ESET researchers uncover a previously unknown security flaw allowing an adversary to decrypt some wireless network packets transmitted by vulnerable devices.

ESET researchers discovered a previously unknown vulnerability in Wi-Fi chips and named it Kr00k.

Assigned CVE-2019-15126, this serious flaw causes vulnerable devices to use an all-zero encryption key to encrypt part of the user's communication. In a successful attack, this allows an adversary to decrypt some wireless network packets transmitted by a vulnerable device.

Kr00k affects devices with Wi-Fi chips madeby Broadcom and Cypress that haven't yet been patched. These are the most common Wi-Fi chips used in contemporary Wi-Fi capable devices such as smartphones, tablets, laptops, and IoT gadgets.

Not only client devices but Wi-Fi access points and routers with Broadcom chips were affected by the vulnerability, thus making many environments with unaffected or already patched client devices vulnerable anyway.

Our tests show that prior to patching, some client devices by Amazon (Echo, Kindle), Apple (iPhone, iPad, MacBook), Google (Nexus), Samsung (Galaxy), Raspberry (Pi 3), Xiaomi (RedMi), as well as some access points by Asus and Huawei, were vulnerable to Kr00k. This totaled to over a billion Wi-Fi-capable devices and access points, at a conservative estimate. Further, many other vendors whose products we did not test also use the affected chipsets in their devices.

Both WPA2-Personal and WPA2-Enterprise protocols, with AES-CCMP encryption, are affected by this vulnerability.

Kr00k is related to ***KRACK*** [1] (Key Reinstallation Attacks), discovered in 2017 by Mathy Vanhoef, but also fundamentally different. In the beginning of our research, we found Kr00k to be one of the possible causes behind the "reinstallation" of an all-zero encryption key, observed in tests for KRACK attacks. This followed our previous findings that ***Amazon Echo was vulnerable to KRACK*** [2].

We responsibly disclosed Kr00k to chip manufacturers Broadcom and Cypress, who subsequently released updates during an extended disclosure period.

We also worked with the Industry Consortium for Advancement of Security on the Internet (*ICASI*) [3] to ensure that all potentially affected parties – including affected device manufacturers using the vulnerable chips, as well as any other possibly affected chip manufacturers – were aware of Kr00k.

According to our information, patches for devices from major manufacturers have been released by now. To protect yourself, as a device owner, make sure you have applied the latest available updates to your Wi-Fi-capable devices, including phones, tablets, laptops, IoT devices, and Wi-Fi access points and routers. As a device manufacturer, please inquire about patches for Kr00k directly with your chip manufacturer.

Special thanks to our colleagues Juraj Bartko and Martin Kalužník, who greatly contributed to this research. We'd also like to commend Amazon, Broadcom, and Cypress for their good cooperation in dealing with the reported issues and ICASI for their assistance informing as many of the impacted vendors as possible.

WeLiveSecurity blogpost [4] | *Kr00k white paper* [5] | *Kr00k website* [6] | *RSAC 2020 presentation* [7]

The Kr00k vulnerability

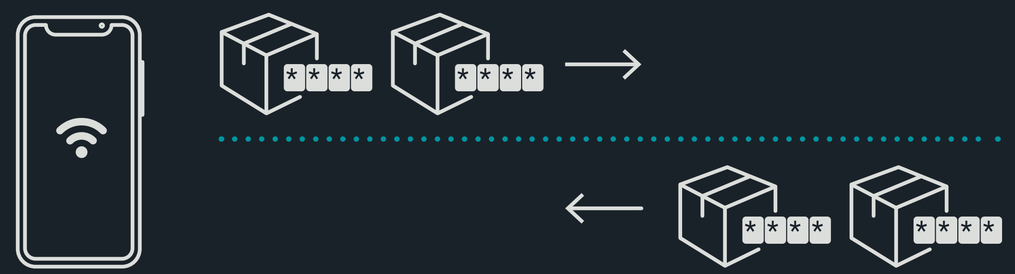
Kr00k manifests itself after a disassociation. Once a station's WLAN session gets disassociated, the session key (TK) stored in the Wireless Network Interface Controller's (WNIC) Wi-Fi chip is cleared in memory – set to zero. This is expected behavior, as no further data is supposed to be transmitted after the disassociation. However, we discovered that all data frames that were left in the chip's Tx (transmit) buffer were transmitted after being encrypted with this all-zero key.

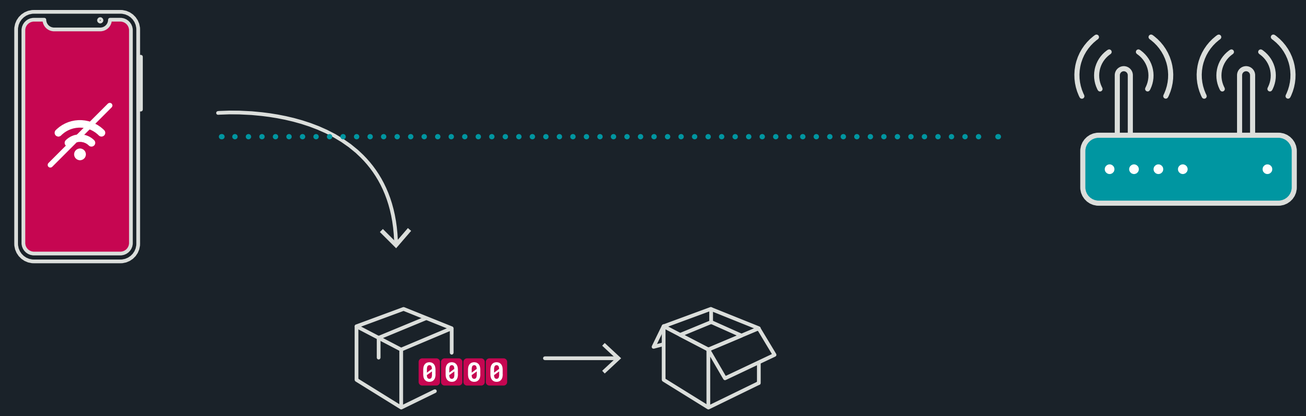
As a result, the Kr00k vulnerability allows an attacker to break into encrypted wireless network traffic of unpatched devices.

Fortunately, there are a few aspects that limit the impact of the bug:

Firstly, it's a vulnerability concerning encryption on the wireless LAN (Wi-Fi) layer. It has nothing to do with TLS – the encryption that secures online banking, email, and any website prefixed with HTTPS. In other words, a successful attack exploiting Kr00k degrades a victim's security a step towards what they'd have on an open Wi-Fi network.

Secondly, as it's tied to Wi-Fi, the attacker would have to be in close proximity to the victim's Wi-Fi signal. But – wouldn't need to know their Wi-Fi password!





Kr00k causes transmission of data encrypted with an all-zero key

NEWS FROM THE LAB

Latest findings from ESET Research Labs across the world

Cryptomining

Stantinko botnet adds cryptomining to its pool of criminal activities

ESET researchers discovered that the criminals behind the half-million-strong *Stantinko botnet* [8] – known to have been active since at least 2012 and mainly targeting users in Russia, Ukraine, Belarus and Kazakhstan – started distributing a Monero-mining module to the computers they control. Previously, the botnet performed click fraud, ad injection, social network fraud and password stealing attacks.

WeLiveSecurity blogpost [9]

Stantinko's new cryptominer features unique obfuscation techniques

In their investigation into Stantinko's new cryptomining module, ESET researchers discovered several obfuscation techniques intended to protect against detection and thwart analysis. Aiming to help the cybersecurity industry improve protection against sophisticated threats, ESET researchers shed light on the techniques and described a possible approach to deobfuscating some of them – most notably obfuscation of strings and control-flow obfuscation.

WeLiveSecurity blogpost [10]

Banking malware

Guildma: The Devil drives electric

ESET researchers dissected Guildma, a highly prevalent, Brazil-targeting banking trojan notable for its innovative methods of execution, sophisticated attack techniques as well as impact in the region.

Besides targeting financial institutions, Guildma also attempts to steal credentials for email accounts, e-shops and streaming services. Like many other Latin American banking trojans, Guildma implements a number of backdoor functions, abuses legitimate tools, and its functionality is split into many modules. It spreads via spam emails with malicious attachments and has affected at least ten times as many victims as other Latin American banking trojans analyzed by ESET.

WeLiveSecurity blogpost [11]

APT GROUP ACTIVITY

Highlights from ESET investigations into Advanced Persistent Threat groups and their campaigns

Winnti Group

The Winnti Group, active since at least 2012, is responsible for high-profile supply-chain attacks against the video game and software industries. It is also known for having compromised various targets in the healthcare and education sectors.

Winnti Group targeting universities in Hong Kong

ESET researchers discovered a new campaign run by the Winnti Group against two Hong Kong universities. The researchers found a new variant of ShadowPad, the group's flagship backdoor, deployed using a new launcher and embedding numerous modules. The Winnti malware was also found at these universities a few weeks prior to the ShadowPad backdoor.

This campaign was taking place as widespread civic protests swept across Hong Kong, including the territory's universities.

In addition to the two confirmed compromised universities, ESET has indications that at least three additional universities may have been affected. The attackers were interested in stealing information from the victims' machines.

ESET contacted the compromised universities and provided the necessary information and assistance to remediate the compromise.

Both ShadowPad and Winnti, found at these universities in November 2019, contain campaign identifiers and command and control URLs matching the names of the universities, which indicates a targeted attack.

Mathieu Tartare, ESET Malware Researcher

ESET researchers recently published a *white paper* [12] updating their understanding of the arsenal of the Winnti Group, following a blog post documenting a *supply-chain attack targeting the videogame industry in Asia* [13]. Additionally, they published a blog post on a *new backdoor named skip-2.0* [14] that targets Microsoft SQL Server.

WeLiveSecurity blogpost [15]

Turla

Turla, also known as Snake, is an infamous espionage group recognized for its complex malware. It is believed to have been operating since at least 2008, when it successfully breached the US military.

New Turla backdoor delivered via watering hole on Armenian websites

ESET researchers found a watering hole operation targeting several high-profile Armenian websites. It relied on a social engineering trick – a fake Adobe Flash update – as a lure to deliver two previously undocumented pieces of malware, dubbed NetFlash and PyFlash by the researchers.

In this operation, Turla compromised at least four Armenian websites, including two belonging to the government. Thus, it is likely the targets included government officials and politicians. ESET notified the Armenian national CERT and shared the analysis with them before publication.

According to ESET telemetry, the following websites were compromised:

- armconsul[.]ru: The consular Section of the Embassy of Armenia in Russia
- mnp.nkr[.]am: Ministry of Nature Protection and Natural Resources of the Republic of Artsakh
- aiisa[.]am: The Armenian Institute of International and Security Affairs
- adgf[.]am: The Armenian Deposit Guarantee Fund

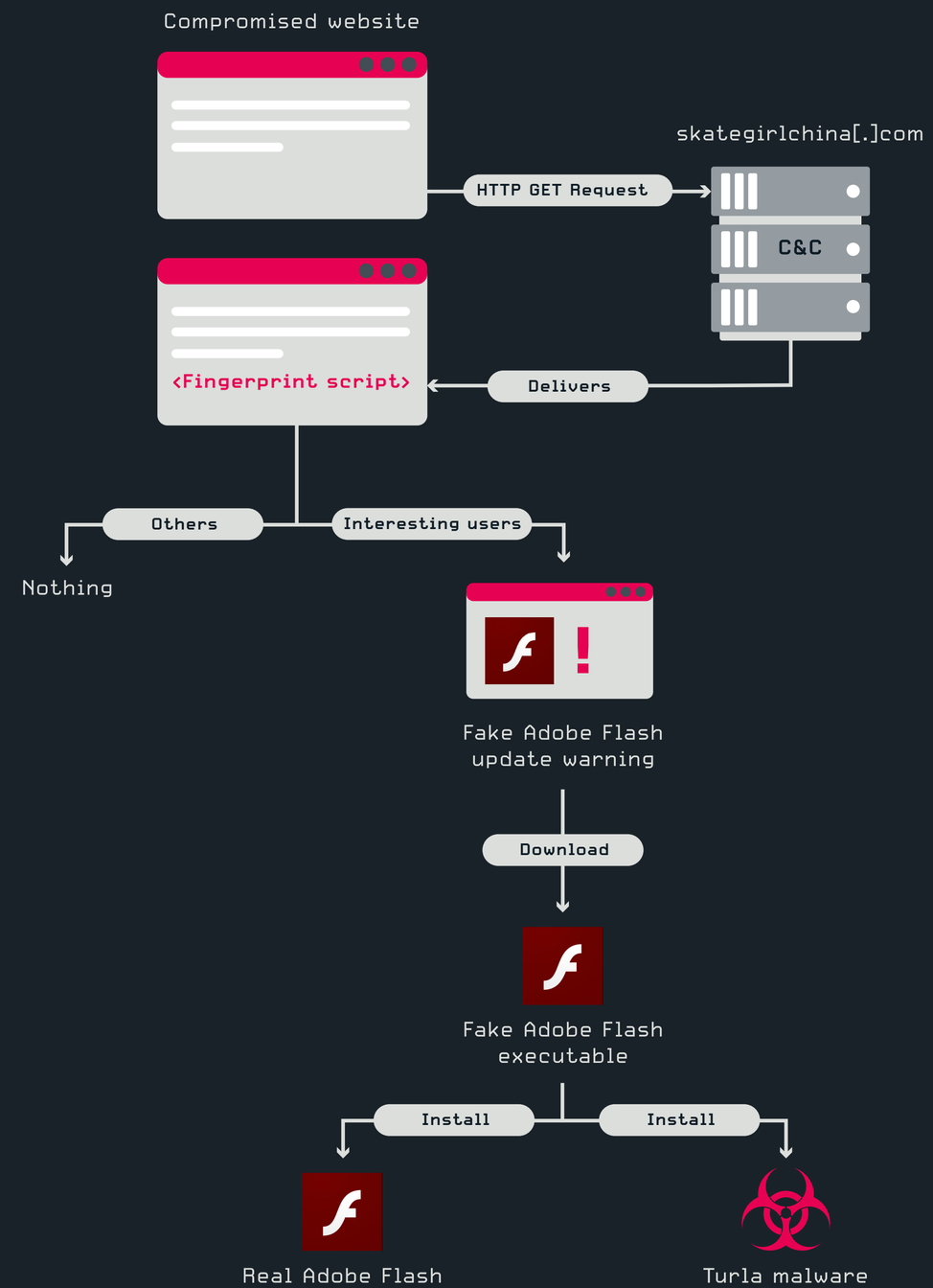
If the website visitor is deemed interesting, the server replies with a piece of JavaScript code that displays a fake Adobe Flash update warning. Data from ESET telemetry suggests that, for this campaign, only a very limited number of visitors were considered interesting by Turla's operators.

Matthieu Faou, ESET Malware Researcher

A fake Adobe Flash update pop-up window warning is displayed to visitors of interest in order to trick them into downloading a malicious Flash installer. Once the malicious executable is downloaded, and if the user launches it manually, a Turla malware variant and a legitimate Adobe Flash program are installed.

The scheme on the right shows an overview of the initial compromise process.

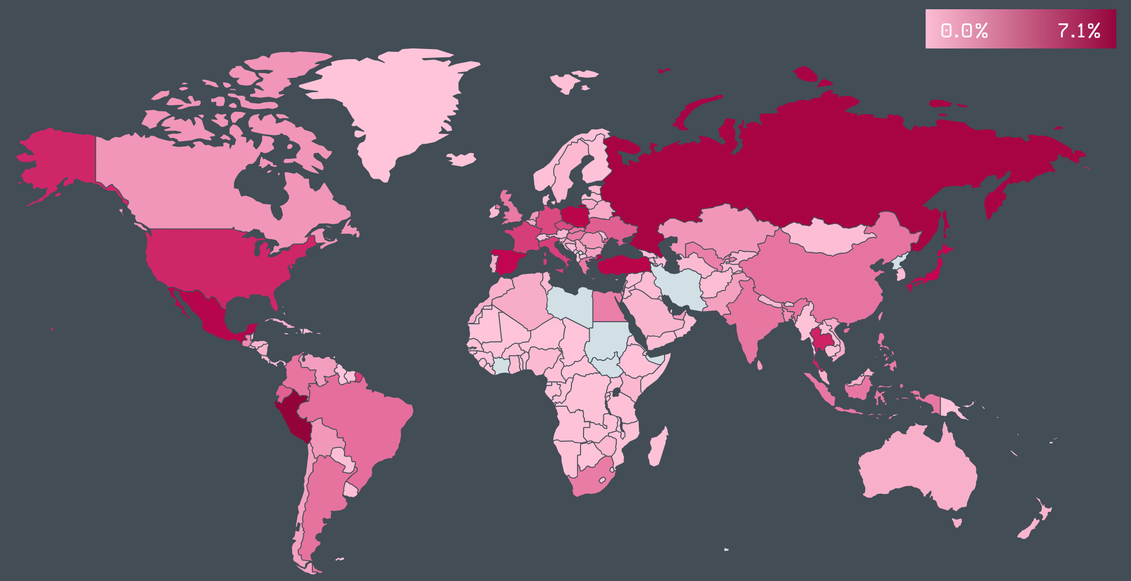
WeLiveSecurity blogpost [16]



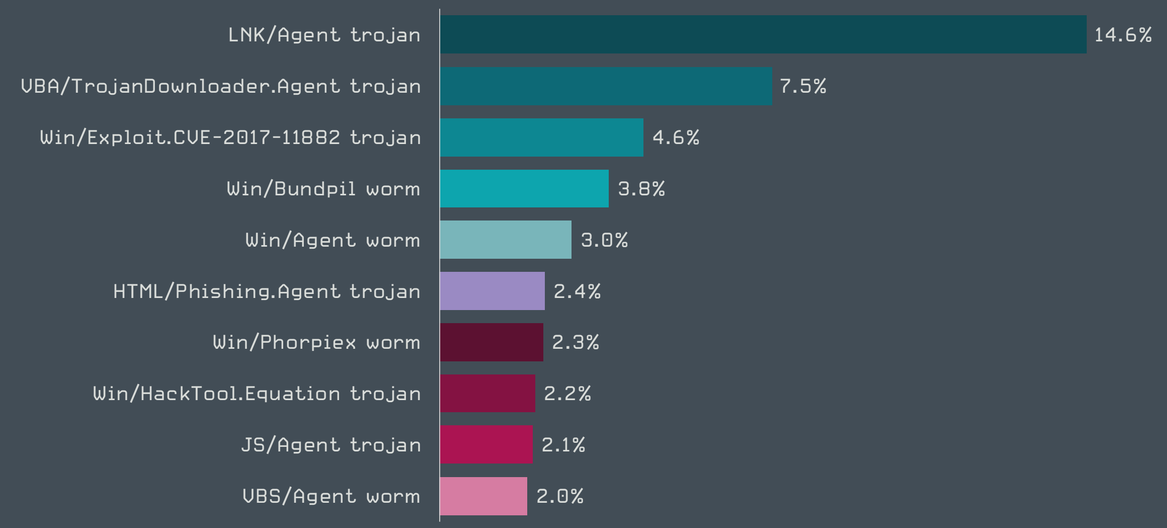
Overview of the watering hole operation

STATISTICS & TRENDS

The threat landscape in Q1 2020 as seen by ESET telemetry



Rate of malware detections in Q1 2020



Top 10 malware detections in Q1 2020 (% of malware detections)

Top 10 malware detections

LNK/Agent trojan Q4 2019: 1 ⇔ Q1 2020: 1

LNK/Agent is a detection name for malware utilizing Windows LNK shortcut files to execute other files on the system. Shortcut files have been gaining popularity among attackers, as they are typically considered benign and less likely to raise suspicion. LNK/Agent files don't contain any payload and are usually parts of other, more complex malware. They are often used to achieve persistence of the main malicious files on the system or as a part of the compromise vector.

VBA/TrojanDownloader.Agent trojan Q4 2019: 2 ⇔ Q1 2020: 2

VBA/TrojanDownloader.Agent is a detection typically covering maliciously crafted Microsoft Office files that try to manipulate users into enabling the execution of malicious macros. Upon execution, the enclosed malicious macro typically downloads and executes additional malware. The malicious documents are usually sent as email attachments, disguised as important information relevant to the recipient.

Win/Exploit.CVE-2017-11882 trojan Q4 2019: 4 ↑ Q1 2020: 3

This detection name stands for specially crafted documents exploiting the *CVE-2017-11882* [17] vulnerability found in the Microsoft Equation Editor, a component of Microsoft Office. The exploit is publicly available and usually used as the first stage of compromise. When the user opens the malicious document, the exploit is triggered and its shellcode executed. Additional malware is then downloaded onto the computer to perform arbitrary malicious actions.

Win/Bundpil worm Q4 2019: 3 ↓ Q1 2020: 4

Win32/Bundpil is a worm capable of spreading via removable media. It is a part of Wauchos, one of the largest botnet families, also known as *Gamarue* [18] or Andromeda. Bundpil was designed to enhance the persistence of Wauchos and to make it harder to perform a global takedown of its network. As part of this, it contains a domain generation algorithm and can alter DNS requests.

Win/Agent worm Q4 2019: 5 ⇔ Q1 2020: 5

This detection name is for various malicious executables capable of self-replication. Their common characteristics are the ability to spread to all available drives and gaining persistence. In order to trick potential victims into executing these malicious files, the filenames are often changed to impersonate harmless folders and files found on the system. They also usually contain basic backdoor capabilities, such as communication with a C&C server, downloading and executing additional files, or keylogging.

HTML/Phishing.Agent trojan Q4 2019: 35 ↑ Q1 2020: 6

HTML/Phishing.Agent is a detection name for malicious HTML code often used in a phishing email's attachment. Attackers tend to use it instead of other file types, since executable attachments are usually automatically blocked or more likely to raise suspicion. When such an attachment is opened, a phishing site is opened in the web browser, posing as an official banking, payment service or social networking website. The website requests credentials or other sensitive information, which is then sent to the attacker.

Win/Phorpiex worm Q4 2019: 6 ↓ Q1 2020: 7

Win/Phorpiex is a worm that is used mainly to download other malware, distribute spam, and perform DDoS attacks. It spreads via removable media and, to trick users into downloading and executing it, replaces legitimate files stored in web or FTP server folders with copies of itself. It communicates through IRC channels.

Win/HackTool.Equation trojan Q4 2019: 7 ↓ Q1 2020: 8

The detection name Win32/HackTool.Equation covers tools attributed to the United States National Security Agency (NSA) and made public by the hacking group Shadow Brokers. Soon after the leak, these tools became widely used by cybercriminals. The detection also includes malware derived from these leaked tools or threats using the same techniques.

JS/Agent trojan Q4 2019: 16 ↑ Q1 2020: 9

This detection name covers various malicious JavaScript files. These are often obfuscated to avoid static detections. They are typically placed onto compromised but otherwise legitimate websites, with the aim of achieving drive-by compromise of visitors.

VBS/Agent worm Q4 2019: 8 ↓ Q1 2020: 10

VBS/Agent is a detection name for malicious Visual Basic scripts (VBS) spreading from one system to another, mostly via removable drives and using various persistence methods. Their purpose is to gather information about the compromised system, send it to a remote machine and potentially download and execute other, usually more complex, malware.

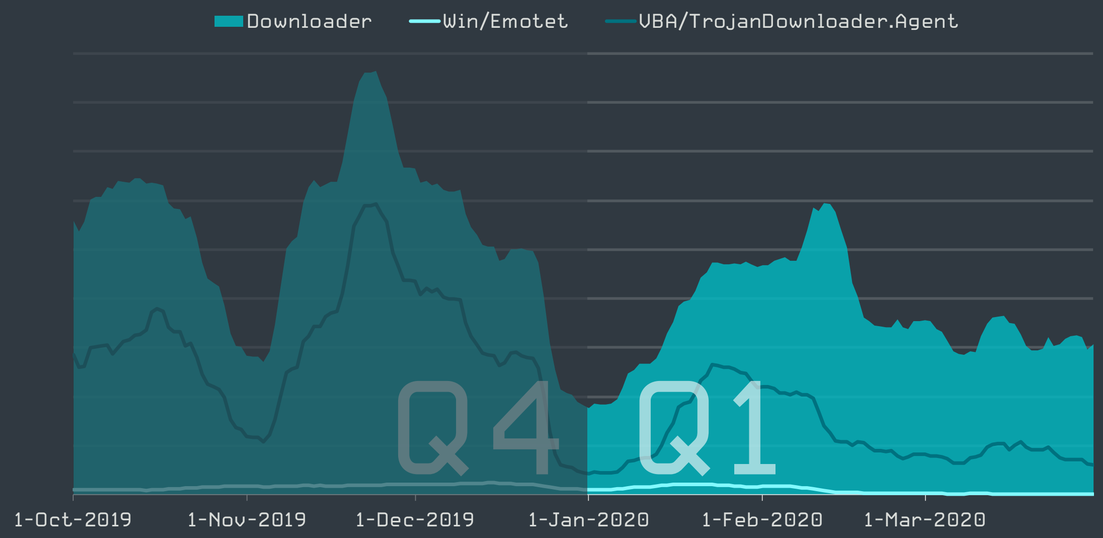
Downloaders

The first quarter of 2020 saw weaker downloader activity but notable updates to the notorious Emotet trojan and its spreading mechanisms.

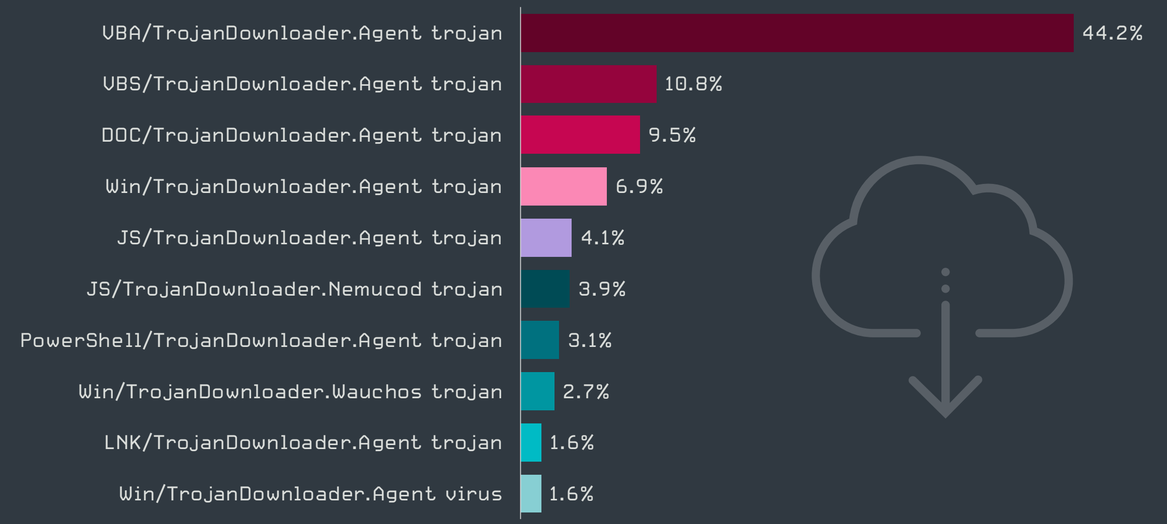
In Q1 2020, downloader families lost quite a bit of steam compared to Q4 2019, dropping in overall numbers by more than 35%. ESET telemetry shows the most significant drop around New Year's Eve, which might be explained by transition from traditionally campaign-heavy Christmas season to a calmer beginning of the year. ***Emotet's "holiday break"*** [19] could have also contributed to the plunge – note that VBA/TrojanDownloader.Agent is often affiliated with Emotet.

The most significant spike of Q1 was observed around February 10. This could be explained by the circumstances around the coronavirus outbreak in the Western Hemisphere. Malware operators exploited the increased tension and fears among the general public to spread coronavirus-themed malicious attachments, targeting mostly European countries in the following order: Spain, Portugal, Czech Republic, Taiwan and Germany.

At the family level, VBA/TrojanDownloader.Agent has led the rankings since Q4. Its detections were four times higher than those of VBS/TrojanDownloader.Agent, the second-most common family. VBA/TrojanDownloader.Agent is distributed through spam campaigns and is predominantly spread via malicious Microsoft Office files. When opened, these macro-enabled documents typically use PowerShell to download Win/Emotet binaries from hacked websites.



Downloader detection trend in Q4 2019-Q1 2020, seven-day moving average



Top 10 downloader families in Q1 2020 (% of downloader detections)

Win/Emotet was particularly interesting this quarter. Researchers have ***spotted samples*** [20] using its worm module to spread into nearby insecure Wi-Fi networks and infecting connected users. ESET telemetry shows our products detected this Wi-Fi module as early as April 2018, but only on a very limited number of occasions.

> ***The low prevalence of the Wi-Fi module suggests that Emotet's operators were trying to keep it out of sight, perhaps reserving it for targeted attacks.***
>
> **Zoltán Rusnák, ESET Malware Analyst**

The Wi-Fi worm module saw a significant update at the beginning of February 2020. The original version from 2018 was a self-extracting archive, containing the Emotet binary and another malicious binary designed to brute-force access to nearby Wi-Fi networks and subsequently to network shares. The updated version of Emotet's Wi-Fi spreader added an additional step after the brute-force attack, downloading second-stage malware from the operator's C&C, which then downloads the Emotet binary itself and runs it on the device, making the update process more flexible.

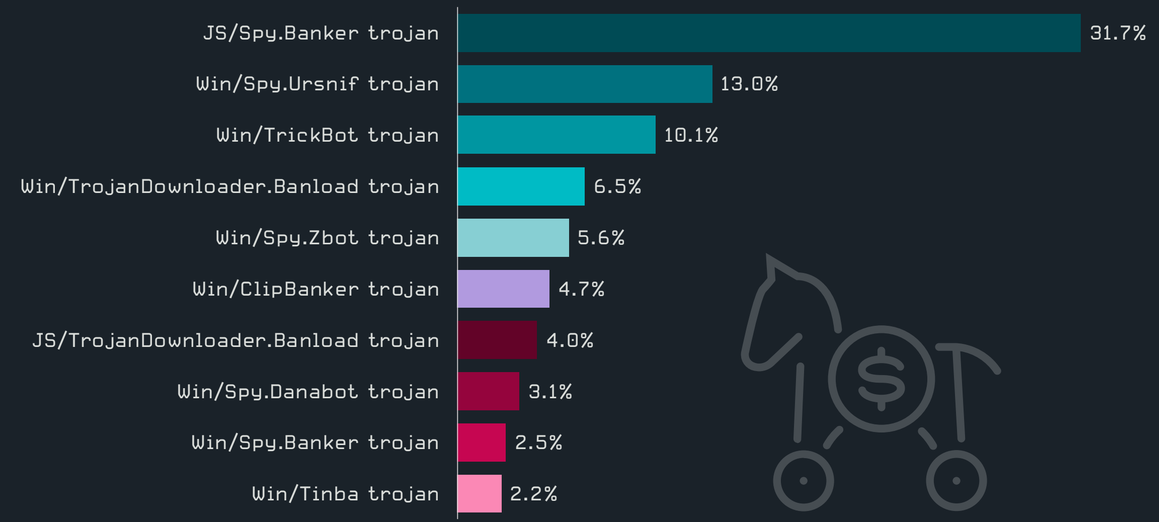
Banking malware

Banking malware detections went up slightly in Q1 2020 according to ESET telemetry, with Win/Spy.Ursnif seeing the biggest increase compared to Q4 2019.

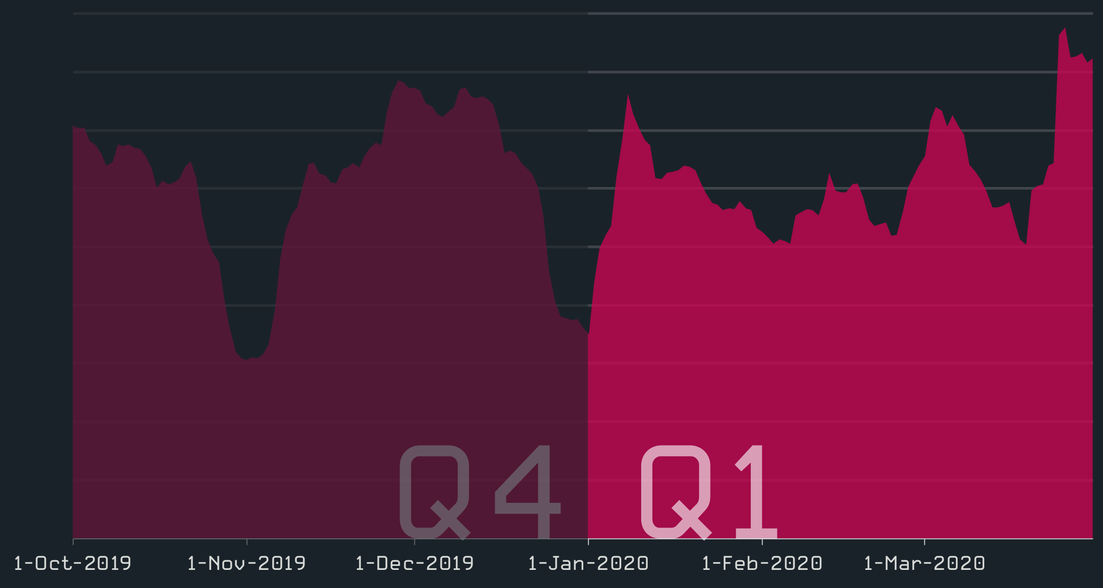
Following a significant drop in December 2019, global banking malware detections were on a slight upwards trend in Q1 2020. The category was dominated by JS/Spy.Banker, which accounted for more than a third of all banking malware detections. This detection name covers a wide range of malicious scripts used to steal sensitive banking and credit card information from victims' browsers.

When comparing the most prevalent banking malware threats from Q1 2020 to those from the previous quarter, Win/Spy.Ursnif saw the most significant change – a jump from 5.9% of banking malware detections in Q4 2019 to 13% in Q1 2020.

Ursnif, also known as a variant of the Gozi malware, is a high-profile and very active banking trojan specializing in credential and data theft. It is known to spread via email through malicious links and attachments, and exploit kits. The uptick in detections in Q1 2020 is connected to a wave of malicious spam attachments we observed at the beginning of the year. These spam messages claimed to be about legislative changes for 2020, while the executable attachments were disguised as PPT or PDF files.



Top 10 banking malware families in Q1 2020 (% of banking malware detections)



Banking malware detection trend in Q4 2019-Q1 2020, seven-day moving average

Besides the most prevalent families, an interesting category of banking malware are the banking trojans that specifically target Latin America. Investigating these threats, ESET researchers have identified more than 10 malware families, interlinked through many common characteristics. In Q1 2020, ESET published its analysis of ***Guildma*** [11], an advanced Brazil-targeting banking trojan.

> ***The Latin American banking trojans we have identified have many things in common: they are written in Delphi, contain backdoor functionality and are usually delivered via quite long execution chains. To steal banking information, they typically rely on a combination of social engineering and fake pop-up windows – rather than web injections commonly used elsewhere.***
>
> **Jakub Souček, ESET Malware Analyst**

When combined, the Latin American banking trojans accounted for more than 7% of banking malware detections in Q1 2020, with Win/Spy.Mekotio, Win/Spy.Amavaldo and Win/Spy.Grandoreiro being the most prevalent.

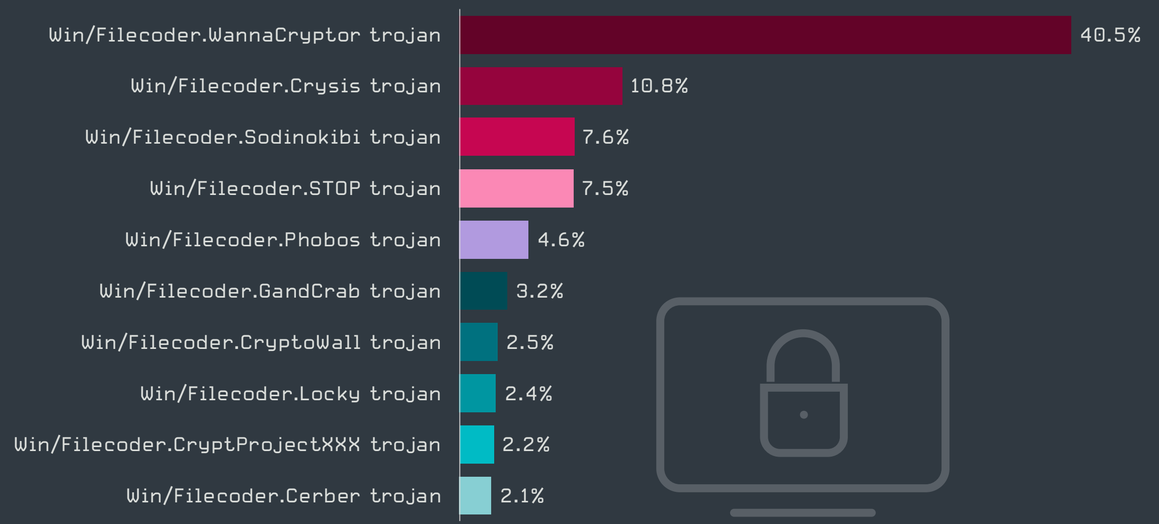
Ransomware

Ransomware operators add doxing as their new go-to tactic, yet vow to spare hospitals during the coronavirus pandemic.

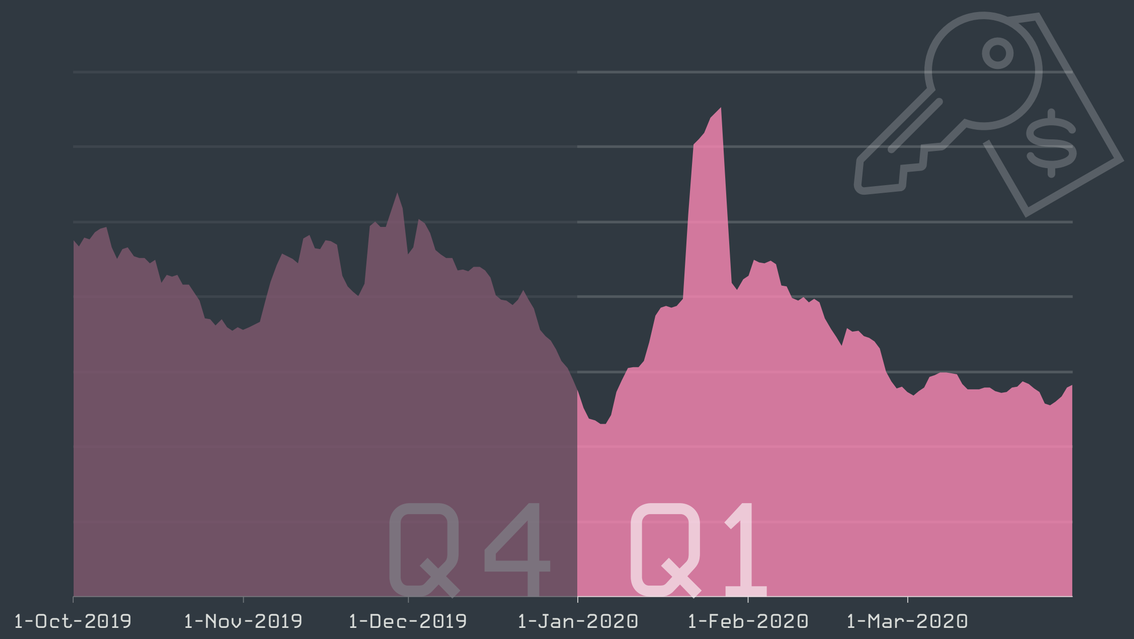
ESET detected an overall drop in ransomware activity in Q1 2020 with January 2020 seeing the most action despite a slow start after New Year's Eve.

According to ESET telemetry, the uptick in January was caused by two major campaigns: one by the Crysis family (12.9% of all Filecoder[1] detections in January) and another targeting South African users by the Sodinokibi family (13.4% of all Filecoder detections in January). The latter malware strain used powershell.exe as its parent process, indicating that the Sodinokibi operators delivered the payload via malicious email attachments using PowerShell to run the ransomware.

WannaCryptor dominated the top 10 ransomware family ranking throughout the first quarter of 2020, even though it has been almost three years since its largest outbreak in May 2017. Most of the Q1 WannaCryptor detections were attributed to well-known samples spread in regions with potentially higher numbers of unpatched devices, namely Turkey, Thailand and Indonesia.



Top 10 ransomware families in Q1 2020 (% of ransomware detections)



Ransomware detection trend in Q4 2019-Q1 2020, seven-day moving average

ESET telemetry showed a similar situation with detections of older variants of GandCrab, some of which originated as far back as 2018. Operators behind the Q1 campaigns used emails to spread these variants mostly to potential victims in Germany, Japan and Italy.

Just as in the music charts, there's plenty of movement in the top positions – different families move up and down in prominence. The most commonly seen, WannaCryptor, was followed by Crysis, Sodinokibi, STOP and Phobos families, which were fighting and replacing each other in the rankings. February 2020 also saw a newcomer in the top 10, Nemty – first observed in the wild in August 2019. However, Nemty was promptly replaced by Cerber in the following month.

The last days of March saw an odd behavior by the DeathRansom operators, who started to mimic an older version of the GandCrab ransomware, version 5.1. The most visible characteristic of this shift was the use of GandCrab's ransom note. What differs is the TOR link that does not include the "gandcrab" string – a "telltale" of the original perpetrators not present in the current DeathRansom page. Further, DeathRansom's landing page does not resemble one that was used by GandCrab.

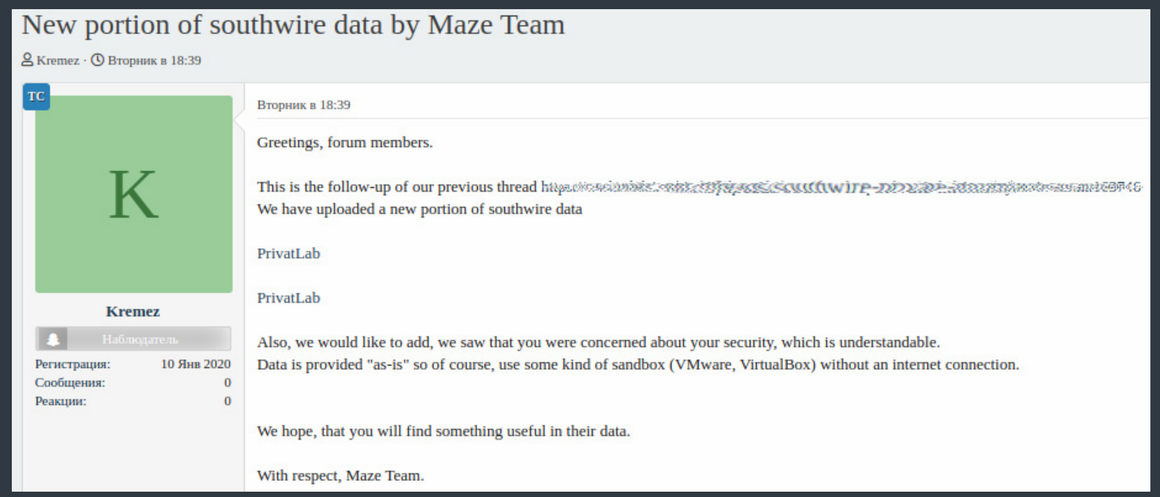
[1] ESET classifies ransomware into Filecoder and Diskcoder categories, depending on whether they target files or disk volumes, respectively.

A significant new trend emerged toward the end of Q4 2019, as ransomware operators started to steal their victims' sensitive data and threaten to make it public, unless the ransom is paid. This technique – also called doxing – is employed in addition to the unwanted encryption of the victim's data.

Attackers use this approach to increase pressure on the victim, who has to cope with multiple problems including stalled business operations, financial loss, reputational harm, reporting to authorities and potential fines (due to GDPR or other legislation) as well as with loss of competitive advantage, if confidential data is leaked online.

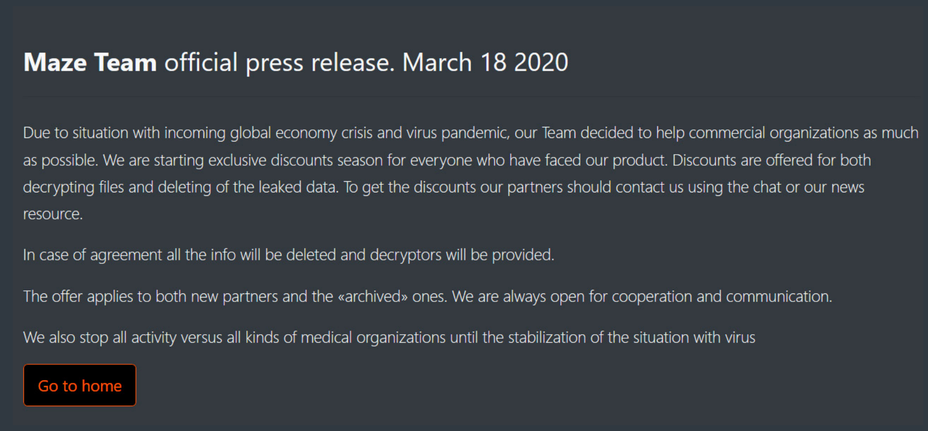
Doxing had initially been used by operators of Maze ransomware; however, inspired by its effectiveness, other ransomware operators followed suit in Q1 2020. High-profile families seen adopting the approach include DoppelPaymer, Sodinokibi, RobinHood, and Nemty.

One of the first victims that was doxed by Maze was the US wire and cable manufacturer Southwire. Maze operators stole 120 GB of its data, encrypted nearly 900 devices and demanded $6 million to restore to the previous state. When Southwire refused to pay, Maze started publishing its data, which was met by a lawsuit and preventive steps against the provider hosting the leaked data.



Post by Maze operators on a Russian hacking forum (Image source: BleepingComputer.com [21])

Another interesting turn in Q1 2020 was prompted by the COVID-19 outbreak in Western countries. Surprisingly, operators of some families (e.g. Maze, DoppelPaymer) released public statements promising *not to target health or medical organizations* [22] so as not to worsen the effects of the pandemic. However, some families – such as Ryuk – have continued business as usual.



"Press release" by Maze operators addressing the coronavirus pandemic (Image source: @CryptoInsane [23])

> ***Some ransomware operators have decided not to attack medical organizations, but that didn't discourage others from doing so. There have been quite a few examples of that in the first quarter of 2020.***
>
> **Igor Kabina, ESET Senior Detection Engineer**

An interesting ransomware-related case was described in a *mid-February 2020 alert* [24] by US-CERT. The cyberattack targeted a natural gas compression facility. The threat actor used a spearphishing link to gain initial access to the IT networks and leveraged that to access the operational technology (OT) network. Both were subsequently compromised with commodity ransomware. The incident led to loss of productivity and revenue but did not cause the organization to lose control of operations. US-CERT also states that the case could have been prevented if the victim had implemented robust segmentation between its IT and OT networks.

Q1 2020 shed some light on the earnings of ransomware operators. According to a *talk delivered by FBI Special Agent Joel DeCapua at the RSA 2020 Conference* [25], attackers using encrypting Filecoders have earned at least $140 million over the past six years. At least that is the sum of all transactions observed on bitcoin wallets associated with ransom notes. Most of the money has been transferred to wallets connected with Ryuk (over $61 million) and Crysis/Dharma (almost $24.5 million).

Agent DeCapua also stressed that in the overwhelming number of cases, RDP is still the primary vector used to compromise businesses. According to FBI data, up to 80% of successful ransomware attacks are accomplished via breaking into the network by brute-forcing RDP credentials. DeCapua's full talk can be found on *YouTube* [26].

Cryptominers

In the cryptomining theater, the most notable trend observed in Q1 2020 was continuing decline of cryptomining activities. Cryptominers classified as potentially unwanted applications have seen the most significant downturn.

ESET security products detect cryptominers as potentially unwanted applications (PUA) or trojans – the latter being those configured to mine cryptocurrency without the victim's knowledge or consent. While in Q4 2019 the trojan:PUA ratio in cryptominers was 52:48, the decline in PUAs led to the ratio growing to 60:40 in Q1 2020.

As seen in the chart below, there was a gradual but consistent decline in global detections of malicious cryptominers, a trend that is a continuation of the decline observed since the beginning of 2019.

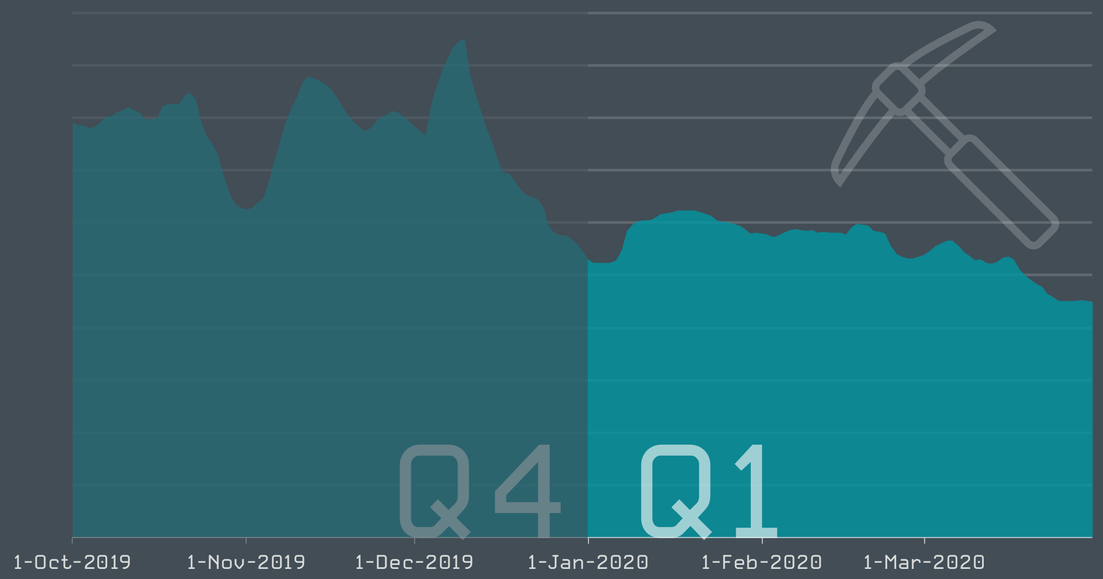
As exchange rates of cryptocurrencies fall, so do the bad actors' revenues. As a result, their interest in having people's devices mine coins wanes.

Juraj Jánošík, Head of Automated Threat Detection and Machine Learning

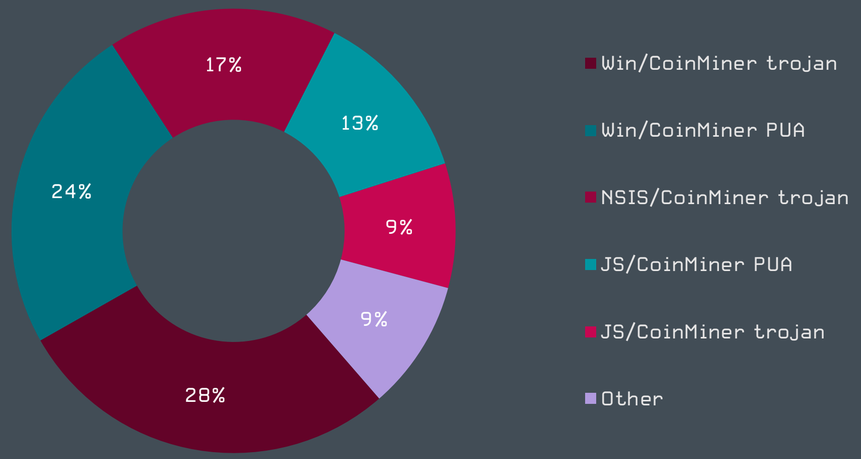
Besides the drop in price of bitcoin and other cryptocurrencies, the decline in cryptomining activities observed in Q4 2019 and Q1 2020 can be, to a large extent, attributed to ***Operation Goldfish Alpha*** [27]. This operation, coordinated by INTERPOL, identified over 20,000 hacked routers in the ASEAN region, which reportedly accounted for 18% of global infections of cryptomining malware. By late November 2019, the number of infected devices had been reduced by 78%, according to INTERPOL.

Malicious JavaScript used for in-browser mining, detected as JS/CoinMiner, didn't recover following the ***demise of the infamous Coinhive*** [28] mining service in March of 2019. While in Q1 2019 these covered around 30% of all the cryptominer detections, in Q1 2020 their share hovered just above 10%, virtually unchanged compared to Q4 2019.

Despite having been predicted by some to grow, Android coinminers – both trojans and PUAs – remain virtually non-existent.



Cryptominer detection trend in Q4 2019–Q1 2020, seven-day moving average



Top cryptominer detections in Q1 2020

Spyware & backdoors

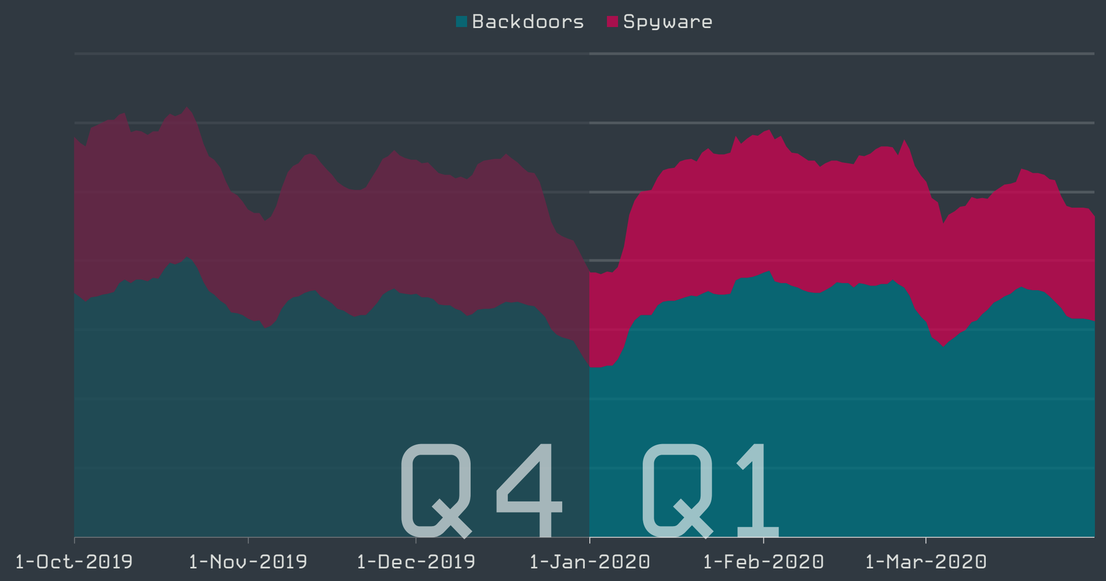
According to ESET telemetry, Q1 2020 saw a steady level of spyware and backdoor detections, with Win/HoudRat dominating the landscape.

Aside from the usual drop at the turn of the year, spyware and backdoor detections were fairly constant across Q4 2019 and Q1 2020. Backdoor detections have been reaching approximately double the number of spyware detections.

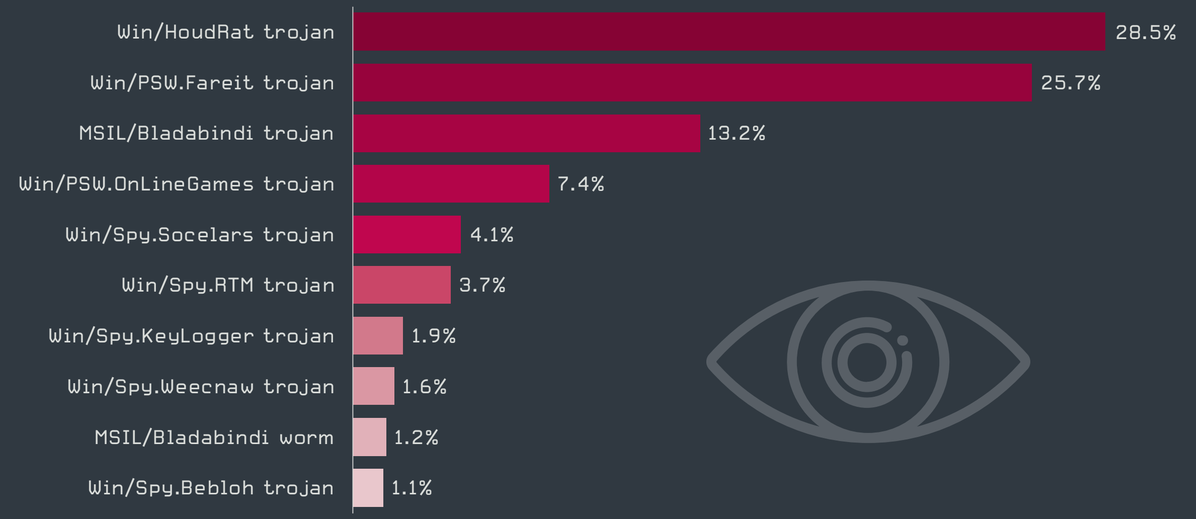
The Spyware category in this report comprises detections of trojans and worms with data-stealing, password-harvesting and keylogging capabilities. Backdoors, also known as Remote Access Trojans (RATs), are defined as applications allowing remote access to a computer without the user's knowledge, and tracked as a distinct detection category.

The most prevalent malware family in the Spyware category in Q1 2020 was Win/HoudRat, which accounted for almost a third of all spyware detections. HoudRat is complex malware used to steal credentials from popular e-stores, payment portals, and widely used web browsers. It utilizes removable media for spreading purposes.

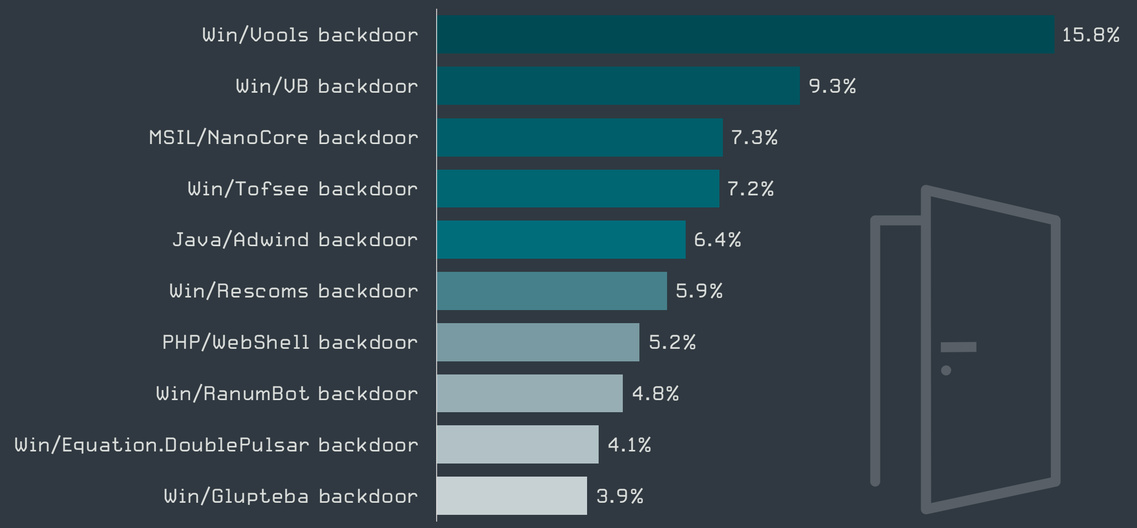
Ranking first among backdoors was Win/Vools, with nearly 16% of all backdoor detections. This malware uses the Microsoft Server Message Block (SMB) vulnerability to spread to vulnerable computers. If successful, Vools collects a victim's sensitive information and sends it to a remote server.



Spyware and backdoor detection trends in Q4 2019-Q1 2020, seven-day moving average



Top 10 spyware families in Q1 2020 (% of spyware detections)



Top 10 backdoor families in Q1 2020 (% of backdoor detections)

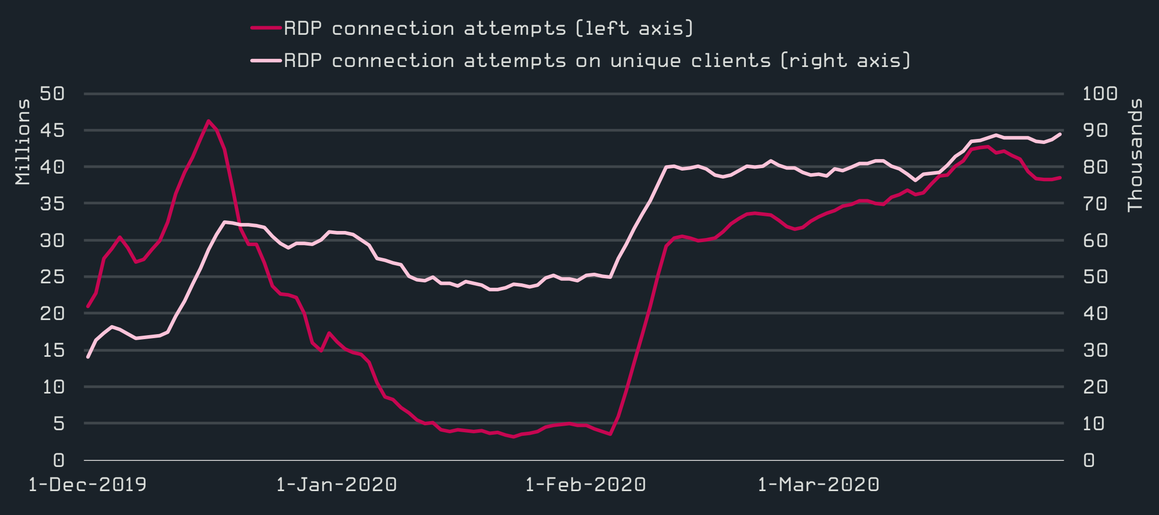
Exploits

Network security has come into the spotlight, with criminals apparently attracted by networks more open to incoming traffic due to more people working from home.

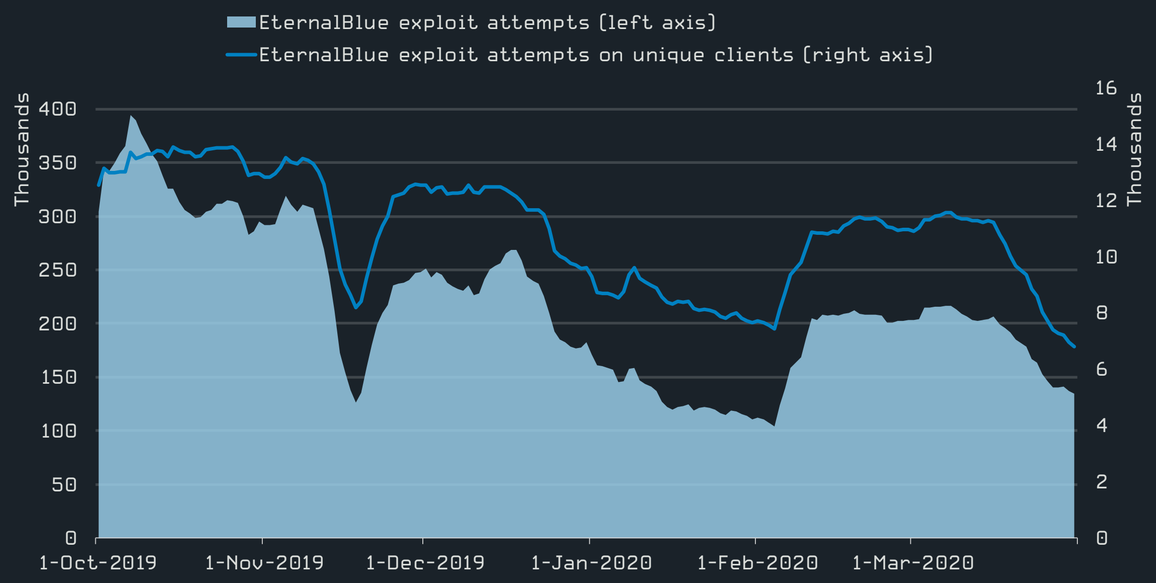
The number of attempted attacks using the infamous EternalBlue exploit continued to decline through Q1 2020, ending at half of the ***historical high*** [29] it reached in Q2 2019. EternalBlue exploits were responsible for the nastiest ransomware outbreak ever: WannaCryptor (or WannaCry). Despite that being almost three years ago, EternalBlue remains a relevant threat with hundreds of thousands of daily attack attempts.

Another vulnerability that saw the number of attack attempts dwindling in Q1 2020 was ***BlueKeep*** [30]. This "wormable" critical Remote Code Execution vulnerability in Remote Desktop Services was disclosed after being patched in May 2019. After some initial dramatic spikes in activity, the number of attacks started to decrease, continuing through Q1 2020.

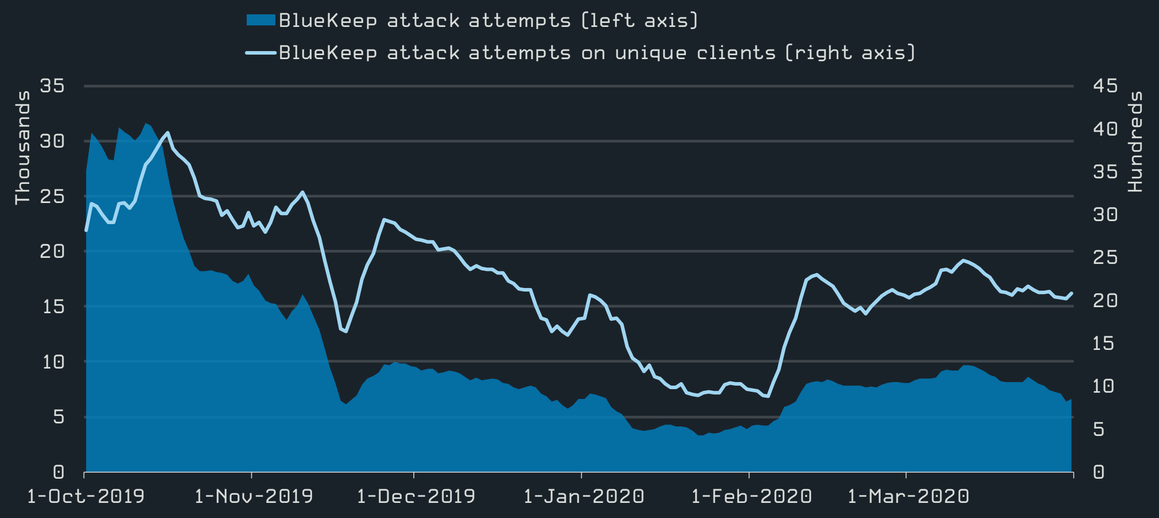
From the network security point of view, one of the key pain points remains the Remote Desktop Protocol (RDP). We witnessed large scale password guessing attacks, a trend that recently strengthened, apparently with the coronavirus-induced lockdowns. In regard to RDP security, refer to ***this ESET advisory*** [31].



Trends of RDP connection attempts in Q4 2019-Q1 2020, seven-day moving average[2]



Trends of EternalBlue exploit attempts in Q4 2019-Q1 2020, seven-day moving average



Trends of BlueKeep attack attempts in Q4 2019-Q1 2020, seven-day moving average

[2] Data prior to December 2019 is not available due to a change in methodology. The increase at the beginning of February was caused in part by lowering the threshold for classifying a sequence of attempts as an attack.

Mac

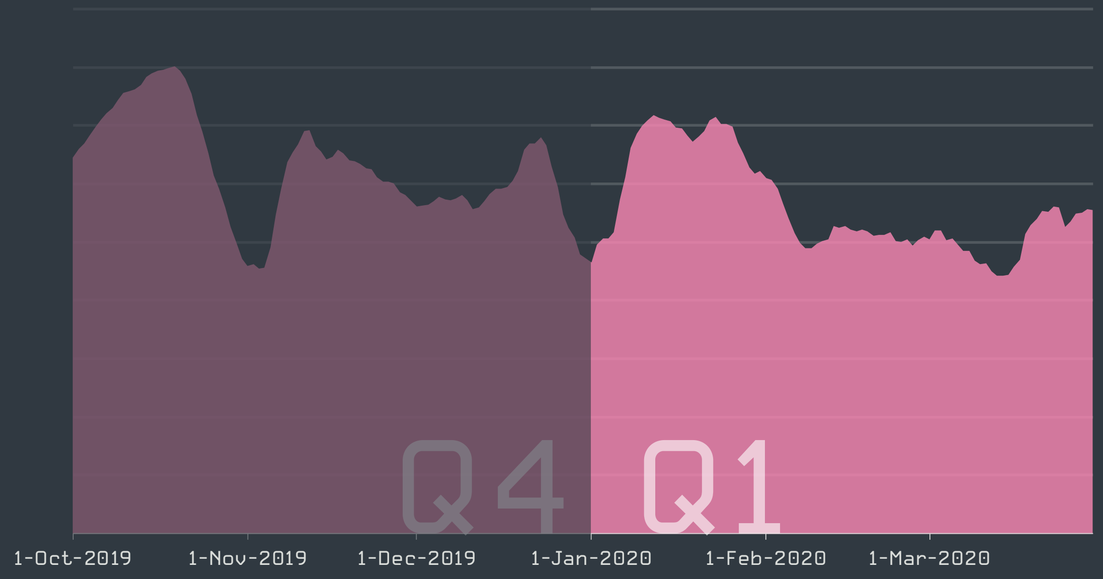
According to ESET telemetry, Mac detections had a steady first quarter in 2020.

The first quarter of 2020 saw a small surge in macOS detections in January and a subsequent return to a steady state slightly below the average for 2019. The vast majority of Mac detections registered by ESET products in Q1 2020 fall into the category of Potentially Unwanted Applications (PUA), followed by Potentially Unsafe Applications (PUsA), adware and trojans.

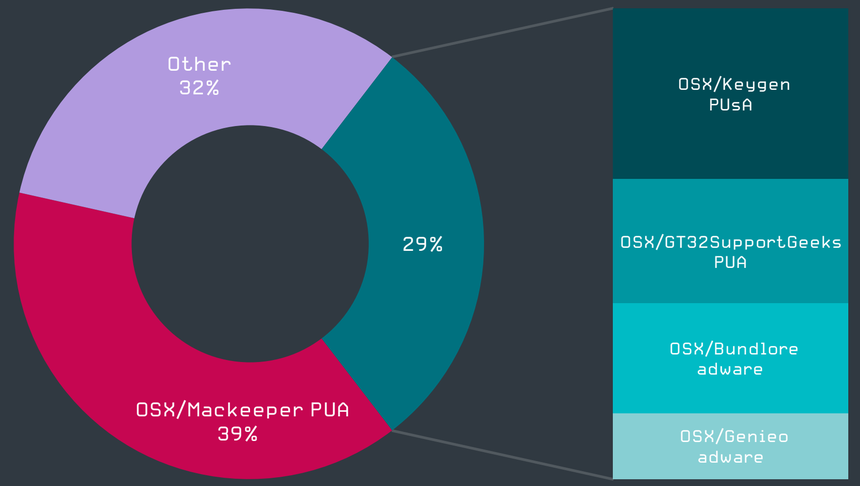
Mac computers (i.e. those powered by the macOS operating system) are less targeted by malware than Windows or Linux devices. Apple's "walled garden" strategy, albeit often criticized for other reasons, makes it difficult for malware to sneak onto a Mac. A key element of macOS security is the mechanism called Gatekeeper that checks if code has been signed by Apple. Apps failing that check can only be installed with the user's explicit permission.

Under the typical scenario, attackers rely on social engineering to trick the victims into installing the malware onto their Macs.

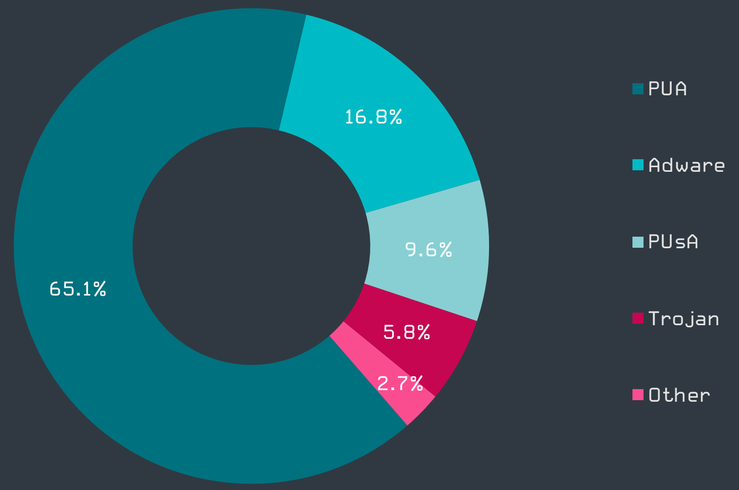
Miroslav Legéň, ESET Senior Detection Engineer



Mac detection trend in Q4 2019–Q1 2020, seven-day moving average



Top Mac detections in Q1 2020



Top Mac detection categories in Q1 2020

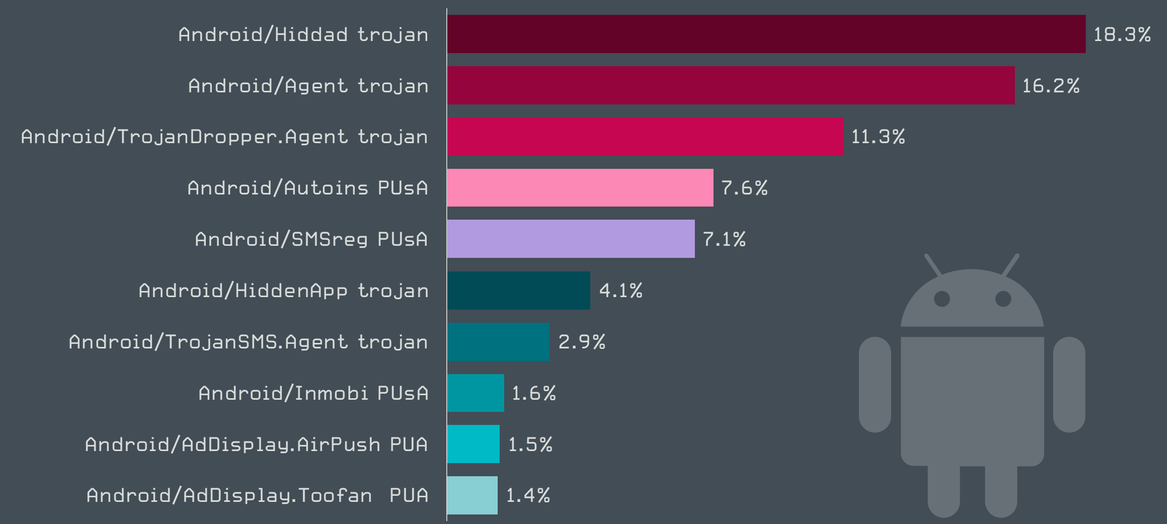
Android

Ad-displaying apps steadily dominate the Android threat landscape, but it's stalkerware that is attracting the greatest attention.

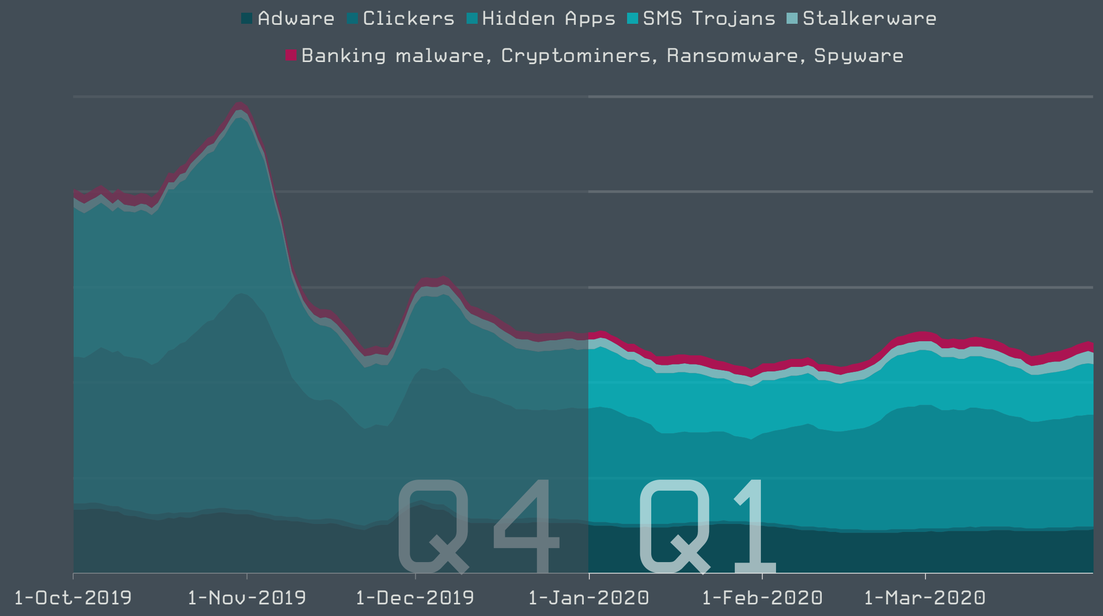
Although overall Android detection levels were steady through Q1 2020, they were at a noticeably lower level than in the first half of Q4 2019. Android/Hiddad continued to rank first among detected families, and along with Android/HiddenApp and others, contributed to Hidden Apps remaining the most prevalent category of Android threats. Their key features are hiding their icons after installation and then going on to bombard users with full-screen ads. These shady apps commonly make it into the Google Play store, masquerading as attractive games or photo editing apps.

Apps in the Hidden Apps category display adware behavior, but their stealth capabilities set them apart from traditional adware, and they are fairly prevalent. For these reasons we have been tracking them outside of the broad adware category.

Lukáš Štefanko, ESET Malware Researcher



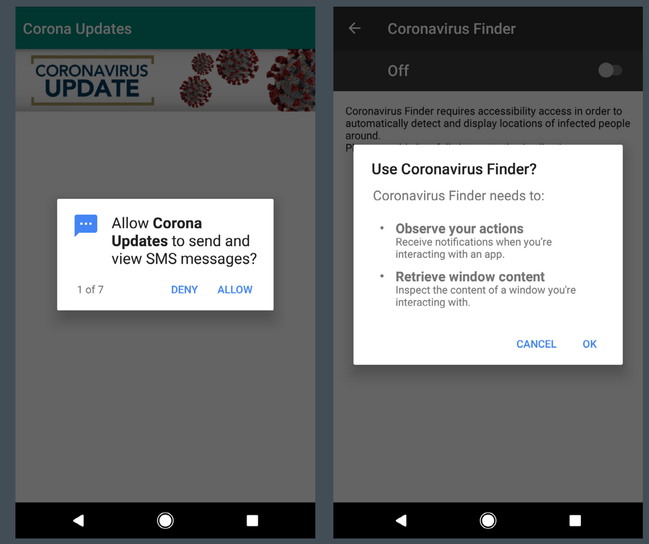
Top 10 Android detections in Q1 2020 (% of Android detections)



Trends of selected Android detection categories in Q4 2019-Q1 2020, seven-day moving average

The Android ecosystem was affected by the coronavirus pandemic that started in Q1 2020. Threat actors quickly started exploiting Android users' hunger for information about COVID-19 and associated protective equipment and potential cures.

ESET researchers witnessed malicious apps distributed in campaigns under coronavirus-themed disguises, e.g., symptom identification, infection maps, tracking applications, and financial compensation. Among malicious apps distributed this way have been various banking trojan families, ransomware, SMS worms, spyware, and adware.



Examples of coronavirus-themed Android malware permission requests

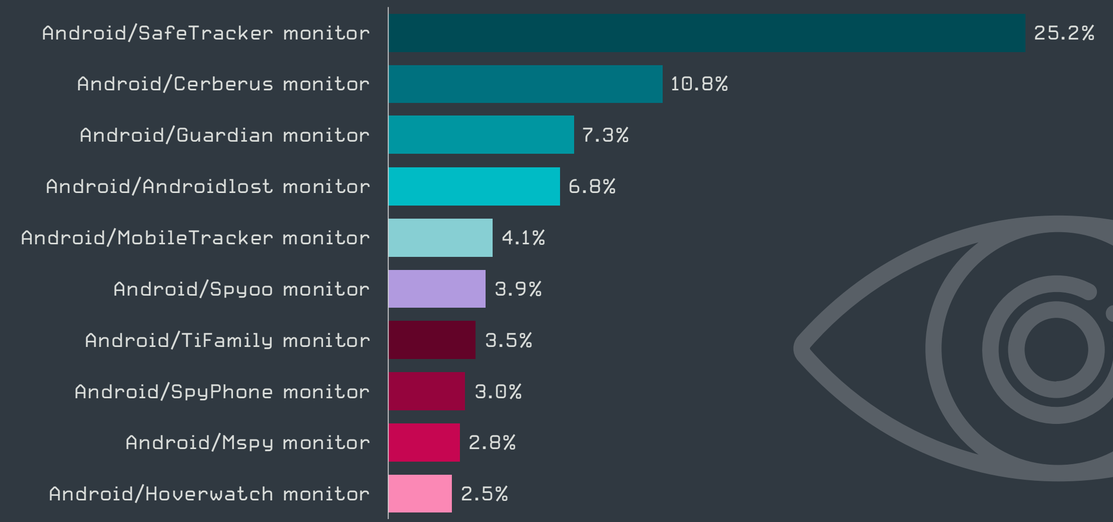
Stalkerware

The number of detections in the Stalkerware category (also called spouseware by some) has risen by about a third compared to Q4 2019.

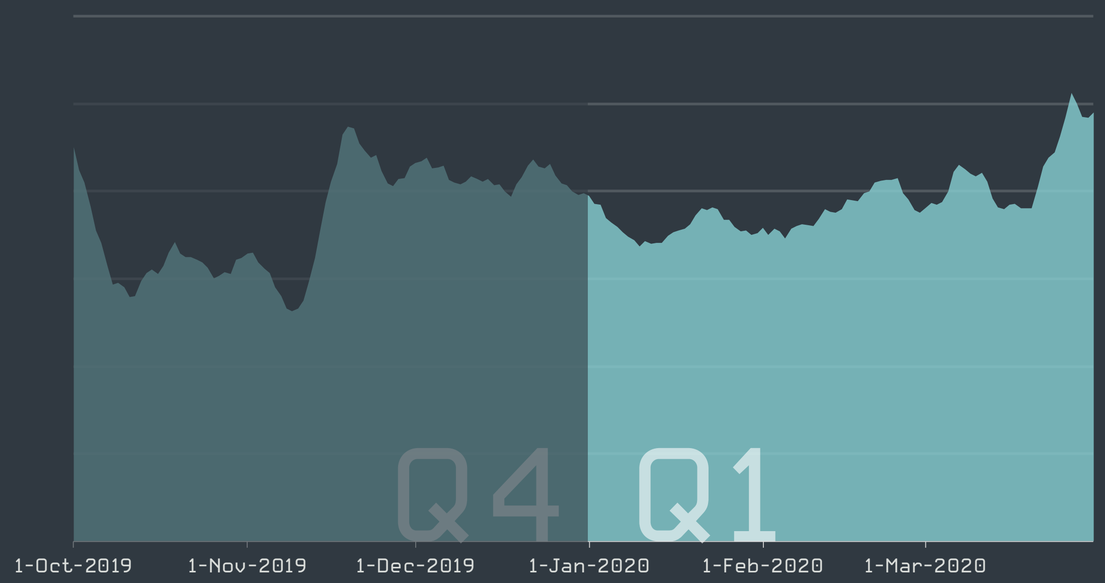
ESET treats the Stalkerware category of Android threats differently from the other types of so-called Potentially Unwanted Applications that it technically belongs to. Stalkerware is a classic example of dual-purpose technology – an otherwise legitimate tool that can be easily misused to serve illegitimate goals.

Typically, stalkerware is marketed as a tool that enables monitoring children, students or employees. In reality, these apps are often used for spying upon unsuspecting spouses or romantic partners, sometimes with tragic consequences for those victims. For this reason, ESET has reclassified these apps from the Potentially Unwanted Applications category in order to raise warnings about their nature independent of the customer's settings.

The class of Stalkerware apps is an extremely fragmented one: ESET researchers keep their eyes on about one hundred families. Of those, all but the top four have a prevalence of under five percent, while the dominant stalkerware family accounts for over 25% of detections in this category.



Top 10 Android stalkerware families in Q1 2020 (% of Android stalkerware detections)



Stalkerware detection trend in Q4 2019–Q1 2020, seven-day moving average

Besides being a threat when used for illegitimate purposes, stalkerware apps tend to have been developed without security considerations. ESET researchers often see these apps communicating with their backend servers via unsecured channels, without any encryption.

> ***Evidently, those behind stalkerware apps put most of their efforts into aggressive marketing while ignoring security.***
>
> **Lukáš Štefanko, ESET Malware Researcher**

As a result, insecure stalkerware applications bring danger not only to those illegitimately spied upon, but also to the legitimate targets of oversight. Personal information of all those with such apps installed on their devices might well find its way into publicly exposed data leaks.

Web threats

Web threats increased in overall volume in Q1 2020 according to ESET telemetry, with the coronavirus pandemic frequently used as a lure.

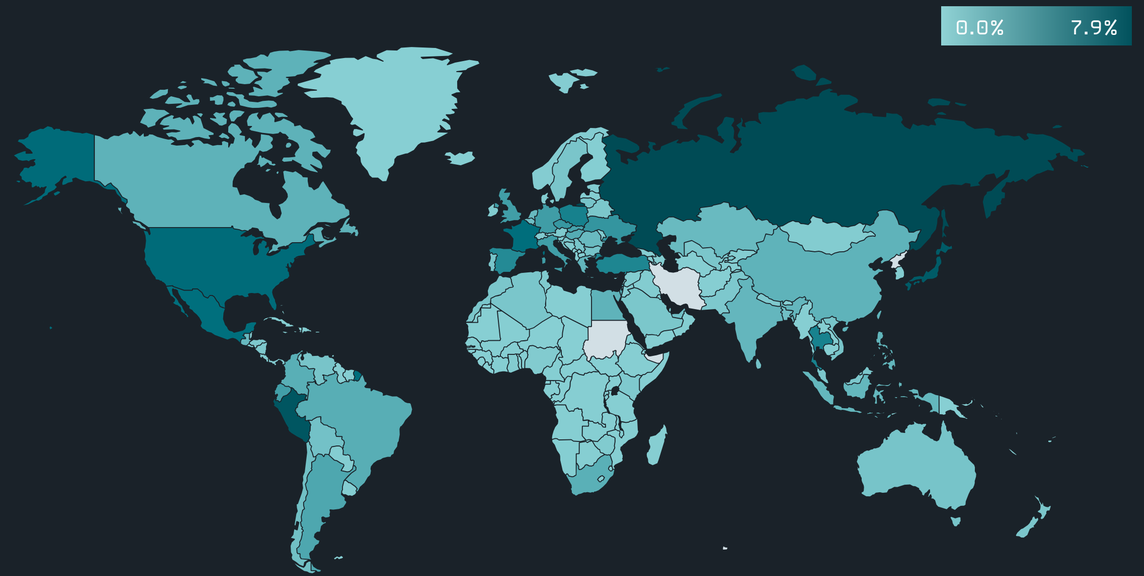
Compared to Q4 2019, the number of malicious and fraudulent websites blocked in Q1 2020 increased by 21%. At the turn of the year, the number of these detections surged, reaching a peak in mid-January 2020 and declining slightly towards the end of the quarter. However, when viewed in terms of unique URLs blocked, we observed the opposite trend – a 33% decrease from Q4 2019 to Q1 2020.

The trend data is broken down into categories based on the type of threat blocked:

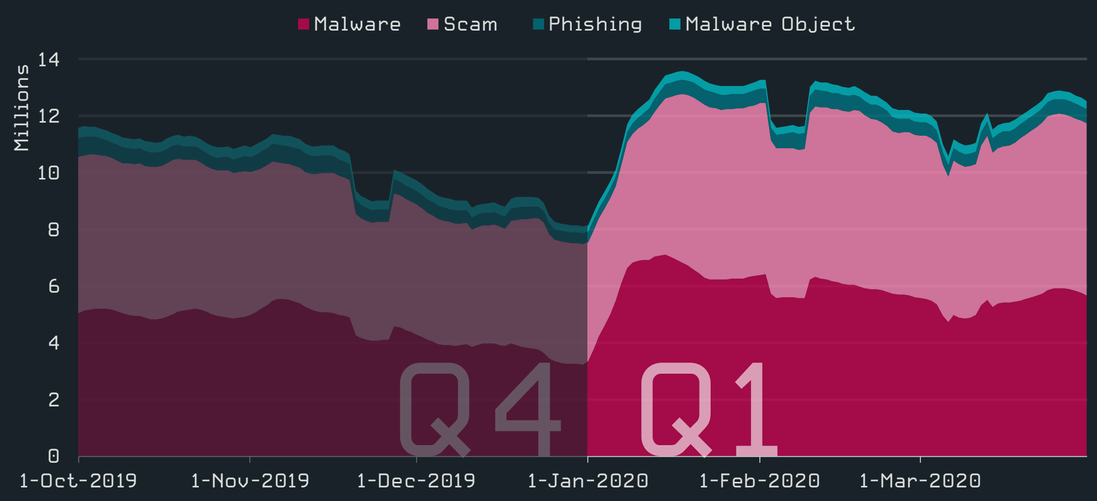
- **Malware**: websites known to serve malware
- **Scam**: websites with fraudulent content
- **Phishing**: websites used to harvest sensitive data
- **Malware Object**: otherwise legitimate websites (e.g. cloud storage services) hosting malicious code

While the Malware category had the most overall blocks, the largest number of unique URLs blocked belonged to the Scam category. Phishing had the most blocked attacks per unique URL – approximately 20.

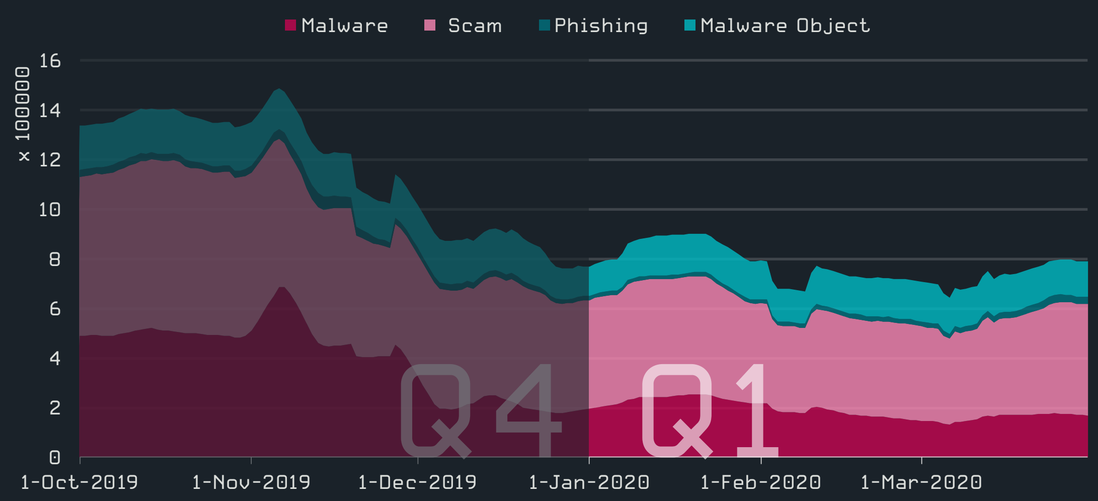
According to ESET telemetry data, ESET customers in Russia, Peru, Japan, the United States and France had the largest numbers of web threat blocks. Domains with the largest numbers of detections are listed on the next page.



Rate of web threat blocks in Q1 2020



Trends of blocked web threats in Q4 2019-Q1 2020, seven-day moving average



Trends of unique URLs blocked in Q4 2019-Q1 2020, seven-day moving average

	Malware	Scam	Phishing
1	adobviewe[.]club	r.remarketingpixel[.]com	d18mpbo349nky5.cloudfront[.]net
2	fingahvf[.]top	ofhappinyer[.]com	mrproddisup[.]com
3	deloplen[.]com	ak.imgfarm[.]com	attacketslovern[.]info
4	runmewivel[.]com	plugins.zonainst[.]xyz	gleaminist[.]info
5	webunstop[.]net	maranhesduve[.]club	update.updtbrwsr[.]com
6	cozytech[.]biz	rudy.adsnative[.]com	update.updtapi[.]com
7	d3qjtdfpbrj6c.cloudfront[.]net	version.zonainst[.]xyz	static.oceanreefs[.]xyz
8	linkangood[.]com	glotorrents[.]pw	update.brwsrapi[.]com
9	videomore[.]club	postlnk[.]com	update.mrbrwsr[.]com
10	hardyload[.]com	koindut[.]com	update.savebrwsr[.]com

Top 10 blocked Malware, Scam and Phishing domains in Q1 2020

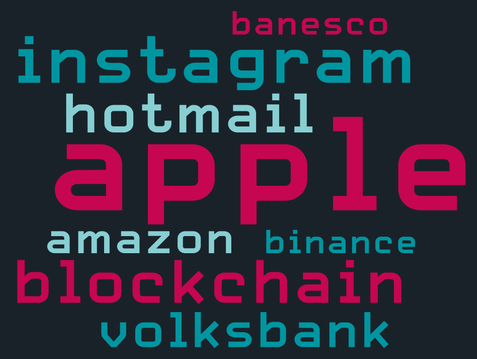
Homoglyph attacks

Homoglyph attacks rely on replacing characters (or glyphs in font design terms) in URLs with ones that look similar – or are even visually identical – but are different to computers, as they belong to different alphabets. These attacks may be very dangerous for users, as they have only a limited chance of detecting the trap.

To protect high-value target domains – banks, financial institutions and payment platforms, prominent email services, and reputable media – ESET products perform a rigorous inspection. They check the letters of protected URLs against a table of similar letters from any other alphabet and warn the customer if any deception attempt is detected.

According to ESET telemetry, the domain most impersonated by "homoglyphed" lookalikes in Q1 2020 was apple.com, followed by instagram.com and blockchain.com. In the case of apple.com, most of the detections came from a single domain that is educational in nature, and not malicious.

The domains impersonating instagram.com and blockchain.com, however, are malicious.

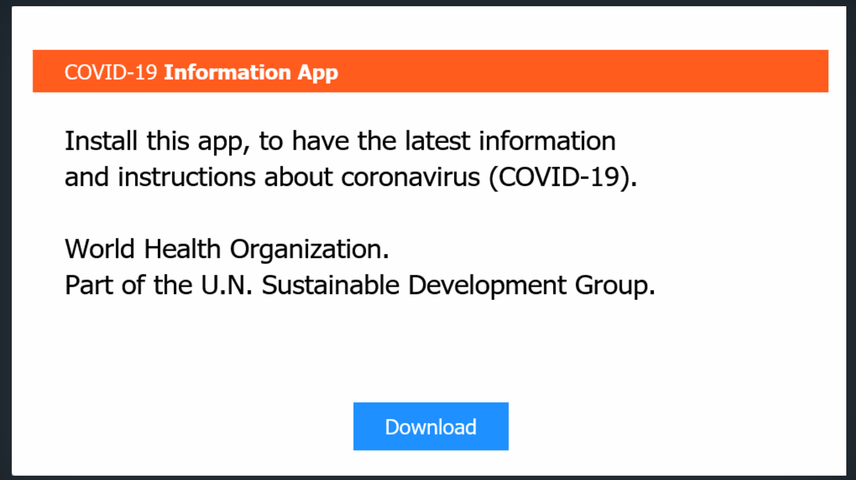


Brands most targeted with homoglyph attacks in Q1 2020

Coronavirus pandemic as a lure

In mid-March, we saw a surge in coronavirus-themed web attacks. These ranged from fraudulent online stores claiming to sell face masks and other personal protective equipment, all the way to websites distributing dangerous malware.

In the latter category, ESET telemetry detected a malicious website impersonating the World Health Organization (WHO) that tried to manipulate users into downloading what is presented as "COVID-19 Information App". Instead, victims ended up downloading malware; we've seen the website serve a malicious cocktail of downloaders, spyware and ransomware, with the payload changing frequently.



Malicious website impersonating the WHO and luring users into downloading malware

As for websites with coronavirus-related strings in their domain names, we detected a spike in mid-March 2020, with a sixty-fold increase when comparing detections from March 1st and March 16th. Detection of these threats was most prevalent among ESET customers in the United States, Russia and Ukraine, whose detections, combined, accounted for 70% of the overall detections of these coronavirus-related web threats.

In the Malware category, coronavirus[.]zone was the most blocked threat, distributing HTML/ScrInject.B – malicious code that redirects the browser to other URLs with further malware. Most prevalent in the Phishing category was chasecovid19v[.]com, while survivecoronavirus[.]org was the most blocked Scam website.

Email threats

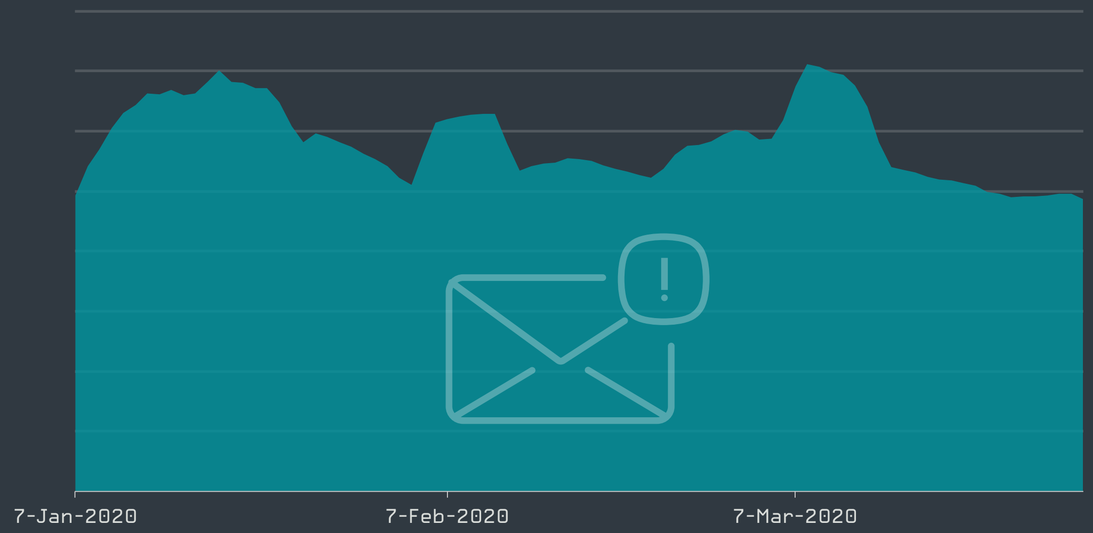
Spam was “business as usual” in Q1 2020, with a slight peak in March 2020 and a wave of coronavirus-themed unsolicited emails.

Q1 2020 did not see any turbulent developments on the spam scene. ESET telemetry shows a relatively steady level with a few minor peaks, with the largest volume of spam detected in the second week of March 2020.

Almost a fifth of all unsolicited emails detected in Q1 came from the United States, followed by Poland, France, Japan and Germany. Emails where the sender country could not be identified accounted for 13% of the spam volume. Looking at spam in relation to all emails sent from the individual countries, Vietnam, Lithuania, Argentina, China and India were in the lead, with spam accounting for more than a half of all email sent.

When interpreting the data, it should be taken into account that our visibility into spam traffic is limited, as emails may be filtered at the internet email service provider, or elsewhere, before reaching ESET’s antispam solution on client machines. However, the fact that the detected spam traffic may have bypassed other antispam solutions further signifies its threat potential.

It is also important to note that the geographic data is distorted by the distribution of the ESET client base. This bias is less prominent on the sender side, where the countries of origin for spam emails are determined from the emails themselves.



Spam detection trend in Q1 2020, seven-day moving average

	Country	Sent spam share in all blocked spam
1	United States	18.4%
2	Unknown	12.9%
3	Poland	6.6%
4	France	5.9%
5	Japan	5.2%
6	Germany	4.5%
7	Russia	4.0%
8	Lithuania	3.8%
9	China	3.4%
10	India	3.1%

Countries with highest volume of spam sent in Q1 2020

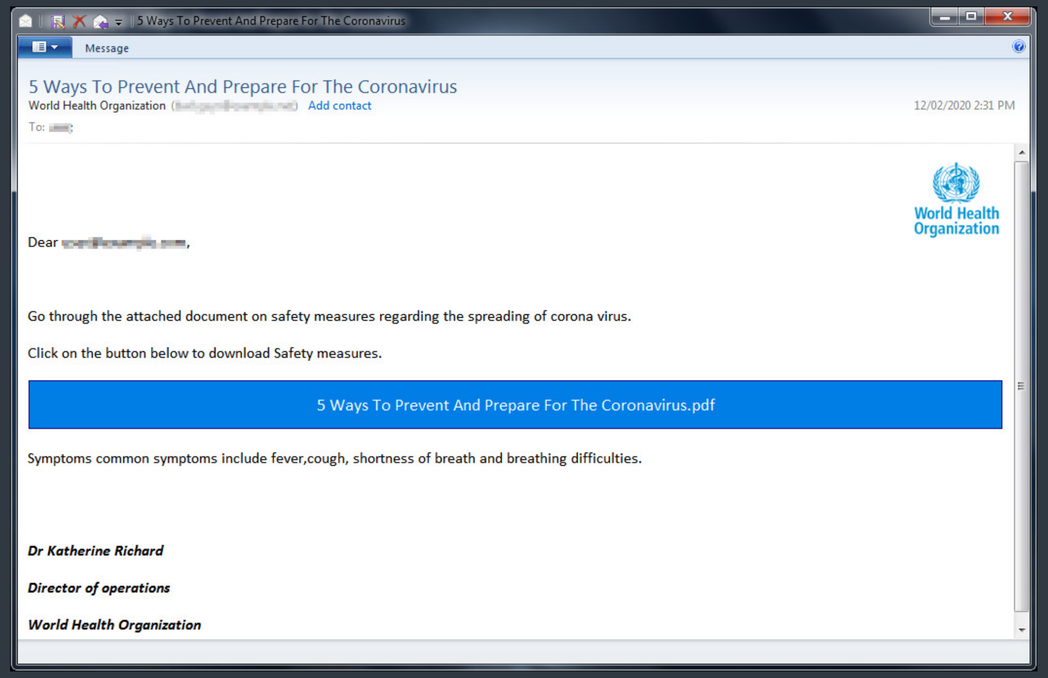
	Country	Spam share in all emails sent from the country
1	Vietnam	71.7%
2	Lithuania	70.6%
3	Argentina	57.2%
4	China	56.1%
5	India	54.3%
6	Brazil	43.9%
7	Indonesia	40.5%
8	Colombia	34.5%
9	South Korea	31.5%
10	France	25.4%

Countries with highest share of spam in all emails sent in Q1 2020

Coronavirus spam

As if the coronavirus outbreak wasn't serious enough by itself, fraudsters wasted no time in trying to profit from the uncertainty, fear, and supply shortages connected to the crisis. In March 2020, we detected a flood of COVID-19 themed spam, spreading malware, phishing for sensitive information, or offering bogus products – face masks, natural coronavirus remedies, or even a purported list of ingredients for a coronavirus vaccine.

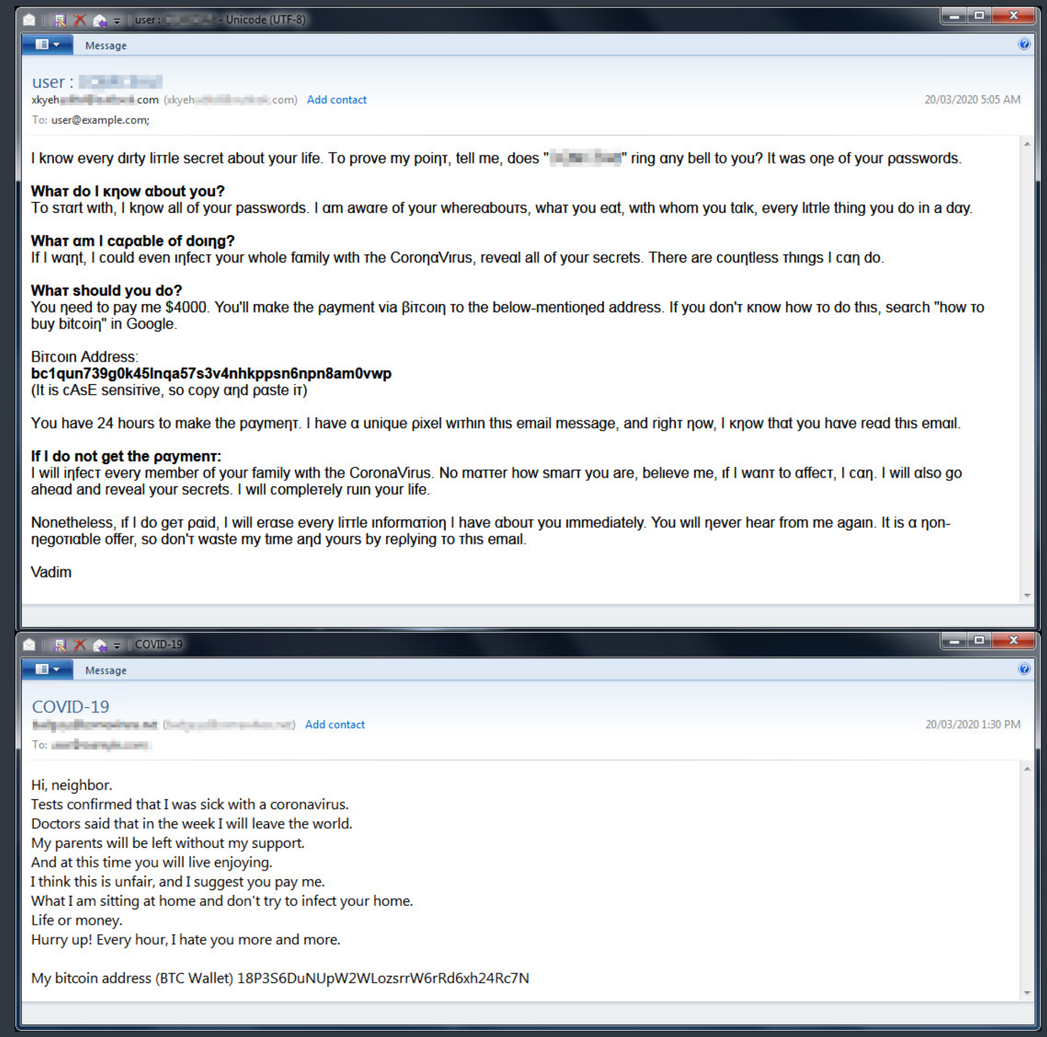
In multiple campaigns, spammers took to impersonating the World Health Organization (WHO), aiming to manipulate unsuspecting users into opening malicious links or attachments. The WHO, a major source of information about the pandemic, has addressed this concerning trend on *its website* [32].



Spam email impersonating the WHO

Upsettingly, cybercriminals in the extortion email business have also been trying to profit from the coronavirus crisis, going as far as threatening to infect email recipients and their families with coronavirus if no ransom is paid.

In the spam campaign shown in the screenshot on the upper right, criminals took an email template from one of the many previous *[s]extortion scam campaigns* [33] and customized it to fit the coronavirus pandemic theme. In an attempt to fool antispam engines, the spammers incorporated characters from the Greek alphabet that look very similar to standard Latin characters into the email's text – for example, α (lowercase Alpha) is used instead of lowercase a. In another twist on the same tactic, extortionists tried to intimidate the recipients by claiming the emails came from a neighbor – someone who is close by and could easily infect them if they didn't pay up.



Coronavirus-themed extortion scam emails

As with most email extortion campaigns, the claims in these emails are unfounded and should be treated as any other spam email.

IoT security

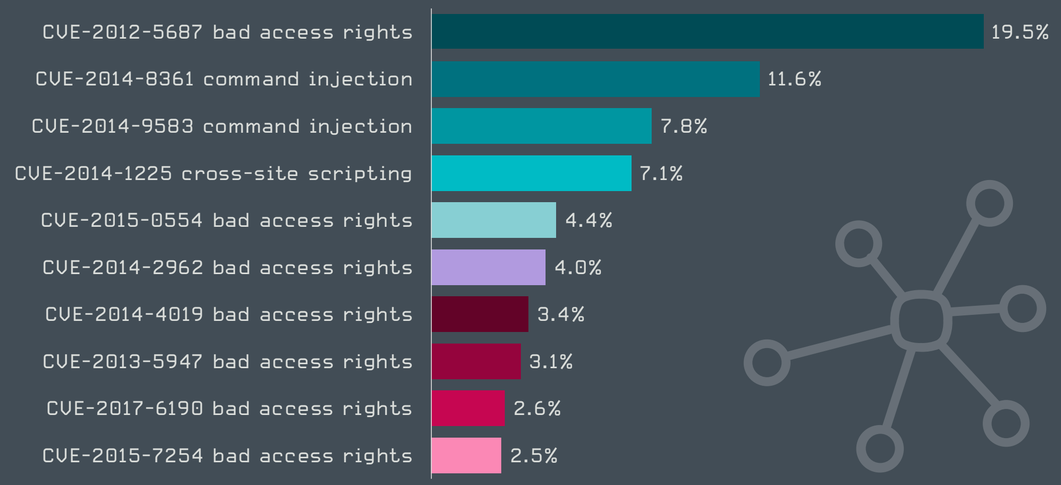
Years-old vulnerabilities that allow attackers to bypass access controls dominate the list of most frequent flaws detected on IoT devices.

Devices referred to as Internet of Things often suffer from vulnerabilities or misconfiguration issues that allow them to be exploited. ESET's router vulnerability scanner module scanned over a hundred thousand routers worldwide this quarter showing vulnerabilities that could result in unauthorized access – such as password or information leakage or directory traversal – to be the predominant type of IoT issues.

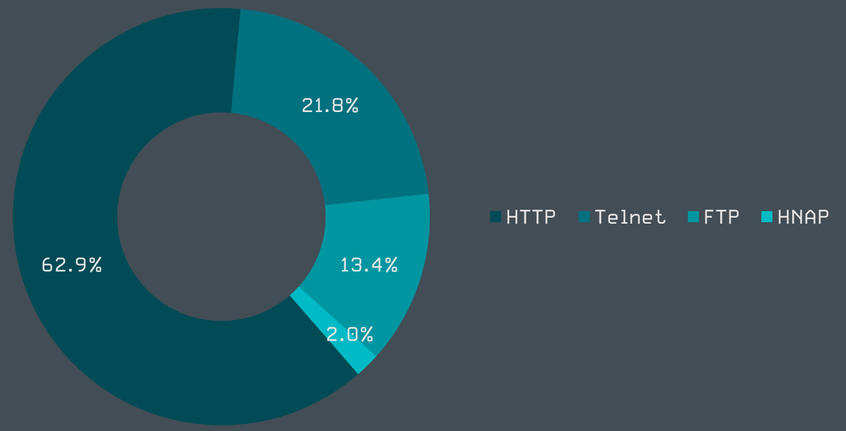
This finding is further bolstered by this kind of flaw representing seven of the top ten IoT vulnerabilities detected by ESET's scanner. What stands out is also the age of the front-runners in that list. According to ESET telemetry, none of the top 10 were discovered after 2017 and five out of the ten have been known since 2014.

The leading vulnerability – ***CVE-2012-5687*** [34] – is even older and was first reported in October 2012. Despite being around for seven-plus years it still accounts for 19% of all vulnerabilities found. Old command-injection vulnerabilities are quite prevalent too, occupying second (CVE-2014-8361 with 12%) and third (CVE-2014-9583 with 8%) places.

ESET's telemetry also provides insight into the prevalence of cases when hosted services are protected by weak or default passwords. Such linkage seems to be particularly strong in cases where HTTP was used, representing 63% of detections, followed by telnet with 22% and FTP with 13%.



Top 10 vulnerabilities detected by ESET's router vulnerability scanner module (% of vulnerability detections)



Weak password prevalence per hosted service in Q1 2020

A powerful illustration of how deficiencies in IoT security can severely weaken security of entire networks is illustrated by the ***Kr00k vulnerability*** [5].

Kr00k manifests itself as wireless network data being encrypted with a WPA2 pairwise session key that is all zeros and occurs on vulnerable chips following a Wi-Fi disassociation ("disconnection"). Such disassociations (and reassociations) occur naturally for a variety of (legitimate) reasons, such as signal interference or roaming between access points. Thus, anyone sniffing network data is theoretically able to decrypt the small amount of data that was that was queued for transmission just before the disassociation. Obviously, such a passive approach would require a large element of luck in order to obtain any data of interest.

For a much more effective attack, an active adversary can exploit Kr00k by manually triggering disassociations on the target's device repeatedly, thus greatly increasing the likelihood of intercepting (potentially sensitive) data of interest.

> ***When compared to other techniques commonly used against Wi-Fi, exploiting Kr00k has a significant advantage for attackers: while they need to be in range of the Wi-Fi signal, they do not need to be authenticated and associated to the WLAN. In other words, they don't need to know the Wi-Fi password."***
>
> **Robert Lipovský, ESET Senior Malware Researcher**

ESET RESEARCH CONTRIBUTIONS

Latest engagements and achievements of ESET Research experts

Presentations

RSAC 2020

Kr00k: How KRACKing Amazon Echo Exposed a Billion+ Vulnerable Wi-Fi Devices [7]

In the first public presentation on the topic, ESET's Robert Lipovský and Štefan Svorenčík unveiled Kr00k, a previously unknown security flaw affecting the encryption of over a billion Wi-Fi devices including some by Apple, Google, and Samsung.

Hunting Linux Malware for Fun and Flags [35]

In a hands-on, technical workshop, ESET researcher Marc-Étienne M.Léveillé addressed the need to train Linux system administrators to analyze and better understand server-side Linux threats. His tutorial aimed at creating an environment where Linux professionals had the opportunity to study such threats safely and effectively.

BlueHat IL

Tactics, Techniques and Procedures of the World's Most Dangerous Attackers [36]

ESET malware researcher Robert Lipovský shared the lessons learned from analyzing some of the most significant cyberattacks in history, focusing on the TTPs of Sednit, also known as APT28, and of Telebots, also known as Sandworm.

Attor: Spy Platform with Curious GSM Fingerprinting [37]

ESET malware researcher Zuzana Hromcová introduced Attor, a novel spy platform used in targeted attacks against high-value targets. Attor's defining features are a complex modular architecture, elaborate network communication and a unique plugin to fingerprint GSM devices.

MITRE ATT&CK contributions

Besides publishing, and presenting their findings at conferences, ESET researchers regularly contribute to *MITRE ATT&CK®* [38] – a globally-accessible knowledge base of adversary tactics and techniques.

As of April 2020, ESET is one of the top five contributors to the ATT&CK *Enterprise Matrix* [39], one of the first and most active contributors to the *Mobile Matrix* [40], and one of the most heavily referenced sources in both matrices.

At the time of writing, there are more than 100 contributors and 300 referenced sources for the Enterprise Matrix and six contributors and more than 100 referenced sources for the Mobile matrix.

Contributions from the threat intelligence community play a critical role in helping us refine and extend the coverage of the MITRE ATT&CK® knowledge base. Making cyberspace safer requires a collaborative effort, and the real-world reporting of adversary tactics and techniques from outside sources helps make ATT&CK a valuable asset for defenders.

Adam Pennington, MITRE ATT&CK Lead

4th out of 100+ contributors

8th out of 300+ referenced sources

ESET among the top 5 contributors and top 10 referenced sources in the MITRE ATT&CK Enterprise Matrix

ESET's contributions include new entries to the Enterprise and Mobile Techniques, Groups and Software categories, as well as extensions of existing entries.

In the Enterprise Techniques category, one of ESET's notable contributions is the unique *Transport Agent (T1505)* [41] arising from ESET's analysis of *LightNeuron* [42], a backdoor used by the Turla group. LightNeuron implements a malicious Microsoft Exchange transport agent for persistence.

The Software category features *LoJax (S0397)* [43], a UEFI rootkit used by Sednit (also known as APT28), *discovered* [44] by ESET and the first UEFI rootkit found in the wild.

In the Groups category, one of ESET's contributions is *Machete (G0095)* [45], a cyberespionage group with high-profile targets in Latin American countries, *reported* [46] by ESET researchers to have stolen gigabytes of confidential data over the course of a year.

ESET's Android threat research also made it into ATT&CK – the Mobile category includes the *Input Injection (T1516)* [47] and *Access Notifications (T1517)* [48] techniques, used by various kinds of data-stealing Android malware.

Along with ESET references on the ATT&CK website, readers will also find tables mapping adversary techniques to the ATT&CK knowledge base in the end sections of ESET research publications on the *WeLiveSecurity blog* [49].

Other contributions

ESET researchers have also been contributing to the YARA code base, a tool widely used by the malware research community. In Q1 2020, ESET had two pull requests merged into the main code base.

The *first accepted pull request* [50], based on research by ESET malware researchers Peter Kálnai and Michal Poslušný, extended YARA's Rich Header functionality to better represent the underlying data and enable full utilization of Rich Header data.

The *second contribution* [51] driven by ESET malware researcher Anton Cherepanov, improves YARA's PE module by adding a new feature for parsing PDB strings. This new feature makes it possible to create better YARA rules to hunt and detect Windows malware that has specific keywords in PDB paths.

Credits

Team

Peter Stančík, Lead

Klára Kobáková, Managing Editor

Aryeh Goretsky

Bruce Burrell

Nick FitzGerald

Ondrej Kubovič

Petr Blažek

Foreword

Roman Kováč, Chief Research Officer

Contributors

Igor Kabina

Jakub Souček

Ján Šugarek

Jean-Ian Boutin

Jiří Kropáč

Juraj Jánošík

Ladislav Janko

Lukáš Štefanko

Martin Abrahámek

Martin Červeň

Martin Lackovič

Mathieu Tartare

Matthieu Faou

Milan Fránik

Miloš Čermák

Miroslav Legéň

Miroslav Rolko

Patrik Sučanský

Robert Lipovský

Zoltán Rusnák

About the data in this report

The threat statistics and trends presented in this report are based on global telemetry data from ESET. Unless explicitly stated otherwise, the data includes detections regardless of the targeted platform and includes only unique daily detections per device.

This data was processed with the honest intention to mitigate all known biases, in an effort to maximize the value of the information provided.

Further, the data excludes detections of *potentially unwanted applications* [52], *potentially unsafe applications* [53] and adware, except where noted in the more detailed, platform-specific sections and in the Cryptominers section.

Most of the charts in this report show detection trends rather than providing absolute numbers. This is because the data can be prone to various misinterpretations, especially when directly compared to other telemetry data. However, absolute values or orders of magnitude are provided where deemed beneficial.

References

[1] https://www.krackattacks.com/#paper

[2] https://www.welivesecurity.com/2019/10/17/alexa-how-amazon-echo-kindle-got-kracked/

[3] https://www.icasi.org/

[4] https://www.welivesecurity.com/2020/02/26/krook-serious-vulnerability-affected-encryption-billion-wifi-devices/

[5] https://www.welivesecurity.com/wp-content/uploads/2020/02/ESET_Kr00k.pdf

[6] https://www.eset.com/int/kr00k/

[7] https://www.rsaconference.com/usa/agenda/kr00k-how-kracking-amazon-echo-exposed-a-billion-vulnerable-wifi-devices

[8] https://www.welivesecurity.com/2017/07/20/stantinko-massive-adware-campaign-operating-covertly-since-2012/

[9] https://www.welivesecurity.com/2019/11/26/stantinko-botnet-adds-cryptomining-criminal-activities/

[10] https://www.welivesecurity.com/2020/03/19/stantinko-new-cryptominer-unique-obfuscation-techniques/

[11] https://www.welivesecurity.com/2020/03/05/guildma-devil-drives-electric/

[12] https://www.welivesecurity.com/2019/10/14/connecting-dots-exposing-arsenal-methods-winnti/

[13] https://www.welivesecurity.com/2019/03/11/gaming-industry-scope-attackers-asia/

[14] https://www.welivesecurity.com/2019/10/21/winnti-group-skip2-0-microsoft-sql-server-backdoor/

[15] https://www.welivesecurity.com/2020/01/31/winnti-group-targeting-universities-hong-kong

[16] https://www.welivesecurity.com/2020/03/12/tracking-turla-new-backdoor-armenian-watering-holes/

[17] https://nvd.nist.gov/vuln/detail/CVE-2017-11882

[18] https://www.welivesecurity.com/2017/12/04/eset-takes-part-global-operation-disrupt-gamarue/

[19] https://www.bleepingcomputer.com/news/security/emotet-malware-restarts-spam-attacks-after-holiday-break/

[20] https://www.binarydefense.com/emotet-evolves-with-new-wi-fi-spreader/

[21] https://www.bleepingcomputer.com/news/security/maze-ransomware-not-getting-paid-leaks-data-left-and-right/

[22] https://www.welivesecurity.com/2020/03/23/good-bad-plain-ugly/

[23] https://twitter.com/CryptoInsane/status/1240668834190839808

[24] https://www.us-cert.gov/ncas/alerts/aa20-049a

[25] https://published-prd.lanyonevents.com/published/rsaus20/sessionsFiles/17627/2020_USA20_SEM-M03H_01_Feds-Fighting-Ransomware-How-the-FBI-Investigates-and-How-You-Can-Help.pdf

[26] https://youtu.be/LUxOcpIRxmg

[27] https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-led-action-takes-aim-at-cryptojacking-in-Southeast-Asia

[28] https://www.welivesecurity.com/2019/02/28/coinhive-cryptocurrency-miner-to-call-it-a-day-next-week

[29] https://www.welivesecurity.com/2019/05/17/eternalblue-new-heights-wannacryptor/

[30] https://www.welivesecurity.com/2019/05/22/patch-now-bluekeep-vulnerability/

[31] https://www.welivesecurity.com/2019/12/17/bluekeep-time-disconnect-rdp-internet/

[32] https://www.who.int/about/communications/cyber-security

[33] https://www.welivesecurity.com/2018/07/26/i-saw-what-you-did-or-did-i/

[34] https://nvd.nist.gov/vuln/detail/CVE-2012-5687

[35] https://www.rsaconference.com/usa/agenda/hunting-linux-malware-for-fun-and-flags

[36] https://www.bluehatil.com/abstracts#collapse-Tactics

[37] https://www.bluehatil.com/abstracts#collapse-GSMFingerprinting

[38] https://attack.mitre.org/

[39] https://attack.mitre.org/matrices/enterprise/

[40] https://attack.mitre.org/matrices/mobile/

[41] https://attack.mitre.org/techniques/T1505/

[42] https://www.welivesecurity.com/wp-content/uploads/2019/05/ESET-LightNeuron.pdf

[43] https://attack.mitre.org/software/S0397/

[44] https://www.welivesecurity.com/wp-content/uploads/2018/09/ESET-LoJax.pdf

[45] https://attack.mitre.org/groups/G0095/

[46] https://www.welivesecurity.com/wp-content/uploads/2019/08/ESET_Machete.pdf

[47] https://attack.mitre.org/techniques/T1516/

[48] https://attack.mitre.org/techniques/T1517/

[49] https://welivesecurity.com/

[50] https://github.com/VirusTotal/yara/pull/1135

[51] https://github.com/VirusTotal/yara/commit/a72945ce44ce70bd7193e94c16e8bef580e35038

[52] https://help.eset.com/glossary/en-US/unwanted_application.html

[53] https://help.eset.com/glossary/en-US/unsafe_application.html

ENJOY SAFER TECHNOLOGY™

About ESET

For more than 30 years, *ESET®* has been developing industry-leading IT security software and services for businesses and consumers worldwide. With solutions ranging from endpoint and mobile security to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give consumers and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company. Backed by R&D centers worldwide, ESET is the first IT security company to earn *100 Virus Bulletin VB100 awards*, identifying every single "in-the-wild" malware without interruption since 2003. For more information, visit *www.eset.com* or follow us on *LinkedIn*, *Facebook*, and *Twitter*.

WeLiveSecurity.com
@ESETresearch
ESET GitHub