w/ 2021 trends & 2022 outlook

THREAT REPORT T3 2021

WeLiveSecurity.com
@ESETresearch
ESET GitHub

ESET Digital Security
Progress. Protected.

CONTENTS

3 FOREWORD

4 EXECUTIVE SUMMARY

5 FEATURED STORY

8 NEWS FROM THE LAB

11 APT GROUP ACTIVITY

17 STATISTICS & TRENDS

- 18 THREAT LANDSCAPE OVERVIEW
- 19 TOP 10 MALWARE DETECTIONS
- 20 INFOSTEALERS
- 23 RANSOMWARE
- 26 DOWNLOADERS
- 28 CRYPTOCURRENCY THREATS
- 31 WEB THREATS
- 34 EMAIL THREATS
- 38 ANDROID
- 41 macOS AND iOS
- 43 IoT SECURITY
- 45 EXPLOITS

48 ESET RESEARCH CONTRIBUTIONS

FOREWORD

Welcome to the T3 2021 issue of the ESET Threat Report!

While 2020 was the year of supply-chain attacks (and, yes, the start of the global COVID-19 crisis), 2021 was defined by shockingly severe vulnerabilities (...and vaccines).

The year started with a bang, when Microsoft Exchange servers around the world found themselves under fire from at least ten APT groups. ProxyLogon, the vulnerability chain at the bottom of these attacks, ended up being the second most frequent external attack vector in 2021, according to ESET telemetry, right after password-guessing attacks. As you'll read in this report, Microsoft Exchange servers ended up under siege again in August 2021, with ProxyLogon's "younger sibling", named ProxyShell, exploited worldwide by several threat groups.

When a critical flaw in the ubiquitous Log4j utility surfaced in mid-December, IT teams everywhere were sent scrambling, again, to locate and patch the flaw in their systems. This vulnerability, scoring a 10 on the CVSS scale, put countless servers at risk of a complete takeover – so it came as no surprise that cybercriminals instantly started exploiting it. Despite only being known for the last three weeks of the year, Log4j attacks were the fifth most common external intrusion vector in our 2021 statistics, showing just how quickly threat actors are taking advantage of newly emerging critical vulnerabilities.

The end of the year was also turbulent in the area of RDP attacks, which escalated throughout all of 2020 and 2021. The numbers from the last weeks of T3 2021 broke all previous records, amounting to a staggering yearly growth of 897% in total attack attempts blocked – despite the fact that 2021 was no longer marked by the chaos of newly imposed lockdowns and hasty transitions to remote work. Probably the only good news from the RDP attack front, as noted in the Exploits section of this report, is that the number of targets has been gradually shrinking, although it doesn't seem like the rampage is about to end any time soon.

Ransomware, previously described in our Q4 2020 Threat Report as "more aggressive than ever" surpassed the worst expectations in 2021, with attacks against critical infrastructure, outrageous ransom demands, and over USD 5 billion worth of bitcoin transactions tied to potential ransomware payments identified in the first half of 2021 alone.

However, the pressure has been growing from the other side, too, represented by feverish law enforcement activity against ransomware and other cybercriminal endeavors. While the intense clampdown forced several gangs into fleeing the scene – even releasing decryption keys – it seems that some attackers are only getting bolder: T3 saw the highest ransom ultimatum yet, USD 240 million, more than triple the record mentioned in our previous report.

And to throw in another all-time high: as the bitcoin exchange rate reached its highest point so far in November, ESET experts observed an influx of cryptocurrency-targeting threats, further boosted by the recent popularity of NFTs (non-fungible tokens).

In the world of mobile, we noted an alarming upsurge in Android banking malware detections, which rose by 428% in 2021 compared to 2020, reaching the detection levels of adware – a common nuisance on the platform. It is needless to say that the damage potential of these two threats cannot be compared, and we can only hope that the downward trend seen for banking malware in T3 2021 will spill over into 2022.

Email threats, the door to a myriad of other attacks, saw their yearly detection numbers more than double. This trend has been mainly driven by a rise in phishing emails, which more than compensated for the rapid decline in Emotet's signature malicious macros in email attachments. Emotet, inactive for most of the year, came back from the dead in T3, with its operators trying to rebuild its infrastructure with support from Trickbot. In 2022, ESET malware analysts expect the botnet to expand rapidly, pushing the malware back into the leading ranks – a process we will be monitoring closely.

The final months of 2021 were also rife with research findings, with ESET Research uncovering: FontOnLake, a new malware family targeting Linux; a previously undocumented real-world UEFI bootkit named ESPecter; FamousSparrow, a cyberespionage group targeting hotels, governments, and private companies worldwide; and many others. T3 also saw our researchers publish a comprehensive analysis of all 17 malicious frameworks known to have been used to attack air-gapped networks, and conclude their extensive series of deep dives into Latin American banking trojans.

This report also provides previously unpublished information about APT group operations. This time, our researchers offer updates on the activity of cyberespionage group OilRig; latest information on in-the-wild ProxyShell exploitation; and new spearphishing campaigns by the infamous cyberespionage group the Dukes.

And, as always, ESET researchers took multiple opportunities to share their expertise at various virtual conferences this period, appearing at Virus Bulletin 2021, SecTor 2021, AVAR 2021 Virtual and others. For the upcoming months, we are excited to invite you to an ESET talk at SeQCure in April 2022, and to the RSA Conference in June 2022 where we will be presenting the recent ESPecter discovery.

Happy reading, stay safe – and stay healthy!

Roman Kováč
ESET Chief Research Officer

EXECUTIVE SUMMARY

FEATURED STORY

Strategic web compromises in the Middle East with a pinch of Candiru

ESET researchers discovered a campaign of strategic web compromises targeting high-profile websites in the Middle East. The attacks are linked to Candiru, a company that sells state-of-the-art offensive software tools and related services to government agencies.

APT GROUP ACTIVITY

OilRig
Latest activity of the Iranian APT group OilRig with targets in Israel, Tunisia, and the United Arab Emirates; Marlin backdoor discovered

ProxyShell vulnerability
Worldwide ProxyShell exploitation by multiple threat actors starting in August 2021

The Dukes
Spearphishing campaigns in October and November 2021 targeting European diplomatic missions and Ministries of Foreign Affairs

STATISTICS & TRENDS

Category	T2-T3	2020-2021	Key points in T3 2021
Overall threat detections	+7.2% ↑	-16.0%	Top threat: HTML/Phishing.Agent trojan
Infostealers	-15.2% ↓	N/A	Rise in banking malware
Ransomware	+0.6% →	-44.6% ↓	Highest ransom ultimatum yet
Downloaders	+46.1% ↑	-39.2 % ↓	Emotet makes a comeback
Cryptocurrency threats	+7.7% ↑	N/A	Targeting of NFT platforms
Web threats	+2.6% ↑	-49.5% ↓	Rise in cryptocurrency-themed phishing
Email threats	+8.5% ↑	+145.4% ↑	Rise in phishing emails
Android	+2.8% ↑	N/A	Yearly increase in banking malware: 428%
macOS	-5.9% ↓	-36.6% ↓	Trojans one third of macOS detections
RDP attacks	+274% ↑	+897% ↑	Rise in attack attempts, fewer targets

FEATURED STORY

Strategic web compromises in the Middle East with a pinch of Candiru

Matthieu Faou

ESET researchers discovered a campaign of strategic web compromises targeting high-profile websites in the Middle East, with a strong focus on Yemen and those with an interest in its civil war.

ESET researchers have discovered strategic web compromise (watering hole) attacks against high-profile websites in the Middle East, with a strong focus on Yemen. The attacks are linked to Candiru, a company that sells state-of-the-art offensive software tools and related services to government agencies and that was recently added to the Entity List (entities subject to licensing restrictions) of the US Department of Commerce.

The victimized websites belong to media outlets in the UK, Yemen, and Saudi Arabia, as well as to Hezbollah; to government institutions in Iran (Ministry of Foreign Affairs), Syria (including the Ministry of Electricity), and Yemen (including the Ministries of Interior and Finance); to internet service providers in Yemen and Syria; and to aerospace/defense companies in Italy and South Africa. The attackers also created a website mimicking a medical trade fair in Germany.

A watering hole attack compromises a website that is likely to be visited by targets of interest, thus opening the door to the infestation of any website visitor's machine. What is interesting to note is that the watering holes in this case are limited to a quite narrow victimology. In this campaign, specific visitors of these websites were likely attacked via a browser exploit. However, ESET researchers were unable to get hold of either an exploit or the final payload.

This shows that the threat actors have chosen to narrow the focus of their operations, perhaps to not burn their zero-day exploits, demonstrating how highly targeted this campaign is. The compromised websites are only used as a jumping-off point to reach the ultimate targets.

Attacks revealed by ESET's custom in-house system

Back in 2018, ESET researchers developed a custom in-house system to uncover watering hole attacks on high-profile websites. On July 11, 2020, this system notified them that the website of the Iranian embassy in Abu Dhabi had been tainted with malicious JavaScript code. ESET researchers' curiosity was piqued by the high-profile nature of the targeted website, and in the following weeks, they noticed that other websites with connections to the Middle East were also targeted.

ESET researchers believe that the strategic web compromises only started in April 2020 when the website of the Middle East Eye, "middleeasteye.net", a London-based digital news site covering the region, started to inject code from the "piwiks[.]com" domain. At the end of July or the beginning of August 2020, all remaining compromised websites were cleaned; it is probable that the attackers themselves removed the malicious scripts from the compromised websites.

The threat group went quiet until January 2021, when ESET researchers observed a

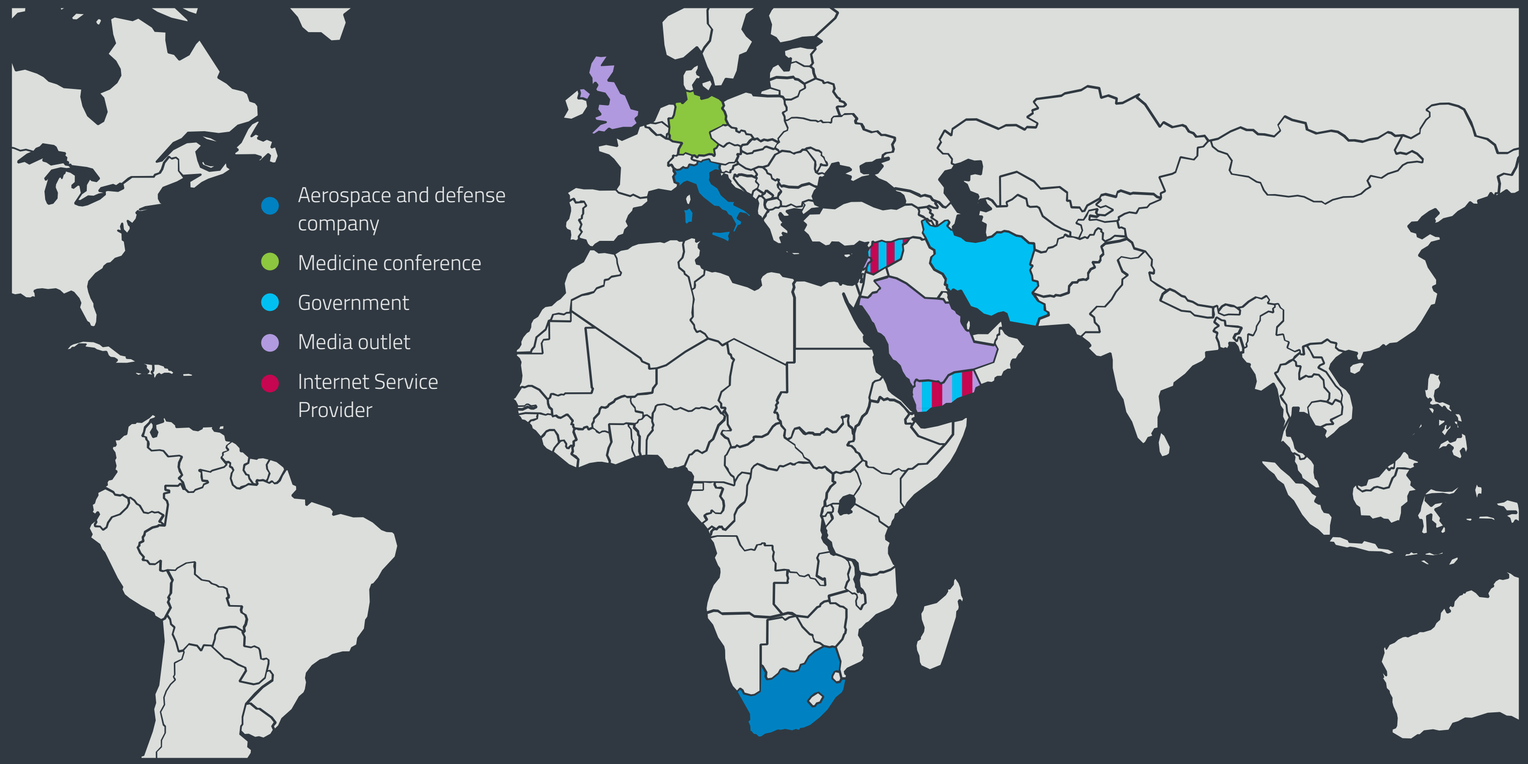
new wave of compromises. This second wave lasted until August 2021, when all websites were cleaned again.

During the 2020 campaign, the malware checked website visitors' operating systems and web browsers. The selection process was based on system software (Windows or macOS), and it is interesting to note this suggests that this operation was intended to compromise computers and not mobile devices such as smartphones. In the second wave, in order to be a bit stealthier, the attackers started to modify scripts that were already on the compromised websites.

Compromised or abused websites

April 2020 – August 2020

- **middleeasteye.net** A UK-based online newspaper covering the Middle East.
- **piaggioaerospace.it** An Italian aerospace company.
- **medica-tradefair[.]co** Fake website impersonating a German medical trade fair in Düsseldorf.
- **mfa.gov.ir** Ministry of Foreign Affairs of Iran.
- **almanar.com.lb** Television channel linked to Hezbollah.



Regional origin of known websites compromised or abused in watering hole attacks

January 2021 – August 2021

- **smc.gov.ye** Ministry of Interior of Yemen.
- **almasirahnews.com** Yemeni television channel linked to the Ansar Allah movement (Houthis).
- **casi.gov.sy** Central Authority for the Supervision and Inspection of Syria.
- **moe.gov.sy** Syrian Ministry of Electricity.
- **almanar.com.lb** Television channel linked to Hezbollah.
- **manartv.com.lb** Television channel linked to Hezbollah.
- **mof.gov.ye** Ministry of Finance of Yemen.
- **scs-net.org** Internet Service Provider in Syria.
- **customs.gov.ye** Customs agency of Yemen.
- **denel.co.za** A South African state-owned aerospace and military technology conglomerate. Additional websites compromised:
  - **pmp.co.za**
  - **deneldynamics.co.za**
  - **denellandsystems.co.za**
  - **denelaviation.co.za**
- **yemen.net.ye** Internet service provider in Yemen.
- **yemenparliament.gov.ye** Parliament of Yemen.
- **yemenvision.gov.ye** Yemeni government website.
- **mmy.ye** Yemeni media linked to the Houthis.
- **thesaudireality.com** Likely dissident media outlet in Saudi Arabia.
- **saba.ye** Yemeni news agency linked to Houthis. However, it seems it was taken over by the Southern Transitional Council in early June 2021, just before this website was compromised.

Cloned version of the Medica Trade Fair website

The outlier in this list is "medica-tradefair[.]co", as it was not compromised but was operated by the attackers themselves. It mimics the legitimate website "medica-tradefair.com", which is the website of the World Forum for Medicine's MEDICA Trade Fair held yearly in Düsseldorf (Germany). The operators simply cloned the original website and added a small piece of JavaScript code.

It is likely that attackers were not able to compromise the legitimate website and had to set up a fake one in order to inject their malicious code. It is interesting to note that the malicious domains mimic genuine web analytics, URL shortener and content delivery network domains and URLs. This is a characteristic of this threat actor.

Links between the watering holes, spearphishing documents and Candiru

In a blogpost about *Candiru by Citizen Lab* [1] at the University of Toronto, the section called "A Saudi-Linked Cluster?" mentions a spearphishing document that was uploaded to VirusTotal and multiple domains operated by the attackers. The domain names are variations of genuine URL shorteners and web analytics websites, which is the same technique used for the domains seen in the watering hole attacks documented here.

Thus, there is a significant likelihood that the operators of these watering hole campaigns are customers of Candiru. The creators of the documents and the operators of the watering holes are also potentially the same. Candiru is a private Israeli spyware company that was recently added to the *US Department of Commerce's Entity List* [2]. This may prevent any US-based organization from doing business with Candiru without first obtaining a license from the Department of Commerce.

ESET stopped seeing activity from this operation at the end of July 2021, shortly after the release of blogposts by the *Citizen Lab* [1], *Google* [3], and *Microsoft* [4] detailing the activities of Candiru. To read more about recent developments with other mercenary spyware vendors, see the *macOS and iOS threats* section.

The operators of these strategic web compromises appear to be taking a pause, probably in order to retool and make their campaign stealthier. ESET Research expects them back in the ensuing months.

WeLiveSecurity blogpost [5]

NEWS FROM THE LAB

Latest findings from ESET Research Labs across the world

UEFI threats Upcoming presentation

UEFI threats moving to the ESP: Introducing ESPecter bootkit

ESET researchers analyzed a previously undocumented real-world UEFI bootkit that persists on the EFI System Partition (ESP), hence our choice of name – ESPecter. It bypasses Windows Driver Signature Enforcement to load its own unsigned driver to facilitate its espionage activities.

ESPecter is the second discovery of a UEFI bootkit persisting on the ESP and shows how real-world UEFI threats are no longer limited to SPI flash implants as used by the first in-the-wild UEFI bootkit, LoJax, which ESET discovered in 2018. This shows that threat actors are not relying only on UEFI firmware implants when it comes to pre-OS persistence, but are also trying to take advantage of disabled Secure Boot to execute their own ESP implants.

The roots of this threat can be traced back to at least 2012; it was previously operating as a bootkit for systems with legacy BIOSes. Despite ESPecter's long existence, its operations and upgrade to UEFI went unnoticed and were not documented until T3 2021. Interestingly, the malware's components barely changed between its 2012 and 2020 versions.

Among other components, ESPecter deploys a backdoor that supports a rich set of commands and contains various automatic data exfiltration capabilities, including document stealing, keylogging, and monitoring of the victim's screen by periodically taking screenshots. All of the collected data is stored in a hidden directory.

WeLiveSecurity blogpost [6]

Downloaders

Wslink: Unique and undocumented malicious loader that runs as a server

ESET researchers discovered a unique and previously undocumented loader for Windows binaries that, unlike other such loaders, runs as a server and executes received modules in memory. We named the loader Wslink after one of its DLLs.

The loader features a well-developed cryptographic protocol to protect exchanged data. Wslink's modules do not have to initiate new outbound connections, since they reuse the loader's functions for communication, keys, and sockets. We were unable to obtain any of the modules it is supposed to receive.

Our telemetry has registered only a few hits in the past two years, with detections in Central Europe, North America, and the Middle East. There are no code, functionality or operational similarities to suggest that this is likely a tool from a known threat actor group.

We implemented our own version of a Wslink client, which could be of interest to beginners in malware analysis – it shows how one can reuse and interact with existing functions of previously analyzed malware. Full source code for the client is available in our WslinkClient GitHub repository.

WeLiveSecurity blogpost [7]

WslinkClient GitHub repository [8]

Infostealers

FontOnLake: Previously unknown malware family targeting Linux

ESET researchers documented a previously unknown malware family that targets Linux systems and utilizes custom modules. We named this family FontOnLake. Modules used by FontOnLake provide the operators remote access to the victim, collect credentials, and act as a proxy server.

The first known file of this malware family appeared on VirusTotal in May 2020 and other samples were uploaded throughout the year.

FontOnLake uses modified, legitimate binaries to collect data or conduct other malicious activities. These binaries are commonly used on Linux systems and can additionally serve as persistence mechanisms. To further conceal its existence, FontOnLake's presence is always obscured by a rootkit.

The malware's currently known components can be divided into three groups that interact with each other: trojanized applications, backdoors, and rootkits. The sneaky nature of FontOnLake's tools, combined with advanced design and low prevalence, suggest that they are used in targeted attacks.

We believe that the operators of FontOnLake are particularly cautious since almost all samples we have seen use unique C&C servers with varying non-standard ports. Furthermore, none of the C&C servers used in samples uploaded to VirusTotal were active at the time of writing – which indicates that they could have been disabled due to the upload. The location of the C&C server and the countries from which the samples were uploaded to VirusTotal might indicate that FontOnLake's targets include Southeast Asia.

WeLiveSecurity blogpost [9]

Banking malware

Numando: Count once, code twice

In the penultimate entry in our series on Latin American banking trojans, ESET Research took a look at Numando, which targets mainly Brazil, with occasional campaigns in Mexico and Spain. Unlike most other Latin American banking trojans, Numando does not show signs of continuous development. Still, it has been active since at least 2018, and we have seen it used consistently since we started tracking it.

This banking malware is distributed almost exclusively by spam. It uses seemingly useless ZIP archives or bundles payloads with decoy BMP images that are suspiciously large. The BMP files are valid images that can be opened by most image viewers and editors without issue.

Numando is similar to other families described in the series: it uses fake overlay windows, contains backdoor functionality and utilizes MSI. Nonetheless, there are some differences: while it is written in Delphi, the same as most other LATAM banking trojans, it uses a non-Delphi injector. Its remote configuration format is also unique, making two reliable factors when identifying this malware family.

WeLiveSecurity blogpost [10]

The dirty dozen of Latin America: From Amavaldo to Zumanek

ESET Research concluded its series of deep dives into Latin American banking trojans, started in August 2019. This series covered the most active ones, namely Amavaldo, Casbaneiro, Mispadu, Guildma, Grandoreiro, Mekotio, Vadokrist, Ousaban and Numando.

These are the key takeaways of the series:

- Latin American banking trojans are an ongoing, evolving threat
- They target mainly Brazil, Spain, and Mexico
- There were at least eight different malware families still active at the time of the publication of the last article
- Three families went dormant during the course of this series
- The vast majority are distributed via spam, usually leading to a ZIP archive or an MSI installer

LATAM banking trojan campaigns come in waves, and more than 90% of them are distributed through spam, usually leading to a ZIP archive or an MSI installer. A typical campaign usually lasts for a week at most.

The families that are no longer active are Krachulka, which was active in Brazil until the middle of 2019; Lokorrito, seen mainly in Mexico until the beginning of 2020; and Zumanek, targeting only Brazil, active until the middle of 2020.

The most significant discovery during the course of our series is likely the expansion of Mekotio and Grandoreiro to Europe. Apart from Spain, we've observed occasional small campaigns targeting Italy, France, and Belgium. We believe these banking trojans will continue to test new territories for future expansion.

WeLiveSecurity blogpost [11]

APT GROUP ACTIVITY

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

Multiple APT groups

Jumping the air gap: 15 years of nation-state effort

ESET researchers analyzed all 17 malicious frameworks known to have been used to attack air-gapped networks. We utilized the knowledge made public by more than ten different organizations over the years and some ad hoc analysis to clarify or confirm some technical details. This exhaustive study allowed us to isolate several major similarities in all of these frameworks.

It is very difficult to detect this type of framework; several were active for many years before being exposed. All of these attacks were carried out by APT groups, and all shared a common purpose: espionage.

They were all built to attack Windows systems. Over 75% of all the frameworks used malicious LNK or autorun files on USB drives to either perform the initial compromise on the air-gapped system or move laterally within the air-gapped network. Interestingly, in every case, the method of initial compromise was a weaponized USB drive.

Having identified the risks, we put together a list of detection and mitigation techniques to protect air-gapped networks against the main methods used by all the malicious frameworks publicly known to date. To ensure better protection, we thus advise that you: prevent email access to connected hosts, disable USB ports and sanitize USB drives, restrict file execution on removable drives, and perform regular analysis of the system.

WeLiveSecurity blogpost [12]

FamousSparrow

FamousSparrow: A suspicious hotel guest

ESET researchers uncovered a new cyberespionage group targeting hotels, governments, and private companies worldwide. We named this group FamousSparrow, and we believe it has been active since at least 2019.

FamousSparrow leveraged the Microsoft Exchange vulnerability known as ProxyLogon, the same code execution vulnerability that was used by more than ten other APT groups to take over Exchange email servers earlier this year.

This APT group is the only known user of the custom backdoor SparrowDoor, and it also uses two custom versions of Mimikatz that could be used to connect incidents to this group.

While we consider FamousSparrow a separate entity, we also found connections to other known APT groups. In one case, attackers deployed a variant of Motnug, a loader used by SparklingGoblin. In another case, on a machine compromised by FamousSparrow, we found a running Metasploit with "cdn.kkxx888666[.]com" as its C&C server. This domain is related to a group known as DRBControl.

FamousSparrow's targets, which include governments worldwide, suggest that the group's intent is cyberespionage.

WeLiveSecurity blogpost [13]

BladeHawk

BladeHawk group: Android espionage against Kurdish ethnic group

ESET researchers investigated a mobile espionage campaign targeted against the Kurdish ethnic group. The espionage activity reported here is directly connected to two publicly disclosed cases published in 2020. QiAnXin Threat Intelligence Center named the group behind these attacks BladeHawk, which we have adopted.

The campaign has been active since at least March 2020, distributing two Android backdoors known as 888 RAT and SpyNote via Facebook, disguised as legitimate apps. We identified six Facebook profiles as part of this BladeHawk campaign. We reported these profiles to Facebook and they have all been taken down. Two of the profiles were aimed at tech users while the other four posed as supporters of the Kurds.

During our research, we found only one old and already analyzed sample of SpyNote, so we focused on the analysis of Android 888 RAT.

This malware is a commercial, multiplatform RAT. Among other things, it can steal and delete files from a device, take screenshots, get device location, phish Facebook credentials, record surrounding audio and phone calls, make calls, and send text messages. In 2019, its Pro version, which enables building Android RATs, was found cracked and available on several websites for free. Since then, we have detected hundreds of cases worldwide using the Android version of 888 RAT.

WeLiveSecurity blogpost [14]

Lazarus

Lazarus group distributes trojanized IDA Pro installer

On Twitter, ESET Research announced the discovery of a trojanized installer of the IDA Pro software, a binary code analysis tool used by reverse engineers, malware analysts and cybersecurity professionals. Due to the nature of the included malware, we attribute these actions to the Lazarus group.

This trojanized version of the IDA Pro installer contains two malicious components. The first is a malicious DLL that replaces `win_fw.dll`, an internal component executed during IDA Pro installation. This DLL then creates a Windows scheduled task that starts a second malicious component, `idahelper.dll`, which attempts to download and execute the next-stage payload.

Twitter thread [15]

OilRig Threat Report exclusive

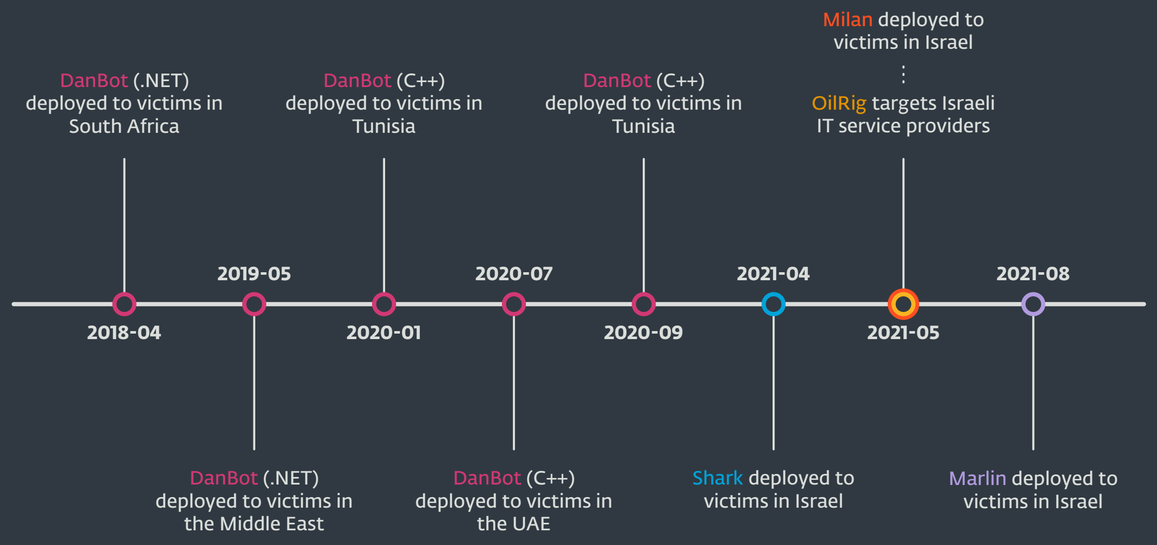
OilRig, also known as APT34, Lyceum, and Siamesekitten, is a cyberespionage group that has been active since at least 2014 and is commonly believed to be based in Iran [16]. The group targets Middle Eastern governments and a variety of business verticals, including chemical, energy, financial, and telecommunications. OilRig carried out the DNSpionage campaign in 2018 and 2019 that targeted victims in Lebanon and the United Arab Emirates. In 2019 and 2020, OilRig continued attacks with the HardPass campaign, using LinkedIn to target Middle Eastern victims in the energy and government sectors.

OilRig: The Out to Sea campaign featuring Marlin

OilRig was particularly active in September – December 2021, iterating on a campaign we are calling Out to Sea. OilRig operators have been developing and deploying iterative improvements to the DanBot backdoor, with Shark, Milan, and Marlin, an ESET exclusive.

Out to Sea campaign featuring Marlin

Carried out over the course of three and a half years, OilRig has been running the Out to Sea campaign; it has used multiple backdoors, beginning with DanBot (discovered by *SecureWorks* [17] but attributed to Lyceum), transitioning from .NET to C++. In April 2021, OilRig began using the Shark backdoor before quickly transitioning to the Milan backdoor in August 2021 (both reported by *Clearsky*



Out to Sea campaign timeline

[18] but attributed to Siamesekitten). As of August 2021, OilRig had begun using a backdoor ESET researchers discovered and are calling Marlin.

DanBot, Shark, and Milan use both DNS, a commonality for OilRig backdoors, and HTTP/S, for network communications with C&C servers. Marlin, however, in a significant departure from typical OilRig tactics, techniques, and procedures, uses the OneDrive API for its C&C operations. Post-compromise activities include data collection (via browser-data theft, and a keylogger) and exfiltration, and also lateral movement.

Victims of the campaign include diplomatic organizations, technology companies, and medical organizations in Israel, Tunisia, and the United Arab Emirates (UAE).

ESET researchers observed two methods for initial access: spearphishing and via the remote administration software *ITbrain* [19], which was found in conjunction with the remote access tool TeamViewer. This attack vector was also alluded to by Clearsky.

Additional tools used after establishing a foothold include:

- a Chrome browser data dumper
- PowerShell backdoor loaders
- WinRAR
- Mimikatz
- an SMB lateral movement tool that leverages *EternalBlue* [20]
- a keylogger
- Tuna, a parser for the Windows Master File Table (MFT), a database in which information about every file and directory on an NT File System (NTFS) volume is kept.

Lyceum and Siamesekitten are OilRig

The first appearance of DanBot in 2019 was originally attributed to a new group, *Lyceum* [17]. At that time, researchers correctly identified links to OilRig but lacked the clarity necessary to fully attribute DanBot to OilRig. Subsequent *reports* [21] further entrenched the *DanBot* [22] attribution to Lyceum. The most recent iteration of this campaign, attributed to a new group, *Siamesekitten* [18], was also linked with Lyceum. However, the similarities between known OilRig backdoors and the backdoors used in the Out to Sea campaign are too numerous and specific to write off to another group that is merely "like" OilRig.

OilRig indicators

Beginning with the *ToneDeaf backdoor* [23], OilRig has shown a propensity for deploying tools with non-functional components. The ToneDeaf backdoor primarily communicated with its C&C over HTTP/S but included a secondary method, DNS tunneling, which does not function properly. Shark has similar symptoms, where its primary communication method uses DNS but has a non-functional HTTP/S secondary option. In a similar vein, the SMB lateral movement tool, when it attempts to determine a remote system's vulnerability to EternalBlue, uses a hard-coded private IP address that is unlikely to ever identify a vulnerable system (unless that system has that specific private IP address).

Another telltale sign of OilRig is the creation and use of multiple folders in a backdoor's working directory that are used for uploading to, and downloading files from, the OilRig C&C server. First documented in the *ALMA backdoor* [24], we see DanBot, Shark, and Milan employing the same methodology. We rarely see similar TTPs from other groups.

Lastly, OilRig operators are well known for using DNS as a C&C communication channel, while also employing HTTP/S as a secondary communication method. The *ISMAgent* [25] and *PoisonFrog* [26] backdoors are some of the earliest documented cases. The *RDAT* [27] and ToneDeaf backdoors continued the trend. And we see it employed in the Out to Sea campaign with DanBot, Shark, and Milan.

Indicators of Compromise (IoCs) [28]

ProxyShell vulnerability Threat Report exclusive

Microsoft Exchange servers under siege, once again.

In March 2021, ESET researchers reported on Microsoft Exchange servers being *exploited around the world by at least 10 APT groups* [29] using a pre-authentication remote code execution (RCE) vulnerability chain (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065) discovered by Orange Tsai and dubbed ProxyLogon. This vulnerability chain allows an attacker to take over any reachable Exchange server.

In April 2021, Orange Tsai discovered another pre-authentication RCE vulnerability chain on Microsoft Exchange that he called ProxyShell and that consists of three vulnerabilities: *CVE-2021-34473* [30], *CVE-2021-34523* [31] and *CVE-2021-31207* [32].

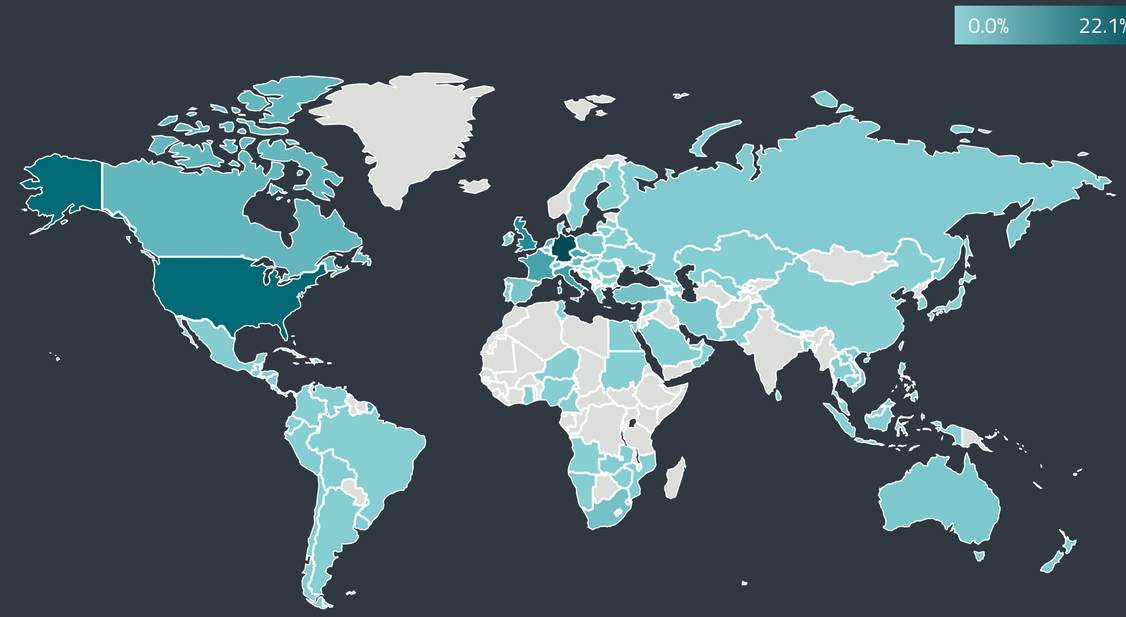
Orange Tsai first described his ProxyShell discoveries during a presentation at Black Hat USA on August 3, 2021. For more details about the ProxyShell vulnerability chain, please refer to Orange Tsai's presentations at *Black Hat USA* [33] and *DEFCON* [34], or the *technical analysis published on his blog* [35].

Microsoft released two security updates addressing the issue on *April 13* [36] and *May 11* [37], 2021. The US Cybersecurity and Infrastructure Security Agency (CISA) released *an alert regarding malicious threat actors actively exploiting the ProxyShell vulnerability* [38] on August 21, 2021. In this exclusive, we document activity by various APT groups that exploited the ProxyShell vulnerability chain in August and September 2021. The complete research was available a few months ago to subscribers of the ESET Threat Intelligence private APT reports.

Since the release of the various warnings regarding active, in-the-wild exploitation of the ProxyShell vulnerability chain, we have been monitoring closely detections of malicious PST files related to these exploits (Personal Storage Table is a file format that can be used to store emails, calendars and mailboxes), as the last stage of the exploitation (*CVE-2021-31207* [32]) consists of the decoding of a malicious PST file that allows dropping a webshell.

The heatmap on the right shows the geographical distribution of the webshell detections, according to ESET telemetry. Due to mass exploitation, it is likely that it represents the distribution of vulnerable Exchange servers around the world on which ESET security products are installed.

From ESET telemetry data, we noticed worldwide ProxyShell exploitation by several distinct APT groups starting on August 12, 2021. Among the numerous exploitation attempts we observed, we have identified four clusters of activities, where threat actors are likely to have leveraged the ProxyShell vulnerability chain in order to install implants on victims' email servers, which we have attributed to established groups, and we also identified one cluster that we have not been able to attribute to a known threat actor:



Geographical distribution of ProxyShell-related webshell detections

- **ApplicationUpdate cluster:** So far, we have not been able to conclusively attribute this activity to a known threat actor. We identified this cluster by analyzing information *tweeted* [39] by *two* [40] security researchers. By looking for similar activity in our telemetry data we found 13 other Exchange servers, all based in the USA, exploited with the ProxyShell vulnerability chain with the same implants as in the cases described in those two researchers' tweets. These victims include several organizations from the healthcare sector, a property development company, a hardware retailer, a building materials supplier, construction and engineering companies, a city hall and two county administrations.
- **TA410:** This APT group is known mostly for targeting US-based organizations in the utilities sector. In 2020, we also saw TA410 targeting diplomatic organizations in the Middle East and Africa. In this case, however, we were able to determine that it used the ProxyShell vulnerability chain to compromise an Exchange server owned by a religious organization in Hungary and an Exchange server belonging to a manufacturing company in Japan.
- **TA428:** This is an APT group active since at least 2014 that targets governments in East Asia with a particular focus on Mongolia and Russia. It used the ProxyShell vulnerability chain to compromise an Exchange server owned by a European Ministry of Foreign Affairs. We attribute this activity to TA428 with medium confidence.
- **SparklingGoblin:** This APT group has some level of connection with Winnti Group and partially

overlaps with APT41. In 2020, the group was very active and remains so in 2021. Even though the group targets mostly East and Southeast Asia, we have seen SparklingGoblin targeting a broad range of organizations and verticals around the world, with a particular focus on the academic sector. This group used the ProxyShell vulnerability chain to compromise an Exchange server owned by a Hong Kong university.

- **RedFoxtrot:** This group has been active since at least 2014 and targets government, defense and the telecommunications sectors in Central Asia, India, and Pakistan. It used the ProxyShell vulnerability chain to compromise an Exchange server owned by a business and IT consultancy based in Pakistan.

Once the vulnerability had been exploited and the webshell was in place, we observed attempts to install additional malware. We also noticed in some cases that several threat actors were targeting the same organization. Unfortunately, we also cannot discount the possibility that some threat actors might have hijacked the webshells dropped by other groups rather than directly using the exploit for the initial compromise.

The Dukes Threat Report exclusive

The Dukes, also known as APT29, Cozy Bear or Nobelium, is an infamous cyberespionage group active for more than a decade. It is one of the groups that hacked the US Democratic National Committee in the run-up to the 2016 Presidential election. In 2019, we exposed Operation Ghost [41], a large-scale espionage operation targeting ministries of foreign affairs in Europe. In 2020, the group received a lot of attention for the supply-chain attack piggybacking on SolarWinds, leading to the compromise of major organizations including many parts of the US government.

The Dukes: Phishing European diplomats

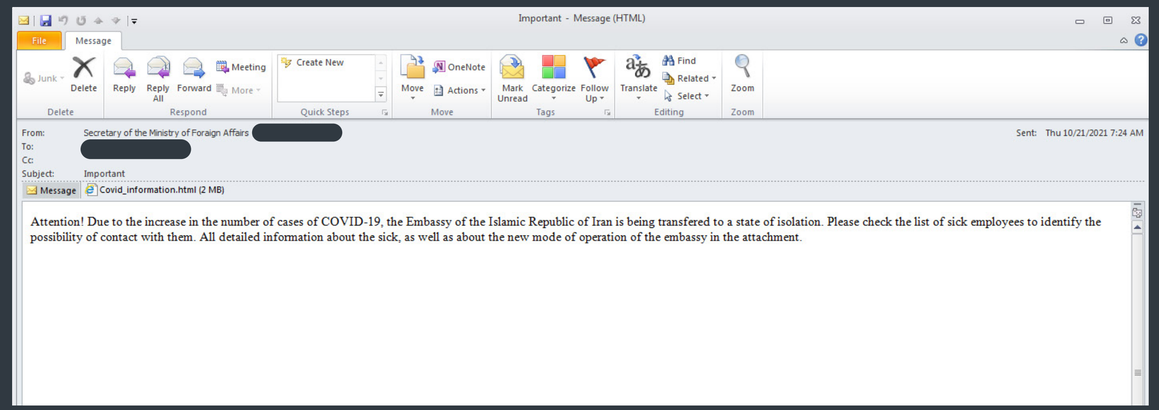
In the previous threat report, ESET researchers highlighted several spearphishing campaigns against European diplomats. These malicious operations were attributed to an infamous cyberespionage group known as the Dukes.

In October and November 2021, ESET detected additional spearphishing campaigns, again targeting European diplomatic missions and Ministries of Foreign Affairs. ESET researchers also attribute these new operations to the Dukes.

This is in line with recent open-source reporting such as *this report* [42] by ANSSI (the French National Agency for the Security of Information Systems) released in early December 2021. It states that several French entities were targeted by the group during 2021, and compromised email accounts belonging to French institutions were in turn used to send spearphishing emails to foreign targets.

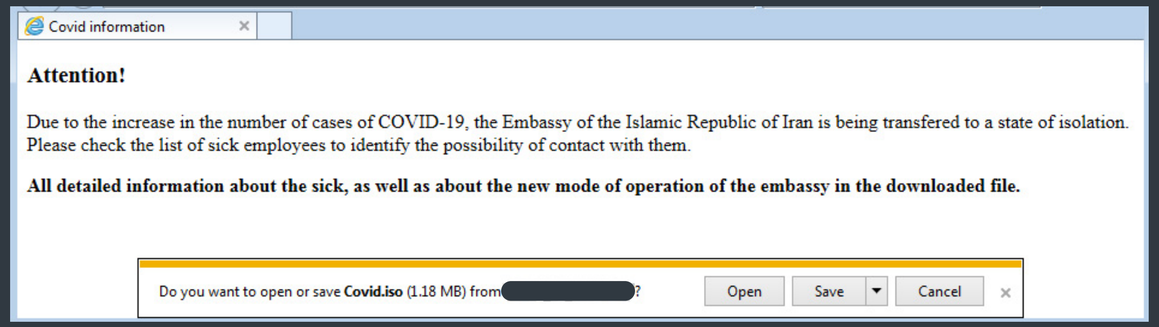
Spearphishing example

As mentioned in the previous threat report, emails sent by the Dukes generally contain an HTML attachment and a small decoy message body to trick targets into opening that HTML file. In the example below, the attackers impersonate the Iranian Ministry of Foreign Affairs and state that the Iranian embassy will be closed because of COVID-19. This email was sent to people working in diplomatic missions of European Union countries.



Example of a phishing email sent by the Dukes

Once opened in a browser, the HTML file automatically triggers what seems like the download of an ISO disk image file. In order to succeed, the intended victim must choose either to save this file and subsequently open it, or to open it directly. If either is chosen, a small piece of JavaScript decodes the ISO file, which is embedded directly in the HTML attachment. It is not downloaded from the internet.



Fake download popup window triggered by opening the HTML attachment in the phishing email

In this ISO disk image, we find a single file named `Covid.hta`. HTA (HTML Application) is a Microsoft Windows file format that can contain HTML and scripts such as JavaScript or VBScript. Such files are executed by the `mshta.exe` program. In this case, `Covid.hta` contains JavaScript code that will in turn execute a PowerShell script.

```
<body onload="start()">
    <div id="c1" style="visibility: hidden;">powers</div>
    <div>
        <p>Due to the increase in the number of cases of COVID-19, the Embassy of the Islamic Republic of Iran is being transfered to a
        state of isolation. Access to the embassy territory is temporarily closed to visitors.</p>
    </div>


    <div>
        <p>
            If you have been in contact with the embassy staff during the last weeks, please reply by return letter to receive detailed
            information about the status of the illness of thes employee.
        </p>
    </div>


    <div id="c2" style="visibility: hidden;">hell -C Invo</div>
    <div id="c3" style="visibility: hidden;">ke-Expression (g</div>
    <div id="c4" style="visibility: hidden;">p HKCU:\\SO</div>
    <div id="c5" style="visibility: hidden;">FTWARE\\JavaSoft).Ver</div>
```

Code inside `Covid.hta`

This PowerShell script loads a DLL into memory that then loads a Cobalt Strike beacon. This is a commercial Red Team implant, but it is also the backdoor of choice for the Dukes and multiple other threat actors.

Variants of the compromise chain

The compromise chain is very click intensive as a typical target would have to click at least four times after opening the email before being compromised. So why bother with HTML and ISO disk images? It's all about evasion.

An ISO disk image doesn't propagate the so-called *Mark of the Web* [43] to the files inside the disk image. As such, and even if the ISO were downloaded from the internet, no warning would be displayed to the victim when the HTA is opened. Similarly, on one occasion, the threat actor embedded a VHDX file (the file format used by Microsoft for virtual disk images) in the HTML instead of an ISO. It has the same properties in terms of evading the Mark of the Web.

The malicious disk images don't always contain an HTA. They sometimes contain a LNK and a DLL, which can be either a Cobalt Strike downloader or loader. This shows that attackers are experimenting and trying several avenues, probably in order to maximize the compromise rate.

What's next?

Once attackers have a foothold on the machine, they usually deploy additional tools to gather information about the host system or other machines in the same network. These include:

- *AdFind* [44] – A tool to query the Active Directory
- *BloodHound* [45] – A tool to graph Active Directory relationships
- *Sharp-SMBExec* [46] – A tool to execute a command on a remote machine using SMB
- *SharpView* [47] – A tool to perform recon on a Windows machine
- *Rubeus* [48] – A tool to interact with Kerberos
- An exploit for *CVE-2021-36934* [49] – a local privilege escalation vulnerability
- The Cobalt Strike Port Scanner

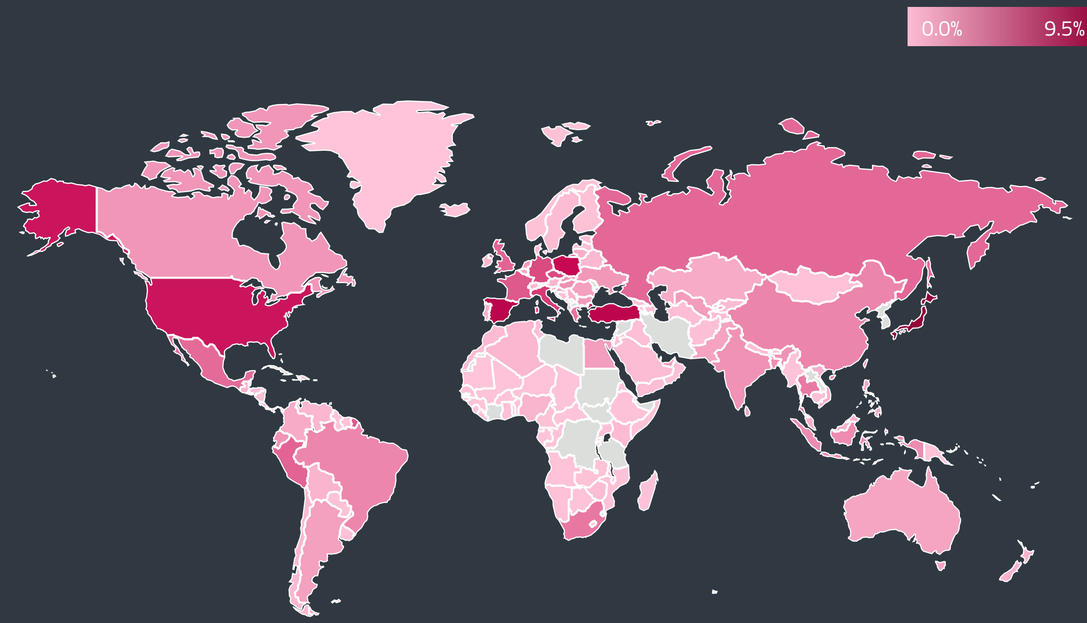
They also usually deploy additional Cobalt Strike loaders (DLL- or PowerShell-based) that would load SMB beacons. These can be used to control machines in the same network that are not directly connected to the internet.

Recent months have shown that the Dukes are a serious threat to western organizations, especially in the diplomatic sector. They are very persistent, have good operational security, and they know how to create convincing phishing messages. ESET researchers expect to continue to see them targeting European diplomats in the next months, with ever-evolving techniques.

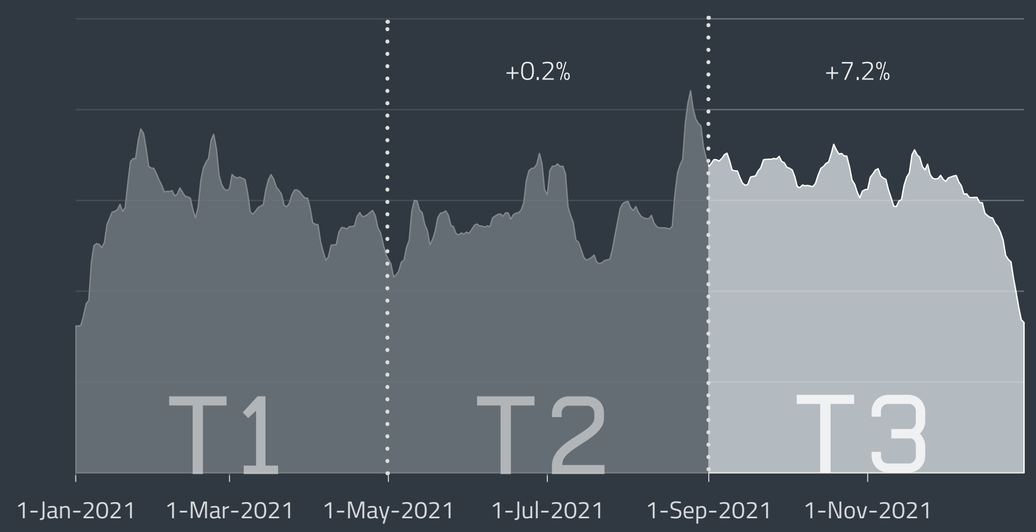
Indicators of Compromise (IoCs) [28]

STATISTICS & TRENDS

The threat landscape in T3 2021 and 2021 as seen by ESET telemetry



Global distribution of malware detections in T3 2021



Overall threat detection trend in 2021, seven-day moving average

THREAT LANDSCAPE OVERVIEW

A summary of the threat landscape developments in T3 2021.

Despite trending downward, the number of all threat detections increased by 7.2% in T3 compared to T2 2021. There were no major spikes in the overall threat detections, but there were certainly many major developments in the threat landscape.

Let's start with some good news: several ***Ransomware*** operators were arrested in T3 2021. Unfortunately, this is where the good news ends – T3 saw the highest ransom ultimatum yet when the Hive gang demanded USD 240 million in the MediaMarkt incident.

Ransomware also played a significant part in the ***Android*** category – it increased by 114%, the most out of all Android threat subcategories. However, looking at yearly data, Android ransomware's growth was far outdone by Android banking malware, which demonstrated a staggering 428% boom in detections between 2020 and 2021.

Infostealers decreased in number but not in threat level, particularly with TrickBot setting the stage for the return of Emotet. Indeed, looking over at the ***Downloaders*** category, we can see that Emotet came back from the dead, and with an improved binary and modules, too. Based on ESET telemetry data, this botnet was waging several campaigns in November and December.

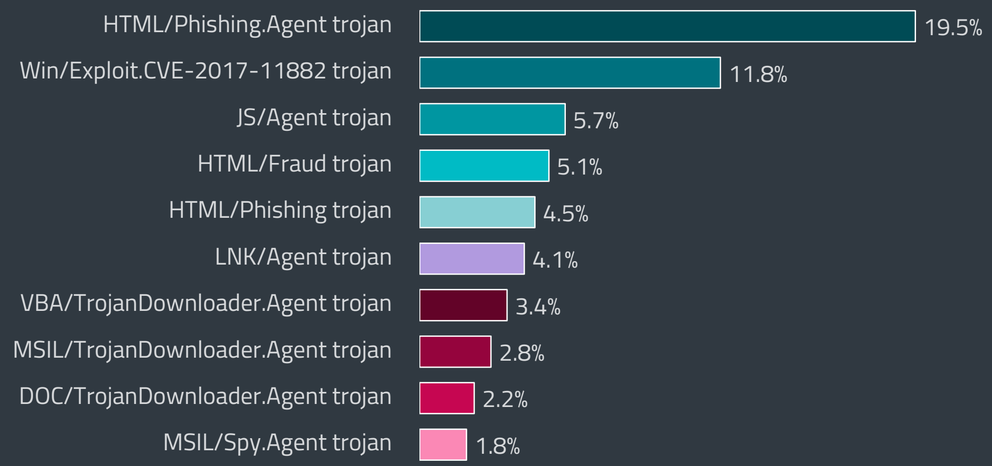
Meanwhile, the bitcoin exchange rate reached its highest point so far in November 2021, which increased the popularity of mining, alongside the rates of PUA and desktop ***Cryptocurrency threat*** detections. It also affected the category of ***Web threats***, boosting the number of phishing websites impersonating cryptocurrency platforms.

The ***Exploits*** category once again brought out the big scary numbers, with RDP attacks jumping from 55 to 206 billion between T2 and T3, and increasing by 897% from 2020 to 2021. In the ***IoT*** category, the ZHtrap botnet started spreading malware from ten payload servers on December 24, resulting in 97,000 attack attempts that targeted mostly D-Link routers.

Email threats continued to grow, driven by phishing emails and maliciously crafted documents using a publicly available exploit (Win/Exploit.CVE-2017-11882).

Lastly, while the overall number of ***macOS detections*** went down in T3, over a third of these detections were trojans, the rate of which increased by 126% from 2020 to 2021.

There were no significant changes in the list of top 10 malware detections, apart from the DOC/Fraud trojan dropping out of the top 10 to twelfth place, and MSIL/Trojan.Downloader.Agent trojan making a comeback, going from fifteenth to eighth place.



Top 10 malware detections in T3 2021 (% of malware detections)

TOP 10 MALWARE DETECTIONS

→ HTML/Phishing.Agent trojan

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

↗ Win/Exploit.CVE-2017-11882 trojan

This detection name stands for specially crafted documents exploiting the *CVE-2017-11882* [50] vulnerability found in 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.

↗ 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.

↗ 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 HMTL-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* [51], such as the notorious Nigerian Prince scam also known as "419 scam".

↘ HTML/Phishing trojan

HTML/Phishing trojan represents generic malware detections that are collected based on scanning malicious URLs in emails and email attachments. If an email or its attachment contains a blacklisted URL, it triggers an HTML/Phishing.Gen detection.

↗ 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 popular among attackers, as they are typically considered benign and less likely to raise suspicion. LNK/Agent files don't contain any payload and are usually parts of other, more complex malware. They are often used to achieve persistence of the main malicious files on the system or as a part of the compromise vector.

↗ VBA/TrojanDownloader.Agent trojan

VBA/TrojanDownloader.Agent is a detection typically covering maliciously crafted Microsoft Office files that try to manipulate users into enabling the execution of 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.

↗ MSIL/TrojanDownloader.Agent trojan

MSIL/TrojanDownloader.Agent is a detection name for malicious software written for the Windows platform, and that uses the .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.

↗ 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.

↘ 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.

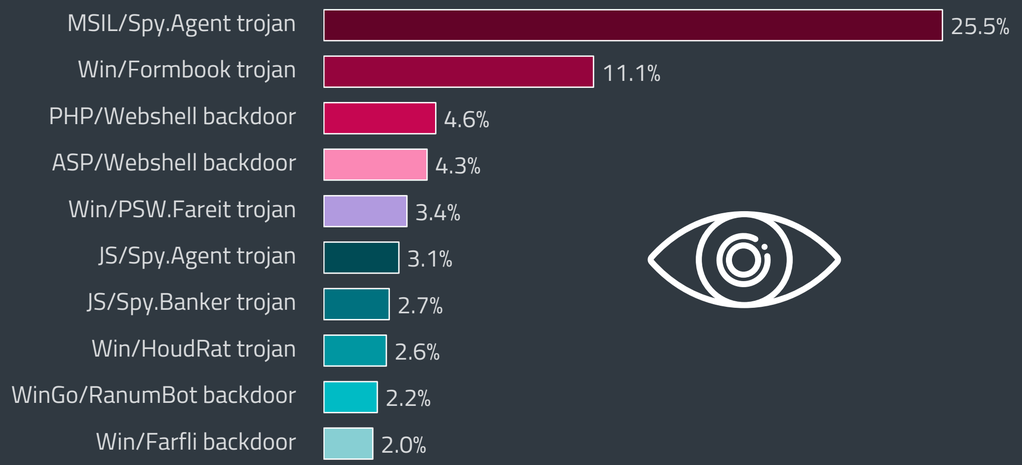
INFOSTEALERS

Banking malware is on the rise, and ESET researchers discover a rare UEFI bootkit in the wild.

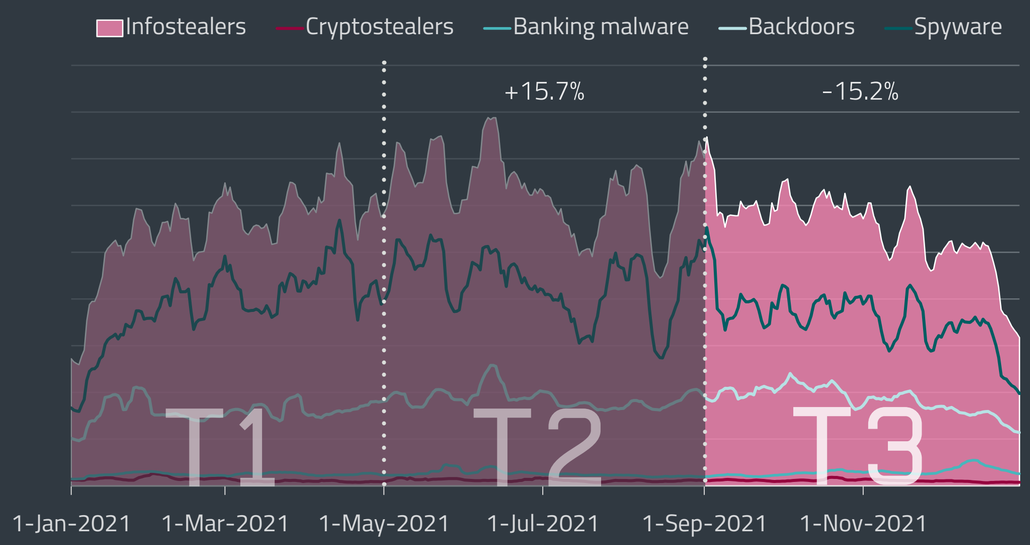
The upward trend in Infostealer detections was reversed in T3 2021, when the category experienced a decrease of 15.2%. Apart from Banking malware, all of the subcategories were in decline. The most significant decrease was registered at the end of the year, which is usually a quieter period both for businesses and for threat actors.

ESET telemetry did not register any major Infostealer spikes, only two smaller ones in the Czech Republic, the first on September 2, and the second on November 18. Both were caused by campaigns of Agent Tesla, the notorious MSIL/Spy.Agent trojan variant. This commonly used malware-as-a-service remote access trojan (RAT) is often spread through phishing emails, frequently abusing legitimate email addresses to which it had gained access during previous attacks.

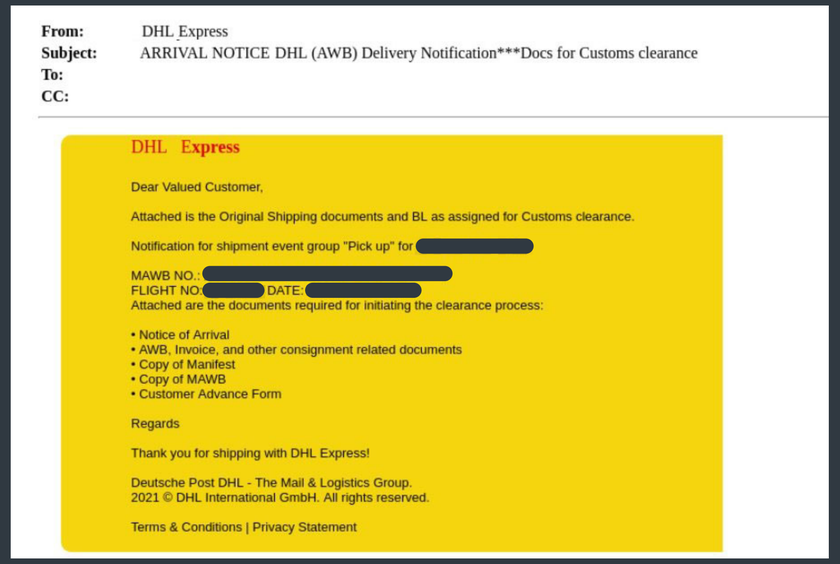
MSIL/Spy.Agent trojan also dominated the top infostealer detections, accounting for 25.5% in T3 2021, with double the number of total detections compared to the second place Win/Formbook trojan. Third place went to the backdoor PHP/Webshell. The top detected families in T3 belonged to Spyware, Backdoor and Banking malware subcategories.



Top 10 infostealer families in T3 2021 (% of infostealer detections)



Infostealer detection trend in 2021, seven-day moving average



From: DHL Express
Subject: ARRIVAL NOTICE DHL (AWB) Delivery Notification***Docs for Customs clearance
To:
CC:

DHL Express

Dear Valued Customer,

Attached is the Original Shipping documents and BL as assigned for Customs clearance.

Notification for shipment event group "Pick up" for [redacted]

MAWB NO.: [redacted]
FLIGHT NO: [redacted] DATE: [redacted]
Attached are the documents required for initiating the clearance process:

- Notice of Arrival
- AWB, Invoice, and other consignment related documents
- Copy of Manifest
- Copy of MAWB
- Customer Advance Form

Regards

Thank you for shipping with DHL Express!

Deutsche Post DHL - The Mail & Logistics Group.
2021 © DHL International GmbH. All rights reserved.

Terms & Conditions | Privacy Statement

Example of an Agent Tesla spam email

Not much changes when looking at the data for the whole year, where MSIL/Spy.Agent trojan remained first with 23.8%, followed, again, by Win/Formbook trojan with 13.2%. The only difference is that third place went to Win/PSW.Fareit trojan, with 5.7%.

Looking at Infostealer subcategories, the most prevalent one thus far always has been Spyware. This did not change in T3 2021, even though the detections in this subcategory went down by almost 21%. It was, after all, the Agent Tesla RAT that was behind the spikes in Infostealers as a whole. Spyware activity was mainly seen in Spain, which registered almost 8% of spyware detections, followed closely by Japan's 7.7% and Turkey's 6.3%.

The top three Spyware positions remained the same in T3 compared to T2. MSIL/Spy.Agent trojan, the family that contains Agent Tesla, was the most-detected spyware with 39.4% and active mainly in Japan. It was followed by Win/Formbook trojan with 17.2% and Win/PSW.Fareit trojan with 9.6%, both of which had the most of their attack attempts in Spain.

Unlike Spyware, the second strongest Infostealer subcategory of Backdoors did not really decline drastically, so much as stagnate. With only a slight 2.6% decrease, there were nevertheless some interesting developments here.

One of them was ESET researchers analyzing a previously undocumented UEFI bootkit that persists on the EFI System Partition (ESP) that they named *ESPecter* [6]. Compared to Serial Peripheral Interface (SPI) flash implant UEFI bootkits, such as *LoJax* [52], ESP threats are easier to deploy but are less persistent and do not survive full-disk formatting or replacement. Consequently, they have a higher compromise potential, while SPI flash implants are more suitable for advanced targeted attacks. ESPecter has backdoor functionality and is most likely used for espionage.

TRENDS & OUTLOOK

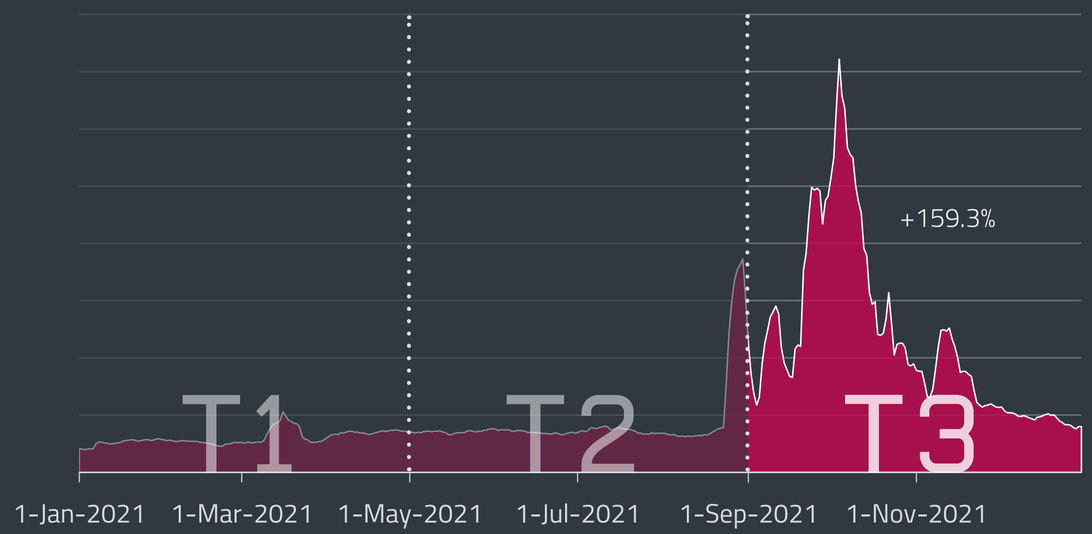
Although UEFI threats are very rare – only six real-world cases have been found in the wild – recent discoveries show they are certainly not going to disappear anytime soon. After all, three of the known six were discovered after September 2021. While we do not expect these threats to become widespread, we are sure that more of them will surface in the future.

UEFI threats are mostly a domain of APT groups, but due to the greater ease of deploying these bootkits on the ESP, we may soon see non-APT actors making use of them.

Martin Smolár, ESET Malware Researcher

Another noteworthy development regarding Backdoors is the dramatic rise of ASP/Webshell backdoor, which started the year in eighth place, moved to sixth in T2 2021 and ended up being the second most detected threat in this subcategory in T3 with 12.6%, its detections skyrocketing by almost 160% from T2. This backdoor, which executes commands from a C&C server, was also responsible for the biggest spike in backdoor detections in T3 2021, on September 21, when it was seen mainly in Germany. The rise in detections likely happened due to the attackers exploiting the *ProxyShell vulnerability* chain, a combination of three Microsoft Exchange Server vulnerabilities.

The major players from T2 2021, PHP/Webshell and WinGo/RanumBot, stayed among the most prevalent backdoor families in T3 – PHP/Webshell backdoor managed to keep its first place with 13.7%, and WinGo/RanumBot backdoor ended up third with 6.5% of detections.



ASP/Webshell detection trend 2021, seven-day moving average

In T3 2021, backdoors were mainly detected on client devices in the United States (7.1%), Turkey (4.6%), and Germany (4.3%).

The only Infostealer subcategory that trended upward in 2021 was Banking malware. In T3, it grew by 14.4%. Our telemetry saw a smaller spike in Banking malware activity on October 18 caused by the LT variant of MSIL/Clipbanker trojan, which was mainly active in Turkey on that day. Detections in this subcategory peaked on December 9 due to JS/Spy.Banker.KB, mainly registered in Poland.

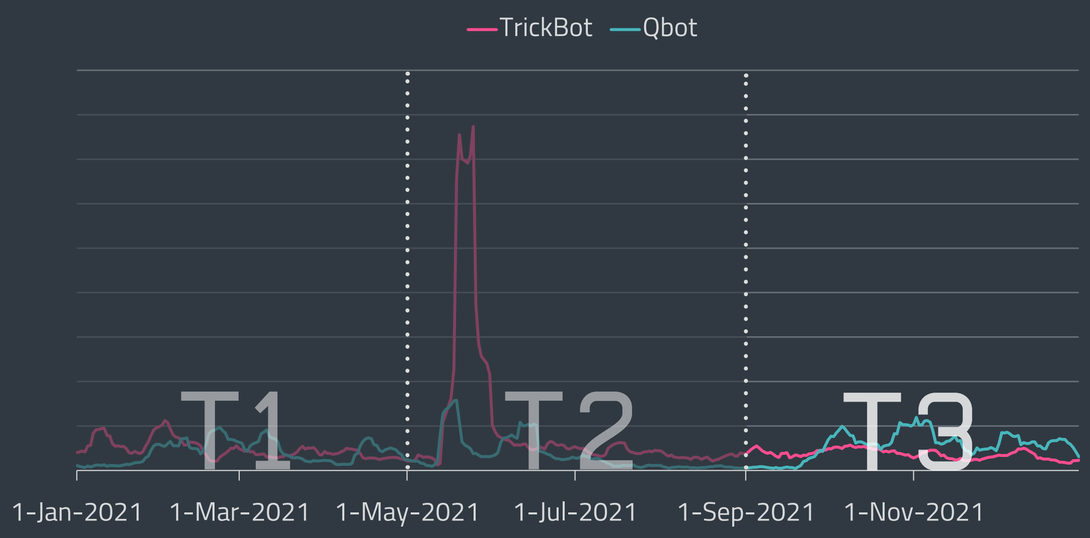
Same as in T2 2021, the top three banking malware detections went to JS/Spy.Banker with 48.8%, MSIL/Clipbanker with 19.4%, and Win/Clipbanker with 5.1%. These three malware families kept

the same positions throughout the year. Unlike T2, a banking malware family managed to get into the overall top 10 infostealer threats this time – JS/SpyBanker trojan placed eighth with 2.7% detections.

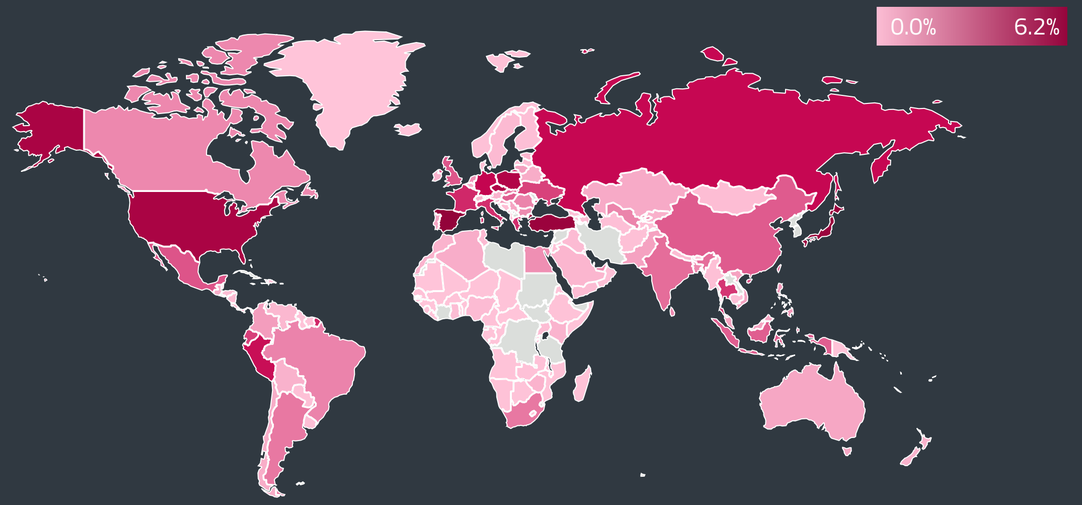
Latin American banking trojans harassed mainly Brazil in T3, but two of them, Grandoreiro and Mekotio, continued their forays into European waters. Grandoreiro even made them its main hunting grounds during this period – 45.2% of the malware's detections were registered in Spain, peaking on November 15. While most Mekotio detections were registered in Brazil (43.3%), Spain was its fourth most targeted country with 13.5%.

Qbot showed a 65.4% rise in detections in T3 and an overall upward trend during 2021. Toward the end of September, researchers at Trend Micro noted a *new campaign* [53] that distributed this malware using VBA macros in Microsoft Word documents. ESET telemetry registered Qbot mainly in the US, both in T3 (25.4%) and throughout the year (18.8%).

TrickBot detections, on the other hand, decreased by 62.4% in T3 2021. It should by no means be taken as a sign that this threat can be written off. Far from its humble banking trojan beginnings, TrickBot now often drops much more dangerous malware, frequently ransomware, on the compromised machine. Earlier in T3, it was seen aggressively *expanding its distribution network* [54], which later on made way for ransomware attacks. Many of these were carried out by Conti, which *partnered* [55] with the TrickBot gang and the Shatak group (TA551). Additionally, TrickBot was *setting the stage for the return of Emotet* [56]: while in the past, Emotet was used to drop TrickBot, now the threat actors are using TrickBot's infrastructure to rebuild the botnet. Like Qbot, TrickBot was seen mainly in the United States, which registered 22.4% of the T3 detections and 17.9% of the overall 2021 detections.



TrickBot and Qbot detection trends in 2021, seven-day moving average



Global distribution of infostealer detections in T3 2021

The United States also topped the T3 2021 banking malware detections with 10.1% of the attack attempts registered by ESET telemetry. Poland followed it with 8.1%, and then Brazil with 5.2%.

Cryptostealers, the smallest Infostealer subcategory detection-wise, were on a downward trend the whole year, going down by 8.4% between T2 and T3 2021. More detailed information on cryptostealers can be found in the *Cryptocurrency threats* section.

In T3, the category of Infostealers as a whole was most prevalent in Spain with 6.2%, and in Japan and Turkey, both with 5.7%. The top three countries are the same when it comes to the yearly statistic, Spain being affected by 7.8% of infostealer attack attempts, Turkey by 6.6%, and Japan by 5.5%.

RANSOMWARE

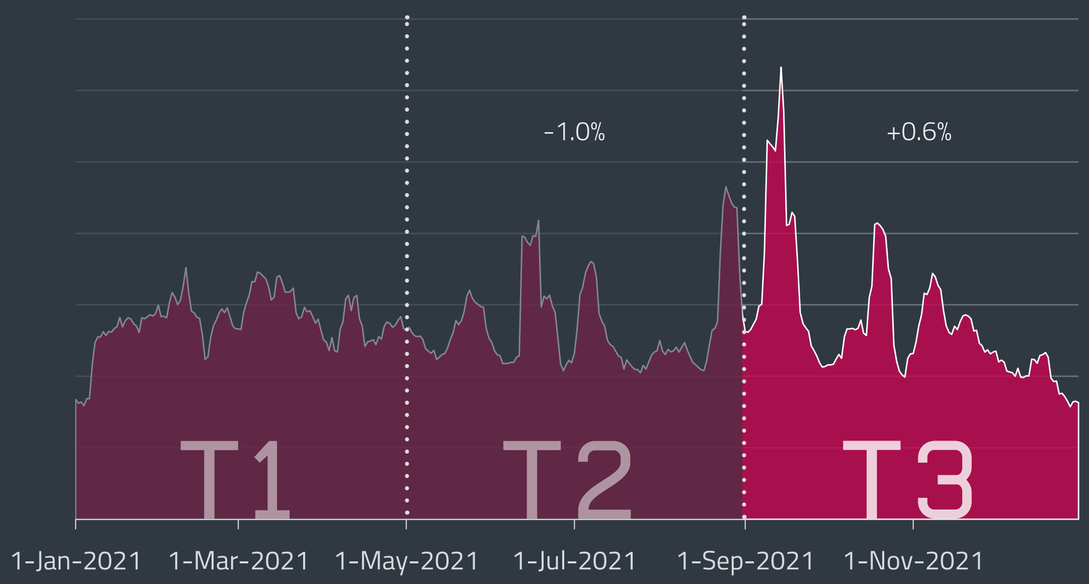
While more ransomware operators are arrested than ever before, over USD 5 billion bitcoin transactions are tied to potential ransomware payments.

According to ESET telemetry, ransomware detection numbers remained steady between T2 and T3 2021, increasing only 1%. However, the overall image of stability hides quite a busy period with several noteworthy peaks.

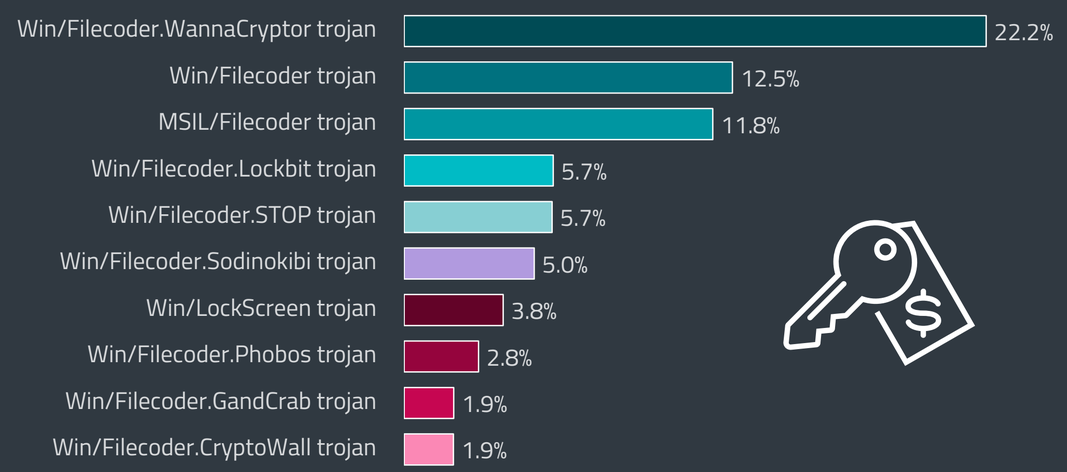
The first and the biggest spike occurred at the beginning of T3 2021, on September 9. A well-known ransomware family Win/Filecoder.Sodinokibi (aka REvil) accounted for 73% of detections that day, hitting South Africa (SA) the hardest – only days before the *SA Department of Justice* [57] compromise.

The next peak followed on September 14, 66% of it caused by MSIL/Filecoder.FU – a fork of the HiddenTear ransomware. To distribute their malware, operators chose spam and filled mainly French inboxes. Although based on the HiddenTear ransomware source code from GitHub, Filecoder.FU uses a different set of parameters and bitcoin address, and attempts to avoid detection by adding obfuscation. Still, there is a chance of recovery using the readily available *HiddenTear decryptor* [58].

The third uptick in ESET telemetry occurred on October 16, led by Win/Filecoder.Lockbit. This malware family accounted for 70% of all detections that day, mostly targeting machines in Honduras.



Ransomware detection trend in 2021, seven-day moving average



Top 10 ransomware families in T3 2021 (% of ransomware detections)

Last but not least, on December 14, ESET spotted a campaign by a *new ransomware family* [59] named Rook. It is based on the leaked code of now-defunct *Babuk* [60] ransomware and uses Sodinokibi's ransom note. On December 14, Rook accounted for over 23% of detections and spread exclusively in the United States.

It is important to note that the detection chart on the left only includes cases where ESET blocked ransomware per se. Attacks detected at an earlier stage – for example, as an RDP brute-force attack, as exploitation of a vulnerability, as malspam or as an attack of a dropper, downloader or infostealer – are not part of these statistics.

The ransomware top 10 represents a mix of old ransomware "worms" that lurk in the wild and somehow still manage to find new targets – WannaCryptor, GandCrab, CryptoWall – malware families used by the big-game hunting gangs – Sodinokibi, Phobos or Lockbit – and smaller families that find their victims via emails or malicious links – such as the already mentioned MSIL/Filecoder.FU.

Rook ransomware leak page with its "specific" artwork

Compared to T2 2021, the Conti and Buran families have been pushed out of the top 10. Still, their attacks are often targeted and use attack vectors described in other sections, including *Exploits*, *Infostealers*, *Email threats* and *Downloaders*.

One of the main trends seen in the last four months of 2021 was the feverish law enforcement activity against ransomware, with agencies offering millions in *rewards* [61] for information and finalizing operations across the globe.

In several busts, police agents handcuffed *two affiliates* [62] and later *five affiliates* [63] of Sodinokibi in Ukraine, Romania and Kuwait, including the person alleged to be responsible for the Kaseya attack. Another law enforcement operation led to the arrest of six members of the *Cl0p* [64] gang, known for the attack against *Accellion* [65] and hits on companies in South Korea and the US.

A dozen individuals ended up in police custody in connection with the *LockerGoga, MegaCortex and Dharma* [66] ransomware attacks, which compromised critical infrastructure organizations such as Altran Technologies and Norsk Hydro.

Yet, the biggest story concerning police activity came shortly after T3 2021 had ended, on January 14, 2022. After being tipped off by the US authorities, Russian agents raided locations around Russia, arresting more than a dozen members of probably the most notorious ransomware gang today – *Sodinokibi* [67].

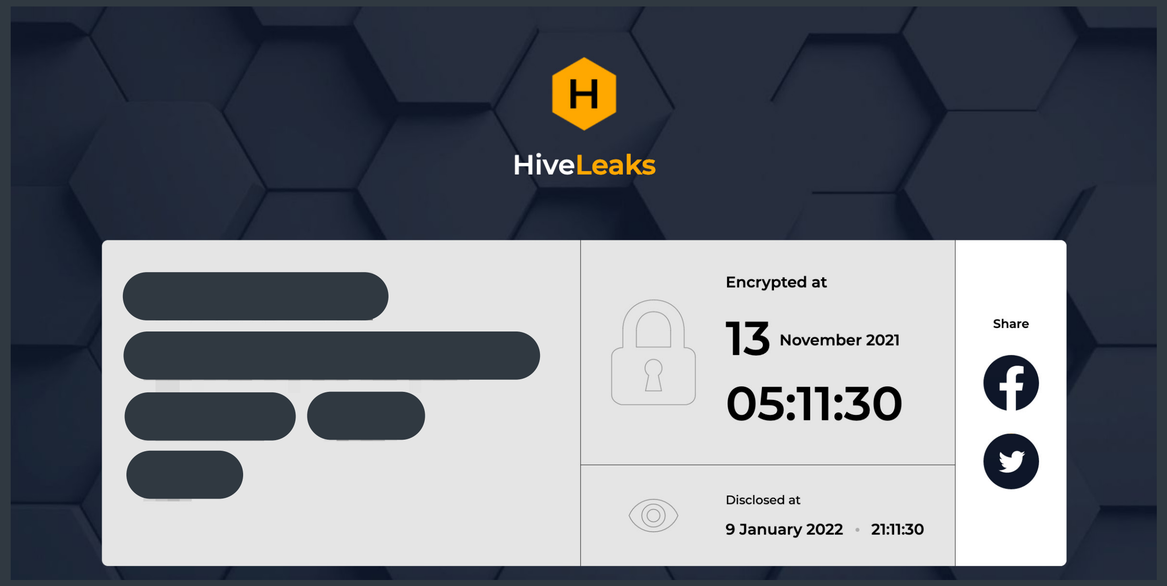
Most police operations also led to the seizure of hardware containing key data and cryptocurrencies, cash, luxury cars, and valuable goods worth tens of millions of US dollars.

The damaging activity of ransomware in 2021 created new international bonds and agreements. One that made the headlines was the special meeting organized by the White House, *uniting 30 nations* [68] in the fight yet keeping Russia out. Also, a new US law was proposed – *The Ransom Disclosure Act* [69] – aiming to tighten the rules for ransomware victims, requiring them to provide the government with payment information within 48 hours of the transaction.

A sigh of relief could almost be heard as several decryptors were released throughout T3 2021. Recovery tools were released for: a number of *Sodinokibi victims* [70]; those attacked by *BlackByte* [71] ransomware; for organizations compromised by *AtomSilo, Babuk and LockFile* [72] and quiet help was offered to *victims of BlackMatter* [73] – a rebrand of the Darkside family. *AvosLocker gang* [74] provided decryption keys itself but only for a case where they hit systems of a US police department.

Despite the growing pressure on cybercrime, T3 2021 saw quite a few new players trying to make a name for themselves. The list includes *AtomSilo* [75], *Yanluowang* [76], the already mentioned Babuk spin-off named Rook, and *Macaw locker* [77] by Evil Corp. One memorable rebrand changed what was known as Nemty, Nefilim, or Gangbang to *Karma* [78].

One ransomware family that appeared back in June 2021 but made the headlines in T3 2021 was *Hive ransomware* [79]. In the first four months of its activity, the gang compromised systems of more than



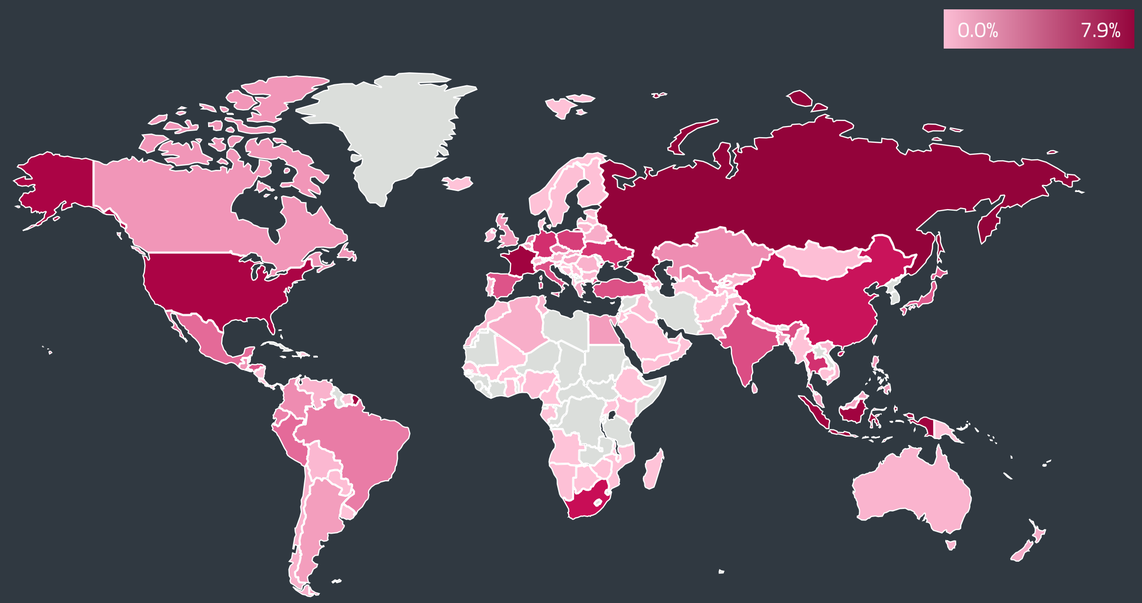
TOR landing page used by Hive ransomware

350 organizations. One of them – a leading EU electronics retailer *MediaMarkt* [80] – was asked to pay an outrageous USD 240 million ransom.

Other high-profile victims in T3 2021 were US farming cooperatives *Crystal Valley* [81] and *New Cooperative Inc.* [82], leading wind turbine manufacturer *Vestas Wind Systems* [83], electronics company *JVCKENWOOD* [84], medical company *Olympus* [85], and the US *National Rifle Association (NRA)* [86] – a target of Evil Corp's Grief ransomware.

As seen since the beginning of the pandemic, ransomware gangs are closely following information about recently published critical vulnerabilities and trying to leverage them for their purposes. In T3 2021, this was mostly represented by attempts to compromise victims via the Log4j vulnerability. The first ransomware family abusing the flaw days after its publication was a newcomer named *Khonsari* [87]. Soon it was followed by the *Conti* [88] gang, the revived *TellYouThePass* [89] ransomware and other cybercriminals and APT actors.

Apart from Log4j, the *Serv-U flaw* [90] in SolarWinds, and *ProxyShell* [91] in MS Exchange servers were abused to hack into unpatched systems in T3 2021, the former by Cl0p and the latter by Conti.



Global distribution of ransomware detections in T3 2021

Regarding the financial aspect of ransomware, the US Financial Crimes Enforcement Network published a *report* [92] summarizing 635 incidents (+30% YoY), pointing to USD 590 million in suspicious activities (+42% YoY). Further analysis of 177 unique crypto wallet addresses associated with the ten most prevalent ransomware variants showed USD 5.2 billion in outgoing bitcoin transactions probably tied to ransomware payments.

Crowdsourced data accumulated by the *Ransomwhe.re* [93] service showed USD 44.5 million tracked ransomware payments in 2021, with 93% of the funds ending in the pockets of the Conti, Sodinokibi, Darkside, and BlackMatter gangs.

In T3 2021, a *lawsuit* [94] was filed in connection with a *baby's death* [95], which according to the parents, didn't receive necessary health care after the hospital suffered a ransomware attack – allegations denied by the facility. It is the second incident – after the one in *2020 in Germany* [96] – where a ransomware attack has been named one of the possible causes contributing to the death of a patient.

TRENDS & OUTLOOK

Christmastime typically brings increased malware and ransomware activity. 2021 was no exception. Most of the new families we've seen pop up on our radar in the last months of the year were amateurish newcomers or well-known players trying to make a comeback, either using their former name or under a new "brand". As in previous years, we expect this activity to fade out in January and February 2022.

We must add that even new families with an amateurish feel seem to have done their homework and implemented the cryptography correctly. In other words, the chance to decrypt the victim's data is gradually becoming lower and lower.

In 2022, we expect ransomware to continue to encrypt and steal victim's data, when targeting the "big game" – large global corporations with the potential for a sizable ransom payment. While targeted attacks were the most common in 2021, mass campaigns didn't completely die out either, as illustrated by malspam waves such as the one seen in T3.

What changed in 2021 was the successful pursuit of cybercriminals by law enforcement agencies. Numerous international operations showed that agents were closely following activities of ransomware gangs and whenever their core member or their affiliates made a mistake, the police were right there to make the bust. We presume this activity will continue in 2022 and bring even more arrests and releases of decryption keys.

Igor Kabina, ESET Senior Detection Engineer

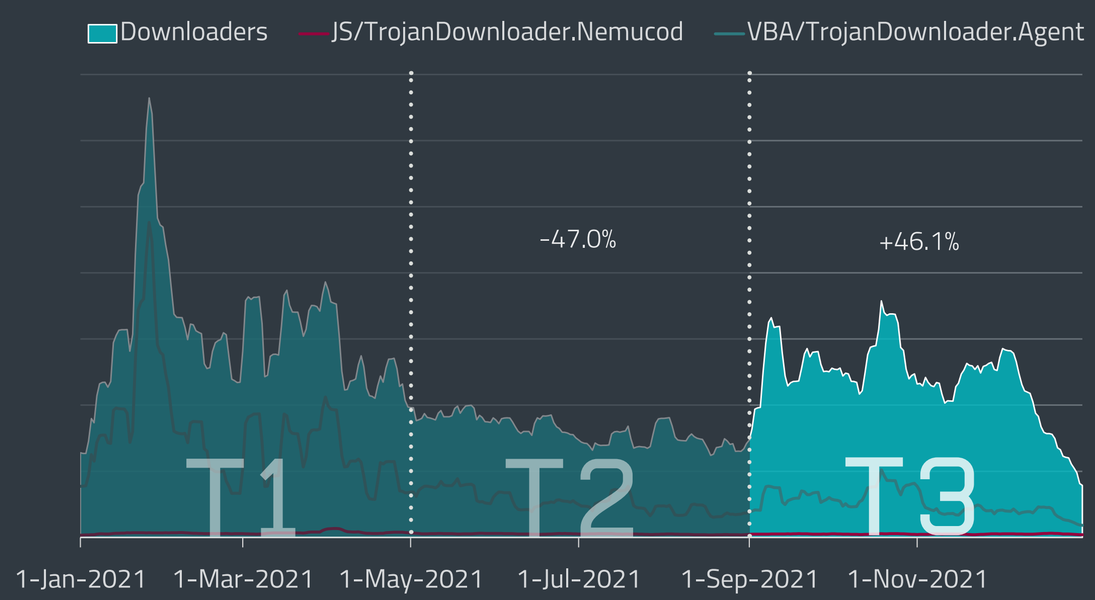
DOWNLOADERS

Emotet returns with Trickbot's help; MSIL downloaders surge in T3 2021.

T3 2021 was a comeback period with regards to the Downloaders category. Probably the most vivid example was Emotet reviving its activities after the January takedown. Its return was *allegedly* [97] sparked by the demand of the Conti ransomware gang and was engineered with support from Trickbot. After a calm T2 2021, the overall detection numbers of downloaders surged in T3 2021, growing by 46%, mostly due to spikes of several MSIL variants.

Downloaders had a strong beginning in 2021. At one point a large spike in detections of these threats even surpassed 100,000 per day and it seemed that the whole category was on its way to reaching new heights. However, at the end of January, law enforcement took down the Emotet botnet. This one action cut off a big chunk of malicious activity in this area and after the mass uninstallation of Emotet in April, the numbers for the Downloaders category dropped by 47%. It took several months for it to regain its footing.

Although Downloader detections started growing again in September, the real bad news hit on November 16. *Emotet research group* [56] reported that the "most dangerous malware" was back and trying to build its botnet, again with support from Trickbot.



Downloader detection trend in 2021, seven-day moving average

ESET telemetry documented the *campaign* [98] with detections from 80 countries. After the initial spike, an even larger one followed between December 6 and December 10, mostly targeting Japan, Spain, and Italy. According to ESET telemetry, the last 2021 uptick in Emotet's activity occurred around Christmas Eve but left a smaller detection footprint due to the low number of active users.

To find out what changed since the Emotet takedown, ESET researchers *dissected* [99] its new binary, uncovering several updates including a new command, a new module designed to extract the process list, and two new modules made to steal information and contacts from the Thunderbird email client.

In December, *Cryptolaemus* [100] reported that Emotet's operators adjusted the pre-takedown compromise chain by skipping one step. Before the law enforcement action, the botnet usually

TRENDS & OUTLOOK

Looking back at 2021, it was a quiet year for the Downloaders category due to the Emotet takedown. Since then, we were expecting that this malware would reappear, as the authorities only arrested admins of the botnet infrastructure but not the true masterminds behind the malicious operation.

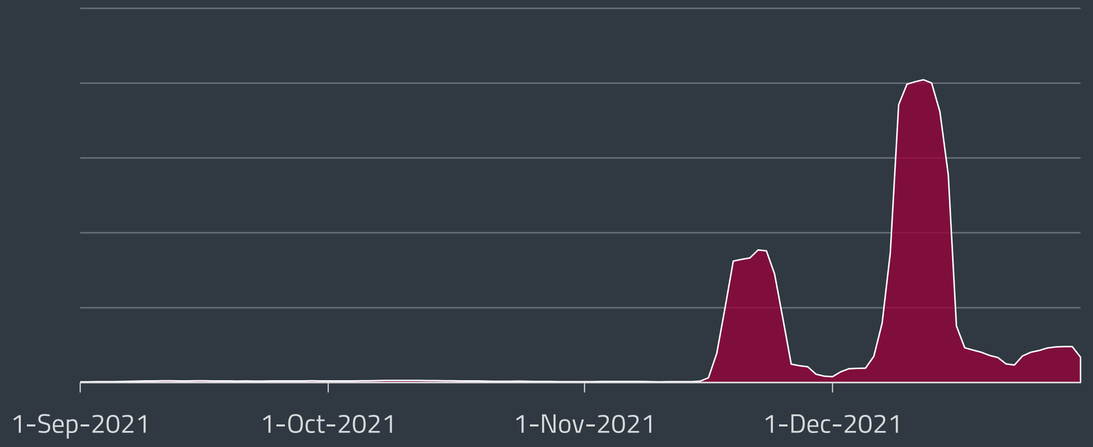
What was surprising to us was the relatively short time creators needed to orchestrate the comeback and even to upgrade their "product". Since the takedown, Emotet authors invested a lot of energy into improving the binary and modules and even added new modules targeting the Thunderbird mail client.

In 2022, we expect Emotet and its botnet to expand rapidly and return to a leading position among downloader families. The main reasons are high-quality malspam based on or abusing genuine email messages and distributing them to potential victims via hijacked, legitimate email accounts.

In the upcoming year, Emotet will probably aim to rebuild its former infrastructure of three separate botnets known as Epochs. It will also offer its services to other cybercrime groups. If we had to guess the primary clients, the list would surely include Emotet's partners in crime Trickbot and Qbot, as well as banking malware and ransomware gangs.

Lastly, the use of the Cobalt Strike beacon suggests that Emotet's operators are seeking to diversify their portfolio and might want to try their luck as one of the big-game hunting ransomware operators.

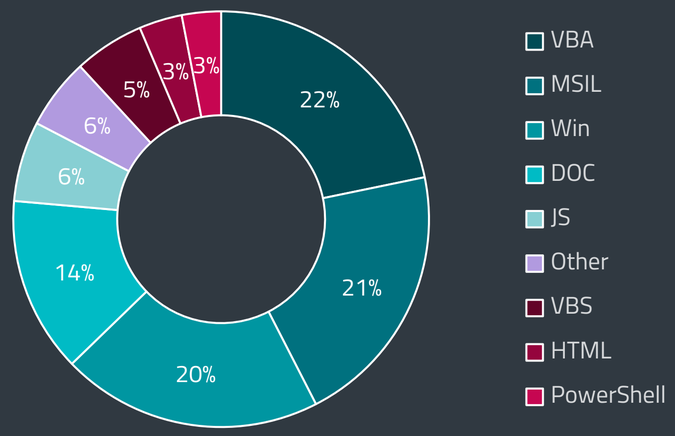
Zoltán Rusnák, ESET Malware Researcher



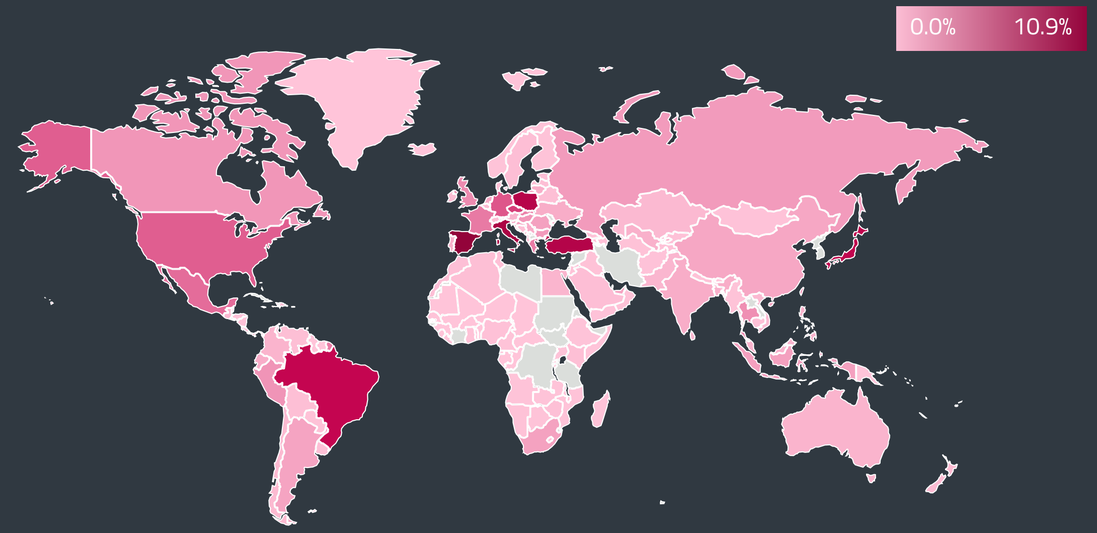
Emotet detection trend in T3 2021, seven-day moving average

downloaded Trickbot or Qbot as its initial payload and left the further attack and download of the final payload to them. After its resurgence, in T3 2021, it switched those malware families for a *Cobalt Strike* [101] beacon. This otherwise legitimate pentesting tool gives the attacker direct access to the victim's environment and can thus potentially shorten the time between Emotet's initial compromise and deployment of its typical final payload – ransomware.

T3 2021 brought four notable spikes in the Downloaders category – on September 9, September 20, October 19, and December 1. The initial three of these upticks were either driven or fueled to a major degree by VBA/TrojanDownloader.Agent, a detection name representing malicious macros written in Visual Basic for Applications (VBA).



Downloader detections per detection type in T3 2021



Global distribution of downloader detections in T3 2021

Despite VBA/TrojanDownloader.Agent detections playing a major role in the spikes, it was far less prevalent in T3 2021 than in T2. This – previously leading – downloader detection type dropped by 11 percentage points (pp) in the last four months and accounted for "only" 22% of all hits in this category.

However, the spike in December had a different culprit – MSIL/TrojanDownloader.Agent. Accounting for over a fifth of downloader detections (21%), this threat grew by 12 pp between T2 and T3 2021. The most active variants were MSIL/TrojanDownloader.Agent.IYB, IUU, and JEG – all distributed via email, downloading two binaries: a payload in the form of an EXE file, and a DLL tool used to execute it. Final payloads included Agent Tesla, Fareit, and MSIL/Agent.CFQ trojan.

In a geographical sense, threats from the Downloaders category mostly focused on potential victims in Spain (9.4%), Italy (8.6%), Japan (8.2%), Poland (6.7%), and Turkey (6.1%).

In October, ESET researchers also published their research on *Wslink* [7], a unique and previously undescribed loader for Windows binaries that runs as a server and executes received modules in memory. The initial compromise vector is currently unknown, yet our researchers were able to analyze Wslink's behavior by creating our own experimental implementation of this malware's client.

T3 2021 also saw news on new custom *Ceeloader* [102] malware used by the Dukes, a threat actor infamous for its supply-chain attack against SolarWinds. Discovered by Mandiant, Ceeloader is a new downloader that enables the attackers to execute shellcode payloads in memory, using heavy obfuscation and several other methods to fly under the radar of security solutions.

CRYPTOCURRENCY THREATS

Cryptominer activity continues to correlate with cryptocurrency exchange rates.

After their decrease in T2, the number of cryptocurrency threat detections grew in T3 2021. Over T1 and T2 2021, the picture painted by the cryptocurrency threat landscape was as dramatic as the situation on the cryptocurrency exchange market, with its peaks and valleys closely following those of the bitcoin and Ethereum exchange rates.

This mostly continued in T3. Near the end of September, the cryptocurrency sphere was hit by further government regulations in China, which ***banned all cryptocurrency-related transactions*** [103]. That news was followed both by a drop in the value of several cryptocoins, and by a significant decrease in the daily detection count of cryptocurrency threats. The volatile cryptocurrency market soon found itself on the upswing though, as both bitcoin and Ethereum reached their all-time highs in November: bitcoin traded for almost USD 69,000 per BTC, and Ethereum's price edged close to USD 4,900.

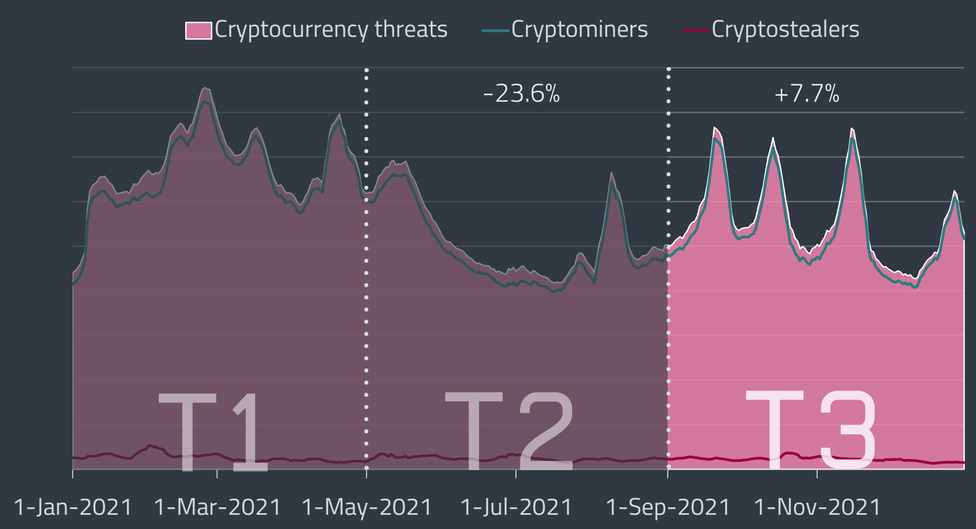
Even with the record exchange rates and the increase from T2 to T3, Cryptocurrency threat detections still showed an overall downward trend in 2021, seeing their highest numbers in February.

In T3 2021, Coinminers managed to grow by 8.4%, peaking on September 20, a few days before the trading ban in China. This detection peak was caused by the potentially unwanted application (PUA) Win/CoinMiner via its RH variant, which was primarily detected in the United States. Coinminers showed additional spikes on October 11 and November 15, both also caused by the Win64/CoinMiner.RH PUA.

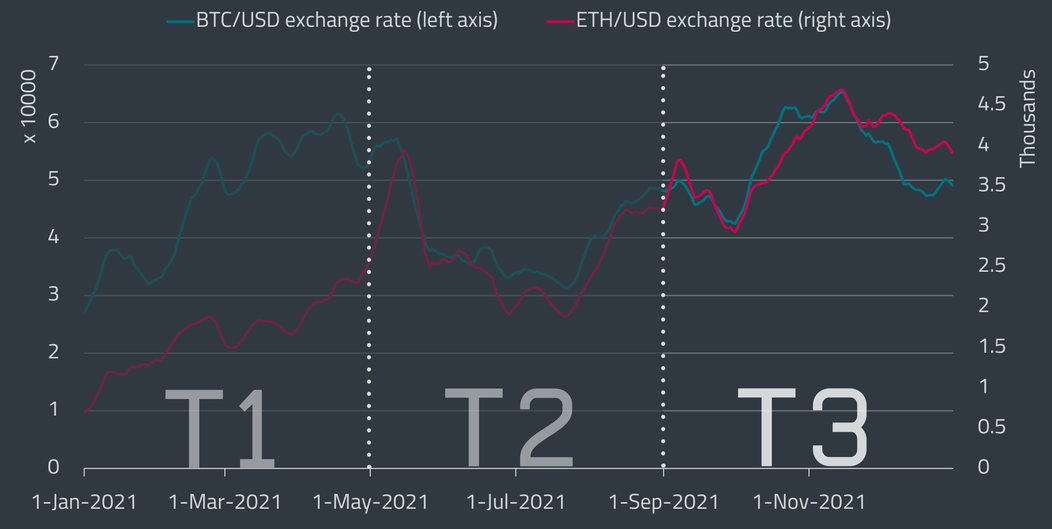
The Win/CoinMiner PUA family also continued its reign as the most detected cryptocurrency threat, with 57.9% of all cryptocurrency threat detections, and 60.3% of coinminer detections. ESET telemetry registered the highest activity of this family in Russia, followed by the United States. The second place in the top cryptocurrency threats went to Win/CoinMiner trojan and third to JS/CoinMiner PUA. The top three cryptocurrency threat malware families were the same in the overall 2021 statistics, showing that while the overall cryptocurrency threat detection numbers fluctuate, the key players are relatively secure in their positions.

Other aspects of this category that changed very little compared to T2 are the PUA:Trojan and desktop:in-browser ratios. It is a logical outcome of mining tools becoming commonplace in recent times, be they installed on purpose by the user or covertly bundled with some other software.

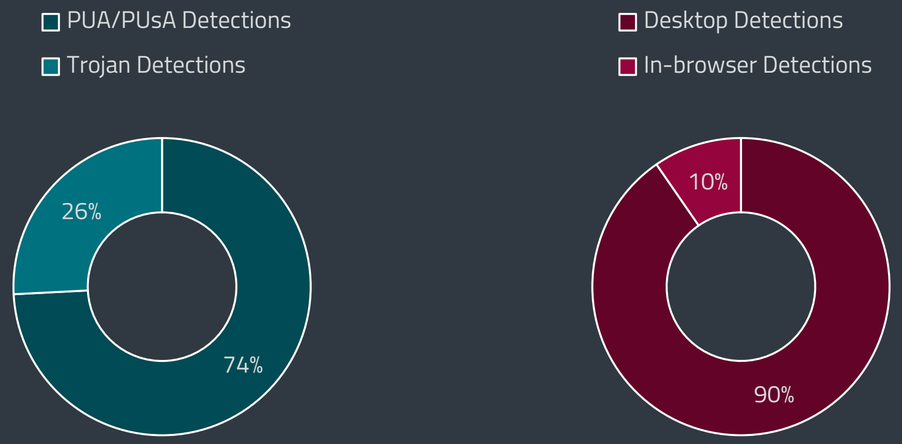
Interestingly, while the changes in these ratios are not exactly significant if we compare T3 to T2, taking a look at their evolution since the beginning of 2021 reveals that the percentage of both PUA



Cryptocurrency threat detection trend in 2021, seven-day moving average



Bitcoin and Ethereum/USD exchange rates in 2021, seven-day moving average



Trojan:PUA and desktop:in-browser ratio of cryptominer detections in T3 2021

and desktop detections is slowly increasing. The ratio of Trojan to PUA detections was 32% to 68% in T1, then 30% to 70% in T2, and lastly, 26% to 74% in T3 2021. Similarly, the desktop:in-browser ratio started at 87% to 13% in T1, was 88% to 12% in T2, and finally arrived at 90% to 10% in T3. It will be interesting to observe if this becomes an ongoing trend.

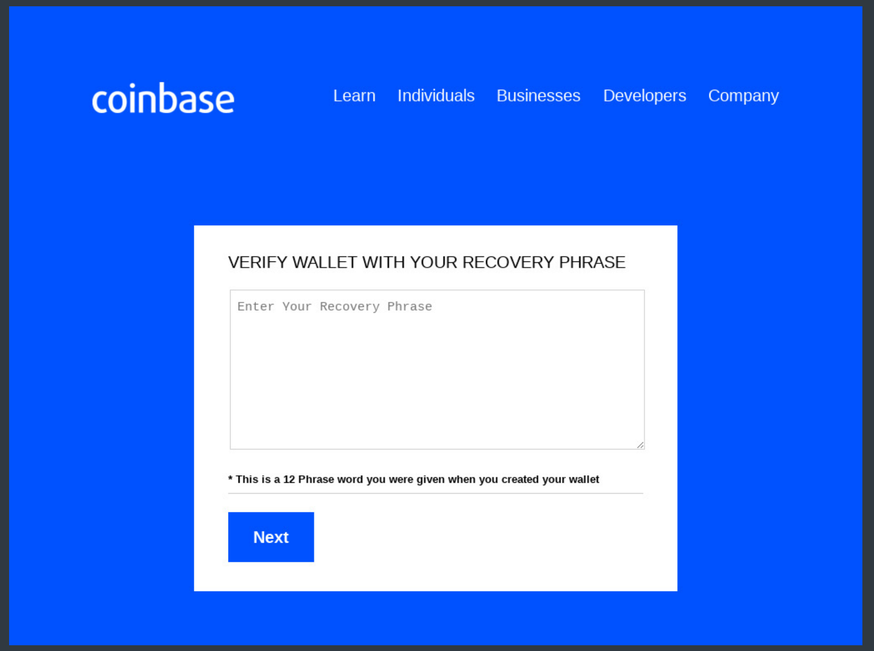
Even if in-browser detections made up only one-tenth of coinminers in ESET detection telemetry, there are still a considerable number of cryptojacking websites out there on the wild seas of the internet. These continue to be mostly torrent sites, free streaming websites, and sites with adult content.

	T3 2021	2021
1	dl-x[.]com	flashx[.]net
2	wypracowanie.edu[.]pl	dl-x[.]com
3	monerominer[.]rocks	newsoholic[.]com
4	carrierecalciatori[.]it	instagrammi[.]ru
5	instagrammi[.]ru	mituus[.]com
6	newsoholic[.]com	carrierecalciatori [.]it
7	mituus[.]com	monerominer[.]rocks
8	idaakulubu[.]com	comamosramen[.]com
9	cumpleañosdefamosos[.]com	wypracowanie.edu[.]pl
10	slovolam[.]sk	phim7z[.]tv

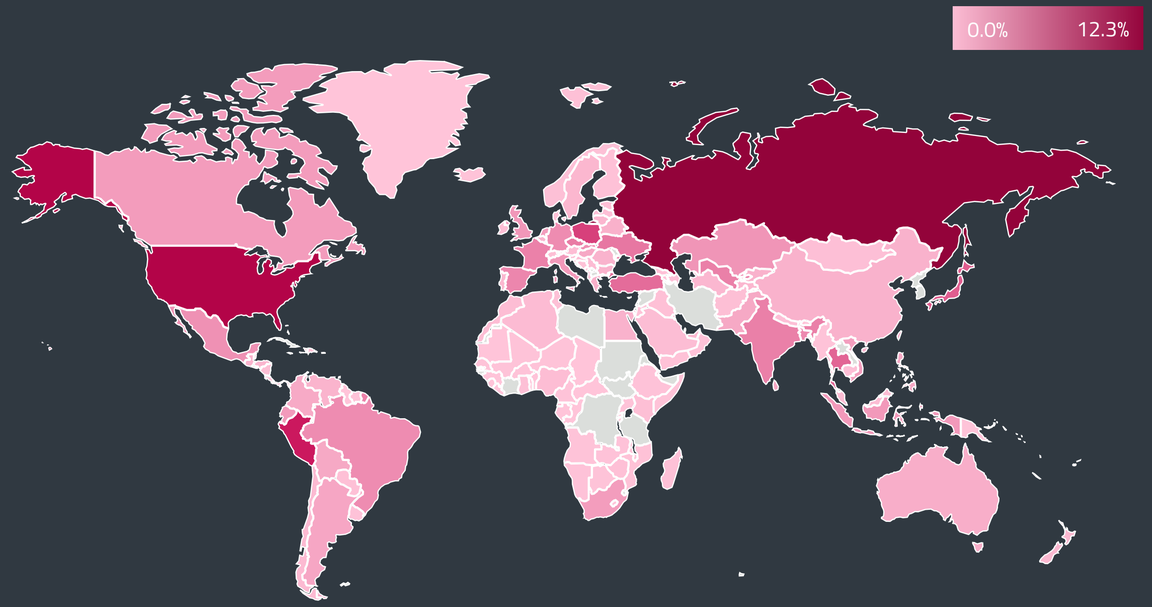
Top 10 most visited cryptojacking domains in T3 2021 and in 2021 overall

Unlike Coinminers, Cryptostealer rates decreased in T3, coincidentally also by 8.4%. The countries most affected by these threats were Peru, Turkey, and India, and it was Turkey that saw the most hits when Cryptostealer detections peaked on October 18. The culprit behind this peak was the MSIL/ClipBanker.LT trojan. MSIL/ClipBanker was also the most detected cryptostealer family with 31.4% of all cryptostealer detections, dethroning Win/PSW.Delf which fell to third place, behind the Win/Spy.Agent trojan family.

Even with the decreasing number of cryptostealer detections, cybercriminals do not look like they will be leaving people's cryptocurrency funds alone any time soon. 2021 saw several large-scale operations targeting cryptocurrency exchange services, emptying the victims' wallets while making the malicious actors a lot of money: in October, *Coinbase disclosed* [104] that between March and May 2021, threat actors bypassed the company's multifactor authentication to steal cryptocurrency from 6,000 users, most probably through a combination of phishing campaigns and exploiting a vulnerability in Coinbase's SMS account recovery process. In December, the cryptocurrency trading platform *BitMart announced* [105] that a security breach related to their Binance smart chain and Ethereum hot wallets had occurred and resulted in the theft of almost USD 150 million. The breach happened most likely due to a stolen private key.



Fake verification screen used in the phishing campaign targeting Coinbase users



Global distribution of cryptocurrency threat detections in T3 2021

Non-fungible tokens (NFTs) were seemingly everywhere in T3: based on *Google Trends* [106], the search term "NFT" jumped in popularity between the end of August and the start of September 2021, and has been steadily rising since. This, unsurprisingly, provided cybercrooks with ample new opportunities. In October, information emerged that threat actors were *stealing cryptocurrency wallets* [107] of the users of the NFT marketplace OpenSea by luring them to click malicious NFT art. Cybercriminals also went after cryptocurrency funds and NFT assets in the recent *Discord malware campaign* [108] targeting channels for cryptocurrency enthusiasts. This campaign used the Babadeda cryptor to obfuscate malicious RATs as legitimate applications.

In T3, cryptocurrency threats continued to be highest in Russia (12.3%), the United States (8.3%), and Peru (5.5%). The same countries were the most affected in 2021 overall, with Russia registering 11.2% of the attacks, Peru 6.4%, and the US 5.8%.

TRENDS & OUTLOOK

Cryptocurrencies are becoming more and more entrenched in our everyday lives. An increasing number of applications now come with integrated mining tools – an unfortunate trend that will most likely continue, despite often being met with user outcry. Hence the rising number of desktop and PUA detections.

NFTs constitute another rising trend, currently making their way into the gaming industry. Even if they do not influence cryptocurrency exchange rates, their rise might lead to an overall increase in cryptostealers.

Geopolitics will continue to influence cryptocurrency exchange rates. Factors such as volatile political landscapes in countries where mining is popular make cryptocurrency rates decrease; a stable political situation in those same countries causes exchange rates to grow, along with cryptocurrency threats and ransomware.

Igor Kabina, ESET Senior Detection Engineer

WEB THREATS

Web threats saw their first growth of 2021; phishers increased their focus on cryptocurrency and e-commerce platforms.

After declining for most of 2020 and 2021, web threat detections stabilized in T3 2021, seeing a minor increase of 2.6%. On average, T3 2021 saw 4.8 million daily web threat blocks and 400 thousand unique URLs blocked daily. Detections peaked in the second half of October due to a short-term spike in Scam blocks, with a few days seeing 7 million daily web threat blocks.

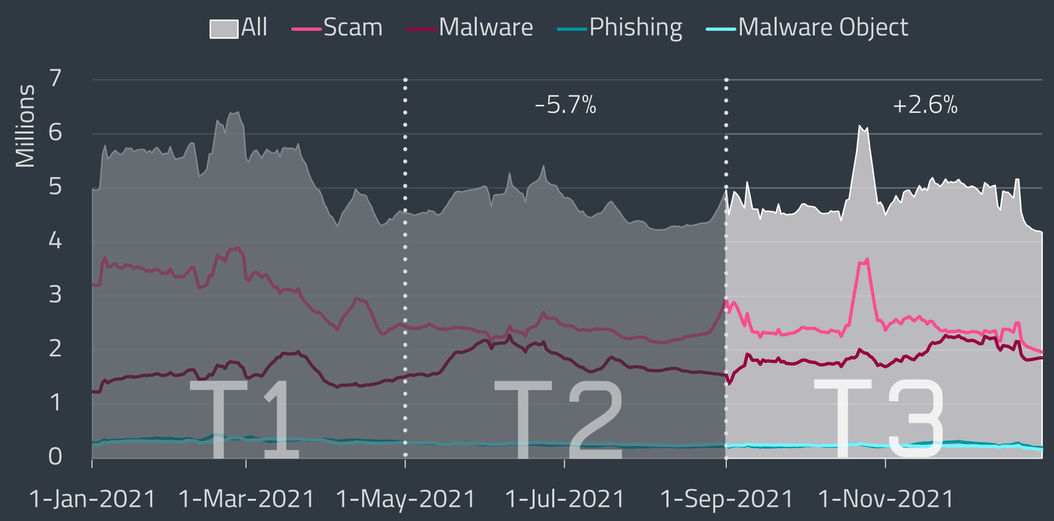
Much like in T2 2021, the most prevalent web threats were fraudulent websites categorized as Scam, representing 51% of all blocking events and 46% of the unique URLs blocked in T3 2021. This category saw growth in both total blocks and in the number of unique URLs. The Malware category grew in terms of total blocks, but the number of unique malicious URLs decreased by 14% compared to T2. On the other hand, the number of phishing URLs kept increasing (5.1%), although their growth slowed down considerably compared to T2 (42%).

Looking at yearly data, ESET telemetry recorded 1.8 billion web threat blocks in 2021 – half of the blocking events seen in 2020. When comparing the yearly trends, however, 2020 saw a steep and steady decline, which gradually stabilized in 2021.

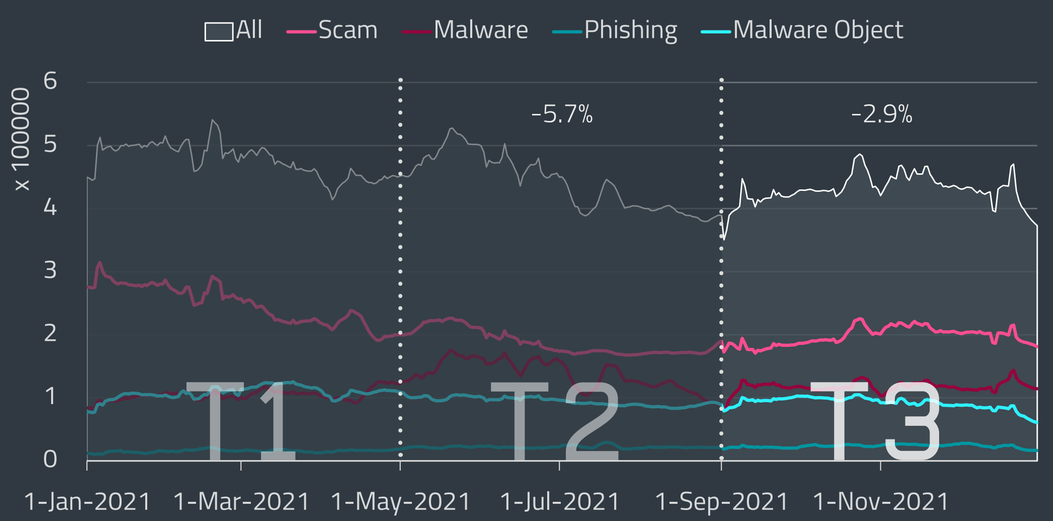
As for the most detected domains in T3, the top 10 list broken down into categories is available in the accompanying table, with those detected for the first time during T3 2021 marked with an asterisk.

	Malware	Scam	Phishing
1	pdloader[.]com	newrrb[.]bid	d18mpbo349nky5.cloudfront[.]net
2	iclickcdn[.]com	cellar.z5h64q92x9[.]net	propu[.]sh
3	pxksnymto[.]ru	loft.z5h64q92x9[.]net	mrproddisup[.]com
4	plehimselves[.]info	survey-smiles[.]com	tech4-you[.]com
5	demotzincky[.]casa	bwukxn[.]com	travelslive[.]biz
6	liveparticipationaudience[.]com*	v.vfghe[.]com	binomo-web[.]com
7	nativewpsh[.]com	sentrynew.sdh.com[.]ua	redirect.appleads-trk[.]com
8	jecromaha[.]info	glotorrents[.]pw	update.updtbrwsr[.]com
9	www.hostingcloud[.]racing	z.cdn.trafficlide[.]com	watchvideoplayer[.]com
10	vk-online[.]xyz	cp1s[.]xyz	quellaplentyresolute[.]com

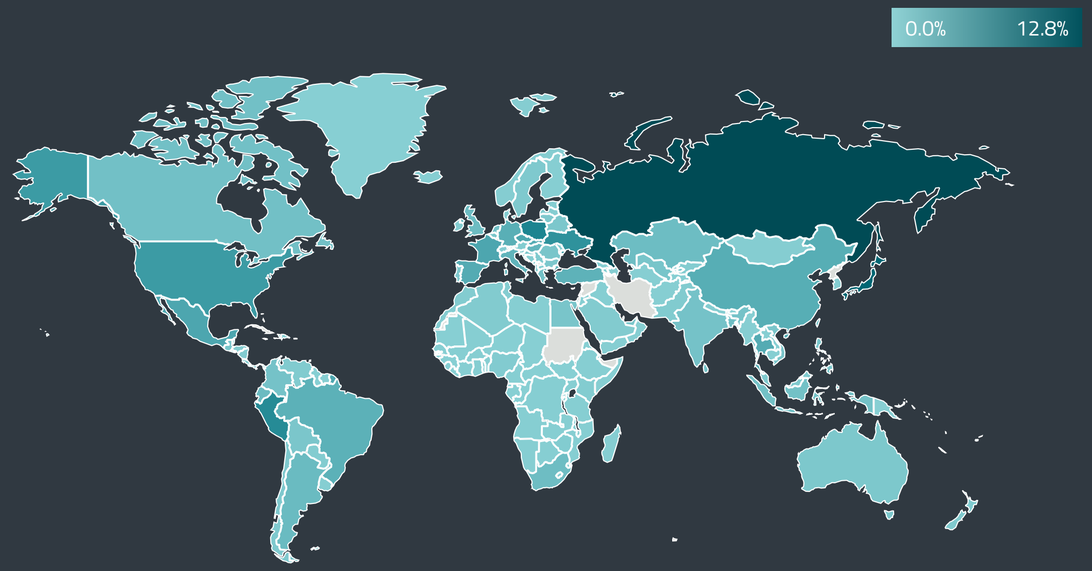
Top 10 blocked Malware, Scam and Phishing domains in T3 2021; domains first detected in this period are marked with *



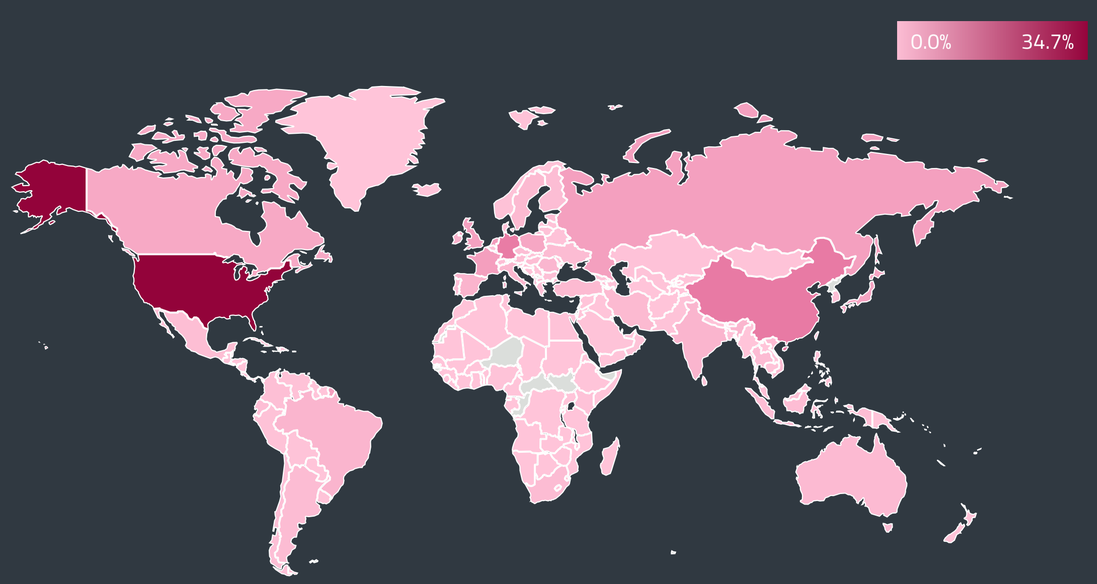
Trends of blocked web threats in 2021, seven-day moving average



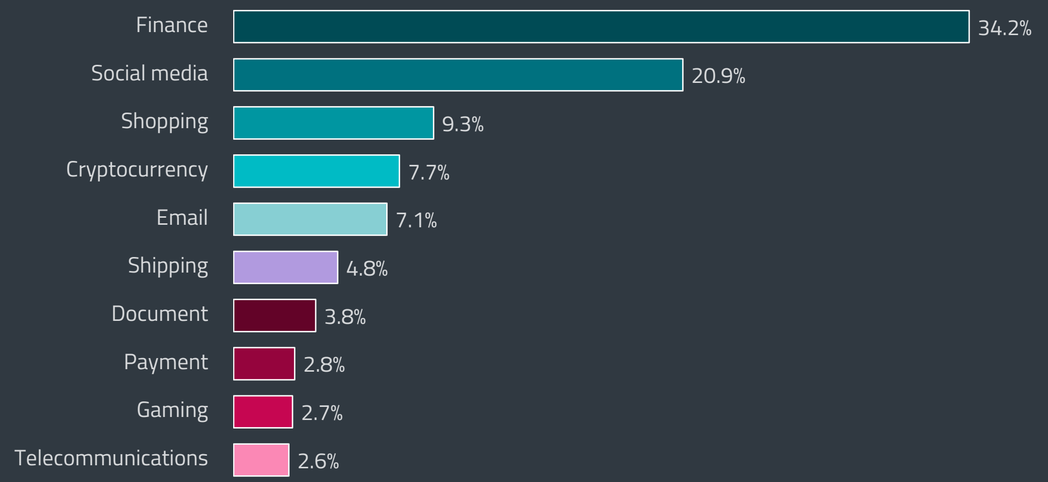
Trends of unique URLs blocked in 2021, seven-day moving average



Global distribution of web threat blocks in T3 2021



Global distribution of blocked domain hosting in T3 2021



Top 10 phishing website categories in T3 2021 by number of unique URLs

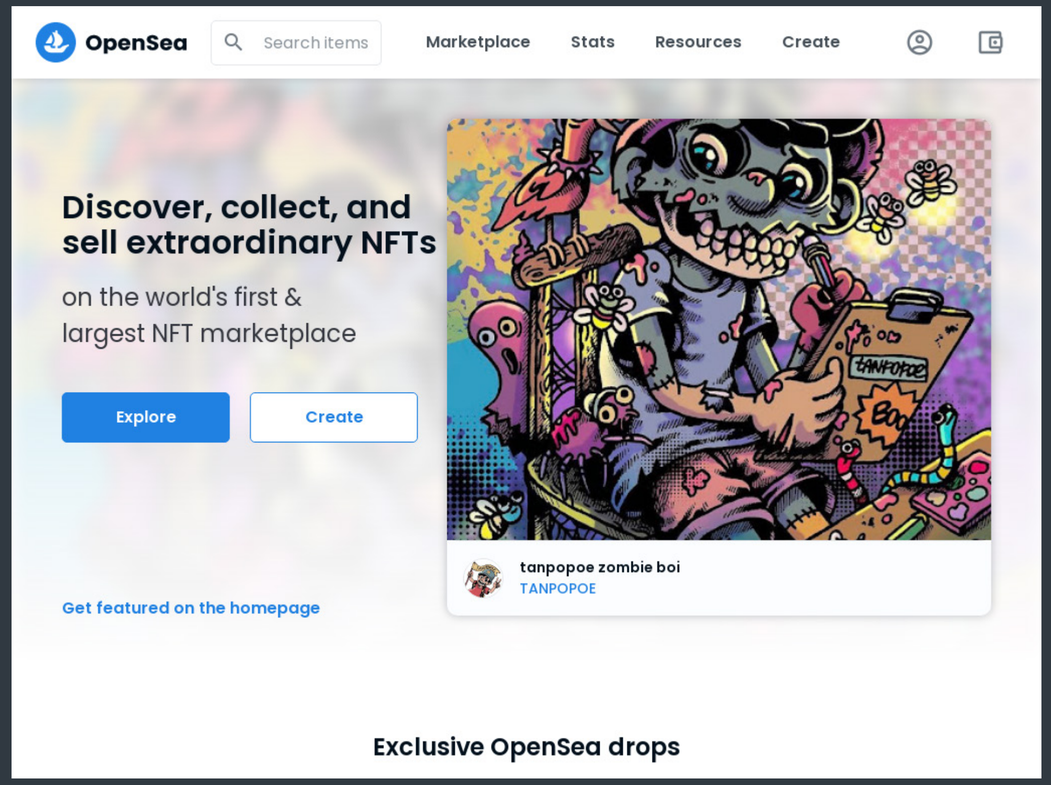
The number of harmful websites blocked in T3 2021 was greatest in Russia (12.8% of all website blocks), followed by Japan (8.2%), Poland (5.0%), Peru (4.6%), and Ukraine (4.1%). As for the source countries of the web threats – determined by the GeoIP of the blocked domains – more than a third of the blocked domains were hosted in the US (34.7%), followed by a wide margin by China (6.7%), Germany (6.5%), Netherlands (3.6%), and France (3.3%).

Based on ESET phishing feeds, approximately a third of the phishing URLs detected in T3 2021[1] impersonated financial organizations, much as in T2. Social media-themed phishing lures, mainly represented by fake Facebook and WhatsApp login pages, became slightly less prevalent, decreasing by 22.6% in the total number of URLs seen. The most significant changes occurred in the Cryptocurrency category, the numbers of which tripled, and the Shopping category, which saw more than double the URLs compared to T2.

In the Shopping category, websites mimicking Amazon were the most common, doubling compared to T2. The second most commonly observed lure was eBay.

In the booming Cryptocurrency category, phishers favored targeting users of cryptocurrency exchanges Kraken and Paxful, cryptocurrency wallets Trust Wallet, Metamask and Exodus, and the Blockchain.com platform. Cryptocurrency giveaway scams purporting to be connected to Elon Musk or Tesla were also a commonly seen lure. A new target emerging in T3 2021 was the *fast-growing* [109] NFT marketplace OpenSea. Cybercriminals' interest in NFTs – and OpenSea in particular – is also outlined in the *Cryptocurrency threats* section.

[1] The statistic is based on phishing URLs that could be categorized.



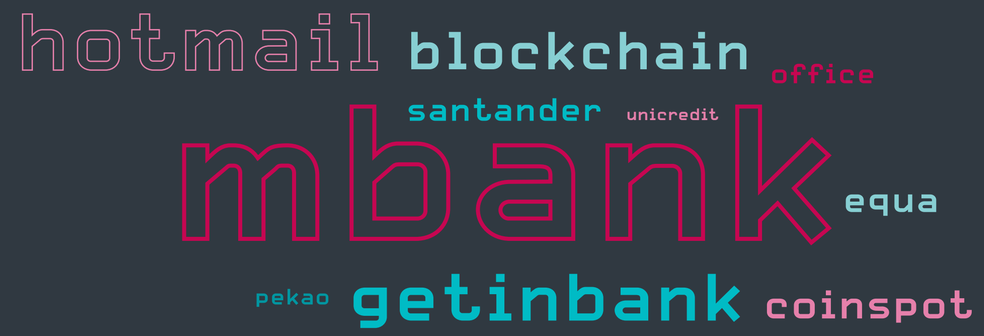
The most commonly seen visual among phishing websites impersonating the OpenSea NFT marketplace according to ESET phishing feeds

The homoglyph attack scene had plenty of newcomers in T3 2021 – six of the top 10 targets were first seen in T3 and most of the previously seen targets had their homoglyph URLs updated.

The most prevalent impostor domain in T3 was "online.mbąnk[.]com", making use of the letter a with a dot below and mimicking the login page of Poland's mBank. Similarly, in third place, "secure.getinbąnk[.]com" attempted to pass for the website of the Polish Getin Bank.

Australian cryptocurrency exchange CoinSpot also became the target of scammers, with the fake domain "coınspot.com" using the dotless i. Other new targets spotted in T3 include the Czech Equa bank, Polish bank Pekao, and international banking groups Santander and UniCredit.

In a yearly breakdown of homoglyph attacks, "blockchain" leads the chart as the most prevalent lure, followed by the fraudulent mBank domain described above and the "netbank.erstebąnk[.]com" impostor domain from T2.



Top 10 brands and domain names targeted with homoglyph attacks in T3 2021

TRENDS & OUTLOOK

The steep decline in web threat detections observed throughout 2020 – likely connected to botnet takedowns – slowed down in 2021, stabilizing in the last months of the year.

In the second half of 2021, we saw a notable increase in phishing URLs, which went hand in hand with a rise in phishing emails. For obvious reasons, financial institutions continued to be the top target of phishers – consistently accounting for about a third of phishing lures seen this year. Cybercriminals also continued to capitalize on the COVID-19 pandemic in whatever ways they could, focusing especially on impersonating government institutions in various phishing and other fraudulent schemes.

As predicted in the Q4 2020 Threat Report, cybercriminals increased their targeting of cryptocurrency enthusiasts in 2021, with cryptocurrency scams, phishing campaigns, and homoglyph attacks rising throughout the year.

In 2022, we can expect to see more opportunistic campaigns designed to harvest sensitive information from unsuspecting victims. And, as cybercriminals are always looking for new means of detection evasion, we can expect the attacks to become sneakier and sneakier. Scammers will continue to take advantage of the revived cryptocurrency market – and as we already saw in T3 with the targeting of NFTs, there is always a new opportunity to jump on.

Jiří Kropáč, ESET Head of Threat Detection Labs

EMAIL THREATS

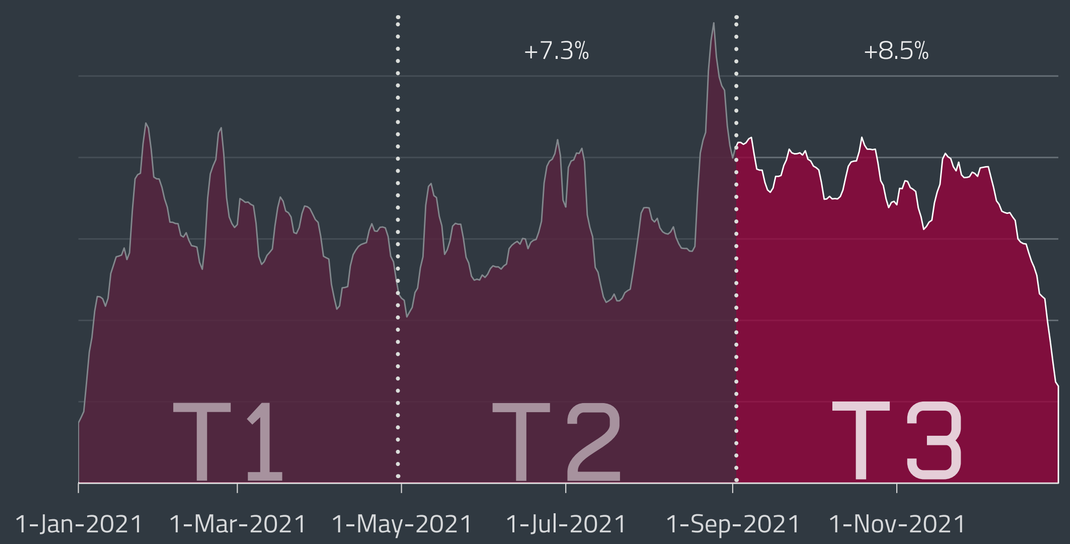
Despite losing a significant cut due to the continued decline in malicious macros, email threat detections continued to grow in T3 2021, fueled by a boom in phishing emails and a publicly available exploit.

Email threats continued to grow in T3 2021, increasing by 8.5% in total detections, despite losing a significant cut to the reduced activity of malicious macros (VBA/TrojanDownloader.Agent).

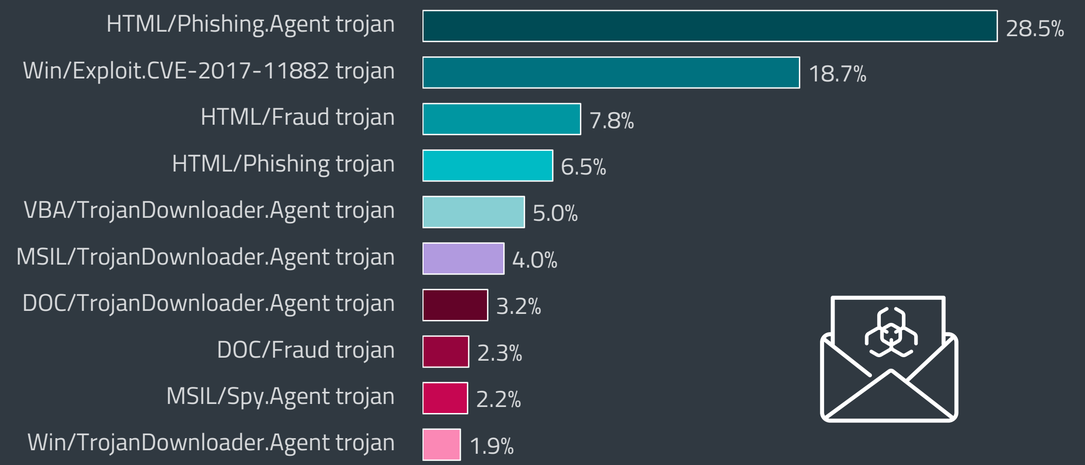
In the top 10, HTML/Phishing.Agent reinforced its first spot with additional 78% growth. Most phishing emails caught under this detection in T3 2021 were blocked in Japan, followed by France and the United States. The most common themes of these emails were fake medication offerings and fake reminders about a supposedly full inbox, luring recipients to click on phishing links.

Previously ranking third in T2, emails detected as DOC/Fraud dropped by 12.6 percentage points to eighth place, after a short-lived peak in detections in August and September. This peak, driven by a surge in so-called *sextortion scam* [110] emails, was one of four such large DOC/Fraud campaigns seen in 2021, all primarily affecting Japan.

Win/Exploit.CVE-2017-11882, a consistently high-ranking threat, saw its highest detection numbers of the year in T3, growing by 60% since T2 and climbing to second place. This detection name represents malicious documents exploiting a vulnerability in Microsoft Equation Editor, a



Malicious email detection trend in 2021, seven-day moving average



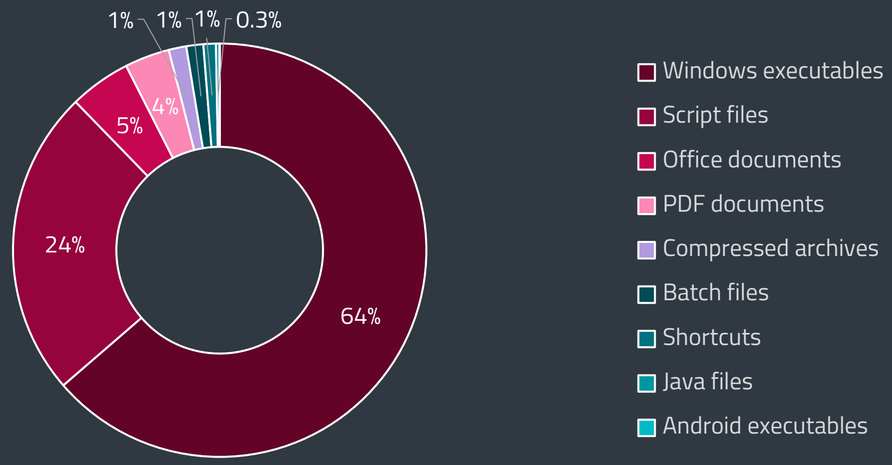
Top 10 threats detected in emails in T3 2021

component of Microsoft Office. The exploit, which is publicly available, is usually used to download additional malware to the compromised computer, with infostealer Agent Tesla (MSIL/Spy.Agent.AES), password stealer Fareit, and notorious downloader Emotet being the most common suspects. Win/Exploit.CVE-2017-11882 was most commonly seen in Spain, Turkey, and Poland.

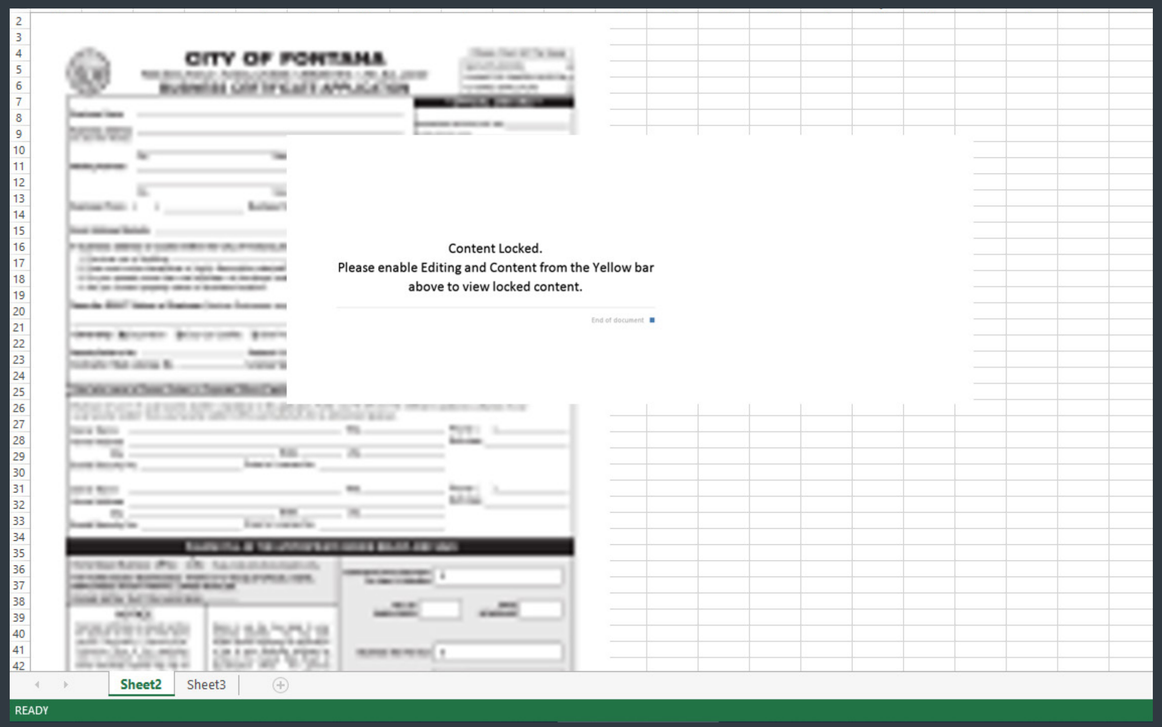
Emails containing this exploit usually try to pass for payment notifications, invoices, and order summaries. The attachments are often password-protected, with the passwords included in the email body – a well-known detection evasion technique. Some of the recently circulating malicious documents are left blank, also possibly in order to dodge detection.

As for brands abused by phishers, emails impersonating Microsoft lost half their steam, dropping by 48% in T3 compared to T2. The opposite was seen for emails using DHL and WeTransfer as phishing lures, which shot up by 145% and 156%, respectively.

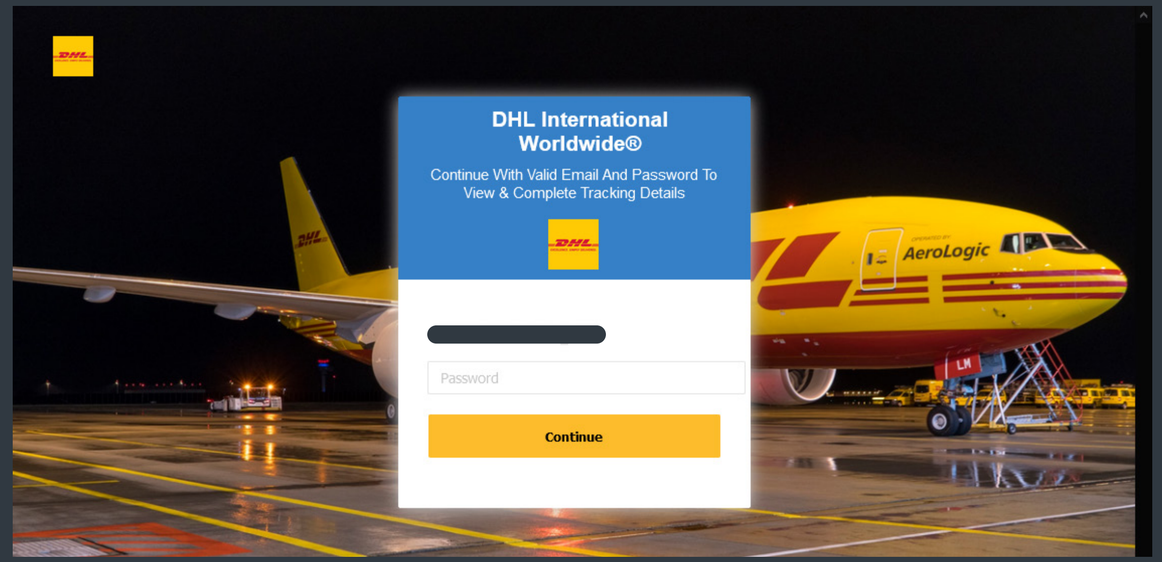
Phishing emails impersonating DHL were especially rampant from the end of September through the end of October, with most detections identified in Japan, Turkey, and Hong Kong. The attachments in the majority of these emails are named "E-Contact Form.htm", which was the second most common filename in malicious attachments in T3 while also being a newcomer in the stats.



Top malicious email attachment types[2] in T3 2021



A recent example of a maliciously crafted document detected as Win/Exploit.CVE-2017-11882



Malicious email attachment detected as HTML/Phishing.DHL, using the filename "E-Contact Form.htm"

Phishing emails impersonating WeTransfer continued to plague users' inboxes in T3, with the largest wave observed in September and detections most commonly occurring in Japan, Turkey, and Spain. The emails kept the same visual as *seen in T2* [111], with only the supposed sender addresses and phishing links changing.

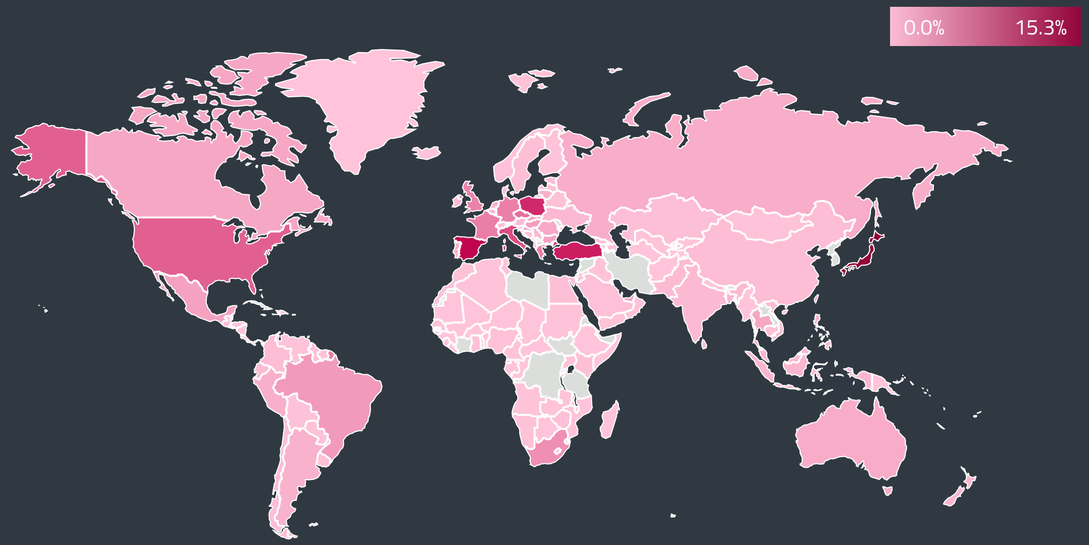
Maliciously crafted Microsoft Office files detected as VBA/TrojanDownloader.Agent trojan, which saw a sharp decrease in T2 (-63.4%) as a consequence of the demise of the Emotet botnet, remained fairly stagnant in T3. While showing a few minor spikes in activity in September and October, their overall detection numbers were reduced by a further 4.3% from T2 to T3.

Looking at the file types of malicious attachments detected in T3, executables remained the dominant format, followed by script files and Office documents.

The most common filename among malicious attachments detected in T3 remained "EU-Business-Register.pdf", a long-known subscription scam. A newcomer in the most detected files was "E-Contact Form.htm", related to the previously mentioned DHL-themed phishing emails. These attachments contain fake forms phishing for login credentials to DHL online services, which might be used by scammers in an attempt to gain access to other accounts via credential-stuffing attacks.

The third most commonly seen attachment filename was "SOA.exe", which carries the well-known infostealer Agent Tesla, detected as MSIL/Spy.Agent.AES.

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



Global distribution of email threat detections in T3 2021

Fake payment requests and fake bank communication remained by far the most used lure in emails carrying malware in T3. In fact, 75% of malicious emails caught in 2021 had a financial theme. The rest were evenly divided between fake shipping and package delivery notifications, and sales-themed emails.

The share of COVID-19-themed emails remained below 1% throughout the year, decreasing across each Threat Report period. Malicious emails seen in T3 included a small number of subjects using the topic of the Omicron variant as a lure, for example in emails purporting to offer important information about the new variant, or guidelines and measures being introduced in response to its emergence.

Geographically, Japan was the most affected by email threats in T3, taking up 19% of the detections, followed by a wide margin by Spain and Italy, each with approximately 5% of email threat detections. In yearly data, Japan remains in the lead, with Spain and Turkey tagging along with 8% and 7%.

Following two periods of decline, spam detections saw a slight increase (4.7%) in T3 2021 compared to T2. Most likely, this change of course was due to the end of the year traditionally being more spam-heavy, with the various holidays driving large-scale campaigns of unsolicited emails. For example, in the days leading up to Black Friday and Cyber Monday in late November, a few days had daily spam detections up to 70% higher than the daily average in T3 2021.

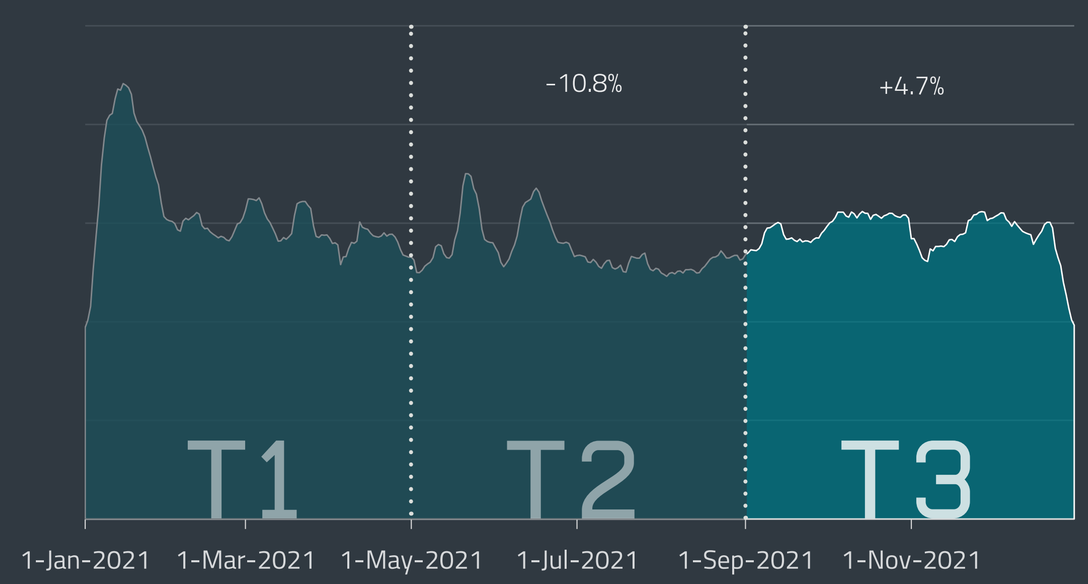
TRENDS & OUTLOOK

Following the takedown of the Emotet botnet at the beginning of 2021, emails distributing malicious macros were greatly reduced – falling from tens or even hundreds of thousands of daily detections to thousands in ESET's telemetry. Unfortunately, prolific phishing and fraud activity, along with the increased use of a public exploit for crafting malicious Office files, effectively "cancelled out" this decline.

Phishing, growing continuously since May, increasingly has been targeting users of popular online and cloud services – be it platforms used for remote work, or various streaming and media providers. Package delivery, which boomed as phishing bait in 2020, continued to be heavily abused in 2021, and we expect this to go on.

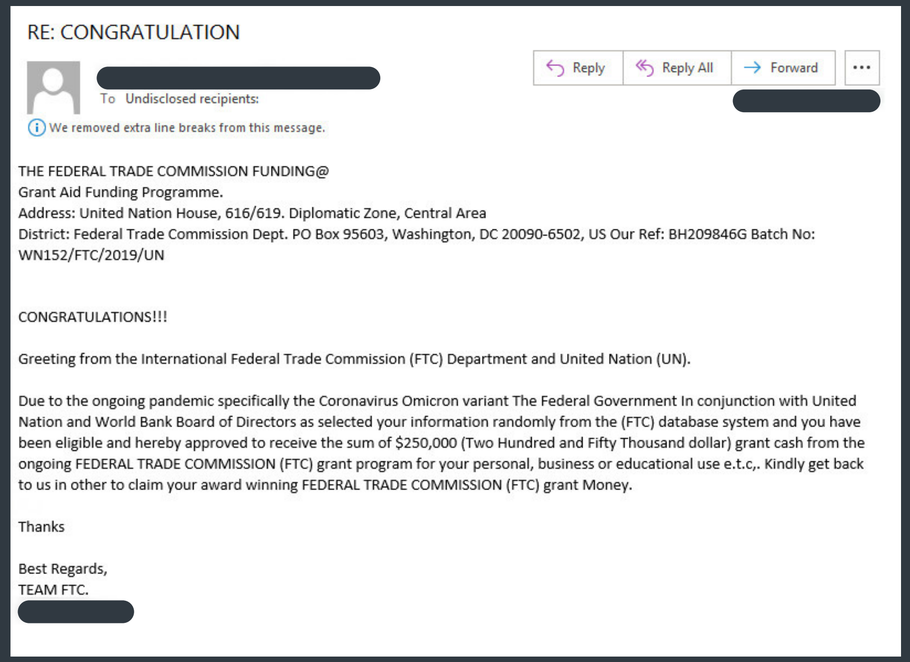
In 2022, we will continue to face campaigns leveraging big brand names, as well as smaller opportunistic campaigns cropping up based on current trends. As we saw in 2021, changes in botnet activity heavily influence the email threat scene, so we're keeping an eye out for any developments in that area.

Jiří Kropáč, ESET Head of Threat Detection Labs



Spam detection trend in 2021, seven-day moving average

Nearly two years into the pandemic, fraudsters continued to leverage COVID-19 in spam emails in T3, trying to lure out sensitive information under the guise of government benefits, regulations, and public health guidelines. Spammers were also quick to hop on the Omicron train, inserting the term into generic spam claiming that the recipient is eligible for a financial reward due to the pandemic.



RE: CONGRATULATION

Reply | Reply All | Forward | ...

[redacted]

To Undisclosed recipients:

[redacted]

We removed extra line breaks from this message.

THE FEDERAL TRADE COMMISSION FUNDING@
Grant Aid Funding Programme.
Address: United Nation House, 616/619. Diplomatic Zone, Central Area
District: Federal Trade Commission Dept. PO Box 95603, Washington, DC 20090-6502, US Our Ref: BH209846G Batch No: WN152/FTC/2019/UN

CONGRATULATIONS!!!

Greeting from the International Federal Trade Commission (FTC) Department and United Nation (UN).

Due to the ongoing pandemic specifically the Coronavirus Omicron variant The Federal Government In conjunction with United Nation and World Bank Board of Directors as selected your information randomly from the (FTC) database system and you have been eligible and hereby approved to receive the sum of $250,000 (Two Hundred and Fifty Thousand dollar) grant cash from the ongoing FEDERAL TRADE COMMISSION (FTC) grant program for your personal, business or educational use e.t.c,. Kindly get back to us in other to claim your award winning FEDERAL TRADE COMMISSION (FTC) grant Money.

Thanks

Best Regards,
TEAM FTC.
[redacted]

COVID-19-themed spam including a mention of the Omicron variant

As for the geographic distribution of spam, 16% of spam emails detected in T3 originated from the United States, followed by Japan (13.3%), China (9.6%), Poland (6.6%) and France (7.0%). The share of spam in all emails sent was highest in China (56%), followed by Singapore, Argentina, India, and Russia, where between 18 and 27% of emails sent constituted spam.

When interpreting this data, it should be noted that ESET's visibility into spam is limited due to email traffic commonly first being filtered at the level of internet email service provider, and elsewhere, before reaching ESET-protected endpoints.

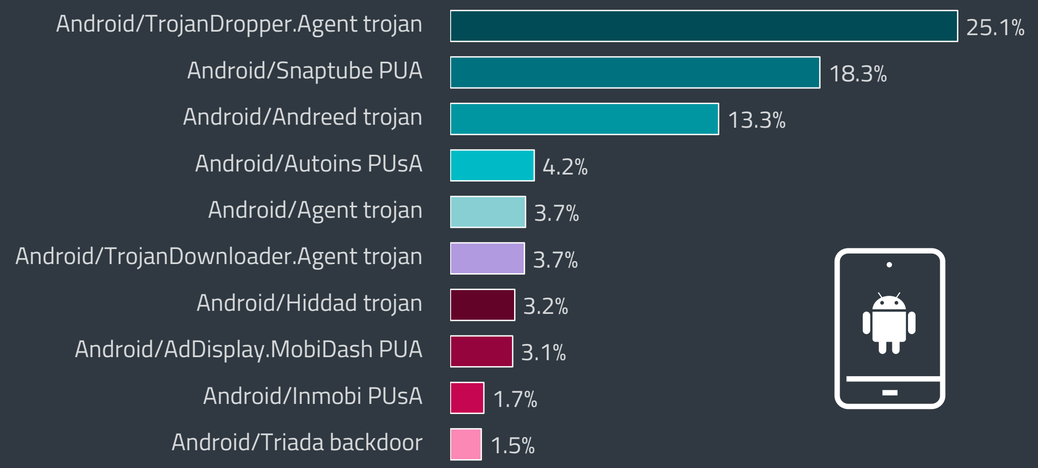
ANDROID

Even though Android banking malware detections dropped by 20% in T3, they increased more than fivefold in 2021 compared to 2020.

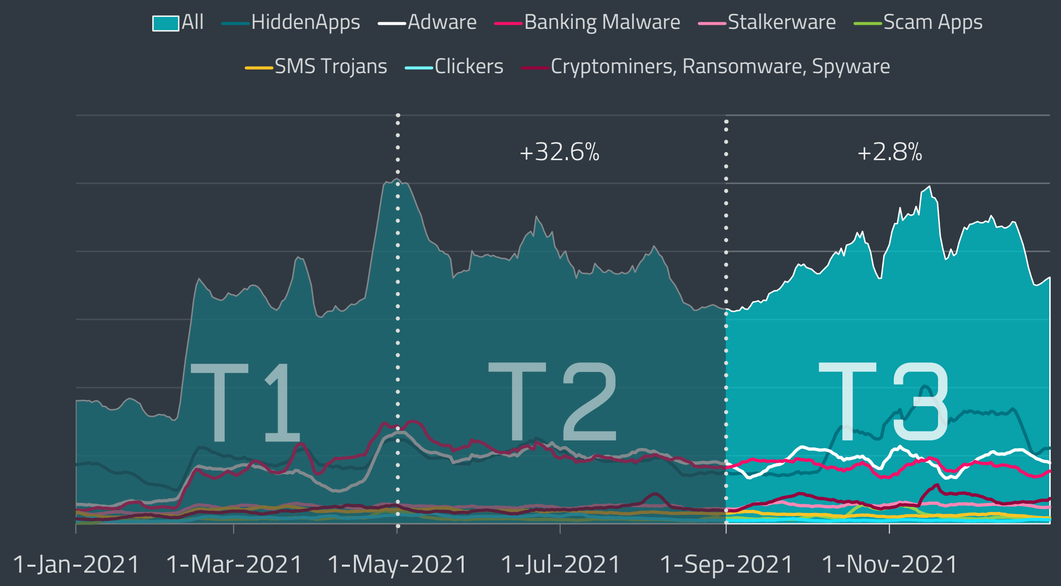
Overall Android detections were relatively stable in T3 2021, rising by only 2.8%. ESET telemetry also shows that the gap between Android threat categories is widening.

Categories that experienced a decline in T3 were Clickers (-48.4%), SMS trojans (-29.6%), Cryptominers (-25.4%), Adware (-9.9%), and surprisingly even Android banking malware (-20.6%). However, even with this decline in T3, Android banking malware detections rose by a staggering 428% in 2021 compared to 2020. Countries with the biggest detection numbers of this type of threat in 2021 were Turkey, Russia, Spain, Ukraine, and Japan.

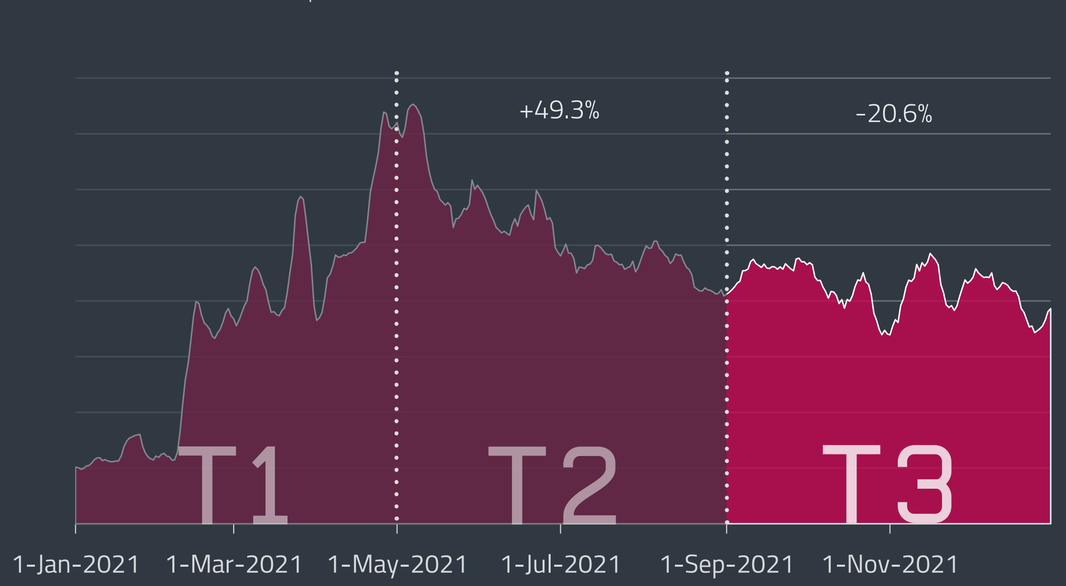
The whole realm of Android banking threats is illustrated by endless numbers of new or evolved Android banking malware samples identified by ESET and other cybersecurity companies. *ThreatFabric* [112] found several fake apps on Google Play (downloaded more than 300,000 times) stealing banking credentials, and a *new Android trojan* [113] (based on the infamous Cerberus banking trojan) targeting Poland, *Check Point* [114] identified a new wave of Android banking trojans focused on



Top 10 Android detections in T3 2021 (% of Android detections)



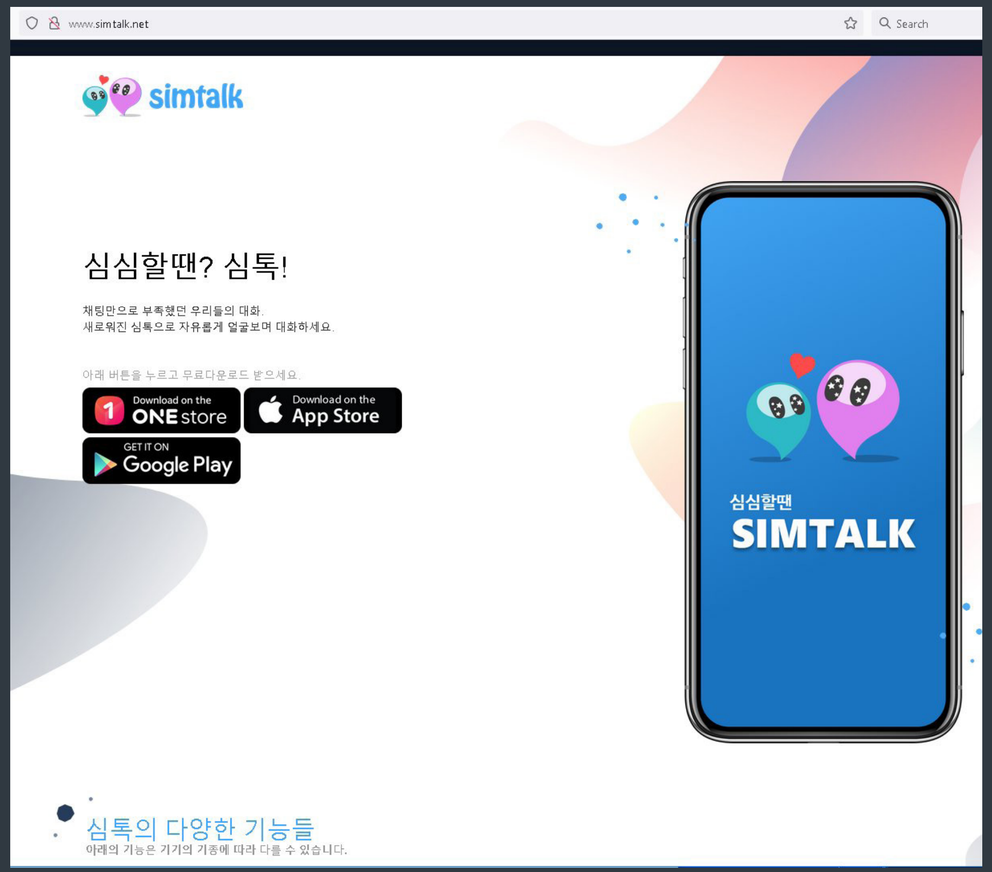
Trends of selected Android detection categories in 2021, seven-day moving average



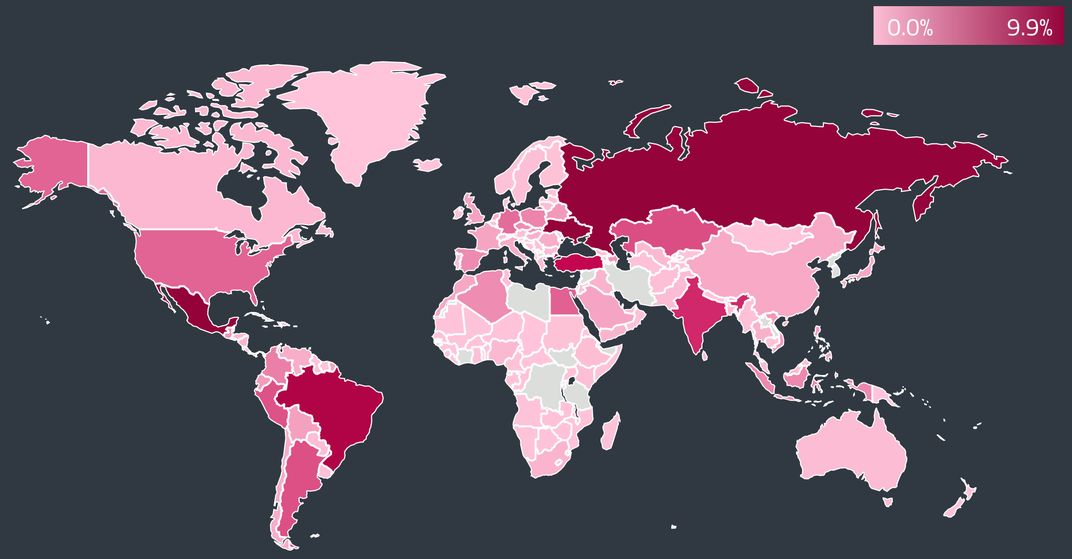
Android banking malware detection trend in 2021, seven-day moving average

customers of the Brazilian PagBank, and *Cleafy* [115] analyzed a new Android trojan that siphons credentials from users of banking and cryptocurrency services located in the United Kingdom, the United States, and Italy.

Various types of Android threats were thriving in T3 – Stalkerware rose by 9.3% (prevalent in Russia, Ukraine, Poland, and the United States), Spyware by 23.2%, and HiddenApps by 29%. A notable sample that ESET researchers detected during this period is *new Android spyware* [116] targeting users in South Korea using malicious chat apps downloaded from fake chat websites. It extracts phone numbers, device locations, text messages, and contact lists including contact photos, all of which are then sent to its C&C server. ESET detects this threat as a variant of Android/TrojanDropper.Agent; according to ESET telemetry, this family was also the most detected Android threat in T3.



The distribution websites of the spyware targeting Android users in South Korea are copycats of a legitimate but already defunct service named Simtalk.



Global distribution of Android detections in T3 2021

Another example is a targeted mobile espionage campaign against the Kurdish ethnic group, which was *investigated by ESET researchers* [14]. In this campaign, which has been active since at least March 2020, dedicated Facebook profiles distribute two Android backdoors disguised as legitimate apps appearing to provide Android news in Kurdish and news for the Kurds' supporters, but in reality spy on their victims. ESET detects these threats as several different variants of the Android/Spy.Agent family.

The largest increase in detections in T3 was seen in ScamApps (63%) and Ransomware (114%). It is interesting to note that nearly 60% of all Android Ransomware detections were seen in Kazakhstan. Compared to T2, and even T1, the top 10 list saw one re-entry – Android/TrojanDownloader.Agent. In the case of this family, the actual malware is not part of the app the victim installs on the device but is downloaded by the app from a server. With this evasion technique, this type of threat tries to hide from Android cybersecurity apps. Using other evasion techniques such as anti-emulation checks is new Android rooting malware, *identified by Lookout* [117]. It was distributed on Google Play, Amazon Appstore and the Samsung Galaxy Store and uses a rooting process to gain privileged access to the victim's Android platform; ESET detects this threat as Android/AbstractEmu.

Countries where ESET telemetry detected the most Android threats during T3 were Mexico (9.9%), Ukraine (9.8%), Russia (9.7%), Brazil (7.0%), and Turkey (5.1%). Looking at 2021 as a whole, all Android threat detections rose by 22% over 2020 and Android users were most likely to encounter a threat during the weekend. The "safest" days for Android devices were Tuesdays, on which ESET telemetry

detected the lowest numbers of Android threats on average globally. It could also mean that Android devices are used more often during weekends and collect dust on Tuesdays; but, ESET telemetry doesn't have access to this type of user data.

As was expected, even in T3 Google continued posting regular fixes to vulnerabilities found in its Android platform. However, ESET Research would like to point out other vulnerabilities that might not get the same treatment – vulnerabilities in mandatory COVID-19 tracing apps and vaccination passports. ESET researchers in Canada took a look at mobile apps allowing the storage of vaccination passports issued by the Quebec government – VaxiCode and VaxiCode Verif – and *found a vulnerability* [118] in VaxiCode Verif that allowed the application to be forced to recognize non-government-issued QR codes as valid, which was later fixed. It is certainly *not the first* [119] *nor the last* [120] vulnerability present in an app that is critically needed in a pandemic world and many times deployed under a restriction that is difficult to mitigate: time. However, the publication of the source code and its analysis by experts might have avoided scandals that could have affected the public's confidence, since many more eyes could, in theory, check the security themselves.

In other service news: a great example of why to think of the smartphone as a key that protects a lot of sensitive data is *Google's announcement* [121] that it has started to auto-enroll users' accounts into two-step verification (2SV). It is a security measure also commonly known as two-factor authentication (2FA). Many users still opt for SMS as a two-step verification delivery mechanism even though cybersecurity experts *don't recommend it* [122], so this change in Google accounts setup can be a good reason to upgrade to a 2FA authentication app. Especially after the surprising (*and very quiet* [123]) announcement that a company that routes billions of text messages – including 2FA codes – has been hacked. Google *also revealed* [124] it has made its Permissions Auto-Reset function available to Android devices using earlier versions of its operating system. This feature works by automatically withdrawing user permissions from an app that hasn't been opened and used for a few months, or even longer, and increases the overall security and privacy of the user as some apps tend to collect user data unrelated to the app.

TRENDS & OUTLOOK

In 2021, the second year of the pandemic, we expected Android threats to continue to ride on this topic, but there was no need for that. As was shown in the abovementioned cases, several mandatory COVID-19 tracing apps and vaccination passports contained vulnerabilities that could have been exploited on a bigger scale. We expect that in 2022 malware developers will focus even more on malicious apps that offer them a higher return on investment, such as ransomware, banking malware and threats mining cryptocurrencies on victims' devices, as was partially seen in 2021.

Regarding the Android ecosystem, it is encouraging to see that the platform itself has tried to provide its users with a safer environment with a higher level of privacy; however, in 2022 we would like users to realize that in many cases, they need to take their security and privacy into their own hands and make some changes to their default smartphone settings.

Lukáš Štefanko, ESET Malware Researcher

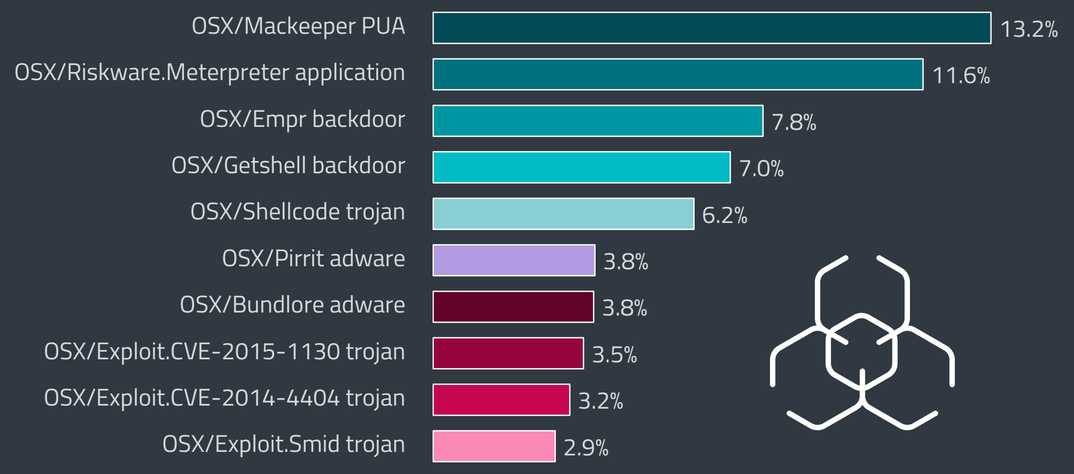
macOS AND iOS

macOS detection numbers saw a slight decline in T3 2021; however, trojans are responsible for more than one-third of all detections.

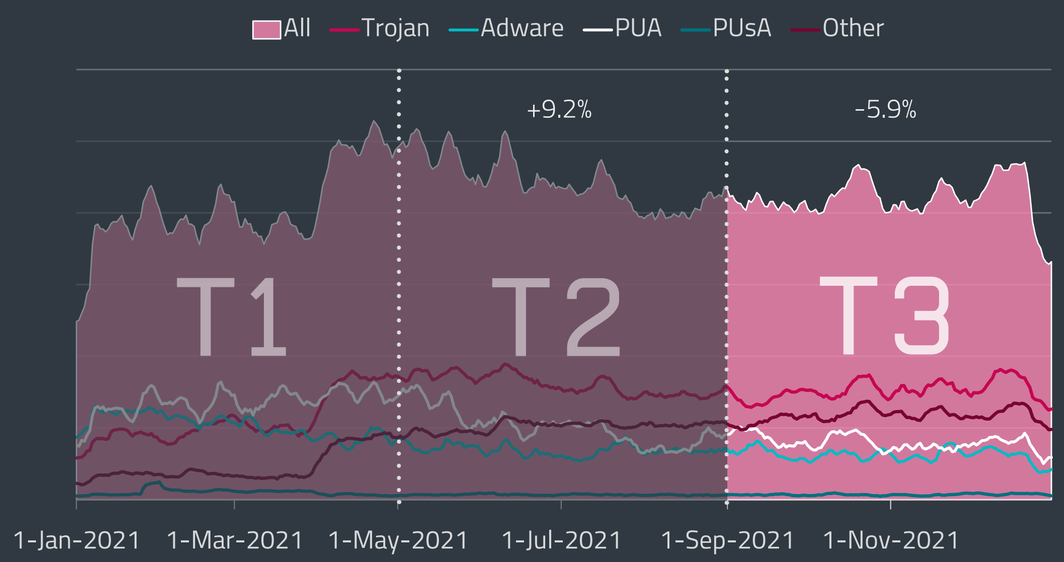
In T3 2021, ESET telemetry saw a 5.9% decline in macOS detections compared with T2. The biggest drop can be seen towards the end of December 2021 and it seems to mirror the end of 2020, where we also saw a noticeable drop in macOS detections that continued into the first days of January 2021. This could be attributed to this specific time of the year during which people around the world celebrate various religious and cultural festivities and simply don't use their computers that often.

The decline was visible in nearly all monitored categories – Potentially Unwanted Applications (PUAs, -22.5%), Adware (-10.6%) and Trojans (-6.2%). Only Potentially Unsafe Applications (PUsAs) saw a negligible uptick in T3 and rose by 1.2%. Overall lower detection numbers could be seen as something rather positive; however, in T3 2021 more than 36% of all macOS detections were of trojans and overall macOS Trojan detections rose by 126% from 2020 to 2021.

Except for some minor shuffles, there are no newcomers in the macOS top 10 detection list. Number seven, the OSX/Bundlore adware, which has been around for many years, has a new variant that poses as a Flash Player installer. Identified by *Confiant* [125], this fake Flash Player was signed with a developer certificate and notarized (and quickly revoked) by Apple. *WizardUpdate* [126], an Infostealer



Top 10 macOS detections in T3 2021



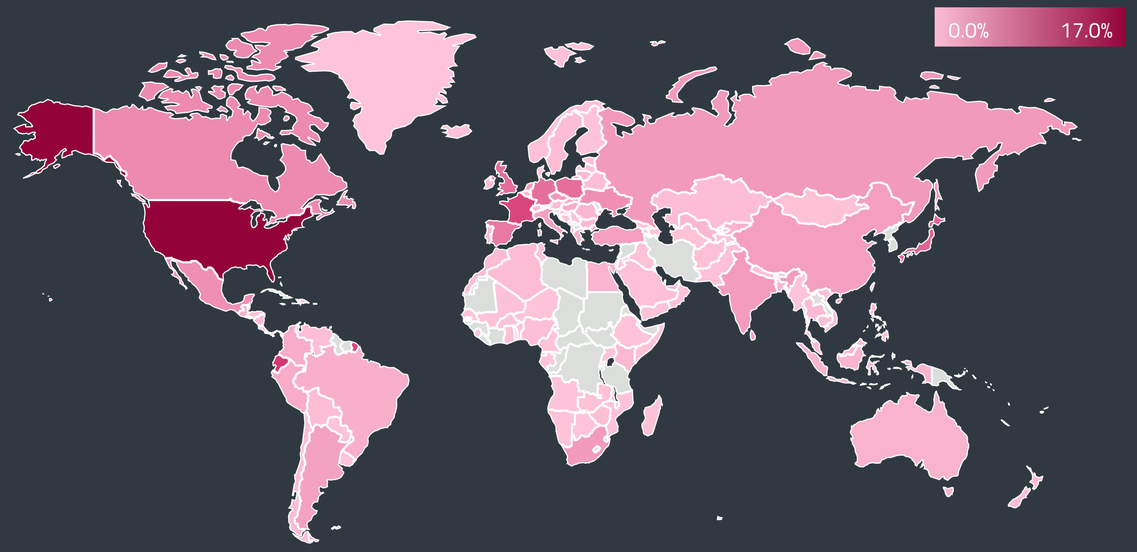
macOS detection trend in 2021, seven-day moving average

with lower detection numbers, received a significant upgrade – via new persistence and evasion tactics. It now impersonates legitimate software and is likely being distributed via drive-by downloads.

According to ESET telemetry, the most macOS detections in T3 2021 were found in the United States, with 17% of detections, followed by Ecuador (6.3%), France (5.6%), Japan (4.3%), the United Kingdom (3.9%), Poland (3.9%), and Germany (3.7%).

As was extensively mentioned in the *Featured story* section of this report, at the end of 2021 ESET researchers revealed watering hole attacks against high-profile websites in the Middle East. This campaign, which targeted several operating systems including macOS, has strong links to Candiru, a private Israeli spyware firm. Nonetheless, Candiru is not the only spyware group on the market. Mentioned already in the T2 2021 ESET Threat Report in connection with their iOS (and Android) Pegasus spyware abusing *zero-click vulnerabilities* [127], the NSO Group and latest revelations about their products were filling up headlines of newspapers around the world.

The University of Toronto's research group *Citizen Lab* [128] is keeping tabs on these threats targeting journalists, politicians, diplomats, and human rights activists located in countries like *Poland* [129],



Global distribution of macOS detections T3 2021

Hungary [130], *Germany* [131], *El Salvador* [132], Azerbaijan, Bahrain, Saudi Arabia, Rwanda, India, Kazakhstan, Mexico, Morocco, Togo, United Arab Emirates and others, including phones of US State Department officials *located in Uganda* [133]. By the time this report is published, the list could have gotten longer.

Both of the mentioned companies, Candiru and NSO Group, have been added to the *US Commerce Department entity list* [2], which may prevent US-based organizations from doing business with them without a license. Apple has obviously also had enough and *filed a lawsuit* [134] against NSO Group, requesting injunctive relief, compensatory damages, punitive damages, and disgorgement of profits, which sounds … expensive. The complaint provides some new information on the zero-click exploits originally *identified by the Citizen Lab* [127]. Apparently, lawsuits from trillion-dollar companies are nothing new to NSO Group: WhatsApp and its parent company Meta Platforms have been *suing them since 2019* [135].

Sadly, Candiru and Pegasus are only two high-profile examples in a whole market offering offensive intrusion capabilities to governments and similar entities. A joint investigation by Citizen Lab and Facebook's parent company Meta Platforms revealed details about *Predator spyware* [136]. Built and sold by previously little-known mercenary spyware firm Cytrox, it targets iOS devices using single-click links sent via WhatsApp.

Since this investigation, Meta Platforms has banned *seven surveillance-for-hire companies* [137] from its services, which include Facebook and Instagram. Other infamous spyware vendors include *Hacking Team* [138] and the developers of *FinFisher* [139], both entities well known to ESET researchers, who have been analyzing their tools for several years.

All of these companies are aiming mainly at high-profile targets; however, more standard macOS threats were also evolving during the last four months of 2021. *Security researcher Zhi* [140] discovered new malware that he dubbed ZuRu, which spreads via malicious sponsored search results. Victims are led to malicious websites serving trojanized applications and once their data is exfiltrated, the malware installs a Cobalt Strike agent, which is a commercial penetration testing product frequently stolen and used also by threat actors. ESET detects this threat as OSX/Spy.ZuRu.

Google's *Threat Analysis Group (TAG) analyzed* [141] a targeted watering hole attack that used iOS and macOS zero-day or N-day exploits aimed at users in Hong Kong. The downloaded payload consists of a previously unreported backdoor called MacMa, which ESET detects under the same name, with features like file downloading, audio recording, and executing terminal commands. TAG researchers believe the threat actor behind this backdoor is a well-resourced group, likely state backed.

The case of MacMa also shows that even though Apple claims to support several versions of macOS, it might take the company *much longer* [142] to patch security holes in older versions of its platform. Another notable vulnerability was reported by security researcher Park Minchan – who found a flaw in *Apple's macOS Finder* [143] system, which is responsible for the launching of other applications, that could have allowed remote threat actors to dupe unsuspecting users into running arbitrary commands on their devices. *Microsoft* [144] also found a vulnerability, nicknamed "Shrootless", that abuses entitlement inheritance in System Integrity Protection to allow execution of arbitrary code with root-level privileges.

TRENDS & OUTLOOK

As was shown in several cases of zero-click vulnerabilities, if a target is interesting enough and the attacker has resources that are extensive enough, it is very difficult to protect that target. Such resources are also used for the improvement of malware obfuscation and in 2022 we foresee a wider use of evasive techniques and more cases of targeted attacks using exploits. However, adware will continue to be the most common threat to the macOS platform, as it is relatively cheap to acquire and does not depend on especially focused targeting.

Regarding the actual development of malware and similar threats, we expect to detect more macOS malware and adware samples written in programming languages not often seen on this platform, such as Kotlin, D and especially Go.

Michal Malík, ESET Detection Engineer

IoT SECURITY

ZHtrap botnet goes live on Christmas Eve; Mozi's spread slows down.

ESET research observed the activity of several IoT botnets in T3 2021. The largest was the Mozi botnet, which in the last four months of 2021 amassed more than 562,000 unique IPs, 26% of which had already been compromised in the previous period.

Most of these enslaved devices (59%) were detected in China, followed by 29% in India, and 2% in each of Russia, the Dominican Republic, and Brazil. The top countries were almost identical to T2, except for Albania – which previously accounted for 4% of detections – replaced by the Dominican Republic.

As previously reported, Mozi is spreading mostly by exploiting known vulnerabilities in Netgear DGN devices (EDB-25978), DASAN (GPON) routers (CVE-2018-10562), D-Link routers (CVE-2015-2051) and Jaws web servers (EDB-41471). According to ESET telemetry, Mozi attempted to abuse these flaws on 5.2 million occasions in T3 2021, a 13% drop against the over 6 million attempts in T2 2021.

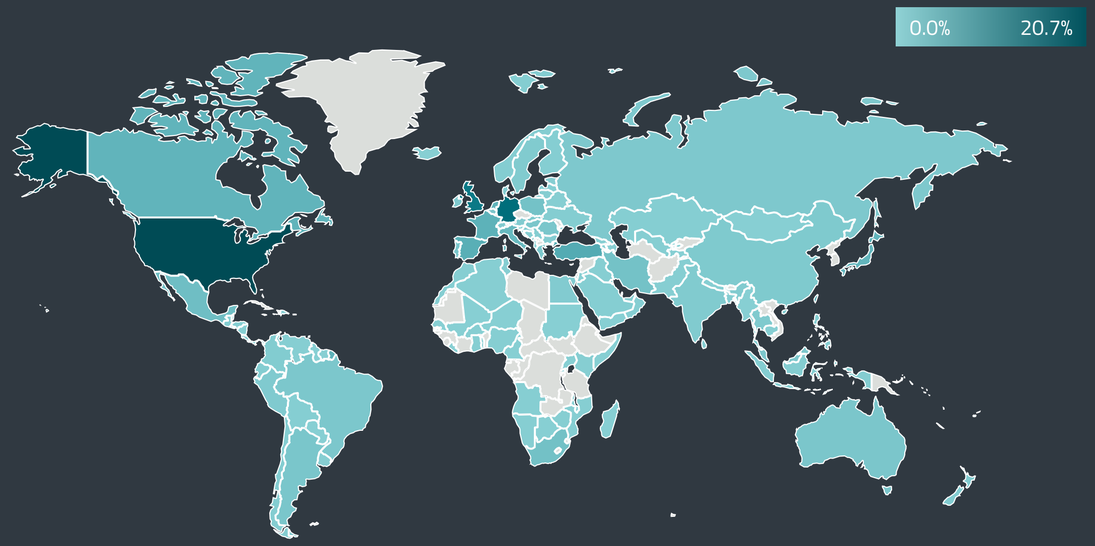
Countries that faced the biggest portion of the attacks were the United States with 20%, followed by the United Kingdom with 8%, Germany with 7%, and the Netherlands and France with 4% each. One important note: it was *reported* [145] that Mozi's authors were arrested by Chinese authorities in T2 2021 and that the malevolent network is probably propagating in a *zombie-like state* [146].

A quite active IoT botnet in T3 2021 was yet another variant of the notorious malware *Mirai* [147]. This latest version used 59 payload servers – most of them in the US – pushing malware via the same Shell Command Execution flaw in the Jaws web server (EDB-41471), as seen in the case of Mozi.

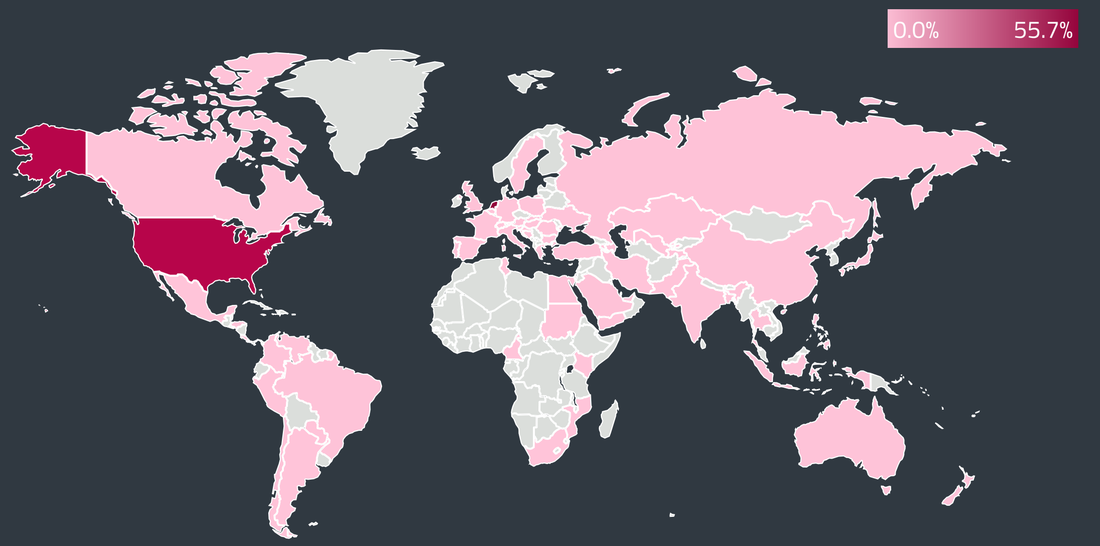
Globally, ESET detected this Mirai variant in over 170,000 attacks. Out of that number, 44% could be traced back to bots in Egypt, 12% led to machines in the United States, 6% were detected without a known country of origin, and 6% came from Brazil. Top targets of the botnet included devices in the United States, the United Kingdom, Germany, France, and the Netherlands.

And then there was the ZHtrap botnet – a malicious "present" pushed by ten payload servers since Christmas Eve. Although only active for the last week of T3, ZHtrap popped up in ESET telemetry almost 97,000 times. Most of these attacks, around 56%, originated in the Netherlands, 36% came from the United States, and 6% had an unknown geographical source.

ZHtrap's top list of targeted countries included the US, Germany, the UK, Taiwan, and Turkey. Like Mozi and Mirai, ZHtrap was going after the Jaws web server (via the EDB-41471 vulnerability), but with only 2,000 detections, it probably wasn't its top priority. Most of the botnet's efforts – close to 95,000 detections – went into exploiting the D-Link routers vulnerable to CVE-2015-2051.



Countries targeted by ZHtrap bots in T3 2021



Countries hosting ZHtrap bots in T3 2021

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

Top 10 weak router passwords in 2021

Between September 13 and September 19, ESET detected the *activity of Dark.IoT* [148] botnet targeting five different vulnerabilities, four of which were first reported in 2021. The list included CVE-2021-38647, one of the *OMIGOD* [149] flaws found in Azure services.

In the last four months of 2021, ESET telemetry reported a 38% jump in customer-requested router scans – from 195,000 in T2 to almost 270,000 in T3 – and a 45% surge in the number of unique-router checks – from 115,000 in T2 to 166,000 in T3.

The list of most frequently found router vulnerabilities didn't see much change, the pack being led by the unauthorized access flaw from 2012 known as CVE-2012-5687 (16%), followed by two 2014 command injection vulnerabilities CVE-2014-8361 (12%) and CVE-2014-9583 (8%). However, there have been *reports* [150] that attackers were trying to exploit the recently published and critical *Log4j vulnerability* to compromise devices with several IoT malware families.

Results of ESET scans also showed one positive trend, namely fewer routers using weak or default passwords. Although almost 4,400 unique devices were reported using one of the factory preset passwords, their ratio dropped between T2 and T3 by 4.7%. According to ESET data, the top five weak router passwords in 2021 were admin, root, 1234, 12345, and guest.

The attackers are aware of the negligence, as shown by the results of a three-year-long *IoT honeypot experiment* [151] by the US National Institute of Standards and Technology (NIST). Its researchers found that "admin" (username) and "1234" (password) was the most common combination used in attacks against IoT. NIST also found that malicious actors often scanned devices for open ports, tried to run commands that would disable firewalls, and aimed to build large botnets for DDoS attacks.

NIST is also behind the US initiative aiming to label all IoT devices with information such as level of security in the product's design, development, and maintenance. These *"nutrition" labels* [152] for hardware and software are designed to help consumers and smaller companies properly evaluate the security of "smart" devices in the buying process. The EU, UK, and private sector have similar programs.

And let's close up this section with a bit of good news for the IoT threatspace. Ukrainian authorities *arrested* [153] the operator of a 100,000-device-strong IoT botnet used for DDoS attacks. Agents caught up with the criminal after he made a mistake and registered his WebMoney account – a platform sanctioned in Ukraine – to his real home address. The attacker is now facing years in jail.

TRENDS & OUTLOOK

Looking back at 2021, Mozi botnet was the top IoT story in our reports. Thanks to each of its bots being the payload server, it spreads in the wild even now after its operators have been arrested. Based on our data and the law enforcement action, we assume Mozi reached its peak in 2021 and will gradually lose steam.

But many other threat actors are targeting IoT devices – some utilizing older malware and vulnerabilities, while others try to exploit freshly reported flaws. The former is well illustrated by the detected activity of a recent Mirai variant and ZHtrap botnets, the latter by the campaign of Dark.IoT botnet abusing several 2021 flaws, including one known to be part of the OMIGOD chain.

We expect 2022 to bring more competition between these newer, modern players and the scene depending on years-old flaws. Our 2021 data shows the dominance of the conservative groups but could also hint at the improvements in the new IoT devices' security, which makes exploitation more time-consuming and costly.

Milan Fránik, ESET Malware Researcher

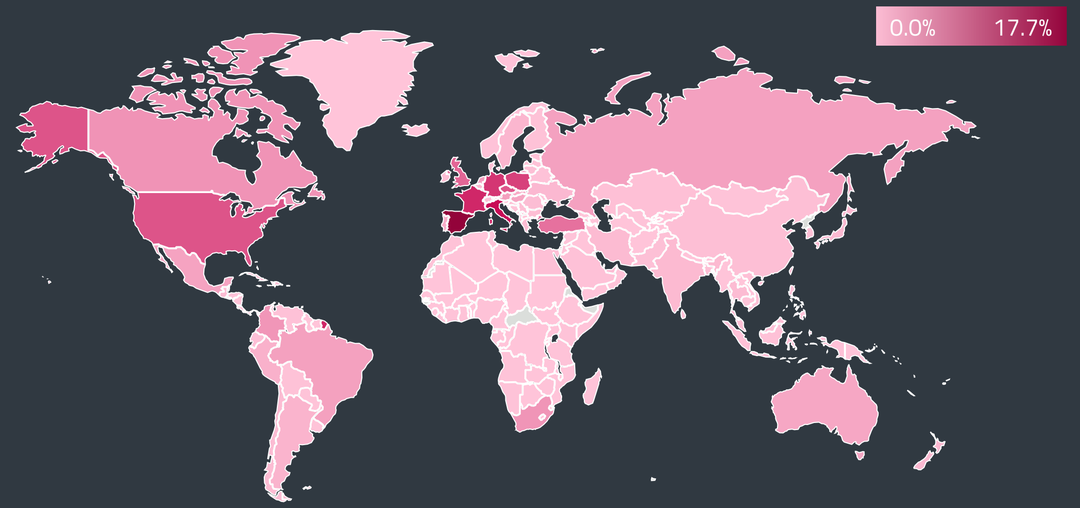
EXPLOITS

The number of RDP brute-force attacks explodes while the Log4j vulnerability becomes one of the top external intrusion vectors within a few days of being published.

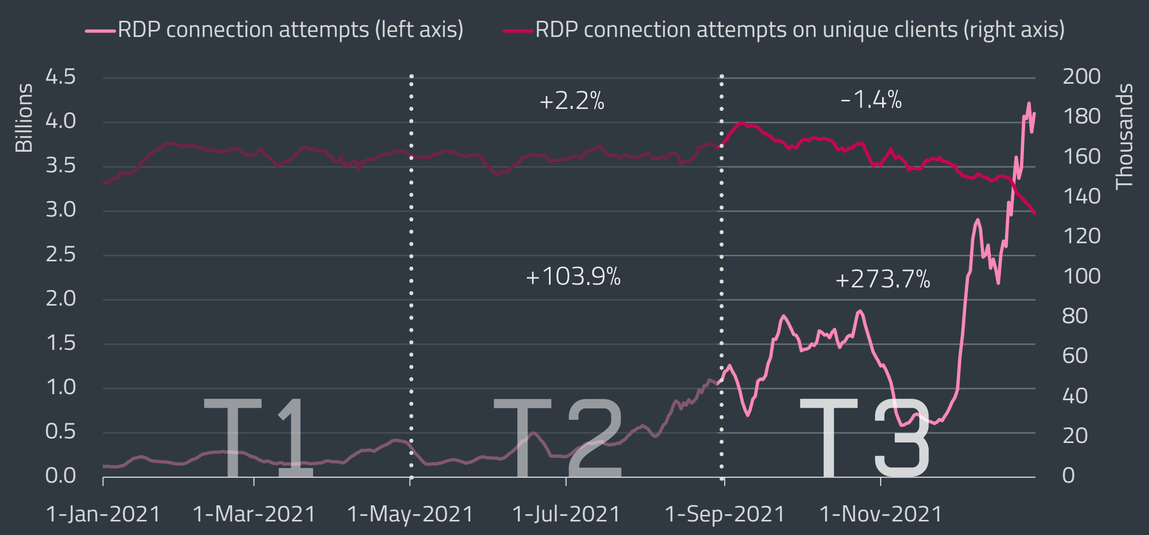
The last four months of 2021 brought a further acceleration of brute-force attacks against remote desktop protocol (RDP), with an increase of 274% from 55 billion in T2 2021 to 206 billion in T3 2021. However, the average number of unique clients that reported at least one such attack per day shrank by 5% from 161,000 in T2 2021 to 153,000 in T3 2021. In other words, the intensity of RDP password-guessing attacks is growing rapidly yet the pool of potential victims is becoming smaller. This is also reflected in the average quantity of password guesses being thrown at a unique client per day, which jumped from 2,783 in T2 2021 to 10,777 in T3 2021.

Looking at the T3 2021 trendline of RDP attack attempts, the seven-day averages were above 1.5 billion for most of September and October, followed by a calmer period in November, where detection averages dropped to the 0.5 –1 billion territory. The most intense period came in the last weeks of T3 2021, when the seven-day averages broke all previous records, passing the 4 billion mark.

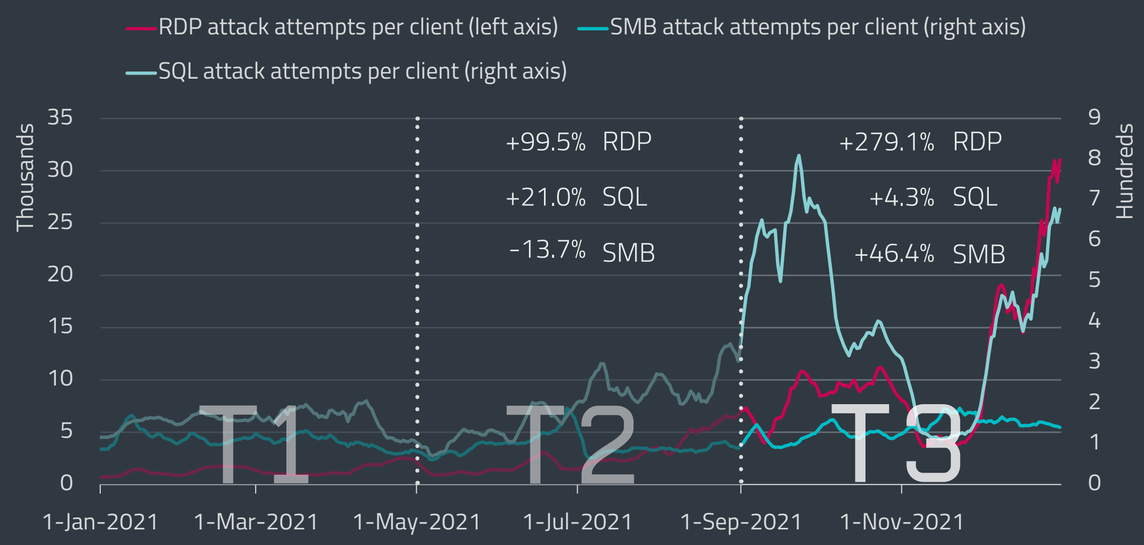
The year-over-year comparison of RDP attacks shows an even more alarming trend. While 2020 was marked by chaos, lockdowns and a hasty transition to remote work that left many RDP services exposed, it created the opportunity for "only" 29 billion malicious password guesses. According to ESET telemetry, this number exploded in 2021, closing the year with 288 billion RDP attacks, an almost tenfold increase in absolute numbers (a YoY increase of 897%).



Global distribution of RDP password guessing attack attempts in 2021



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



Trends of RDP, SMB and SQL attack attempts per client in 2021, seven-day moving average

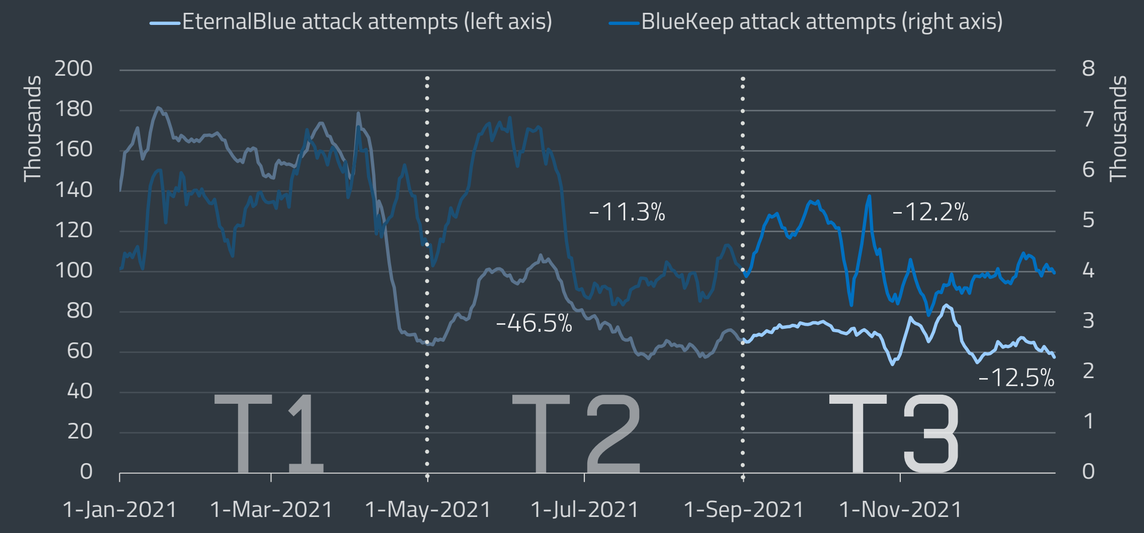
The countries that saw the most malicious RDP password guesses in 2021 were Spain with 51 billion, Italy with 25 billion, France with 21 billion, Germany with 19 billion and Poland with 18 billion.

T3 2021 brought increased malicious activity on other fronts, with notable growth of password-guessing attacks aimed at public-facing SQL and SMB services.

ESET telemetry reported 2 billion brute-force attack attempts against SQL services in T3 2021, compared to 908 million seen in T2 – an increase of 124%. Correspondingly, the average number of malicious guesses that each unique client had to face per day more than doubled from 194 in T2 to 391 in T3.

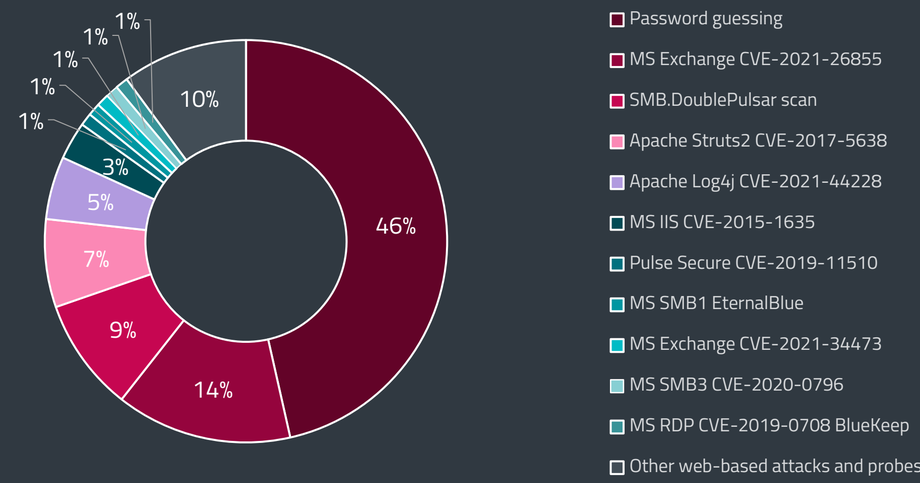
After decreasing for the first eight months of 2021, SMB brute-force attacks saw a turnaround in T3 2021 with a 63% increase and 402 million blocked attempts compared to 246 million in T2. The average number of malicious guesses thrown against a unique client per day went up by 45% from 96 to 139.

A bit of good news brought by T3 2021 is related to the EternalBlue exploit detections and attempts to misuse the BlueKeep vulnerability. As reported in previous Threat Reports, both these vectors have been declining throughout 2021 with T3 cementing the trend further by shaving off an additional 13% of EternalBlue detections and 12% of BlueKeep detections. On top of that, part of the detections may have been caused by legitimate pentesting.



Trends of EternalBlue and BlueKeep attack attempts in 2021, seven-day moving average

Looking at the external network intrusion vectors, ESET detection data from 2021 confirms that password guessing was by far the most common "weapon of choice". At least one such attack in 2021 was detected by 46% of reporting clients.



External network intrusion vectors reported by unique clients in 2021

TRENDS & OUTLOOK

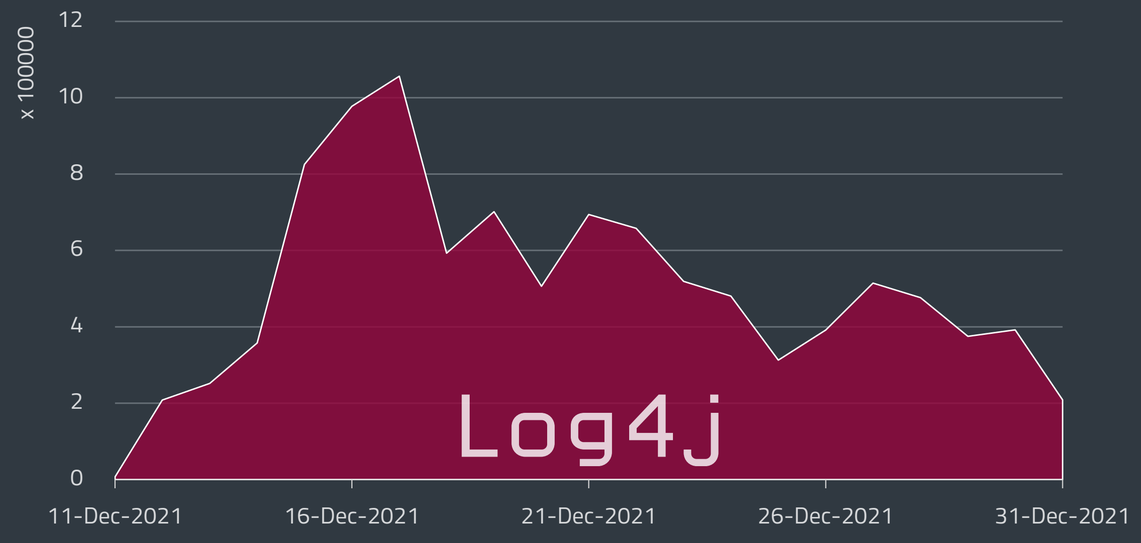
Our data shows that password guessing is becoming extremely popular, almost as if feeding off the information published. Interestingly, in 2021 Italy and Spain made it to the top of the RDP target list. The reason for this is difficult to pinpoint, but our hypothesis is that some entities in these states keep potentially valuable systems exposed to the internet attracting the attention of criminals.

As at every end of the year, in 2021 defenders along with other employees use their days off around Christmas. What made things different this year was the Log4j vulnerability, which presented further workload for IT teams – sending them scrambling to find and patch the flaw in their systems, while facing an exploding number of password-guessing attacks against any exposed service.

If 2021 trends persist, 2022 will bring further growth of detected RDP brute-force attack attempts and hit each unique client with increasing intensity. The detection dynamics from the past two years also suggest that the attackers tend to ramp up password-guessing toward the end of the year.

As for the Log4Shell exploit, it is here to stay in 2022. Similar to other well-known attack vectors – such as ProxyLogon or EternalBlue – it will become a part of security testing suites. This will contribute to the recurring detections seen by our systems along with actual malicious attempts to compromise systems.

Ladislav Janko, ESET Senior Malware Researcher



Log4j exploitation attempt trend in 2021

The second most frequent attack avenue this year was the vulnerability chain in Microsoft Exchange known as ProxyLogon (CVE-2021-26855), reported by 14% of unique clients. Apart from the *10 APT groups* [29] that abused the flaw around the time it became public, in T3 ESET researchers identified another – previously unknown – cyberespionage group that was using it, which we named *FamousSparrow* [13]. Interestingly, ProxyLogon's "younger sibling" named *ProxyShell*, first publicly described in August 2021 (CVE-2021-34473), was probed on 1% of unique reporting clients.

T3 2021 saw a rise of another interesting newcomer among the external network attack vectors – a critical vulnerability in a Java-based Apache code library called Log4j. It was publicly disclosed on December 10 and scored a perfect 10 out of 10 on the *CVSS* [154] scale. Due to the wide usage of this open-source library in products, services and software components, *state actors* [155] and *cybercriminals* [156] – including *ransomware gangs* [87] – instantly started exploiting it.

ESET's detection engine has been blocking these attack attempts since December 11, less than 24 hours after the Log4j CVE was publicly released. Interestingly, despite the attack vector being known for only a fraction of the year, many unique clients have seen at least one attempt to exploit it. Counting those instances, Log4j attacks made their way into ESET's 2021 top 10, landing in fifth place with 5%.

Countries with the most unique clients reporting Log4j exploitation attempts were the United States with 37%, followed by the United Kingdom with 12% and the Netherlands with 8%.

ESET RESEARCH CONTRIBUTIONS

Latest engagements and achievements of ESET Research experts

UPCOMING PRESENTATIONS

RSA Conference 2022

ESPecter: Previously undocumented real-world UEFI bootkit persisting on ESP [157]

This session by ESET head of threat research Jean-Ian Boutin and ESET malware researcher Martin Smolár will describe ESET's recent discovery, ESPecter – a previously undocumented real-world UEFI bootkit persisting on the EFI System Partition (ESP). ESET Research traced the roots of this threat back to at least 2012, previously operating as a bootkit for legacy BIOS systems. Despite its long existence, its operations and upgrade to UEFI went unnoticed and had not previously been documented. This session raises awareness of UEFI threats affecting the ESP and provides guidance and resources for defenders to help secure their pre-OS environments. Jean-Ian and Martin's analysis of this previously unknown, real-world UEFI ESP bootkit will help attendees understand details of the techniques used by these threats. Although UEFI threats are very rare, ESET's recent discovery of ESPecter shows they are definitely not mere specters.

SeQCure

Disclosure of vulnerabilities: A challenge even in 2022 [158]

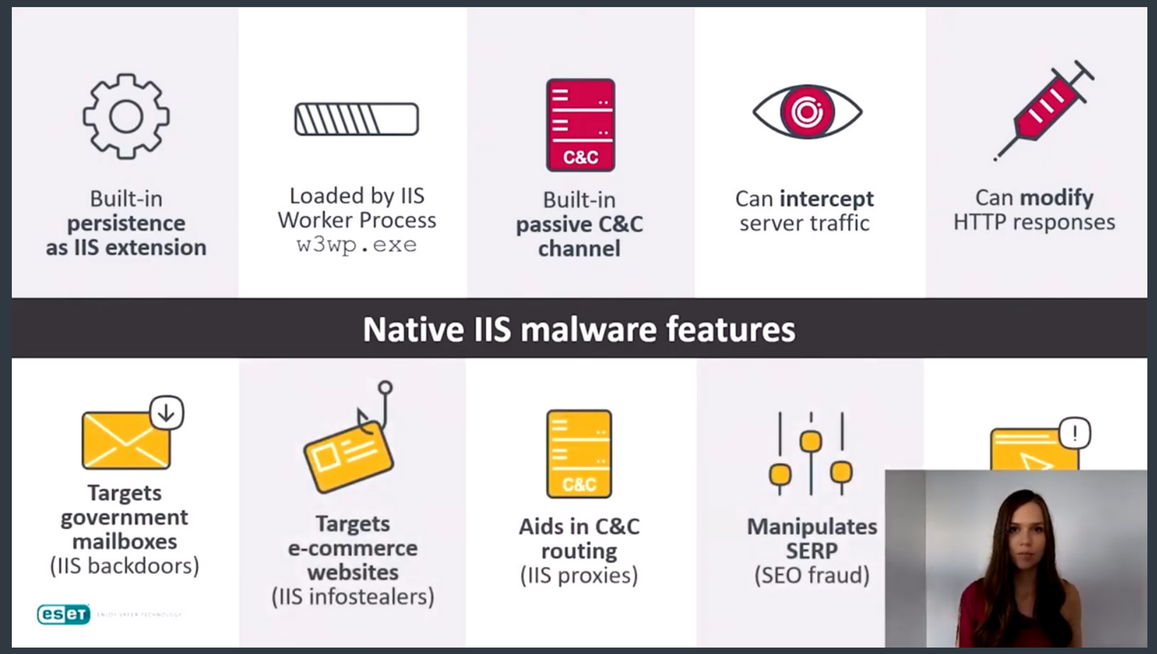
Finding vulnerabilities is not inherently associated with being a malware researcher. Yet ESET researchers regularly expose different types of vulnerabilities in the course of their work and actively participate in the coordinated disclosure process. This presentation by Alexis Dorais-Joncas, who leads the ESET security intelligence team, and ESET malware researcher Mathieu Tartare, will explain how malware research can lead to the discovery of vulnerabilities. Throughout the presentation of real-world case studies, Alexis and Mathieu will detail the different types of vulnerabilities that are most frequently discovered, how the disclosure process works, and the lessons that were learned. Among the presented case studies will be vulnerabilities in the Microsoft Office suite (CVE-2017-0262 and CVE-2017-0263), various detections in compromised third-party infrastructure used in supply-chain attacks, and the case of Quebec vaccine proof app VaxiCode Verif.

DELIVERED PRESENTATIONS

Virus Bulletin 2021 SecTor 2021

Anatomy of native IIS malware (Virus Bulletin 2021) [159]

Many stunts, one design: A crash course in dissecting native IIS malware (SecTor 2021) [160]



In these presentations ESET malware researcher Zuzana Hromcová talked about Internet Information Services (IIS) backdoors that were being deployed via the infamous Microsoft Exchange pre-authentication RCE vulnerability chain ProxyLogon, among other methods, with government institutions included in their targets. The audience received a walk-through of the essentials of reverse-engineering native IIS malware: dissecting its architecture, module classes, RegisterModule entry point, request-processing pipeline hooks, and malicious event handlers. The presentation also discussed parsing and processing HTTP requests, modifying responses, and clearing logs. This talk didn't focus on any single threat actor, malware family or campaign, but rather on the whole class of IIS threats – ranging from traffic redirectors to backdoors. Zuzana also shared some hands-on knowledge on how best to kick-start an analysis, test out the malware's functionalities, and search for more breeds of native IIS malware.

Virus Bulletin 2021

Sandworm: Reading the indictment between the lines [161]

During their presentation, ESET senior malware researchers Anton Cherepanov and Robert Lipovský revealed details about activity ESET Research observed back in 2019 and that they were able to link to Sandworm, arguably the most dangerous APT group. Throughout the years of its existence, this group has performed a number of notorious, destructive attacks, including the first-ever malware-driven electricity blackout (Kiev, December 2015), the costliest cyberattack ever (NotPetya), and attacks against entities that were involved in organizing the 2018 Winter Olympics in Pyeongchang (Olympic Destroyer). ESET Research was able to establish a link between the 2019 activity and Sandworm thanks to the details published in the 2020 US Department of Justice indictment against six computer hackers who allegedly prepared and conducted the Sandworm attacks. Some of the details presented in the indictment were already known, but some of them were published for the first time in the indictment. This presentation revealed details about that activity and provided an in-depth analysis of the malware. In addition, Anton and Robert discussed detection opportunities for the techniques used by this malware.

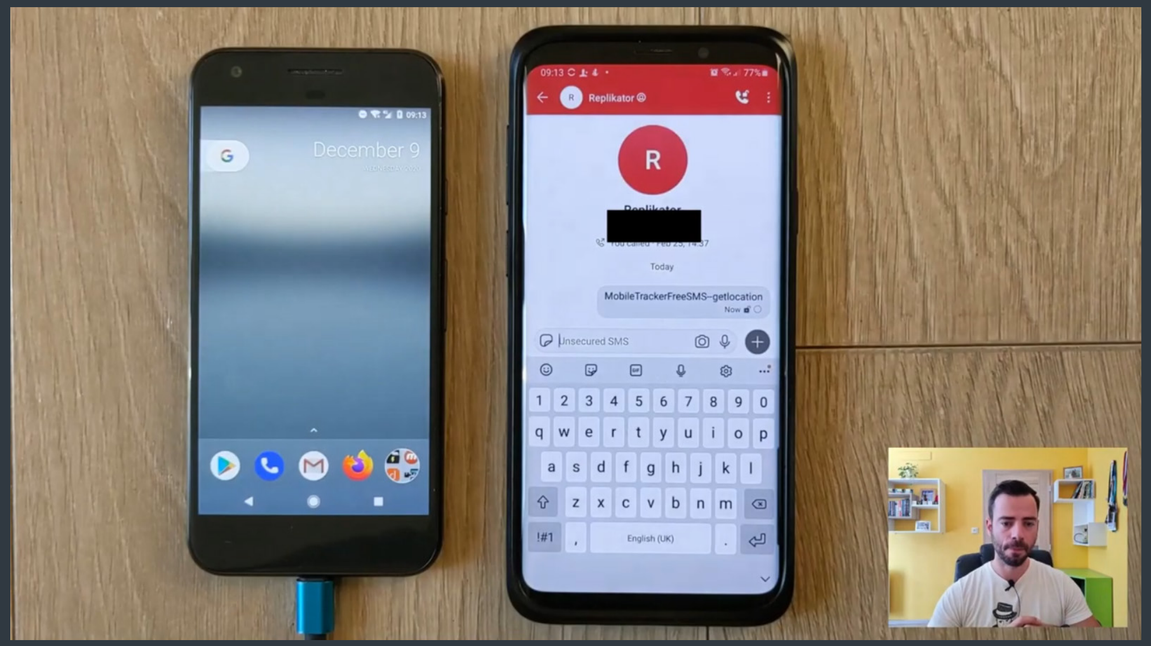
Virus Bulletin 2021 DefCamp 2021 Ekoparty 2021 The Hack Summit 2021

Security: The hidden cost of Android stalkerware (Virus Bulletin 2021) [162]

Vulnerabilities discovered in Android stalkerware apps (DefCamp 2021) [163]

Vulnerabilities discovered in Android stalkerware (Ekoparty 2021) [164]

Vulnerabilities discovered in Android stalkerware apps (The Hack Summit 2021) [165]



ESET malware researcher Lukáš Štefanko presented his 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. During his presentation, Lukáš covered over 80 different families of Android stalkerware and focused on security analysis of their code.

Virus Bulletin 2021

"Fool Us!", or is it "Us Fools!"? ... 11 "Fools" years later... [166]

ESET senior research fellow Righard Zwienenberg has revisited his "Attacks from the inside..." presentation that was delivered at the Virus Bulletin 2010 conference. And just like 11 years ago, it was co-presented with Eddy Willems, global security officer from G DATA. In 2010, Righard and Eddy outlined and provided examples of a variety of possible scenarios for internal attacks. They concluded with a top nine problems of "in-the-cloud services". In 2021, they were both surprised to find that their predictions and warnings seemed to have been completely ignored, with all of the identified problems having materialized. In this presentation, Eddy and Righard "relived" their 2010 presentation, while illustrating with recent examples that their message and warnings are as current and relevant now as they were then. Nothing has changed, except that "internal attacks" now also come from the outside.

CYBERWARCON 2021

Strategic web compromises in the Middle East with a pinch of Candiru [167]

Over the past two years, ESET researchers uncovered strategic web compromises on more than twenty different high-profile websites mainly located in the Middle East. Targets include Middle Eastern governments and media, European and African defense contractors, a media outlet based in the United Kingdom and a medical conference in Germany. In this presentation, ESET malware researcher Matthieu Faou showed how the spyware firm Candiru fits into the whole picture and provided a breakdown of the targeting, including the switch in 2021 to a focus on Yemen and entities linked to the war in Yemen. He also presented a technical analysis of the scripts used to gather information on visitors to the compromised websites. In addition, he also showed the attendees how the infrastructure was improved over the months to make the tracking more difficult and to prevent researchers from grabbing the exploits and payloads.

BSides Montreal

Poking around at scale: One year of scanning the internet [168]

When analyzing malware, researchers often find ways to remotely identify whether a system is compromised, especially when looking at server-side threats. This requires thoroughly reverse engineering the network protocol of whatever malware is in use to understand how to properly trigger a behavior or response that could be used as a fingerprint. This presentation by ESET senior malware researcher Marc-Étienne Léveillé explained how ESET researchers built their own internet scanner from scratch and overcame the challenges of performing internet-wide scans. Marc-Étienne also presented cases where these scans revealed needles in haystacks, based on in-the-wild malware that ESET researchers had analyzed, and provided tips for anyone who wants to perform scans at scale.

Copenhagen CyberCrime Conference

Android employee monitoring apps: Not all of them protect the business [169]

In his presentation about Android employee monitoring apps, ESET malware researcher Lukáš Štefanko discussed the results of his security analyses of over 80 of the most popular vendors of these apps that are known to monitor their users and gather, transmit and store users' personally identifiable information (PII). Considering employees use smartphones not only for work-related, but also personal, tasks, this means that data leaks might impact both parties significantly. Lukáš has shown that vulnerabilities discovered in these products, once exploited, could result in serious issues such as account takeover, user-data leaks, credential leaks over the network and on-device, admin console access without restriction, or even using fabricated data to frame the monitored person. This talk has provided the most accurate picture so far of these apps, their security issues, and the developers' lack of responsibility to their clients and to their clients' data.

AVAR 2021 Virtual

FontOnLake [170]

FontOnLake is a previously unknown malware family targeting systems running Linux. The first instance was spotted in 2020 and several other samples have been discovered since. The group's tools had not been fully described before and their sneaky nature, in combination with advanced design and low prevalence, suggest that they might be used in targeted attacks. Locations of its C&C servers and the countries from which the samples were uploaded to VirusTotal indicate that the group operates at least in Southeast Asia. This presentation by ESET malware researcher Vladislav Hrčka described custom components developed by the group and the way they cooperate.

WHITE PAPERS

Jumping the air gap: 15 years of nation-state effort [171]

This white paper by Alexis Dorais-Joncas, who leads the ESET security intelligence team, and ESET security intelligence analyst Facundo Munõz, describes how malware frameworks targeting air-gapped networks operate, and provides a side-by-side comparison of their most important tactics, techniques and procedures (TTPs). ESET researchers also propose a series of detection and mitigation techniques to protect air-gapped networks from the main techniques used by all the malicious frameworks publicly known to date.

FontOnLake: Previously unknown malware family targeting Linux [172]

ESET researchers uncovered a previously unknown malware family that uses well-designed, custom modules to target Linux systems; we named it FontOnLake. This white paper by ESET malware researcher Vladislav Hrčka describes modules used by this malware family, which are constantly under development, provide the operators with remote access to victimized systems, collect login credentials, and serve as a proxy server.

MITRE ATT&CK EVALUATIONS

ESET has participated in the latest round of evaluations that have focused on TTPs applied by the Wizard Spider and Sandworm APT groups – *Carbanak/Fin7 MITRE Engenuity ATT&CK evaluation* [173]. Results from this assessment will be announced in upcoming months but based on preliminary results, ESET continues to maintain solid visibility into adversary behavior behind ransomware and other malicious tools used by these groups.

Wizard Spider has been conducting ransomware campaigns using infamous tools like TrickBot, a botnet that has infected over a million computers. In 2020, ESET researchers participated in a global operation to *disrupt this botnet* [174] and now continue to monitor 50 new variants of this threat, new TrickBot modules, and new ransomware used by this group.

Sandworm is one of the most dangerous APT groups in existence. ESET's outstanding visibility into this group is demonstrated by high-profile research analyzing the *attacks against the Ukrainian power grid* [175], cyberattacks on *high-value targets in the Ukrainian financial sector* [176], the *supply-chain attacks against Ukraine* [177], and the devastating *NotPetya ransomware* [178], just to name a few.

ESET's research into other APT groups like Turla, Gamaredon, OceanLotus and many others has directly or indirectly helped many organizations and nation-states successfully thwart potential attacks by providing much-needed visibility into TTPs used by those very same groups for economic, espionage, geopolitical, or criminal purposes.

ESET's research also continues to be one of the most referenced intelligence sources of tactics and techniques for *MITRE ATT&CK® Matrix for Enterprise* [179], which now covers network infrastructure devices, container technologies and platforms like Windows, macOS, Linux and cloud (Azure AD, Office 365, Google Workspace, etc.).

OTHER CONTRIBUTIONS

Support of SAFER – a new security group founded to help protect the research and education sector

Nominated by the company, ESET senior malware researcher Marc-Étienne Léveillé became a founding member of the *Security Assistance For Education & Research* [180] (SAFER) Trust Group, a new organization of independent security experts who have united to better secure the research and education sector (R&E) against global threats. ESET, as the only organization from the private sector, joins a number of public sector organizations in support of the founding members, who will contribute their expertise to protect and further support safer education and research.

SAFER is a new organization focused on fighting cyberthreats to academia, research, and the education sector globally. It has been founded by security experts supported by their respective organizations, including ESET, and aims to offer a truly global incident response capability to research and education organizations under attack.

Backed by ESET's malware research team, Marc-Étienne Léveillé collaborated with the R&E sector during his extensive research on *Windigo* [181] and *Kobalos* [182]. The Operation Windigo research paper was awarded the inaugural Péter Szőr Award at the Virus Bulletin Conference in 2014. Ironically, the research paper was also recognized by the creators of the malware behind Operation Windigo, who said "Good job, ESET!" within their code one month after that research was published.

Kobalos is a Linux backdoor that targets supercomputers, especially those used in academia and scientific institutions. The research ESET pursued on Kobalos was done in collaboration with *CERN* [183], another organization supporting SAFER.

CREDITS

Team

Peter Stančík, Team Lead
Klára Kobáková, Managing Editor

Aryeh Goretsky
Branislav Ondrášik
Bruce P. Burrell
Hana Matušková
Nick FitzGerald
Ondrej Kubovič
Zuzana Pardubská

Foreword

Roman Kováč, Chief Research Officer

Contributors

Adam Burgher
Anton Cherepanov
Dušan Lacika
Igor Kabina
Ján Šugarek
Jean-Ian Boutin
Jiří Kropáč
Juraj Jánošík
Kamil Sadkowski
Ladislav Janko
Lukáš Štefanko
Martin Červeň
Martin Lackovič
Martin Smolár
Mathieu Tartare
Matthieu Faou
Michal Malík
Miloš Čermák
Milan Fránik
Miroslav Legéň
Patrik Sučanský
Robert Kapp
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 detections regardless of the targeted platform.

Further, the data excludes detections of *potentially unwanted applications* [184], *potentially unsafe applications* [185] and adware, except where noted in the more detailed, platform-specific sections and in the Cryptocurrency threats section.

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

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://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/

[2] https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list

[3] https://blog.google/threat-analysis-group/how-we-protect-users-0-day-attacks/

[4] https://www.microsoft.com/security/blog/2021/07/15/protecting-customers-from-a-private-sector-offensive-actor-using-0-day-exploits-and-devilstongue-malware/

[5] https://www.welivesecurity.com/2021/11/16/strategic-web-compromises-middle-east-pinch-candiru/

[6] https://www.welivesecurity.com/2021/10/05/uefi-threats-moving-esp-introducing-especter-bootkit/

[7] https://www.welivesecurity.com/2021/10/27/wslink-unique-undocumented-malicious-loader-runs-server/

[8] https://github.com/eset/wslink-client

[9] https://www.welivesecurity.com/2021/10/07/fontonlake-previously-unknown-malware-family-targeting-linux/

[10] https://www.welivesecurity.com/2021/09/17/numando-latam-banking-trojan/

[11] https://www.welivesecurity.com/2021/12/15/dirty-dozen-latin-america-amavaldo-zumanek/

[12] https://www.welivesecurity.com/2021/12/01/jumping-air-gap-15-years-nation-state-effort/

[13] https://www.welivesecurity.com/2021/09/23/famoussparrow-suspicious-hotel-guest/

[14] https://www.welivesecurity.com/2021/09/07/bladehawk-android-espionage-kurdish/

[15] https://twitter.com/ESETresearch/status/1458438155149922312

[16] https://attack.mitre.org/groups/G0049/

[17] https://www.secureworks.com/blog/lyceum-takes-center-stage-in-middle-east-campaign

[18] https://www.clearskysec.com/wp-content/uploads/2021/08/Siamesekitten.pdf

[19] https://www.teamviewer.com/en/remote-management/

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

[21] https://malware.news/t/deep-dive-into-the-lyceum-danbot-malware/36216

[22] https://securelist.com/apt-trends-report-q1-2021/101967/

[23] https://www.mandiant.com/resources/hard-pass-declining-apt34-invite-to-join-their-professional-network

[24] https://unit42.paloaltonetworks.com/unit42-oilrig-deploys-alma-communicator-dns-tunneling-trojan/

[25] https://unit42.paloaltonetworks.com/unit42-oilrig-uses-ismdoor-variant-possibly-linked-greenbug-threat-group/

[26] https://unit42.paloaltonetworks.com/behind-the-scenes-with-oilrig/

[27] https://unit42.paloaltonetworks.com/oilrig-novel-c2-channel-steganography/

[28] https://github.com/eset/malware-ioc/tree/master/quarterly_reports/2021_T3

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

[30] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34473

[31] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34523

[32] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-31207

[33] https://www.blackhat.com/us-21/briefings/schedule/index.html#proxylogon-is-just-the-tip-of-the-iceberg-a-new-attack-surface-on-microsoft-exchange-server-23442

[34] https://www.youtube.com/watch?v=5mqid-7zp8k

[35] https://blog.orange.tw/2021/08/proxyshell-a-new-attack-surface-on-ms-exchange-part-3.html

[36] https://support.microsoft.com/en-us/topic/description-of-the-security-update-for-microsoft-exchange-server-2019-2016-and-2013-april-13-2021-kb5001779-8e08f3b3-fc7b-466c-bbb7-5d5aa16ef064

[37] https://support.microsoft.com/en-us/topic/description-of-the-security-update-for-microsoft-exchange-server-2019-2016-and-2013-may-11-2021-kb5003435-028bd051-b2f1-4310-8f35-c41c9ce5a2f1

[38] https://www.cisa.gov/uscert/ncas/current-activity/2021/08/21/

urgent-protect-against-active-exploitation-proxyshell

[39] https://twitter.com/GossiTheDog/status/1422178411385065476

[40] https://twitter.com/buffaloverflow/status/1425831100157349890

[41] https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Operation_Ghost_Dukes.pdf

[42] https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-011/

[43] https://docs.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/ms537628%28v=vs.85%29

[44] http://www.joeware.net/freetools/tools/adfind/

[45] https://github.com/BloodHoundAD/BloodHound

[46] https://github.com/checkymander/Sharp-SMBExec

[47] https://github.com/tevora-threat/SharpView

[48] https://github.com/GhostPack/Rubeus

[49] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36934

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

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

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

[53] https://www.trendmicro.com/en_us/research/21/k/qakbot-loader-returns-with-new-techniques-and-tools.html

[54] https://securityintelligence.com/posts/trickbot-gang-doubles-down-enterprise-infection/

[55] https://www.bleepingcomputer.com/news/security/trickbot-teams-up-with-shatak-phishers-for-conti-ransomware-attacks/

[56] https://www.bleepingcomputer.com/news/security/emotet-malware-is-back-and-rebuilding-its-botnet-via-trickbot/

[57] https://www.bleepingcomputer.com/news/security/ransomware-encrypts-south-africas-entire-dept-of-justice-network/

[58] https://www.bleepingcomputer.com/download/hidden-tear-decrypter/

[59] https://twitter.com/darktracer_int/status/1465536251961163776

[60] https://twitter.com/teachemtechy/status/1464317136944435209?s=20

[61] https://www.bleepingcomputer.com/news/security/us-targets-darkside-ransomware-and-its-rebrands-with-10-million-reward/

[62] https://www.interpol.int/en/News-and-Events/News/2021/Ransomware-gang-arrested-in-Ukraine

[63] https://www.europol.europa.eu/media-press/newsroom/news/five-affiliates-to-sodinokibi/revil-unplugged

[64] https://www.interpol.int/News-and-Events/News/2021/INTERPOL-led-operation-takes-down-prolific-cybercrime-ring

[65] https://www.bleepingcomputer.com/news/security/global-accellion-data-breaches-linked-to-clop-ransomware-gang/

[66] https://www.europol.europa.eu/media-press/newsroom/news/12-targeted-for-involvement-in-ransomware-attacks-against-critical-infrastructure

[67] https://www.bleepingcomputer.com/news/security/russia-arrests-revil-ransomware-gang-members-seize-66-million/

[68] https://www.zdnet.com/article/the-white-house-is-having-a-big-meeting-about-fighting-ransomware-it-didnt-invite-russia/

[69] https://www.zdnet.com/article/ransomware-law-would-require-victims-to-disclose-ransom-payments-within-48-hours/

[70] https://www.zdnet.com/article/bitdefender-releases-universal-decryptor-for-revilsodinokibi-victims-hit-before-july-13/

[71] https://www.bleepingcomputer.com/news/security/blackbyte-ransomware-decryptor-released-to-recover-files-for-free/

[72] https://therecord.media/free-decrypters-released-for-atomsilo-babuk-and-lockfile-ransomware-strains/

[73] https://www.bleepingcomputer.com/news/security/blackmatter-ransomware-victims-quietly-helped-using-secret-decryptor/

[74] https://www.bleepingcomputer.com/news/security/ransomware-gang-coughs-up-decryptor-after-realizing-they-hit-the-police/

[75] https://www.bleepingcomputer.com/news/security/new-atom-silo-ransomware-targets-vulnerable-confluence-servers/

[76] https://www.bleepingcomputer.com/news/security/new-yanluowang-ransomware-used-in-targeted-enterprise-attacks/

[77] https://www.bleepingcomputer.com/news/security/evil-corp-demands-40-million-in-new-macaw-ransomware-attacks/

[78] https://www.bleepingcomputer.com/news/security/new-karma-ransomware-group-likely-a-nemty-rebrand/

[79] https://www.bleepingcomputer.com/news/security/hive-ransomware-enters-big-league-with-hundreds-breached-in-four-months/

[80] https://www.bleepingcomputer.com/news/security/mediamarkt-hit-by-hive-ransomware-initial-240-million-ransom/

[81] https://www.bleepingcomputer.com/news/security/second-farming-cooperative-shut-down-by-ransomware-this-week/

[82] https://www.bleepingcomputer.com/news/security/us-farmer-cooperative-hit-by-59m-blackmatter-ransomware-attack/

[83] https://www.bleepingcomputer.com/news/security/wind-turbine-giant-vestas-data-compromised-in-cyberattack/

[84] https://www.bleepingcomputer.com/news/security/jvckenwood-hit-by-conti-ransomware-claiming-theft-of-15tb-data/?s=20

[85] https://www.bleepingcomputer.com/news/security/olympus-us-systems-hit-by-cyberattack-over-the-weekend/

[86] https://twitter.com/BrettCallow/status/1453391567163559941?s=20%3B

[87] https://thehackernews.com/2021/12/hackers-exploit-log4j-vulnerability-to.html

[88] https://www.bleepingcomputer.com/news/security/conti-ransomware-uses-log4j-bug-to-hack-vmware-vcenter-servers/

[89] https://www.bleepingcomputer.com/news/security/tellyouthepass-ransomware-revived-in-linux-windows-log4j-attacks/

[90] https://www.bleepingcomputer.com/news/security/clop-gang-exploiting-solarwinds-serv-u-flaw-in-ransomware-attacks/

[91] https://www.bleepingcomputer.com/news/security/conti-ransomware-now-hacking-exchange-servers-with-proxyshell-exploits/

[92] https://www.fincen.gov/sites/default/files/shared/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf

[93] https://ransomwhe.re/

[94] https://www.documentcloud.org/documents/21072978-kidd-amended-complaint

[95] https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116

[96] https://www.zdnet.com/article/first-death-reported-following-a-ransomware-attack-on-a-german-hospital/

[97] https://www.bleepingcomputer.com/news/security/emotet-botnet-comeback-orchestrated-by-conti-ransomware-gang/

[98] https://twitter.com/ESETresearch/status/1463500831236534275?s=20

[99] https://twitter.com/ESETresearch/status/1469283535559303176

[100] https://twitter.com/Cryptolaemus1/status/1468266929014157316

[101] https://www.bleepingcomputer.com/news/security/emotet-now-drops-cobalt-strike-fast-forwards-ransomware-attacks/

[102] https://www.bleepingcomputer.com/news/security/russian-hacking-group-uses-new-stealthy-ceeloader-malware/

[103] https://www.bloomberg.com/news/articles/2021-09-24/china-deems-all-crypto-related-transactions-illegal-in-crackdown

[104] https://www.bleepingcomputer.com/news/security/hackers-rob-thousands-of-coinbase-customers-using-mfa-flaw/

[105] https://thehackernews.com/2021/12/hackers-steal-200-million-worth-of.html

[106] https://trends.google.com/trends/explore?date=2021-01-01%202021-12-31&q=NFT

[107] https://www.bleepingcomputer.com/news/security/opensea-nft-platform-bugs-let-hackers-steal-crypto-wallets/

[108] https://www.bleepingcomputer.com/news/security/discord-malware-campaign-targets-crypto-and-nft-communities/

[109] https://techcrunch.com/2022/01/04/nft-kingpin-opensea-lands-13-3b-valuation-in-300m-raise-from-paradigm-and-coatue/

[110] https://www.welivesecurity.com/2020/04/30/new-sextortion-scam-claims-know-your-password/

[111] https://www.welivesecurity.com/wp-content/uploads/2021/09/eset_threat_report_t22021.pdf#page=30

[112] https://www.threatfabric.com/blogs/deceive-the-heavens-to-cross-the-sea.html

[113] https://www.threatfabric.com/blogs/ermac-another-cerberus-reborn.html

[114] https://research.checkpoint.com/2021/pixstealer-a-new-wave-of-android-banking-trojans-abusing-accessibility-services/

[115] https://www.cleafy.com/cleafy-labs/sharkbot-a-new-generation-of-android-trojan-is-targeting-banks-in-europe

[116] https://twitter.com/ESETresearch/status/1443131537629884416

[117] https://resources.lookout.com/blog/lookout-discovers-global-rooting-malware-campaign

[118] https://www.welivesecurity.com/2021/08/31/flaw-quebec-vaccine-passport-vaxicode-verif-analysis/

[119] https://techcrunch.com/2021/10/27/docket-vaccine-records-covid-security/

[120] https://nethemba.com/sk/kriticka-zranitelnost-v-aplikacii-moje-ezdravie-unik-databazy-pacientov-testovanych-na-covid-19/

[121] https://www.welivesecurity.com/2021/10/06/google-turn-on-2fa-default-150-million-users-2-million-youtubers/

[122] https://krebsonsecurity.com/2021/03/can-we-stop-pretending-sms-is-secure-now/

[123] https://www.vice.com/en/article/z3xpm8/company-that-routes-billions-of-text-messages-quietly-says-it-was-hacked

[124] https://android-developers.googleblog.com/2021/09/making-permissions-auto-reset-available.html

[125] https://twitter.com/Confiantintel/status/1451641996800454660

[126] https://twitter.com/MsftSecIntel/status/1451279679059488773

[127] https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/

[128] https://citizenlab.ca/category/research/targeted-threats/

[129] https://www.newsweek.com/polish-leader-admits-country-uses-nso-group-spyware-denies-targeting-government-critics-1666850

[130] https://www.dw.com/en/hungary-admits-to-using-nso-groups-pegasus-spyware/a-59726217

[131] https://www.zeit.de/politik/deutschland/2021-09/spionagesoftware-pegasus-nso-israel-bundeskriminalamt-kauf-innenausschuss-bundestag-unterrichtung

[132] https://citizenlab.ca/2022/01/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware/

[133] https://www.reuters.com/technology/exclusive-us-state-department-phones-hacked-with-israeli-company-spyware-sources-2021-12-03/

[134] https://www.apple.com/sk/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/

[135] https://www.nytimes.com/2019/10/29/technology/whatsapp-nso-lawsuit.html

[136] https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/

[137] https://about.fb.com/news/2021/12/taking-action-against-surveillance-for-hire/

[138] https://www.welivesecurity.com/2018/03/09/new-traces-hacking-team-wild/

[139] https://www.welivesecurity.com/2018/01/23/guide-makes-possible-peek-finfisher/

[140] https://twitter.com/CodeColorist

[141] https://blog.google/threat-analysis-group/analyzing-watering-hole-campaign-using-macos-exploits/

[142] https://arstechnica.com/gadgets/2021/11/psa-apple-isnt-actually-patching-all-the-security-holes-in-older-versions-of-macos/

[143] https://www.welivesecurity.com/2021/09/23/bug-macos-finder-remote-code-execution/

[144] https://www.microsoft.com/security/blog/2021/10/28/microsoft-finds-new-macos-vulnerability-shrootless-that-could-bypass-system-integrity-protection/

[145] https://twitter.com/360Netlab/status/1420390398825058313

[146] https://www.welivesecurity.com/wp-content/uploads/2021/09/eset_threat_report_t22021.pdf#page=36

[147] https://en.wikipedia.org/wiki/Mirai_%28malware%29

[148] https://twitter.com/ESETresearch/status/1440052837820428298?s=20

[149] https://blog.wiz.io/secret-agent-exposes-azure-customers-to-unauthorized-code-execution/

[150] https://blog.netlab.360.com/threat-alert-log4j-vulnerability-has-been-adopted-by-two-linux-botnets/

[151] https://arxiv.org/pdf/2112.10974.pdf

[152] https://www.darkreading.com/endpoint/iot-nutrition-labels-aim-to-put-security-on-display

[153] https://www.bleepingcomputer.com/news/security/ukrainian-police-arrest-ddos-operator-controlling-100-000-bots/

[154] https://www.first.org/cvss/

[155] https://www.securityweek.com/chinese-iranian-state-hackers-exploiting-log4j-flaw-mandiant

[156] https://www.bleepingcomputer.com/news/security/log4j-vulnerability-now-used-to-install-dridex-banking-malware/

[157] https://www.rsaconference.com/usa/agenda/session/ESPecter%20First%20Real-World%20UEFI%20Bootkit%20Persisting%20on%20ESP

[158] https://www.seqcure.org/en/#speakers

[159] https://vblocalhost.com/presentations/anatomy-of-native-iis-malware/

[160] https://sector.ca/sessions/many-stunts-one-design-a-crash-course-in-dissecting-native-iis-malware/

[161] https://vblocalhost.com/presentations/sandworm-reading-the-indictment-between-the-lines/

[162] https://vblocalhost.com/presentations/security-the-hidden-cost-of-android-stalkerware/

[163] https://def.camp/speaker/lukas-stefanko-2/

[164] https://www.youtube.com/watch?v=jnf8EgLwGsk

[165] https://thehacksummit.com/en/

[166] https://vblocalhost.com/presentations/fool-us-or-is-it-us-fools-11-fools-years-later/

[167] https://www.cyberwarcon.com/matthieu-faou

[168] https://bsidesmtl.ca/program

[169] https://cyberhub.dk/event/copenhagen-cybercrime-conference-2021/

[170] https://aavar.org/avar2021/index.php/fontonlake/

[171] https://www.welivesecurity.com/wp-content/uploads/2021/12/eset_jumping_the_air_gap_wp.pdf

[172] https://www.welivesecurity.com/wp-content/uploads/2021/10/eset_fontonlake.pdf

[173] https://attackevals.mitre-engenuity.org/enterprise/wizard-spider-and-sandworm/

[174] https://www.eset.com/int/about/newsroom/press-releases/research/eset-takes-part-in-global-operation-to-disrupt-trickbot-a-botnet-that-has-infected-over-a-million-c/

[175] https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/

[176] https://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks/

[177] https://www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine/

[178] https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/

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

[180] https://www.safer-trust.org/

[181] https://www.welivesecurity.com/2017/10/30/esets-research-fbi-windigo-maxim-senakh/

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

[183] https://home.cern/

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

[185] 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*.

WeLiveSecurity.com
@ESETresearch
ESET GitHub

Digital Security
Progress. Protected.

© 2022 ESET, spol. s r.o. - All rights reserved.
Trademarks used herein are trademarks or registered trademarks of ESET, spol. s r.o.
All other names and brands are registered trademarks of their respective companies.