THREAT REPORT T1 2022

WeLiveSecurity.com
@ESETresearch
ESET GitHub

ESET
Digital Security
Progress. Protected.

CONTENTS

FOREWORD

Welcome to the T1 2022 issue of the ESET Threat Report!

After more than two years of shielding from a global pandemic, we get a reward: war! Several conflicts are raging in different parts of the world, but for us, this one is different. Right across Slovakia's eastern borders, where ESET has its HQ and several offices, Ukrainians are fighting for their lives and sovereignty in this unprovoked war, facing an opponent that possesses nuclear weapons. As you will read in the following pages, Ukraine is resisting attacks not only in the physical world but also in cyberspace.

Our *Featured story* recounts various cyberattacks connected to the ongoing war that ESET researchers analyzed or helped to mitigate. This includes the resurrection of the infamous Industroyer malware, attempting to target high-voltage electrical substations.

Shortly before the Russian invasion, ESET telemetry recorded one of two sharp drops in RDP attacks. The decline in these attacks comes after two years of constant growth – and as we explain in the *Exploits* section, this turn of events might have a connection to the war in Ukraine. But even with this fall, almost 60% of incoming RDP attacks seen in T1 2022 came from Russia. Another side effect of the war: while in the past ransomware threats tended to avoid targets located in Russia, in this period, according to our telemetry, Russia was the top targeted country. We even detected lock-screen variants using the Ukrainian national salute "Slava Ukraini" (Glory to Ukraine).

Unsurprisingly, the war has also been noticeably exploited by spam and phishing threats. Immediately after the invasion on February 24, scammers started to take advantage of people trying to support Ukraine, using fictitious charities and fundraisers as lures. On that day, we detected a large spike in spam detections. We can also confirm that Emotet – the infamous malware, spread primarily through spam emails – is back after last year's takedown attempts, and has shot back up in our telemetry. Its operators spewed spam campaign after spam campaign, with Emotet detections growing by more than a hundredfold!

Our telemetry has of course seen many other threats unrelated to the Russia-Ukraine war – I invite you to read the *Statistics & Trends* section of this report to see the full picture. The past months were also full of interesting research findings. Our researchers uncovered – among other things – the abuse of kernel driver vulnerabilities; high-impact UEFI vulnerabilities; cryptocurrency malware targeting Android and iOS devices; and the campaigns of Mustang Panda, Donot Team, Winnti Group, and the TA410 APT group.

With their deep dive into Industroyer2, breaches of air-gapped networks, analyses of campaigns deployed by InvisiMole, OilRig, MuddyWater, FreshFeline, and TA410 APT groups, ESET researchers made it to the S4x22, CARO Workshop, Botconf, and NorthSec conferences – you can find wrap-ups of their talks in the final section of this report. For the upcoming months, we would like to invite you to ESET talks at RSA, REcon, Virus Bulletin, and many other conferences.

I wish you an insightful read.

Roman Kováč
ESET Chief Research Officer

EXECUTIVE SUMMARY

FEATURED STORY

Cyberattacks in Ukraine
ESET Research uncovered several new wiper attacks deployed in Ukraine and analyzed the return of the infamous Industroyer, connecting all of these attacks to the ongoing war.

APT GROUP ACTIVITY

Donot Team
ESET Research analyzed recent campaigns by the Donot Team (also known as APT-C-35 and SectorE02), which focuses on cyberespionage and targets primarily in South Asia.

Mustang Panda
ESET Research uncovered a still-ongoing cyberespionage campaign by the Mustang Panda APT group, using Hodur, a previously undocumented Korplug variant.

Winnti Group
ESET Research found new Winnti Group PipeMon variants.

TA410
ESET Research unveiled a detailed profile of TA410, a cyberespionage umbrella group loosely linked to APT10.

STATISTICS & TRENDS

Category	T3 2021/T1 2022	Key points in T1 2022
Overall threat detections	+20.1% ↑	Emotet campaigns raise overall threat activity
Infostealers	+12.0% ↑	JS/Spy.Banker aka Magecart grows more prevalent
Ransomware	-4.3% ↓	Russia increasingly targeted by ransomware
Downloaders	+121.5% ↑	Emotet launches mass-scale spam campaigns
Cryptocurrency threats	-29.3% ↓	Overall decline in cryptocurrency threat activity
Web threats	-1.8% →	Number of phishing URLs shoots up in March
Email threats	+36.8% ↑	Emotet floods inboxes with malicious documents
Android threats	+8.0% ↑	Android spyware grows more prevalent
macOS threats	-14.9% ↓	Decline in all monitored threat categories
RDP attacks	-40.8% ↓	RDP attacks see first decline since 2020

FEATURED STORY

Cyberattacks in Ukraine

ESET Research

ESET researchers have uncovered several new wiper attacks deployed in Ukraine and analyzed the return of the infamous Industroyer, connecting all of these attacks to the ongoing war.

On the eve of the Russian invasion of Ukraine, ESET researchers discovered new data-wiper malware deployed in Ukraine on that day, which was installed on hundreds of machines in at least five organizations in that country. The attack came just hours after a series of distributed denial-of-service (DDoS) onslaughts knocked several important Ukrainian websites offline. The data wiper was first spotted just before 17:00 local time (15:00 UTC), February 23. ESET researchers stayed up late analyzing the malware and published the discovery *on Twitter* [1], not knowing what global media would cover the next morning as breaking news.

ESET researchers assess with high confidence that the affected organizations were compromised well in advance of the wiper's deployment based on these three findings:

- The attackers used a genuine code-signing certificate issued to a company called Hermetica Digital Ltd., issued on April 13, 2021. That is also the reason why ESET decided to name the malware *HermeticWiper* [2], as was suggested in a reply to *ESET Research's tweet* [3].
- Initial access vectors varied from one organization to another, but the deployment of HermeticWiper through Group Policy Object (GPO) in at least one instance suggests the attackers had prior access to one of that victim's Active Directory servers.
- Its compilation timestamp shows it was compiled on December 28, 2021.

HermeticWiper overwrites several locations (such as master boot record and master file table) on compromised systems with random bytes; symbolic links and large files in

Timeline of the attacks detected by ESET researchers around the time of the Russian invasion of Ukraine

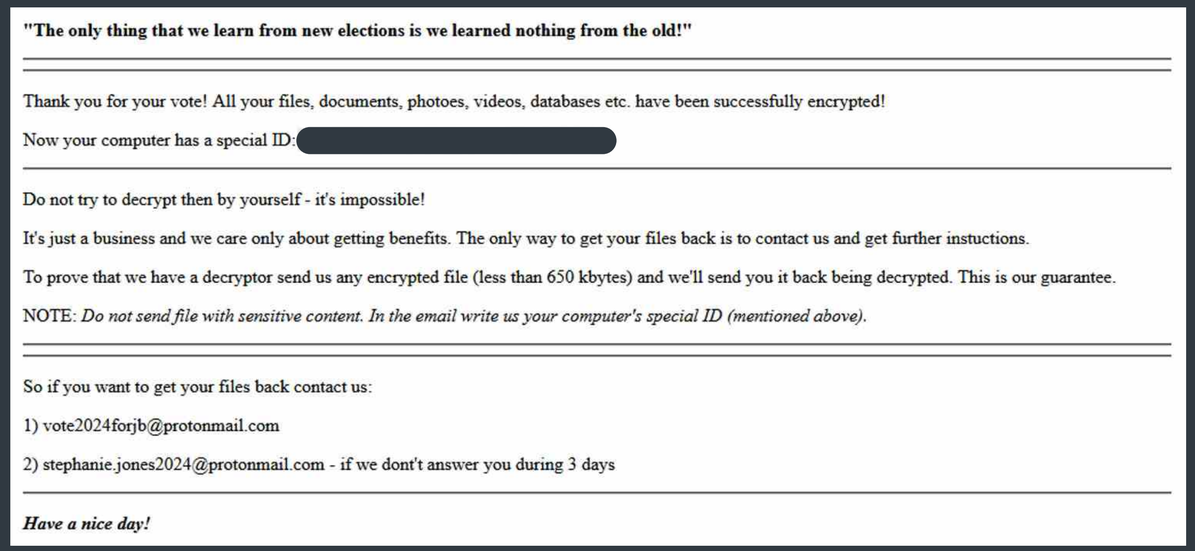
`My Documents` and `Desktop` folders are overwritten with random bytes too. It recursively wipes folders and files in `Windows`, `Program Files`, `Program Files(x86)`, `PerfLogs`, `Boot`, `System Volume Information`, and `AppData` folders. The wiper even wipes itself from the disk by overwriting its own file with random bytes. This anti-forensic measure is likely intended to prevent post-incident analysis. The machine is restarted; however, it will fail to boot because most files were wiped. ESET researchers believe that without backups, it is not possible to recover the impacted machines.

Hermetic campaign with faux ransomware

Looking for other samples signed by the same code-signing certificate, ESET researchers found a new malware family they named *HermeticWizard* [4]. It is a worm that was deployed on a system in Ukraine at 14:52:49 UTC on February 23, 2022. First, HermeticWizard tries to find other machines on the local network. It gathers known local IP addresses and then tries to connect to those IP addresses (and only if they are local IP addresses) to see if they are still reachable. When it has found a reachable machine, it drops its spreader modules. Finally, it drops HermeticWiper and executes it. The whole spreading mechanism is very rudimentary, implying that the deployment of this attack was rushed.

ESET researchers also observed HermeticRansom – "ransomware" written in Go – being used in Ukraine at the same time as the HermeticWiper campaign. HermeticRansom was first reported in the early UTC morning hours of February 24, 2022, in a *tweet* [5] from AVAST. ESET telemetry shows a much smaller deployment compared to HermeticWiper. This ransomware was deployed at the same time as HermeticWiper, potentially in order to hide the wiper's actions. Because HermeticRansom's motivations were not financial, as is usual with ransomware, ESET researchers refer to it as "faux ransomware".

On one occasion, ESET researchers observed HermeticRansom being deployed through GPO, just like HermeticWiper. A few strings were left in the HermeticRansom binary by the attackers – they reference US President Biden and the White House; the ransom message displayed to the victim once files are encrypted mentions that "The only thing that we learn from new elections is we learned nothing from the old!"



"The only thing that we learn from new elections is we learned nothing from the old!"

Thank you for your vote! All your files, documents, photoes, videos, databases etc. have been successfully encrypted!

Now your computer has a special ID: [redacted]

Do not try to decrypt then by yourself - it's impossible!

It's just a business and we care only about getting benefits. The only way to get your files back is to contact us and get further instuctions.

To prove that we have a decryptor send us any encrypted file (less than 650 kbytes) and we'll send you it back being decrypted. This is our guarantee.

NOTE: *Do not send file with sensitive content. In the email write us your computer's special ID (mentioned above).*

So if you want to get your files back contact us:

1) vote2024forjb@protonmail.com

2) stephanie.jones2024@protonmail.com - if we dont't answer you during 3 days

Have a nice day!

The ransom note mentioning a proverb

IsaacWiper

On February 24, 2022, ESET researchers detected yet another new wiper in a Ukrainian governmental network and named it IsaacWiper. It was seen in an organization that was not affected by HermeticWiper. It has no code similarity with HermeticWiper and is much less sophisticated. Given the timeline, it is possible that both are related but ESET researchers haven't found any strong connection yet. If its PE compilation timestamp (October 19, 2021) was not tampered with, IsaacWiper might have been used in previous operations months earlier.

IsaacWiper starts by enumerating physical drives; it then wipes the first 0x10000 bytes of each disk using the Mersenne Twister pseudorandom number generator (PRNG). It then enumerates logical drives and recursively wipes every file of each disk with random bytes also generated by the Mersenne Twister PRNG. It is interesting to note that it recursively wipes the files in a single thread, meaning that it would take a long time to wipe a large disk. On February 25, 2022, attackers dropped a new version of IsaacWiper with debug logs. This may indicate that the attackers were unable to wipe some of the targeted machines and added log messages to understand what was happening.

CaddyWiper

On March 14, 2021, ESET researchers uncovered yet another destructive data wiper that was used in attacks against organizations in Ukraine, spotted on several dozen systems in a limited number of organizations. *CaddyWiper* [6], as named by ESET, bears no major code similarities to either HermeticWiper or IsaacWiper. However, much like with HermeticWiper, there's evidence to suggest that the actors behind CaddyWiper infiltrated the targets' networks before unleashing the wiper.

Contrary to *NotPetya* [7], another faux ransomware, these wipers were deployed in a limited number of organizations and in a targeted fashion. ESET researchers believe that, unlike the previous outbreak, attackers targeted specific organizations with these wiper campaigns probably aiming to impair their ability to respond

adequately to the invasion. ESET Research identified victims in the financial, media and government sectors; based on their findings, we attribute CaddyWiper and HermeticWiper to the infamous Sandworm group.

Even shortly before the war, Ukraine had been a target of various other attacks. The above-mentioned *DDoS* [8] preceded a *Viasat attack* [9] that targeted the company's satellite internet network and affected residential modems in Ukraine. According to Ukrainian authorities, this attack seriously hindered their communication at the outset of the war. In January, a number of websites of various Ukrainian government entities suffered defacements with a message warning "be afraid and expect the worst". Shortly after that, Microsoft Threat Intelligence Center published a *blogpost* [10] about destructive malware named *WhisperGate* [11] that targeted Ukrainian organizations. After inspecting relevant information, ESET researchers believe that the defacements and WhisperGate attack are connected events.

The return of Industroyer

Looking into the more distant past, Ukraine is the country that suffered the first-ever malware attack specifically designed to attack power grids, on December 23, 2016. ESET researchers discovered this malware deployed by Sandworm and named it *Industroyer* [12]. Its sophistication was second only to Stuxnet and it targeted the Kyiv North transmission substation. For over five years, ESET researchers have wondered why Industroyer, as sophisticated as it was, was never deployed again.

This April, the wait was over, when we collaborated with *CERT-UA* [13] to respond to a cyber-incident affecting an energy provider in Ukraine and helped to remediate and protect this critical infrastructure. This collaboration resulted not only in the disruption of the attack but also in the discovery of a new Industroyer variant, which we, together with CERT-UA, named *Industroyer2* [14].

In this case, the Sandworm attackers made an attempt to deploy Industroyer2 against high-voltage electrical substations in Ukraine.

In addition to Industroyer2, Sandworm used several destructive malware families including CaddyWiper, ORCSHRED, SOLOSHRED and AWFULSHRED. ESET researchers don't know how attackers compromised the initial victim, nor how they moved from the IT network to the Industrial Control System (ICS) network. If successful, this attack could have left two million people without electricity, *claimed Farid Safarov* [15], Ukraine's Deputy Minister of Energy.

Destructive malware on Linux and Solaris

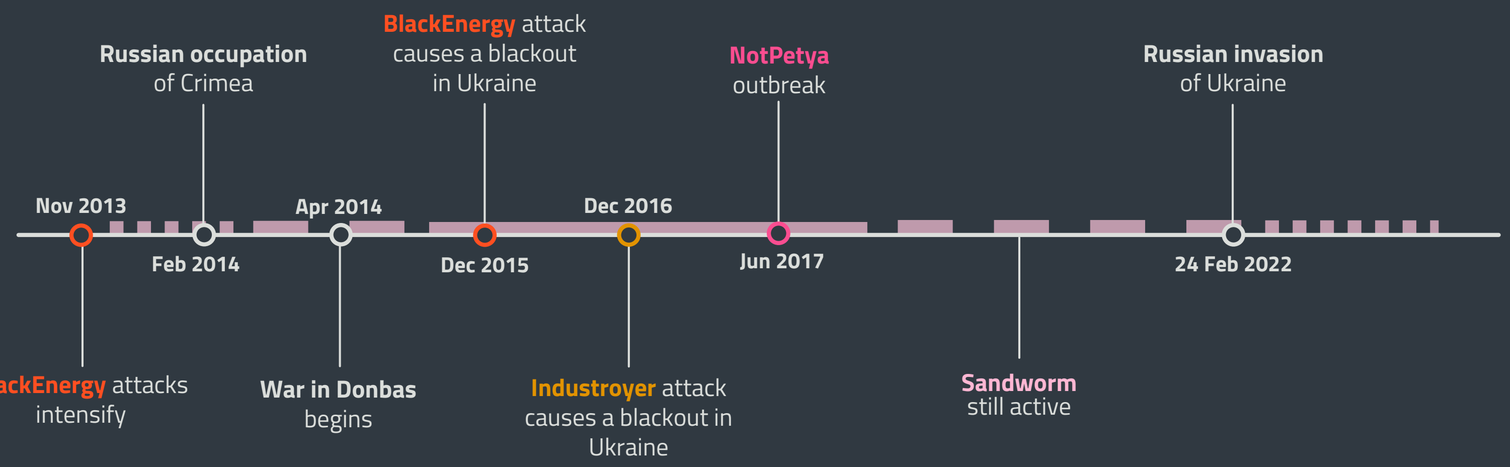
Industroyer2 was compiled on March 23, 2022, according to its PE timestamp, and set up to be deployed, using a scheduled task, at 16:10:00, April 8, 2022, UTC, suggesting the attackers had planned the intended attack for more than two weeks. In coordination with Industroyer2, the attackers deployed a new version of the CaddyWiper destructive malware in the ICS network.

In addition to Windows malware, attackers also deployed destructive malware on Linux and Solaris systems; wipers for these types of operating systems are a very rare sight. ESET researchers believe this was intended to slow down the recovery process and prevent operators of the energy company from regaining control of their ICS consoles in a timely manner. A wiper was also deployed on the machine where Industroyer2 was executed, likely to cover its tracks.

How we help

In addition to *humanitarian support* [16], ESET is providing security research and insights to the many European and global bodies endeavoring to address, resolve, and mitigate the cyberthreats stemming from the Russia-Ukraine war and this article presents only a fraction of these findings.

However, it is important to note that cyberattacks related to this war are not directed only against government bodies but also against businesses and the general public in Ukraine, as was seen in *many examples* [17] of *phishing lures* [18] abusing the situation in Ukraine, and detected by ESET.



High-profile attacks, detected and analyzed by ESET researchers, that targeted Ukraine well before the war

Past high-profile cyberattacks

Ukraine has been under heavy fire from cyberattacks for years now. Here are the most notable examples of nation-state APT groups focusing on Ukraine that have been *tracked by ESET researchers* [19] extensively *throughout the years* [4]:

Sandworm

From the end of 2013 and the beginning of 2014, ESET telemetry saw Sandworm *intensify attacks* [20] in Ukraine utilizing their BlackEnergy malware. This was shortly before the Russian occupation of Crimea and the subsequent war in Donbas. In December 2015, the group *attacked the Ukrainian power grid* [21], which became the first-ever blackout caused by a cyberattack and the homes of around 230,000 Ukrainians went dark. A year later, the group *deployed Industroyer* [12]. In the following years, Sandworm split its activities – the *GreyEnergy cluster* [22] continued attacks against the energy sector, and the *TeleBots cluster* [23] carried out attacks mainly against the financial sector in Ukraine – for instance, the disruptive *NotPetya outbreak* [7] in 2017. To this day, NotPetya is financially the most devastating cyberattack in history.

Sednit

Besides harassing Ukraine, this group is also known for targeting NATO countries. The technical sophistication of Sednit was revealed in 2018 in an ESET research analysis that detailed how this group managed to establish the most resilient type of persistence on a compromised system by *deploying LoJax* [24], the first UEFI rootkit found in the wild.

Gamaredon

Operating since 2013, this has been the most active APT group in Ukraine in recent years. *Gamaredon deploys* [25] high-volume and brute force attacks, keeping its malware in constant development. It focuses on breaching target organizations, usually utilizing spearphishing campaigns, to conduct cyberespionage. Over the years and on a few occasions, ESET researchers have seen this group pass some of its targets to the InvisiMole group.

InvisiMole

Also active since 2013, however, in stark contrast with Gamaredon, the *modus operandi of InvisiMole* [26] is highly covert, and focuses on espionage in Ukraine and Eastern Europe. Its operators perform highly targeted cyberespionage attacks against governmental institutions, military entities, and diplomatic missions.

Turla

This espionage group is recognized for its *complex malware* [27]. It is believed to have been operating since at least 2008, when it successfully breached the US military. It has also been involved in major attacks against many government entities in Europe and the Middle East; its main targets are government and military organizations.

Buhtrap

This group is well known for its targeting of financial institutions and businesses in Russia and Ukraine. Since late 2015, ESET researchers *have witnessed* [28] a change in the profile of the group's traditional targets – evolving from a purely criminal group perpetrating cybercrime for financial gain, its toolset has been expanded with malware used to conduct cyberespionage.

NEWS FROM THE LAB

Latest findings from ESET Research Labs across the world

Exploits

Signed kernel drivers – Unguarded gateway to Windows' core

ESET researchers released a deep dive into the abuse of kernel driver vulnerabilities. These vulnerabilities are most commonly leveraged by game cheat developers to circumvent anti-cheat mechanisms, but they have also been used by several APT groups and in commodity malware.

The kernel is the central component of the Windows operating system and kernel drivers comprise the software layer that provides hardware-specific and non-hardware-related features. Although in the newer versions of Windows it is no longer possible to directly load a malicious, unsigned driver, malicious code can still be loaded into the kernel by abusing legitimate, vulnerable drivers. This technique is also known as Bring Your Own Vulnerable Driver or BYOVD.

The BYOVD technique has been employed by various APT groups, such as the Slingshot APT group and the InvisiMole group. Additionally, the ESET-discovered *LoJax* [29], the first-ever UEFI rootkit found in the wild, abused the RWEverything driver to gain access to victims' UEFI modules.

Our researchers also looked for new kernel driver vulnerabilities and notified the impacted vendors, who were eager to fix the uncovered issues. The full list of the discovered vulnerabilities along with useful mitigation techniques can be found in the blogpost.

WeLiveSecurity blogpost [30]

Android

Fake e-shops on the prowl for banking credentials using Android malware

ESET researchers analyzed three malicious Android applications targeting customers of eight Malaysian banks. As the number of people using their smartphones to shop increases, so do the opportunities for cybercriminals to make a profit. In this ongoing campaign, the threat actors are trying to steal banking credentials by using fake websites that pose as legitimate services. These websites use similar domain names to the services they are impersonating.

In order to trick their victims into downloading their malicious apps, the copycat websites do not provide an option to shop directly through them. Instead, they include buttons that claim to download apps from Google Play, but actually lead to servers under the threat actors' control.

After the victims make their orders through these apps, they are presented with several payment options, out of which it is only possible to select direct transfer. Picking it then leads the victims to a fake FPX payment page where they are asked to select one out of eight Malaysian banks. Once they enter their bank credentials, those are sent to the attackers. The fake e-shop applications also forward all SMS messages received by the victims to the operators in case they contain two-factor authentication codes.

Even though the campaign exclusively targets Malaysia, it might expand to other countries and banks later on. At this time, the attackers are after banking credentials, but they may also enable the theft of credit card information in the future.

WeLiveSecurity blogpost [31]

Android and iOS

Crypto malware in patched wallets targeting Android and iOS devices

ESET Research uncovered a sophisticated scheme that distributes trojanized Android and iOS apps posing as popular cryptocurrency wallets. These malicious apps were able to steal victims' secret seed phrases by impersonating Coinbase, imToken, MetaMask, Trust Wallet, Bitpie, TokenPocket, or OneKey.

The attackers made sure that the apps had the same functionality as the originals, inserting their own malicious code into hard-to-detect places. This requires an in-depth analysis of the legitimate applications because the threat actors have to find spots in the code where the seed phrase is either generated or imported by the user.

We found these apps being promoted on dozens of Telegram groups, likely created by their authors looking for further distribution partners. Starting in October 2021, we found that these Telegram groups were shared and promoted in at least 56 Facebook groups. There were also two legitimate Chinese websites that we found in November 2021 that distributed these malicious wallets. Worryingly, the source code of the apps has been leaked and shared online, which will help them spread even further.

The malicious apps behave differently based on which operating system they are installed on. If the legitimate version of the app exists on Android, it cannot be overwritten by the counterfeit app, because it is signed by a different certificate. Only new cryptocurrency users without a legitimate wallet application are therefore targeted. However, on iOS, the victim can have both the legitimate and the malicious app installed, since they do not share the same bundle ID.

These trojanized apps are not available directly on the App Store, but some were available on Google Play. Based on our request as a *Google App Defense Alliance partner* [32], Google removed 13 malicious applications found on the official store in January 2022.

WeLiveSecurity blogpost [33]

Downloaders

ESET takes part in global operation to disrupt Zloader botnets

ESET Research collaborated with partners Microsoft's Digital Crimes Unit, Lumen's Black Lotus Labs, Palo Alto Networks' Unit 42, and others in an attempt to disrupt known Zloader botnets. We contributed by providing technical analysis, statistical information, and known command and control server domain names and IP addresses.

Zloader, one of the many banking trojan families heavily inspired by the famous Zeus banking trojan, evolved to become a distributor of other malware, including ransomware.

The coordinated disruption operation targeted three specific botnets, each one using a different version of Zloader. We helped with the identification of 65 domains that had been used by these botnet operators recently.

Similar to other commodity malware, Zloader is being advertised and sold on underground forums. When purchased, affiliates are given all they need to set up their own servers with administration panels and to start building their bots. Affiliates are then responsible for bot distribution and maintaining their botnets.

Since this malware is still relatively easily available, we will monitor it for any new activity following this disruption operation against its existing botnets.

WeLiveSecurity blogpost [34]

Under the hood of Wslink's multilayered virtual machine

ESET researchers described Wslink, a previously undocumented loader that runs as a server and features a virtual-machine-based obfuscator. There were no code, functionality or operational similarities that allowed us, at the time, to attribute Wslink to any known threat actor.

Virtualized Wslink samples do not contain any clear artifacts that easily link it to a known virtualization obfuscator, but we were able to develop a semiautomated solution to aid us in the analysis of the program's code.

This virtual machine introduced a diverse arsenal of obfuscation techniques, which we were able to overcome to reveal a part of the deobfuscated malicious code. The white paper published on the topic provides an overview of the internal structure of virtual machines in general and contains detailed information on various steps required to see through Wslink's obfuscation techniques used. In the last sections of our white paper, we also present parts of the code we developed to facilitate our research.

WeLiveSecurity blogpost [35]

White paper [36]

UEFI threats

When "secure" isn't secure at all: High-impact UEFI vulnerabilities discovered in Lenovo consumer laptops

ESET researchers discovered and analyzed three vulnerabilities affecting various Lenovo laptop models. Two of these vulnerabilities, *CVE-2021-3971* [37] and *CVE-2021-3972* [38], concern UEFI firmware drivers originally meant to be used only during the manufacturing process but that were mistakenly included in the production firmware images without being properly deactivated. Exploiting these vulnerabilities would allow attackers to deploy and successfully execute SPI flash or ESP implants, like LoJax or our latest UEFI malware discovery, *ESPecter* [39], on the affected devices.

While investigating those two drivers, we discovered the third vulnerability – SMM memory corruption inside the SW SMI handler function (*CVE-2021-3970* [40]). This vulnerability allows arbitrary read/write from/into SMRAM, which can lead to the execution of malicious code with SMM privileges and potentially lead to the deployment of an SPI flash implant.

We reported the vulnerabilities to Lenovo on October 11, 2021. The full list of affected devices, containing more than one hundred different consumer laptop models, is published in the *Lenovo Advisory* [41].

Since UEFI threats are executed early in the boot process, allowing them to bypass almost all security measures, they can be extremely stealthy and dangerous. In the last year, we saw numerous high-impact UEFI firmware vulnerabilities being publicly disclosed, which together with our discovery demonstrates that deployment of UEFI threats might not always be as difficult as expected.

WeLiveSecurity blogpost [42]

APT GROUP ACTIVITY

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

Donot Team

DoNot Go! Do not respawn!

ESET Research analyzed recent campaigns carried out by the Donot Team group (also known as APT-C-35 and SectorE02). We monitored Donot Team from September 2020 to October 2021 and found that the group carries out cyberespionage, focusing on a small number of targets primarily in South Asia. A recent report by Amnesty International links the group's malware to an Indian cybersecurity company. These threat actors are very persistent in their attacks, consistently targeting the same entities with waves of spearphishing emails every two to four months.

We traced several Donot Team campaigns that leverage Windows malware derived from the group's signature yty malware framework, whose main purpose is to collect and exfiltrate data. It consists of a chain of downloaders that ultimately download a backdoor with minimal functionality, used to then download and execute further components of the APT group's toolset. Our researchers analyzed two variants of the malware framework: Gedit and DarkMusical.

DarkMusical was distributed via spearphishing emails with PowerPoint documents containing a macro that deploys the first component of a chain of downloaders and persists using a scheduled task. Gedit was also spread via a spearphishing email, but this time it contained a malicious RTF document that exploits *CVE-2017-11882* [43] to drop two DLL files from the document and execute one of them. Other components are downloaded to the compromised computer in various stages.

WeLiveSecurity blogpost [44]

Unattributed campaign

Watering hole deploys new macOS malware, DazzleSpy, in Asia

ESET researchers discovered that the website of the Hong Kong pro-democracy radio station D100 was compromised to serve a Safari exploit that installed cyberespionage malware on site visitors' Macs. The website delivered new macOS malware that we named DazzleSpy.

In order to gain code execution in the browser, the attackers used an exploit that had more than 1,000 lines of code. Some parts of the code suggest that the vulnerability could also have been exploited on iOS, even on devices such as the iPhone XS and newer.

DazzleSpy is used for cyberespionage, with its targets probably being politically active, pro-democracy individuals in Hong Kong. This malware can: collect information about the compromised computer; search for specified files and scan files in Desktop, Downloads, and Documents folders; execute the supplied shell commands; start or end a remote screen session; and write a supplied file to disk.

Because of the complexity of the exploits used in this campaign, we conclude that the group behind this operation has strong technical capabilities. This campaign has similarities to *one from 2020* [45] where LightSpy iOS malware was distributed the same way, using iframe injection on websites for Hong Kong citizens leading to a WebKit exploit. We cannot confirm at this point whether both campaigns were carried out by the same group.

WeLiveSecurity blogpost [46]

Mustang Panda

Mustang Panda's Hodur: Old tricks, new Korplug variant

ESET researchers uncovered a still-ongoing cyberespionage campaign by the Mustang Panda APT group, using a previously undocumented Korplug variant. We named it Hodur based on its resemblance to the THOR variant previously documented by *Unit 42* [47] in 2020. In Norse mythology, Hodur is Thor's blind half-brother, who is tricked by Loki into killing their half-brother Baldr. We attribute this campaign to Mustang Panda with high confidence. It is a cyberespionage group that targets mainly governmental entities and NGOs, with its victims being located mostly in East and Southeast Asia.

The current campaign abuses the latest events in Europe as phishing lures, including Russia's invasion of Ukraine. Other phishing lures mention updated COVID-19 travel restrictions, an approved regional aid map for Greece, and a Regulation of the European Parliament and of the Council – showing that this APT group is able to swiftly react to current affairs.

Mustang Panda is known for its elaborate custom loaders and Korplug variants, which can be clearly seen in the samples used in this campaign. What sets this particular campaign apart is the heavy use of control-flow obfuscation and anti-analysis techniques at every stage of the deployment process.

WeLiveSecurity blogpost [17]

Winnti Group

New PipeMon variants discovered

ESET researchers found new Winnti Group PipeMon variants that were virtualized using Oreans' Code Virtualizer, and persisted as a print processor outside of the dedicated system print-processor directory. We first documented the PipeMon backdoor in *2020* [48] when it was used against several video gaming companies based in South Korea and Taiwan.

Even though Microsoft documentation specifically mentions that print processor DLLs must be located in the system print-processor directory, it is possible to place such DLLs anywhere on the system drive and use a relative path in the registry that points to the DLL, instead of using just a filename. This way, an attacker could stay under the radar when persisting a malicious DLL as a print processor without dropping it in the dedicated print-processor directory.

Twitter thread [49]

TA410

A lookback under the TA410 umbrella: Its cyberespionage TTPs and activity

ESET Research unveiled a detailed profile of TA410, a cyberespionage umbrella group loosely linked to APT10, known mostly for targeting US-based organizations in the utilities sector, and diplomatic organizations in the Middle East and Africa.

We believe the group consists of three different teams using different toolsets, including a new version of the FlowCloud espionage backdoor discovered by ESET. These teams, referred to as FlowingFrog, LookingFrog, and JollyFrog, have overlaps in TTPs, victimology, and network infrastructure. We assume that these subgroups operate somewhat independently, but that they may share intelligence requirements, an access team that runs their spearphishing campaigns, and also the team that deploys network infrastructure.

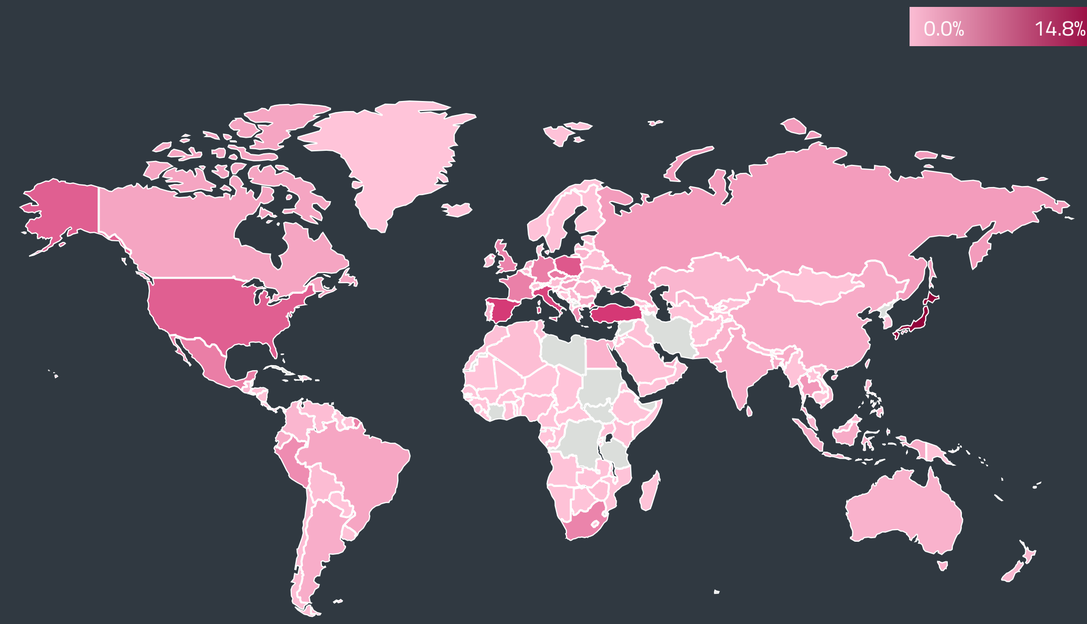
Most TA410 targets are high-profile organizations in the diplomacy and education sectors, but ESET has also identified victims in the military sector, a manufacturing company in Japan, a mining company in India, and a charity in Israel.

The new version of FlowCloud, which is a complex and modular C++ RAT used by the FlowingFrog team, has several interesting capabilities. They include: monitoring clipboard events to steal clipboard content, monitoring file system events to collect new and modified files, controlling attached camera devices to take pictures of the compromised computer's surroundings, and even controlling connected microphones and triggering recording when sound levels above a specified threshold volume are detected. The last function is triggered by any sound over 65 decibels, which is in the upper range of normal conversation volume.

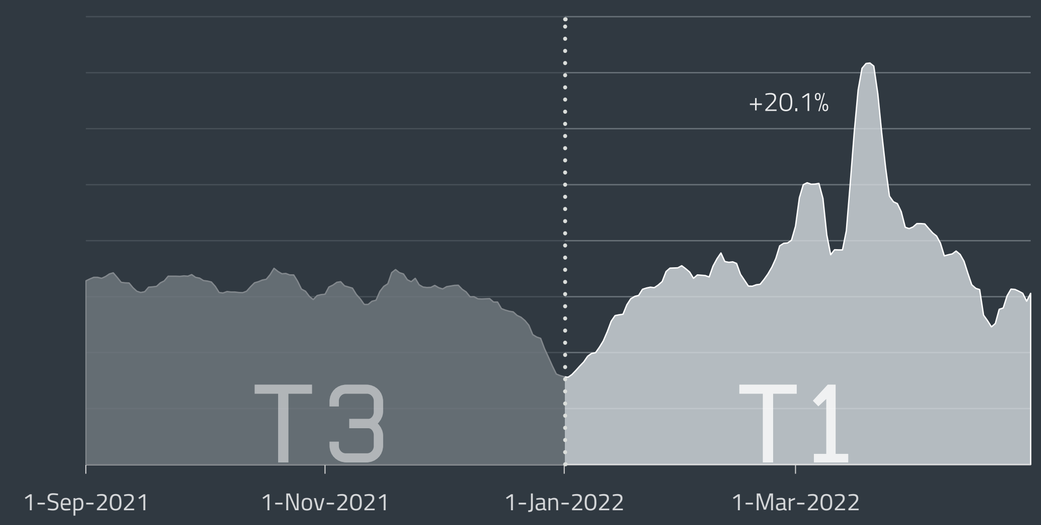
WeLiveSecurity blogpost [50]

STATISTICS & TRENDS

The threat landscape in T1 2022 as seen by ESET telemetry



Global distribution of malware detections in T1 2022



Overall threat detection trend in T3 2021 – T1 2022, seven-day moving average

THREAT LANDSCAPE OVERVIEW

A summary of the threat landscape developments in T1 2022.

After being generally stable for some time now, the number of threat detections rose by 20.1% in T1 2022. There were two notable spikes, on March 2 and 15, caused by the DOC/TrojanDownloader.Agent trojan. Both the higher overall threat detection numbers and the spikes were caused by the dramatic return of Emotet.

It comes as no surprise, then, that the ***Downloaders*** category was dominated by the recent Emotet campaign. Even if the comparison is made based on the malware's relatively low numbers in T3, its astronomical, over a hundredfold, increase still boggles the mind. Talk about coming back with a vengeance!

Emotet's campaign also influenced the ***Email threats*** category, which grew by 37% as a result. Additionally, the campaign led to an 829% jump in the incidence of DOC/TrojanDownloader.Agent, which climbed to the second place in the Email threats top 10 list.

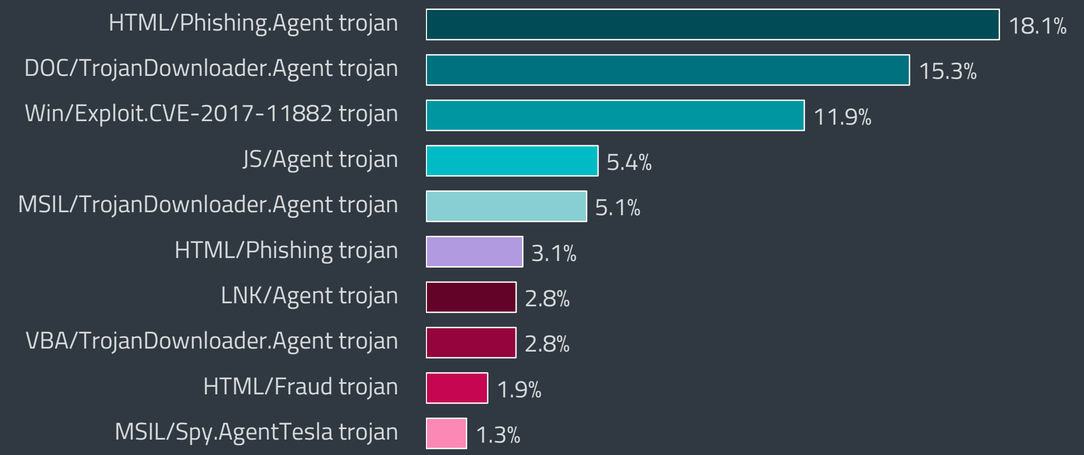
Over in the ***Exploits*** section, the number of RDP attacks, the usual source of the big scary numbers for the Threat Report, dropped by 43% after experiencing non-stop growth since the beginning of 2020.

As usual, the ***Ransomware*** threat landscape was far from boring, with Sodinokibi core members being arrested, the Conti gang suffering major internal information leaks, and Russia becoming the number one ransomware target in T1, according to our telemetry.

macOS threats saw declines in all of their subcategories, with the overall decrease being 14.9%. Almost half of the monitored threats were categorized as potentially unwanted applications (PUAs). A slight rise in detections marked the ***Android*** category, which went up by 8%. However, two of its subcategories, Android SMS trojans and Android Spyware, grew dramatically, the former by 145% and the latter by 170%.

When it came to ***Cryptocurrency threats***, T1 2022 was marked by several high-profile cryptocurrency platform hacks, which made cybercriminals a lot of money, even while the overall number of detections in this category decreased by 29.3%.

The ***IoT*** category data shows that years after the online publication of the Mirai source code, botnets using the code are still very common, attacking hundreds of thousands of devices. While the rate at which the notorious Mozi botnet is spreading slowed down by 11%, ZHTrap managed to increase the number of its attacks by 9%.



Top 10 malware detections in T1 2022 (% of malware detections)

Regarding ***Web threats***, our telemetry registered a 29% increase in phishing URLs caused by a spike in new URLs in March. As cybercrooks are always ready to make a profit out of human misery, there was also a surge in phishing and scam websites exploiting interest in and concerns about the Russia-Ukraine war.

Finally, after a pause in T3 2021, ***Infostealers*** were growing again. They increased by 12%, with the highest subcategory growth (74.5%) being demonstrated by Banking malware. Most of this growth was due to JS/Spy.Banker, which went up by 177.7% and made for 77.6% of Banking malware.

The Emotet surge also affected the overall top ten malware detections: while it did not succeed in dethroning the HTML/Phishing.Agent trojan, which constituted 18.1% of all detections, DOC/TrojanDownloader.Agent jumped from being the ninth most detected malware family to the second with 15.2%. Compared to T3 2021, its numbers rose by 758.4%.

MSIL/TrojanDownloader.Agent, which drops malware such as Agent Tesla and Fareit, also grew significantly in T1, and this 117.9% growth landed it in fifth place instead of T3's eighth. The rest of the top ten malware detections mostly shuffled down a position or two, but the list itself did not lose any of the previous top 10 families, nor were there any newcomers.

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.

↗ 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.

↘ Win/Exploit.CVE-2017-11882 trojan

This detection name stands for specially crafted documents exploiting the *CVE-2017-11882* [51] 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.

↗ 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.

↘ 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.

↘ 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* [52], such as the notorious Nigerian Prince scam also known as "419 scam".

→ MSIL/Spy.AgentTesla trojan

MSIL/Spy.AgentTesla is a .NET-based spyware-as-a-service trojan available on underground forums. It gets data and commands from remote hosts and serves to acquire sensitive information, log keystrokes, and gain control over the camera or the microphone of the victim.

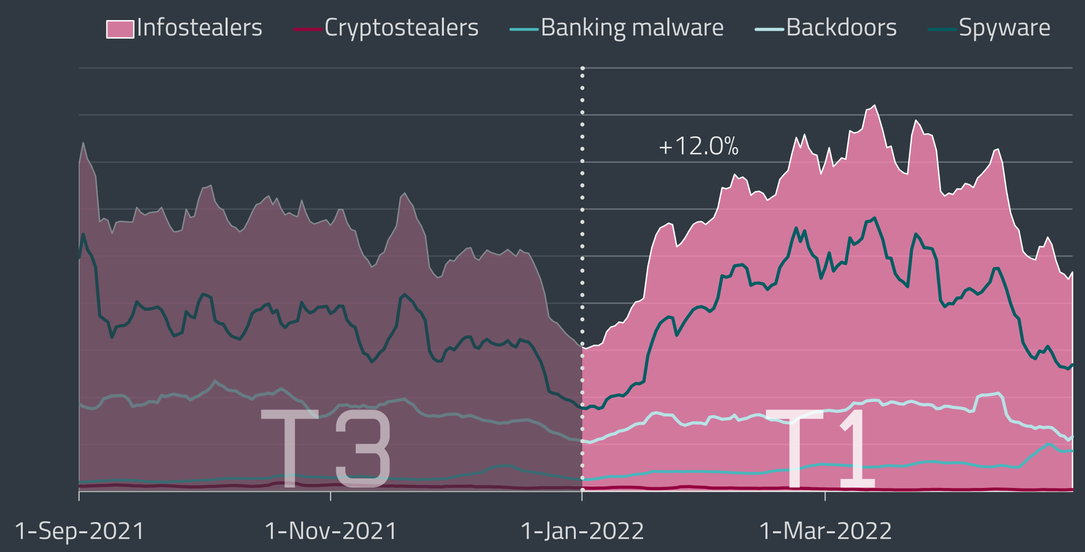
INFOSTEALERS

TrickBot bows out while JS/Spy.Banker dominates the banking malware threat landscape.

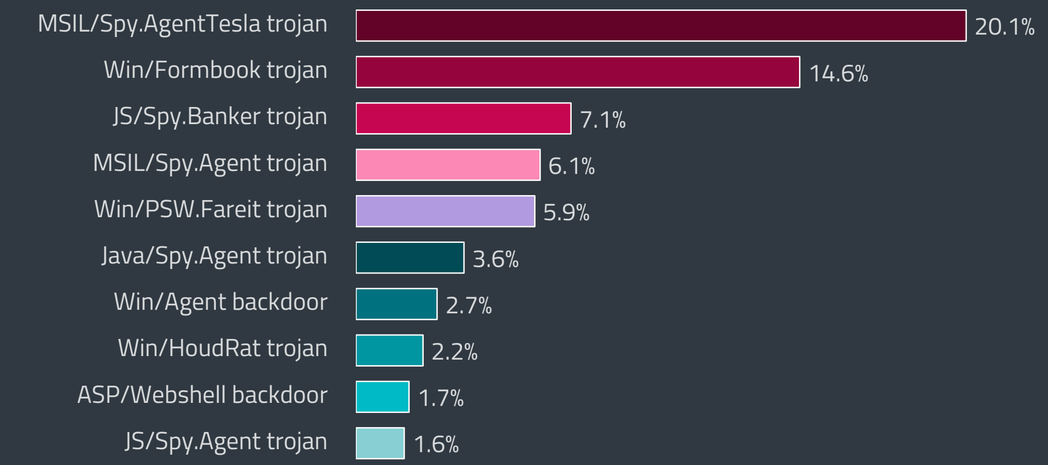
After a brief pause in T3 2021, the category of Infostealers resumed its growth in T1 2022, going up by almost 12%. As usual, the driving force behind most of the detections was spyware, which also accounted for the most significant spike on March 22, 2022, courtesy of MSIL/Spy.AgentTesla. Spyware and Banking malware increased in number of detections, Backdoors decreased, and Cryptostealers declined steeply in trend and numbers both.

In T1 2022, Spyware grew by 18.2% and made for 64.4% of all Infostealer detections, further cementing its status as the largest Infostealer subcategory. It was aided by the relative affordability of spyware-as-a-service malware on underground forums. A typical example of this business model, the MSIL/Spy.AgentTesla trojan, or simply Agent Tesla, was again the most prominent spyware according to ESET telemetry data, growing by 243.6% between T3 2021 and T1 2022. In T1, it was being spread by *malicious PowerPoint documents* [53] in phishing campaigns. Additionally, ESET registered its distribution in another phishing campaign alongside the Win/Agent backdoor near the end of April.

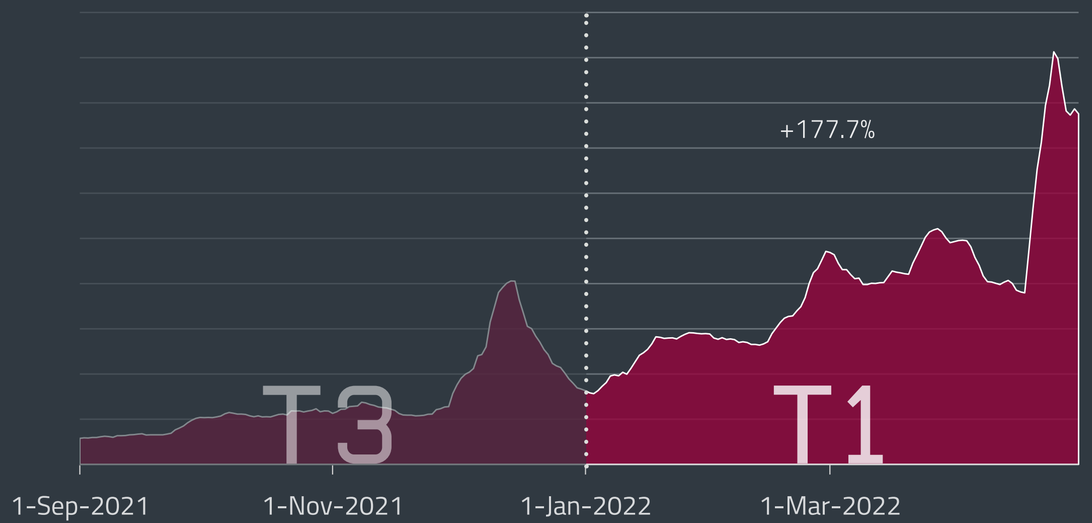
Top 10 Infostealer detections were also led by spyware, which took up the first two spots in the list. Agent Tesla had the highest numbers, with 19.3% of all Infostealer detections and 29% of Spyware



Infostealer detection trend in T3 2021 – T1 2022, seven-day moving average



Top 10 infostealer families in T1 2022 (% of Infostealer detections)



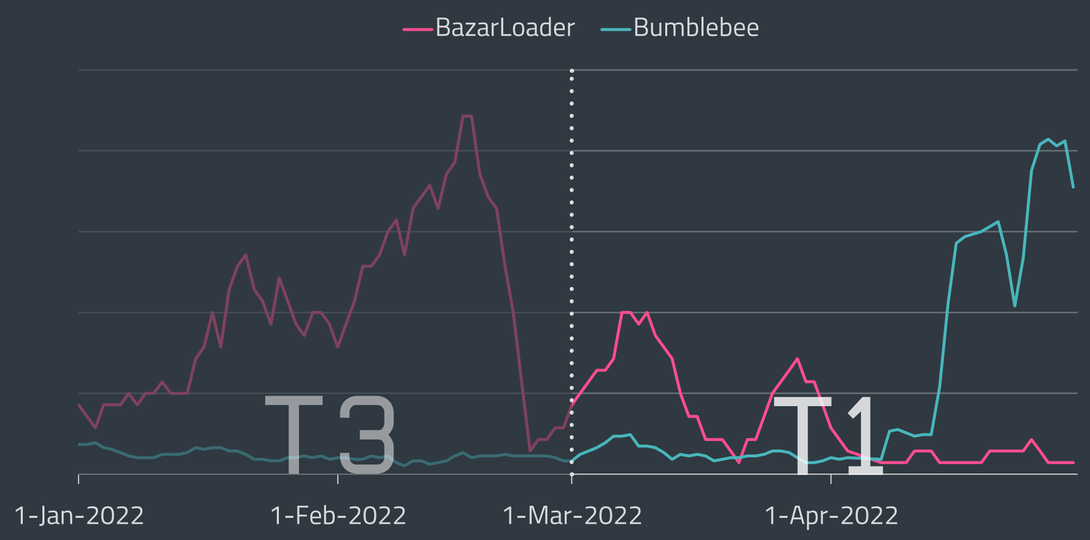
JS/Spy.Banker detection trend in T3 2021 – T1 2022, seven-day moving average

detections. It was followed by Win/Formbook trojan, which accounted for 14% of Infostealers and 21.1% of Spyware. The MSIL/Spy.Agent trojan placed fourth in the overall ranking with 5.8% and was the third most detected spyware with 8.8%.

While the top ranks in the list have traditionally been taken by spyware and backdoors, this time around a banking malware family rose to third spot. The JS/Spy.Banker trojan represented 6.8% of Infostealers. This malware family, also known as Magecart, injects JavaScript skimmer code into websites in order to harvest credit card information. Between T3 2021 and T1 2022, it grew by 177.7% and became more or less synonymous with the Banking malware subcategory, accounting for 77.6% of Banking malware detections. The next most detected malware in the subcategory, the MSIL/ClipBanker trojan, was left with mere peanuts compared to JS/Spy.Banker, having decreased by 59.4% and constituting only 4.5% of Banking malware.

This subcategory grew by 75% in T1 2022 and accounted for 8.5% of all Infostealer detections. It experienced a major spike on April 19, which was caused by the aforementioned JS/Spy.Banker, with Thailand as the most affected country.

TrickBot, banking malware turned multipurpose attack tool targeting enterprises, and one of the mainstays of the threat landscape, *ended its operations* [54] in February. It was speculated that the gang behind TrickBot, which has close ties to the Conti ransomware group, decided to switch its focus to BazarLoader instead. While TrickBot was very successful and even managed to come back from the disruption efforts in 2020, there were no significant updates to its core afterward.



BazarLoader and Bumblebee detection trends in T3 2021 – T1 2022, seven-day moving average

BazarLoader, another tool in the TrickBot creators' arsenal, uses more advanced techniques, and is harder to track and analyze. Interestingly, it is possible that even BazarLoader has been replaced, as *reports* [55] started emerging that a new loader named Bumblebee has been spreading since March. Bumblebee is being used by the same threat actors that would previously use BazarLoader. It remains to be seen which one of these loaders will win out in the end, or if they both stay in circulation.

EXPERT COMMENT

Since the beginning of the year 2021, BazarLoader has been in continuous development, the pace of which has ramped up considerably in the first three months of 2022, when we saw progress in its anti-analysis techniques. The malware now sports an improved API call obfuscation technique, which combines three hashes instead of one, and added code flow obfuscation.

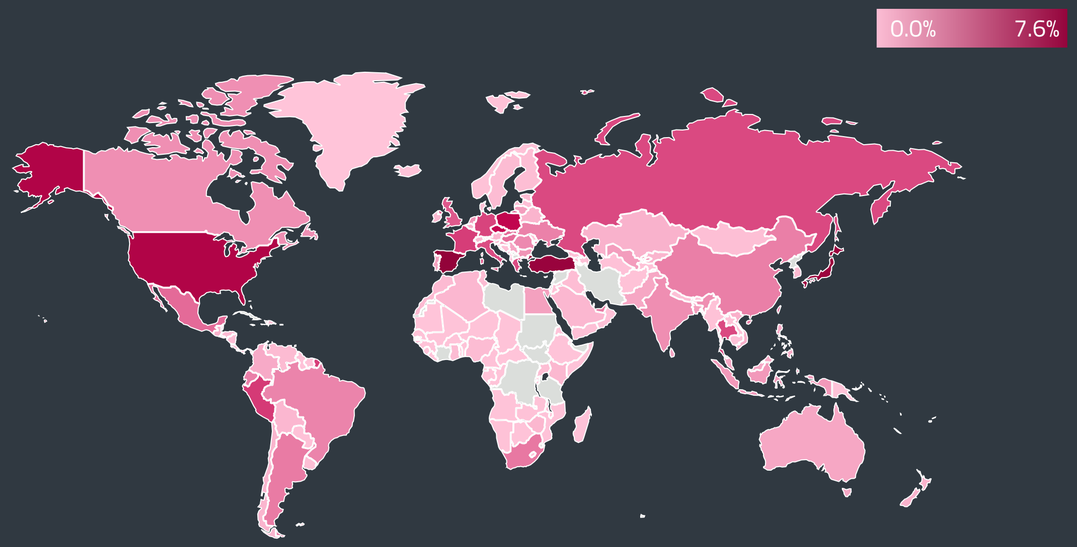
I find our latest research pointing towards Bumblebee replacing BazarLoader quite surprising. From an analyst's point of view, BazarLoader is actively being worked on and has become sophisticated malware that is hard to track and analyze. These factors do not indicate that it is a tool that should be discarded, so I believe that we will meet BazarLoader again.

Compared to that, Bumblebee in its current state is not obfuscated whatsoever at its core and partially uses open-source code. It is likely that Bumblebee will undergo more development in the near future.

Jakub Tomanek, ESET Malware Analyst

Most Latin American banking trojans did not stray far from their ordinary patterns, stealing bank credentials and targeting mostly Mexico and Brazil with the occasional foray into Spain. However, it looks like one of the members of this malware cluster is trying to expand its horizons considerably: *Grandoreiro* [56] added *over 900 new targets* [57] to its portfolio, among them cryptocurrency exchanges and NFT games. This LATAM banking trojan can currently be considered the most active of the group.

It seems that while Grandoreiro started encroaching onto cryptostealers' turf, cryptostealers themselves were not very active. Their detection numbers dropped by 51.6% in T1 2022, continuing their downward trend that ought to make all cryptocurrency owners quite happy. This subcategory experienced one notable spike on January 25 caused by the Win/PSW.Delf trojan, whose attack attempts were registered mostly in Japan and Hong Kong at the time.



Global distribution of Infostealer detections in T1 2022

The usually strong subcategory of Backdoors declined in detections, now for the second period in a row. Despite their 11.1% decrease, they still constituted the second-largest portion of Infostealer detections – 25.5% of which were categorized as backdoors.

They were also represented in the top 10 Infostealer detections list, coming in sixth, eighth, and tenth overall. The first among them was the PHP/Webshell backdoor (15.6% of Backdoors, 4.1% of Infostealers), followed by the Win/Agent backdoor (9.7% of Backdoors, 2.6% of Infostealers), and ASP/Webshell backdoor (6.4% of Backdoors, 1.7% of Infostealers). There was one significant backdoor spike, on April 7, caused by the Win/Agent backdoor and its TJS variant, with over three-fourths of its attack attempts registered in Spain. Win/Agent.TJS is the same variant that ESET products caught spreading through emails along with Agent Tesla at the end of April.

Another variant of this backdoor, more precisely Win/Agent.NE aka the G3ll3rt Grind3lwald RAT, was being distributed in a ***new campaign*** [58] discovered by ESET researchers at the beginning of the year. While our telemetry did not show that many hits at the time, some criminal gangs such as Zloader were taking an active interest in this malware. After its activity surges in January and February, G3ll3rt Grind3lwald's numbers gradually dropped.

In T1, Infostealers were most prevalent in Spain, which saw 7.6% of all attack attempts, then Turkey with 7.1%, and Japan third, registering 6.9%.

RANSOMWARE

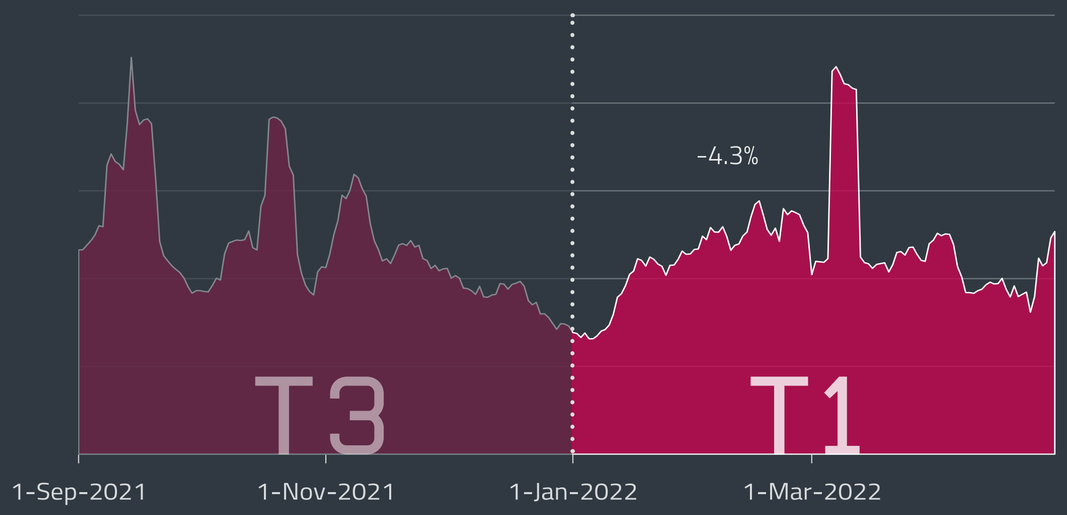
War in Ukraine sparks an increase in ideology-motivated ransomware attacks with ransomware increasingly targeting Russia.

T1 2022 started with big news. In January, the Russian Federal Security Service (FSB) raided 25 addresses and arrested 14 alleged core members of the infamous ***Sodinokibi/REvil*** [59] ransomware gang. The operation was sparked by the US authorities reporting on the leader of the group. During the raids, agents seized crypto- and fiat currencies worth over $6 million, 20 luxury cars, and hardware used to run the malicious operation.

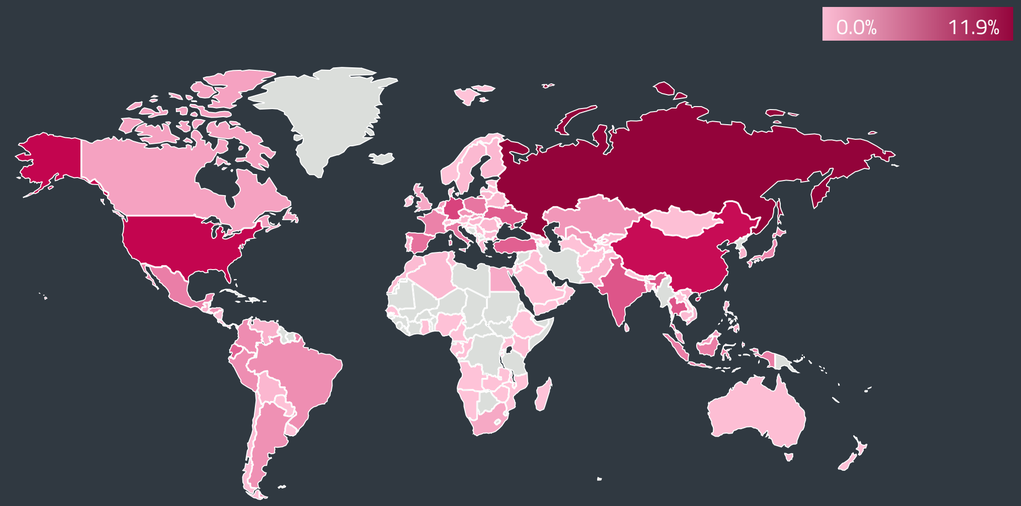
However, the arrests didn't have a lasting effect as ***Sodinokibi's TOR leak site*** [60] came alive only a few weeks later and started listing new victims. After analyzing the samples from the attacks, researchers confirmed these were ***new Sodinokibi instances*** [61], compiled from the original source code. This suggests that one of the former core members – with access to the gang's resources – is still free and running the operation.

But law enforcement activity around Sodinokibi was soon to be overshadowed by much grimmer events. The Russian invasion of Ukraine had numerous influences on the Ransomware category. Apart from the ***HermeticRansom*** [4] attacks on several high-profile Ukrainian organizations, the ransomware detection trend continued its slow downward pace, dropping by 4% compared to T3 2021.

Looking at the upticks in the chart, the first dent was caused by the Conti gang attacking systems in Honduras, accounting for 53% of the daily detections. The second spike, on March 6, was even larger



Ransomware detection trend in T3 2021 – T1 2022, seven-day moving average



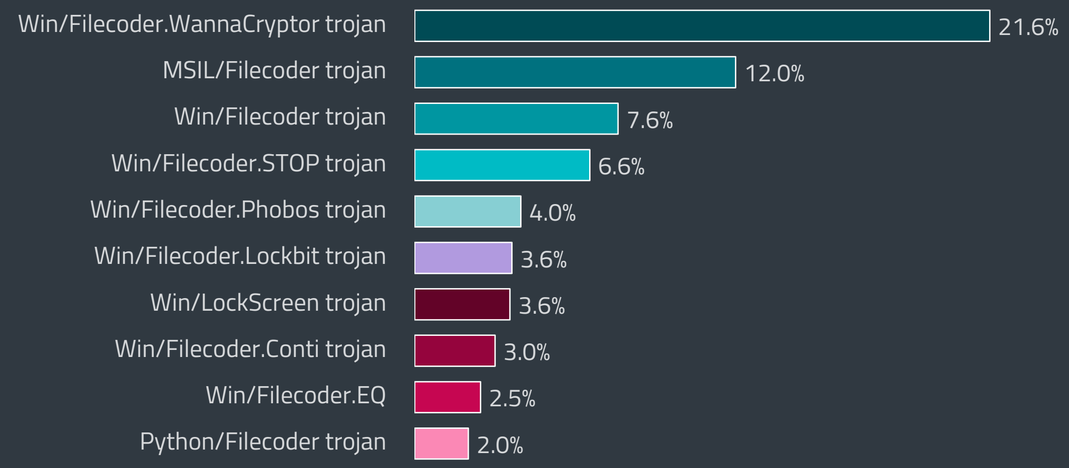
Global distribution of Ransomware detections in T1 2022

and was caused by MSIL/Filecoder.ACB attacking a network of a single large organization in Russia, attempting to encrypt its data from within the environment.

This incident points to a potential shift in the ransomware scene. Before the invasion, Russia and some of the Commonwealth of Independent States (CIS) were excluded from many ransomware target lists. This was probably due to criminals residing in those countries or fearing Russia's retribution. T1 2022 hints at a possible change, as Russia faced the highest proportion of detections (12%) in the Ransomware category. Although not unheard of, Russia has never had to eat so much of its own dog food.

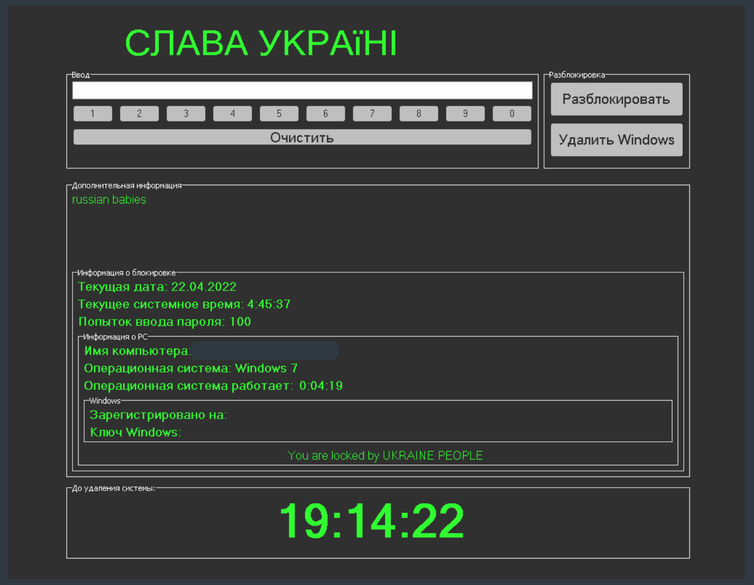
A series of incidents against high-profile Russian targets seems to support this interpretation. One group that started attacking victims such as Russian space agency Roscosmos and the state-owned Russian TV and radio was ***NB65*** [62]. In a reaction to the massacre in Bucha, Ukraine, NB65 used the leaked source code of Conti ransomware to breach its targets and leak their sensitive info online.

A second actor that misused the topic of the war was ***OldGremlin*** [63]. This group reportedly used well-crafted spearphishing emails and custom backdoors to breach Russian banks, industrial enterprises, medical organizations, and software developers.



Top 10 ransomware families in T1 2022 (% of Ransomware detections)

An interesting data point that stood out in T1 2022 was the increased number of screen-locking ransomware incidents, which jumped to the seventh most frequent ransomware detection. Close to 40% of these attacks were aimed at Russia and 11% at Ukraine. The Win/LockScreen.AWI variant targeting Russia even displayed the title "Slava Ukraini" (in uppercase Ukrainian Cyrillic) or "Glory to Ukraine" – a national salute used by the Ukrainians.



Win/LockScreen.AWI variant targeting Russian victims using the title "Glory to Ukraine"

Another major ransomware story connected to the war in Ukraine is the already mentioned Conti data leak. The material was published by a Ukrainian computer *researcher* [64], who became irritated by the gang's *pledge* [65] to support Russia in its aggressive war efforts. In turn, he started a *Twitter account* [66] leaking the group's data, including source code for several of their malware families and years of *sensitive internal communication* [67] that contained hints at a possible link to the Russian government. Other actors such as *LockBit* [68] tried to avoid similar fallout and published statements in multiple languages saying they will stay impartial.

For a bit of good news, T1 2022 saw a large number of free decryptors released. The list includes some of the most notorious names such as *Maze, Egregor, Sekhmet* [69] and *Diavol* [70], but also less known strains such as *TargetCompany* [71], and *Yanlouwang* [72]. Regarding the war in Ukraine, a free decryptor has been published for victims of *HermeticRansom* [73], described in our *Featured story*. South Korean researchers also detailed vulnerabilities in the *Hive ransomware* [74] encryption algorithm and showed how to exploit them to recover affected data.

The beginning of 2022 was also the period when some of the ransomware actors heard their sentences. An Estonian man will spend the next *66 months in jail* [75] and pay $36 million in restitution due to his ties to 13 attacks, causing cumulative losses of more than $50 million. A Canadian NetWalker affiliate was *sentenced to 80 months* [76] for his involvement in attacks hitting 17 victims.

Despite some of the actors ending up arrested, there still seem to be enough greedy criminals who want to have a part of those large payouts and join the ransomware scene with their gangs. *NightSky* [77] was one of the first and most visible ones that popped up in T1 2022, targeting corporate networks and *exploiting Log4J* [78]. On top of eCh0raix, NAS devices are under attack from new ransomware called *DeadBolt* [79]. Another newcomer, White Rabbit, seems to be a side-project of the FIN8 hacking group.

But not all ransomware gangs are focused on corporations and big payouts. A new RaaS called *Sugar ransomware* [80] seems rather interested in regular users and small businesses, demanding significantly smaller ransoms than the competition. Also new in T1 2022 were *Black Basta* [81] and *Onyx* [82] ransomware, the latter mostly destroying data instead of just encrypting it.

EXPERT COMMENT

Since the Russian invasion of Ukraine, we have observed an increased number of amateurish ransomware and wipers. Their authors often pledge support for one side or the other and make the attacks an act of personal vendetta. What's interesting is that the pro-Ukrainian variants outnumber the pro-Russian ones by a small margin. We expect attacks supporting a particular side to continue in the upcoming months and even escalate as ideology and war propaganda are becoming the central driving forces for their spread.

Igor Kabina, ESET Senior Detection Engineer

DOWNLOADERS

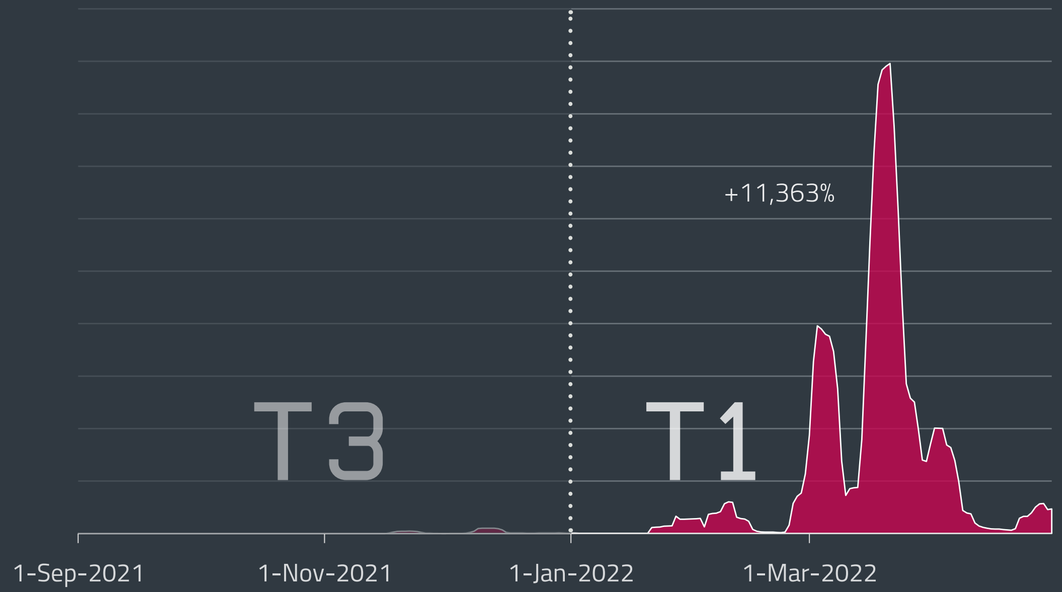
Emotet shifts to a higher gear and adds new distribution method, Zloader faces a takedown attempt.

In T3 2021, we detailed the resurrection of Emotet, improvements to its binary and modules, and adjustments to its technique mostly aiming at the switch to Cobalt Strike beacon as its payload. While that list might seem extensive, T1 2022 shows it was only a preparatory stage for what was yet to come.

In March and April 2022, Emotet operators shifted into a higher gear, their botnet spewing spam campaign after spam campaign, using malicious Word documents (DOC/TrojanDownloader.Agent) as attachments. Comparing that with the relatively small initial campaigns seen after its return in T3 2021, Emotet's detections in T1 2022 shot up more than a hundredfold (growth of over 11,000%).

The first larg uptick occurred on March 2, aiming very directly at Japan (67% of detections). On March 16, it was followed by the largest spike since Emotet's resurrection, hitting mostly victims in Japan (50%), Italy (16%), and Mexico (4%). There was also one smaller aftershock on March 21 with similar targets.

As ***announced*** [83] in February, Microsoft disabled downloaded Visual Basic for Applications (VBA) macros by default. This ***effectively cut*** [84] one of the most popular distribution avenues used by Emotet, Trickbot, Qbot, Dridex, and many others.



Emotet detection trend in T3 2021 – T1 2022, seven-day moving average

Emotet operators tried to adapt to the new reality by experimenting with other compromise vectors on smaller samples of victims. One such test ***campaign*** [85] was documented by ESET researchers between April 26 and May 2, where botnet operators replaced the typical Office document attachment with malicious LNK files (LNK/TrojanDownloader.Agent.AMQ). One of the frequently seen filenames was `form.lnk` and tried to lure victims from Japan (28%), Italy (16%), and Mexico (11%) to download and run the Emotet binary.

A different technique was documented by ***Proofpoint*** [86] in Emotet's campaign between April 4 and April 19. Operators used salary- and bonus-related bait, leading to a ZIP archive stored on OneDrive, which upon unpacking, contained Microsoft Excel Add-in (XLL) files. If executed, these files dropped and ran the main Emotet binary.

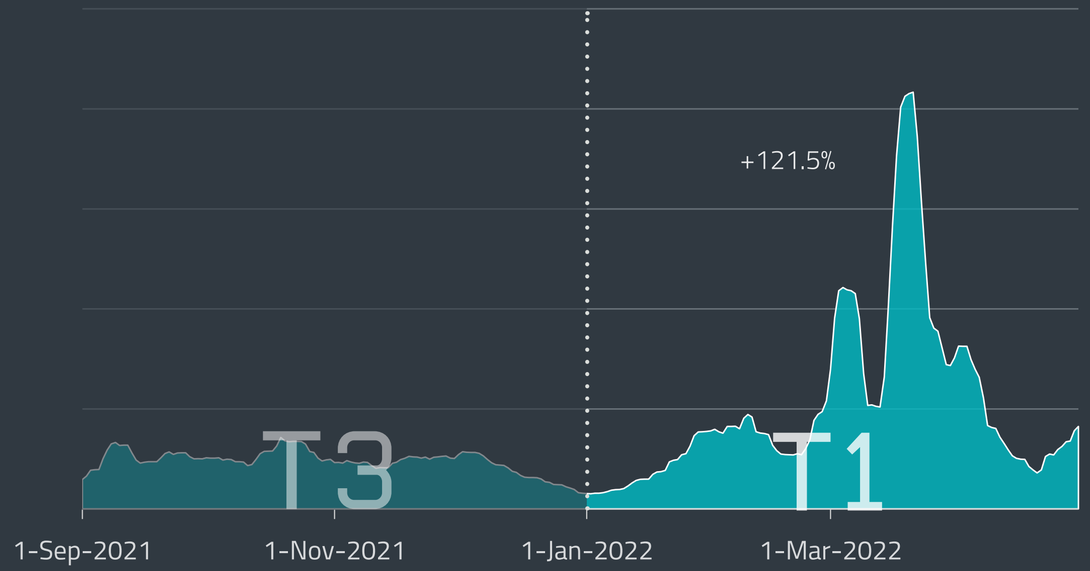
EXPERT COMMENT

The size of Emotet's latest LNK and XLL campaigns was significantly smaller than those distributed via compromised DOC files seen in March. This suggests that the operators are only using a fraction of the botnet's potential while testing new distribution vectors that could replace the now disabled-by-default VBA macros. As soon as one of the tested approaches yields satisfactory results, we can expect Emotet to shift back into high gear.

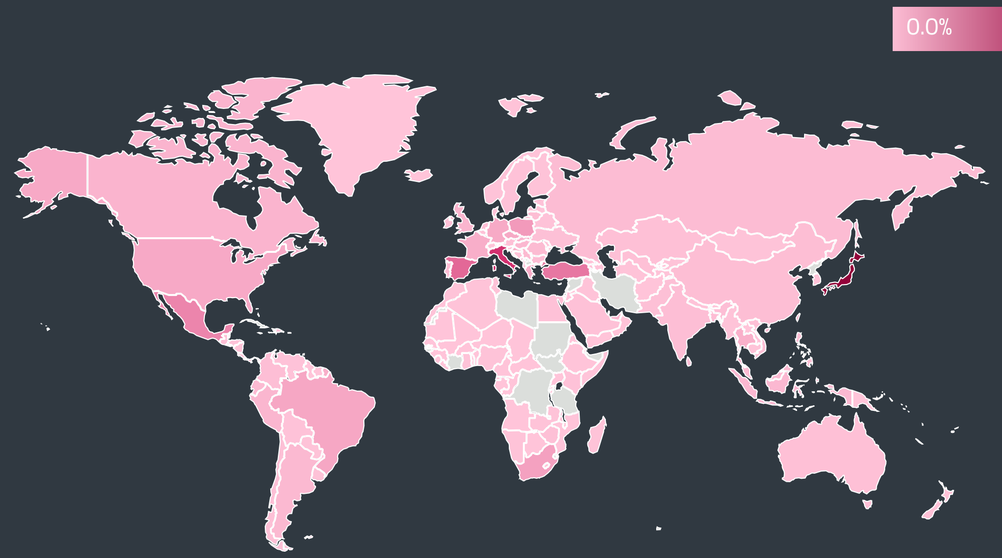
Dušan Lacika, Senior Detection Engineer

Looking at the Downloader category in general, the detection trend was mostly influenced by upticks of the Emotet botnet, significantly contributing to the 121% growth of the whole category between T3 2021 and T1 2022.

However, there was one other threat supporting those numbers – MSIL/TrojanDownloader.Agent. This downloader family increased its activity by 118% compared to T3 2021 and ended up second in the top 10 with 18%. Four out of its top five variants (MSIL/TrojanDownloader.Agent.JBZ, .IYB, .IUU, .JEG) were downloading two binaries: a payload in the form of an EXE file, and a DLL tool used to execute it. The final payloads were downloaded from the Discord platform and included Agent Tesla, Fareit, and MSIL/Agent.CFQ trojan.

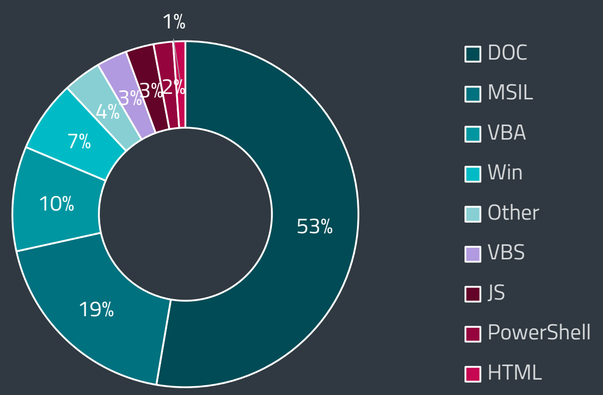


Downloader detection trend in T3 2021 – T1 2022, seven-day moving average



Global distribution of Downloader detections in T1 2022

T1 2022 is the first period since ESET started publishing Threat Reports in which the VBA platform lost its lead, landing only in third place with 10%. Due to Microsoft disabling macros by default, we expect to see a continuous decline of VBAs in the future as attackers will replace this vector with new, more effective ones. The highest share of the DOC platform is primarily caused by the massive Emotet campaigns in March, using weaponized Word documents.



Downloader detections per detection type in T1 2022

T1 2022 also brought a takedown attempt. A coalition of vendors led by Microsoft's Digital Crimes Unit made a move against Zloader – a former banking trojan that evolved into a distribution channel for other malware strains. The disruption effort took aim at three specific botnets tied to the malware family. ESET Research contributed to the operation by providing technical analysis and threat intelligence. For a more detailed account of the Zloader takedown, read the ***News from the Lab*** section or our ***blogpost*** [34].

A new loader named ***Verblecon*** [87] was spotted for the first time in T1 2022 by Symantec's Threat Hunter team. According to their findings, it is complex, powerful and polymorphic malware that uses anti-analysis mechanisms to avoid the watchful eye of security solutions and researchers. ESET detects the threat as Java/Agent.OR.

CRYPTOCURRENCY THREATS

Cryptocurrency platforms hacked for significant profit even as cryptocurrency threat detections decline.

T1 2022 was not the best period for cryptocurrencies. Even though their exchange rates did not by any means crash, the most prominent cryptocoins were having a hard time reaching their previous highs. The price of bitcoin hovered around USD 40,000 throughout T1, and Ethereum only managed to breach USD 3,500 at the start of the year and then for a few days in April. Faring even worse than the currencies themselves, the number of Cryptocurrency threat detections decreased by 29.3% in T1 2022.

As stated numerous times in our Threat Reports, the number of cryptocurrency threats correlates with cryptocurrency exchange rates to a certain extent. It could safely be said that the period from January to April was not very generous to these alternate forms of payment and investment. The stagnation in cryptocurrency values can be ***attributed to*** [88] the general turmoil in the market, caused mostly by Russia waging war on Ukraine, along with the anticipation of monetary regulations in the US.

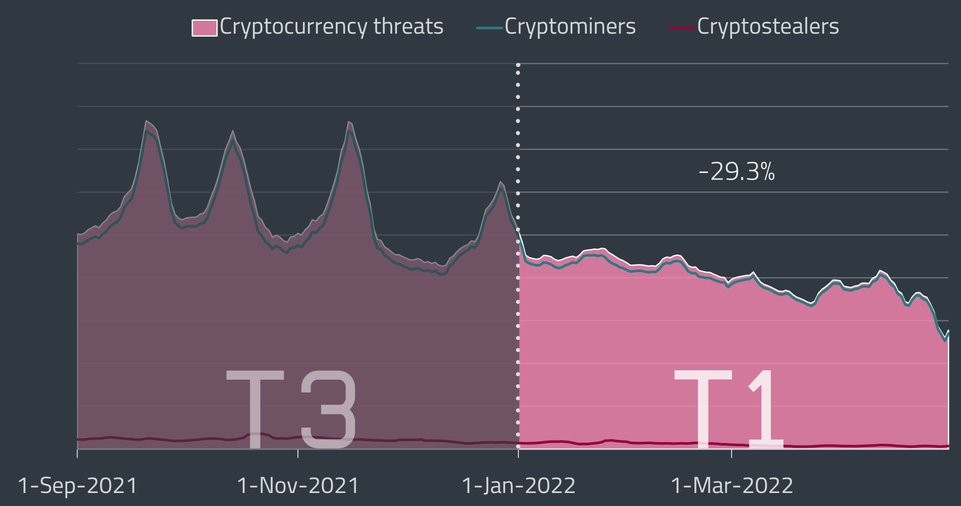
However, even though the number of cryptocurrency threats went down, they remain as dangerous as ever. The beginning of the year saw several high-profile cryptocurrency platform hacks: cryptocurrency exchange Crypto.com users lost more than ***USD 30 million*** [89] in mostly Ethereum and bitcoin after malicious actors bypassed the site's two-factor authentication; the cross-chain cryptocurrency platform Wormhole was hacked for ***USD 326 million*** [90] when cybercrooks exploited a vulnerability in their network; and finally, the NFT marketplace OpenSea was once again targeted by hackers, who managed to steal about ***USD 1.7 million*** [91] worth of digital tokens in a phishing attack.

EXPERT COMMENT

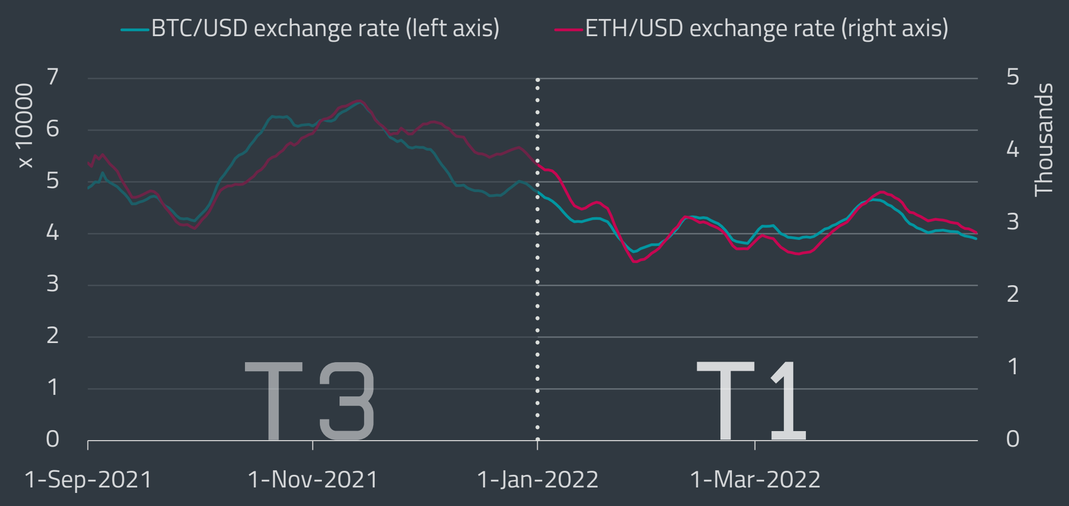
The war in Ukraine, strict sanctions on Russian cryptomining companies, and the increased targeting of cryptocurrency platforms in cyberattacks have all lessened the motivation of malicious actors to create and spread cryptocurrency-related malware. On the other hand, cryptocurrency exchange rates grew thanks to the Central African Republic adopting bitcoin as an official currency. Because of the current situation, it is quite difficult to predict how the threat landscape will develop, but we can expect a rise in large-scale targeted attacks, similar to what is happening with ransomware.

Igor Kabina, ESET Senior Detection Engineer

Coinminers, usually the more active of the cryptocurrency threat subcategories, decreased by 28.4% between T3 2021 and T1 2022. There were no major jumps in their activity up until April, which saw two smaller spikes in the numbers of the potentially unwanted application (PUA) Win/CoinMiner. The first was on April 11 when a surge of the AGen.D variant was registered in France, and the second was on April 20, led by the TA and SF variants, both mainly seen in Japan.



Cryptocurrency threat detection trend in T3 2021 – T1 2022, seven-day moving average



Bitcoin and Ethereum/USD exchange rates in T3 2021 – T1 2022, seven-day moving average

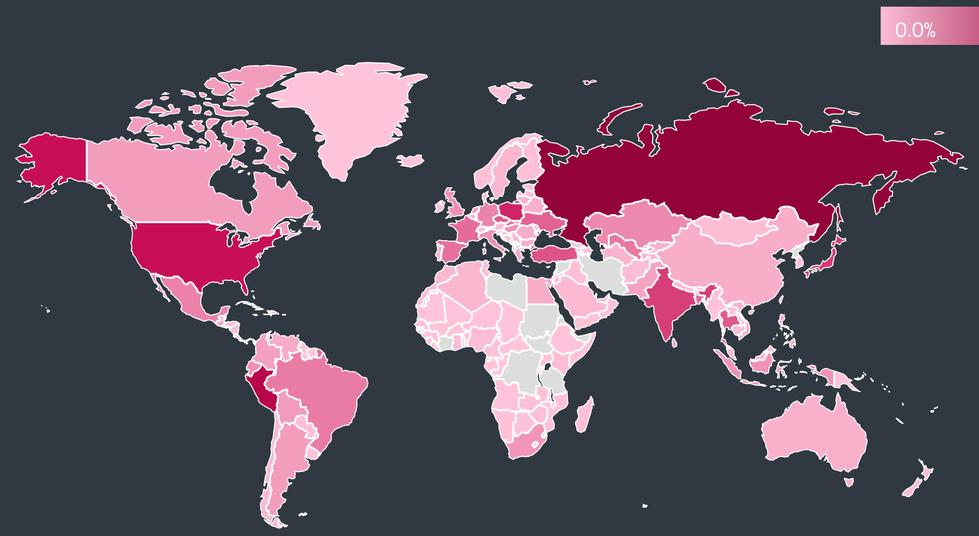
Trojan:PUA and desktop:in-browser ratio of cryptominer detections in T1 2022

The three most detected coinminers in T1 were Win/CoinMiner PUA, Win/CoinMiner trojan and JS/CoinMiner PUA. Win/CoinMiner PUA constituted almost half of all coinminer detections with 49.2%, even while its numbers went down by 41.5% when compared to the previous period. Win/CoinMiner trojan had a 12.4% share of detections and also decreased in number by 16.4%. JS/CoinMiner PUA was close behind with 11.8% and suffered the smallest decline out of the top three, which was 9.6%. Despite the falling numbers, the top three players have managed to keep the same positions as in T3 and indeed the overall 2021 statistics.

In the last report we mentioned that an interesting trend regarding PUA-vs.-Trojan and Desktop-vs.-In-browser ratios had emerged over 2021, namely that PUA and Desktop detections were steadily growing each period. This time around, however, both Trojans and In-browser detections managed to regain some lost ground. In T3 2021, the ratio of PUA to Trojan detections was 74% to 26%, while in T1 2022 it was 69% to 31%. As for the Desktop:In-browser ratio, it was 90% to 10% in T3 and 87% to 13% in T1.

	T3 2021	T1 2022
1	dl-x[.]com	webminepool[.]com
2	wypracowanie.edu[.]pl	dl-x[.]com
3	monerominer[.]rocks	wypracowanie.edu[.]pl
4	carrierecalciatori[.]it	slovolam[.]sk
5	instagrammi[.]ru	carrierecalciatori [.]it
6	newsoholic[.]com	arafifblues[.]com
7	mituus[.]com	kaizoku-ehime[.]jp
8	idaakulubu[.]com	mainevnap[.]com
9	cumpleañosdefamosos[.]com	mituus[.]com
10	slovolam[.]sk	monerominer[.]rocks

Top 10 most visited cryptojacking domains in T3 2021 and T1 2022



Global distribution of Cryptocurrency threat detections in T1 2022

The increased percentage of In-browser coinminers should serve as a reminder to be wary of free streaming websites and sites with adult content, as some of them can hijack the user's computer to mine for cryptocurrencies. You can find the list of the top 10 most visited cryptojacking domains in T3 2021 and T1 2022 on the left-hand side of the page.

Coinminers were seen mainly in Russia, where ESET registered 10.6% of their detections, then Peru with 6.4%, and the United States, which saw 5% of all their attack attempts.

Cryptostealers' decline was even sharper than that of coniminers – the subcategory went down by 51.6%. There was one spike in their detections: on January 25, the OSF variant of Win/PSW Delf trojan had its peak, with the most attack attempts seen in Turkey, Japan, and Hong Kong.

Compared to T3 2021, the top three cryptostealers stayed the same, even if they shuffled their positions a bit. The Win/Spy.Agent trojan was the most detected cryptostealer, accounting for 37.4% of cryptostealer detections. The Win/PSW.Delf trojan had the second-highest share of detections at 24.3%, followed by MSIL/ClipBanker with 19.5%. As with coinminers, all three most-detected cryptostealers were on a downward trend in T1. MSIL/ClipBanker suffered the worst decline out of the three and dropped by almost 70%.

Based on our telemetry, cryptostealer attacks were pretty spread out all over the world. Still, somebody had to be the one that faced the most cryptostealer attack attempts, and in T1 2022 it was Peru with 6.9%. The next in line was Turkey with 4.9% and the third-place holder was Spain and its 4.5%.

The country statistics of all cryptocurrency threat detections had the same three countries on top as in the coinminer list: Russia with 10.4%, Peru with 6.4%, and the US with 4.9%.

WEB THREATS

The number of phishing URLs shoots up; scammers exploit interest in the Russia-Ukraine war.

The first four months of 2022 saw a stable level of overall web threats blocked, with only a negligible decline of 1.8%. In regard to the number of unique URLs blocked, there was a 14.9% decline in T1 2022. On average, ESET telemetry recorded 4.8 million daily web threat blocks and 370 thousand harmful URLs daily.

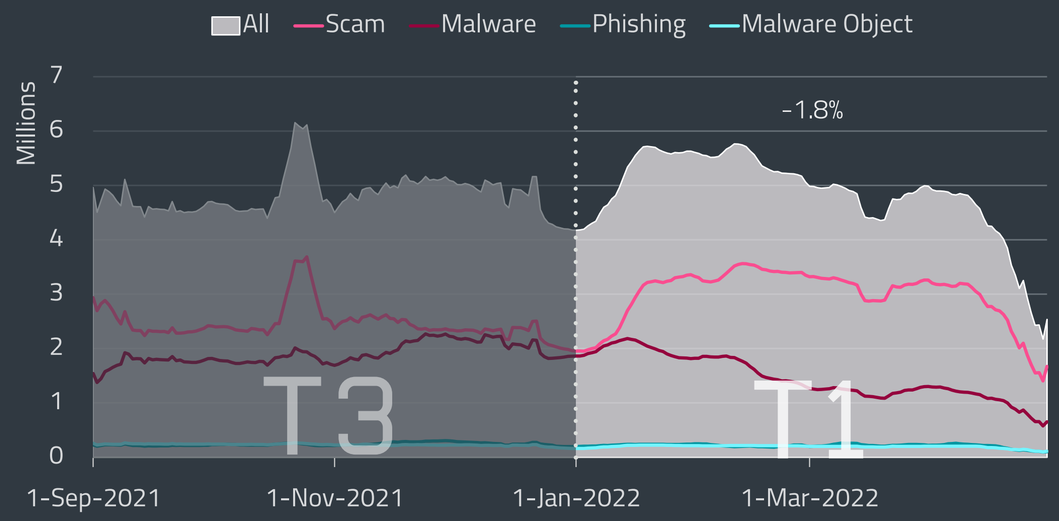
Malware-distributing websites, represented by the Malware category, saw the steepest decline in both total blocks and the number of URLs seen, declining by 26% and 23%, respectively. In the Phishing category, the number of URLs blocked increased by almost 30%. Interestingly, this didn't result in a growth in total phishing blocks, and these even saw a decline of 13.2%.

The number of blocked phishing URLs started increasing sharply in March and the levels stayed way beyond the T1 and preceding T3 average for the rest of the period. The peak detection level, reached on March 7, was three times higher than the daily T1 average, with 82,000 unique URLs blocked.

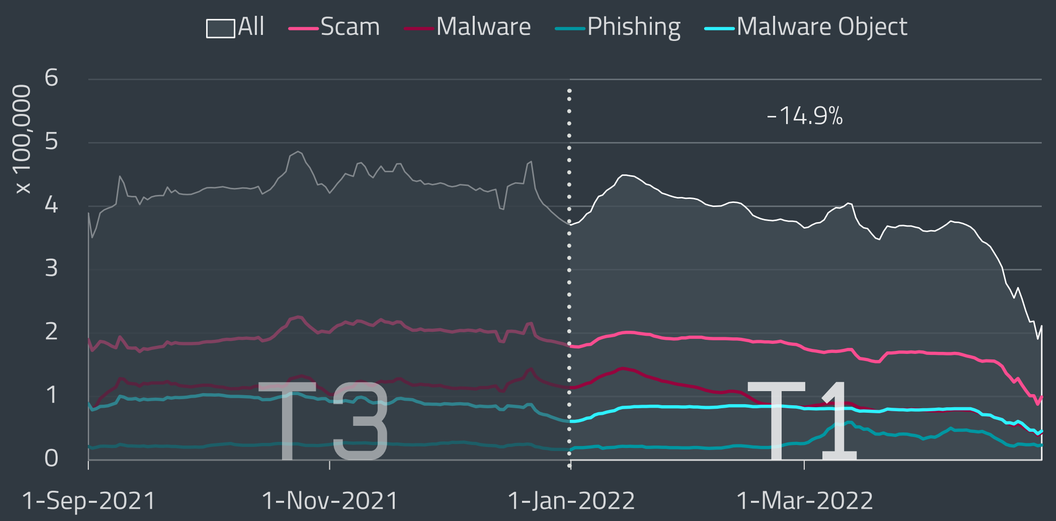
The opposite was true for websites categorized as Scam, which had approximately 20% more total blocks, but this increase wasn't reflected in the number of URLs seen. Scam blocks started increasing in the second half of January, remained at the raised levels until mid-April, and then dropped to T1's minimum.

	Malware	Scam	Phishing
1	pdloader[.]com	survey-smiles[.]com	propu[.]sh
2	iclickcdn[.]com	newrrb[.]bid	mrproddisup[.]com
3	demotzincky[.]casa	v.vfghe[.]com	tech4-you[.]com
4	aj2396[.]online	bwukxn[.]com	www--bancosantafe--com--ar.insuit[.]net
5	plehimselves[.]info	cellar.z5h64q92x9[.]net	thecred[.]info
6	jecromaha[.]info	loft.z5h64q92x9[.]net	foreign-movies.baby-supernode[.]xyz
7	vk-online[.]xyz	prirodnolijecite[.]com	watchvideoplayer[.]com
8	www.hostingcloud[.]racing	sentrynew.sdh.com[.]ua	update.updtbrwsr[.]com
9	d.ftte[.]fun*	glotorrents[.]pw	medvitro[.]info
10	buikolered[.]com	serch07[.]biz	gelturla[.]com

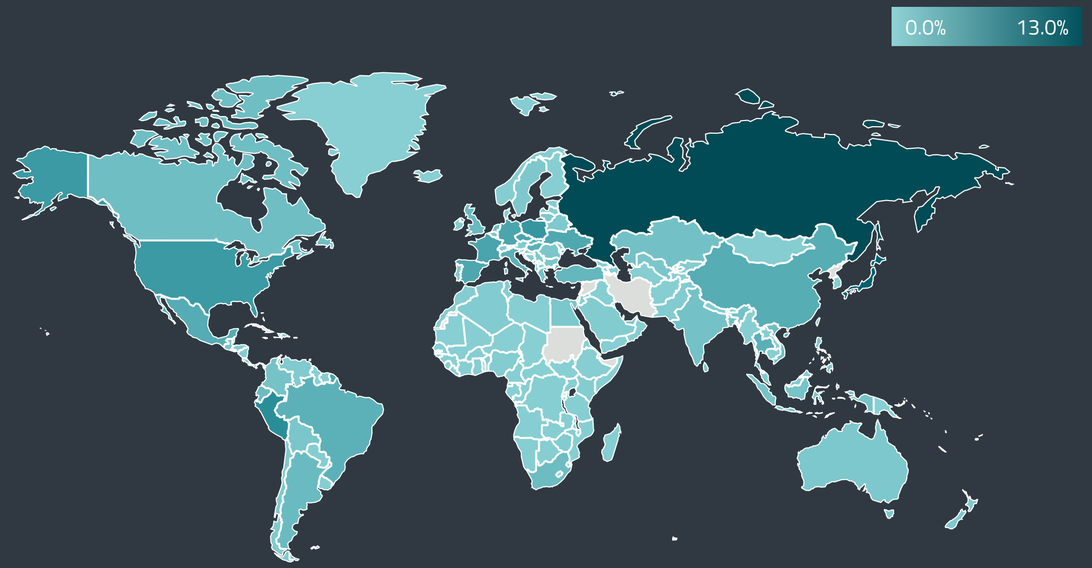
Top 10 blocked Malware, Scam and Phishing domains in T1 2022; domains first detected in this period are marked with *



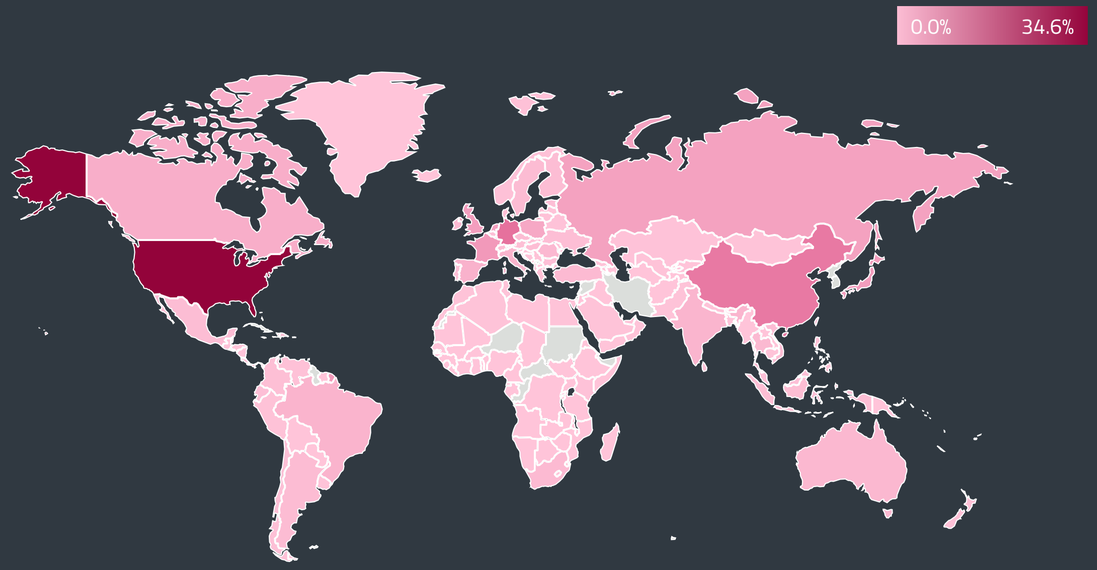
Web threat block trend in T3 2021 – T1 2022, seven-day moving average



Unique URL block trend in T3 2021 – T1 2022, seven-day moving average



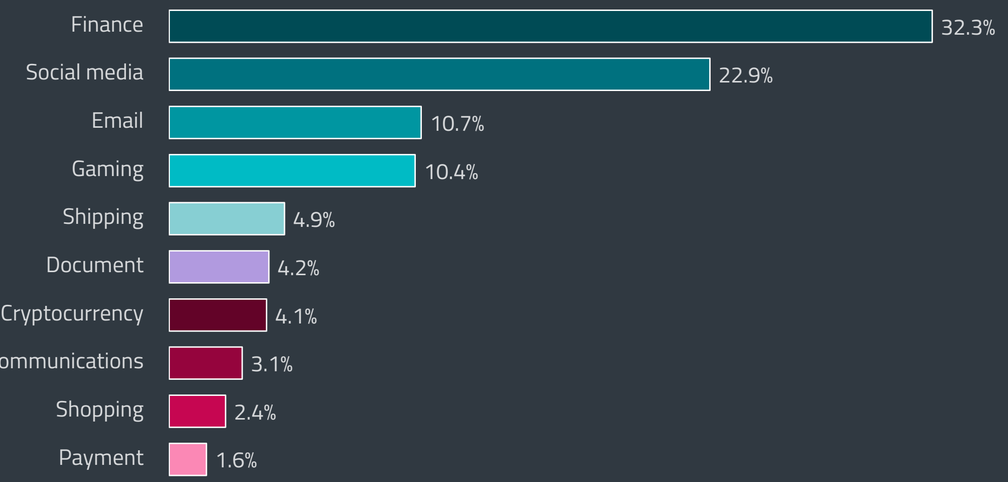
Global distribution of Web threat blocks in T1 2022



Global distribution of blocked domain hosting in T1 2022

The Russian invasion of Ukraine brought on an influx of phishing and scam campaigns attempting to take advantage of people trying to support Ukraine during the war. Most commonly, the campaigns used fictitious charities and fundraisers as lures. The first fraudulent domains exploiting the war started cropping up almost immediately after the start of the invasion, as documented by ESET Research on *Twitter* [92].

Overall, the number of harmful websites blocked in T1 2022 was greatest in Russia (13.0% of all website blocks), followed by Japan (9.1%), Peru (4.4%), Poland (3.9%), and the United States (3.6%). 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 (34.2%), followed by a wide margin by Germany (7.4%), China (6.6%), France (3.9%), and Japan (3.5%).

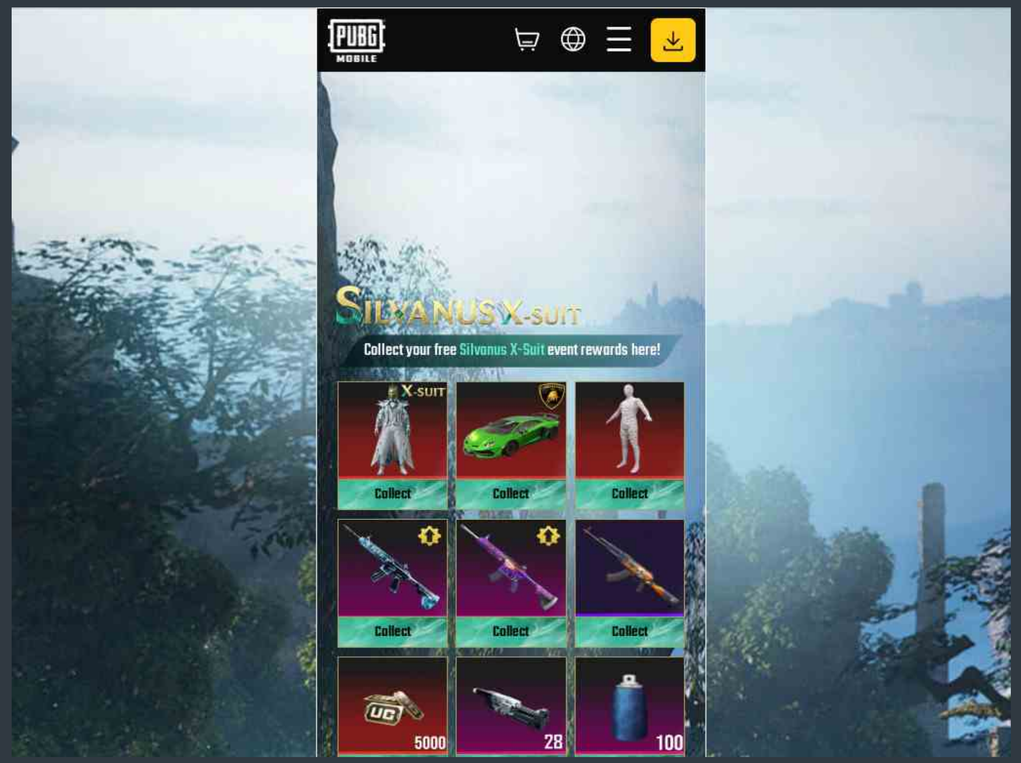


Top 10 phishing website categories in T1 2022 by number of unique URLs

Based on ESET phishing feeds, approximately a third of the phishing URLs detected in T1 2022[1] impersonated financial organizations, much as in T3 2021. Social-media-themed phishing lures, mainly represented by fake Facebook and WhatsApp login pages, came in second with 23% of URLs seen.

After booming in T3 2021, the Shopping and Cryptocurrency categories were both on the decline in T1 2022. Online-shopping-themed phishing, represented mostly by websites impersonating Amazon, was significantly reduced in the number of URLs in circulation, decreasing by 73.6% and dropping from third to ninth place. Phishing websites impersonating cryptocurrency platforms retreated from fourth to sixth place, declining by 45% in the number of unique URLs detected.

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



Example of a phishing website (pubgmystical[.]com) impersonating a marketplace for the PUBG MOBILE game

On the other hand, phishing websites masquerading as email services and gaming platforms were on the rise this period, the former increasing by 54% and the latter by a remarkable 291% in numbers of URLs seen. In the Gaming category, websites impersonating marketplaces for various online games were widespread.

Although not placing in the top 10 categories, there was a notable 126% increase in travel-themed phishing URLs. These were almost exclusively represented by Airbnb copycats, often residing on deceptive domains, with "airbnb" used as a subdomain on what is actually an unrelated domain (e.g., airbnb.com[.]ee).

A similar trend of rising travel-themed lures was also noted in ***Email threats***, presumably the result of lifting pandemic restrictions.

In the area of homoglyph attacks, the top 10 targets saw a bit of reshuffling, with eight of the targets being newcomers to the top 10 and about a half of the underlying fraudulent domains first appearing only in T1 2022.

On the other hand, several of the previously prevalent homoglyph domains completely disappeared from the scene in T1, and the overall number of blocks recorded was almost halved compared to T3 2021. Interestingly, fake cryptocurrency-themed websites, which previously led the charts along with those impersonating banks and social media, were not among the top detected homoglyph domains during this period.

The second most prevalent impostor domain, new in T1, "ecц[.]online" (ц instead of u), likely attempted to impersonate the website of Eastman Credit Union. At the time of writing, the fraudulent domain was no longer operational.

Other homoglyph domains first seen in T1, albeit with only a handful of blocks, impersonated Mastercard (mastercaṛd[.]com – ṛ instead of r), Suncoast Credit Union (suncoastcreditunlọn[.]com – l instead of i and ọ instead of o), LinkedIn (lınkedin[.]com – ı instead of i) and Twitter (twịtter[.]com - ị instead of i).

Top 10 brands and domain names targeted with homoglyph attacks in T1 2022

EMAIL THREATS

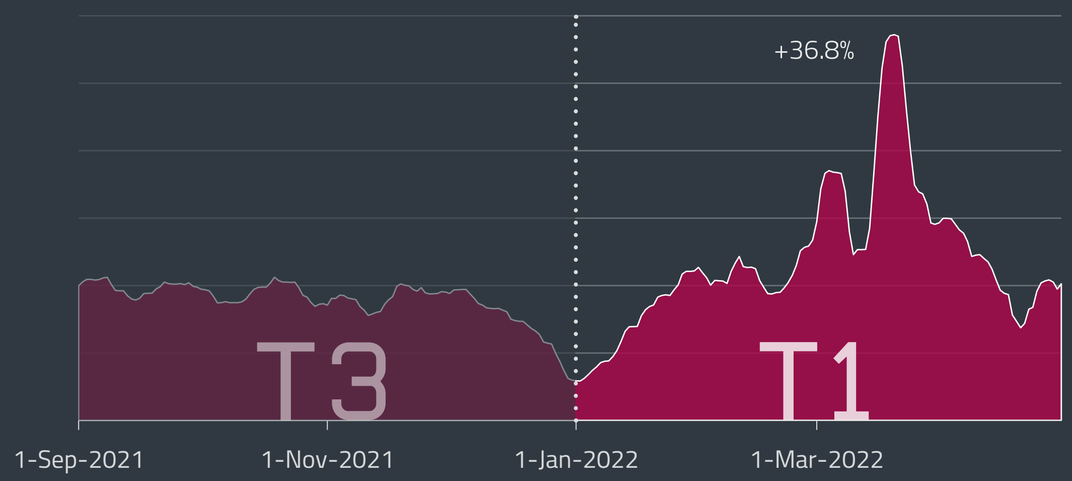
Email threats spike as Emotet's malicious documents flood back to users' inboxes.

Email threats grew by 37% in T1 2022 – the largest increase observed in this category since 2020. Threat activity rose continually throughout January and February, peaked in mid-March – daily email threat detections more than tripled the T1 average – and declined throughout April.

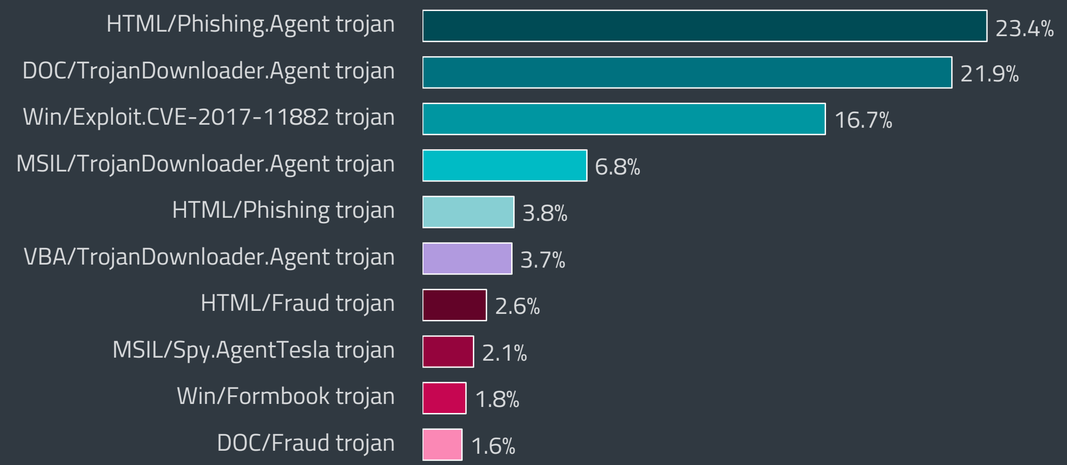
The March peak was driven by mass-scale email campaigns of the notorious Emotet, relying on malicious Microsoft Word documents, detected as variants of DOC/TrojanDownloader.Agent. The incidence of DOC/TrojanDownloader.Agent in email inboxes sprung up by a whopping 829% compared to T3 2021, making it the second most prevalent email threat of the T1 period.

DOC/TrojanDownloader.Agent detections were dominated by its DPV and DWJ variants, which built the majority of the mid-March spike. Japan was the country most affected by these Emotet campaigns, followed by Italy and Spain. These three countries were also in the lead in terms of overall email threat detections.

As discussed in the ***Downloaders*** section, this campaign preceded Microsoft's move to block macros from the internet, by default in Office programs. Toward the end of T1, just when the change was set to roll out, ESET researchers noticed Emotet operators shifting their tactics and switching to malicious LNK email attachments – although operating on a much smaller scale than with their infamous document-based campaigns.



Malicious email detection trend in T3 2021 – T1 2022, seven-day moving average



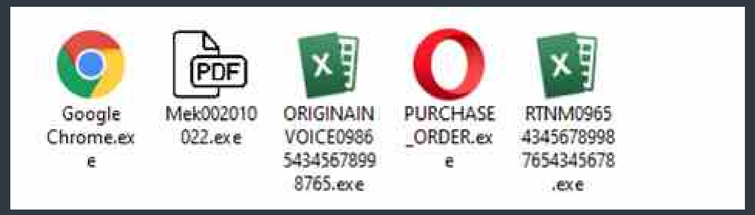
Top 10 threats detected in emails in T1 2022

EXPERT COMMENT

The Emotet email campaigns seen in T1 2022 brought on an unpleasant flashback to the botnet's prolific pre-takedown era in 2020. With macros now blocked by Microsoft, however, the March wave may well have been the last onslaught of malicious documents delivered by Emotet that we'll see – but unfortunately, it's only a question of the time until cybercriminals find another distribution avenue with similar potential.

Jiří Kropáč, ESET Director of Threat Detection

Another threat seeing substantial growth in T1 was MSIL/TrojanDownloader.Agent, marking a 130% increase from T3. Most often seen in email inboxes was MSIL/TrojanDownloader.Agent.KJO, a trojan used to download further malware from the communication platform Discord. It is distributed via Discord messages and email, in EXE attachments often using icons mimicking Excel or HTML files.

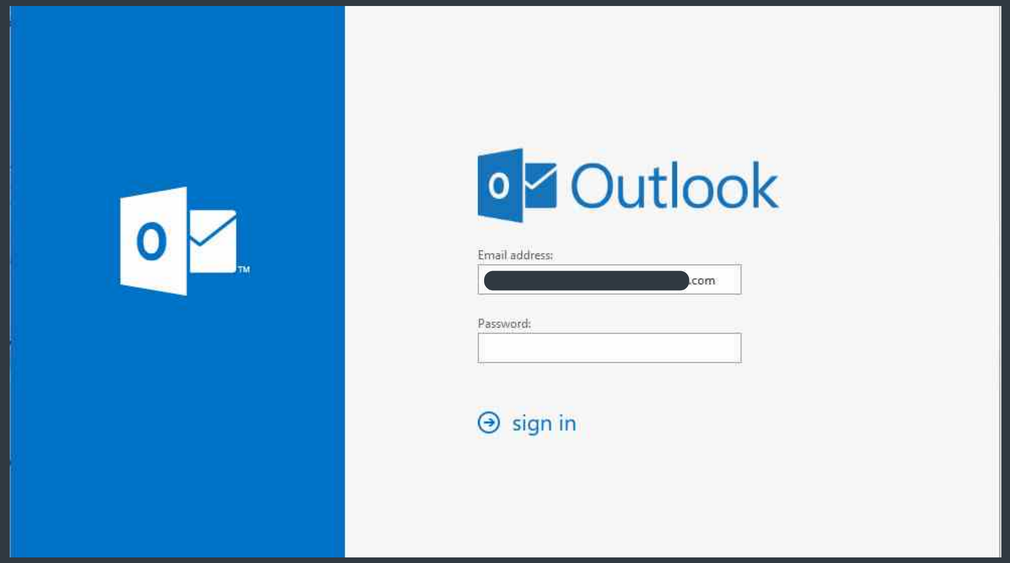


Examples of MSIL/TrojanDownloader.Agent email attachments

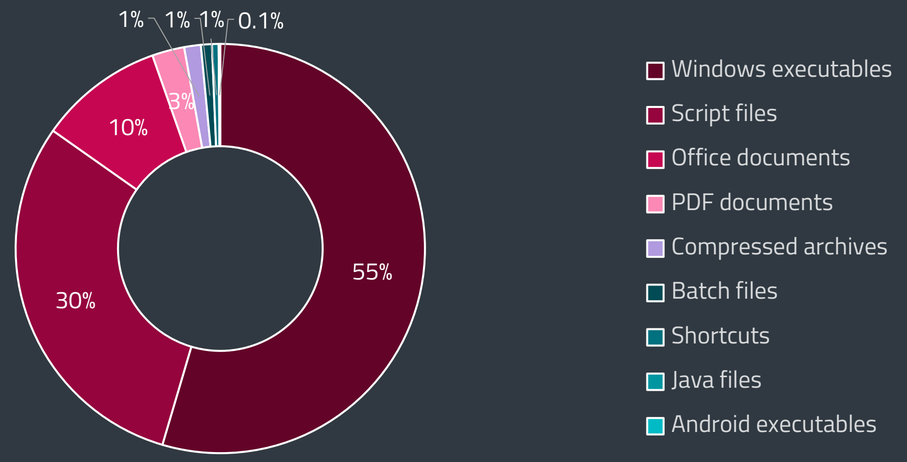
The downloaded malware is typically a high-profile infostealer, such as Agent Tesla or QBot. ESET telemetry shows a large but short-lived MSIL/TrojanDownloader.Agent.KJO email campaign in February, with highest detection numbers in Turkey, Japan, and Spain.

Outlook, DHL, and Microsoft were brands most commonly seen impersonated in phishing emails in T1 2022. Emails purporting to include an Outlook login page were detected in large waves in February and April, overtaking the previously leading DHL-themed lures in the overall number of detections. In fact, these emails, detected as HTML/Phishing.Outlook, just failed to make it into the top 10, placing eleventh with 1.5% of all Email threat detections caught in T1.

According to ESET telemetry, HTML/Phishing.Outlook was most commonly detected in the UK, followed by New Zealand and the US However, pre-filled email addresses in the phishing forms suggest the phishing might have been targeted against extractive industries in Kazakhstan and Africa.



Phishing form impersonating Outlook, detected as HTML/Phishing.Outlook



Top malicious email attachment types[2] in T1 2022

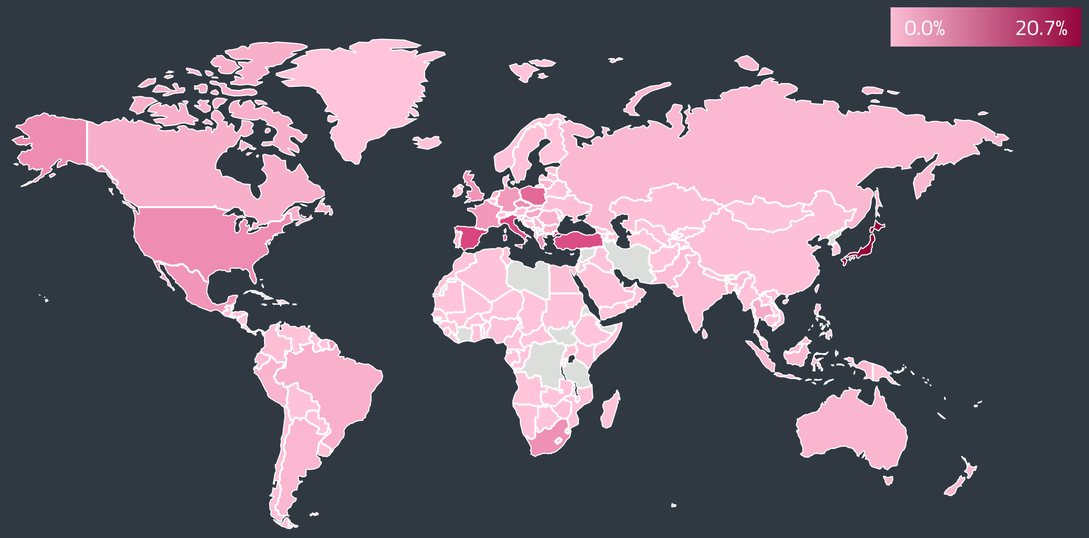
On the other hand, previously active phishing campaigns posing as the document-signing service DocuSign subsided in T1 2022, their detections declining by 75% compared to T3 2021.

Looking into the subject lines of the malicious emails detected in T1, the most common subject line was "EU Business Register 2022/2023", updated messaging of a long-circulating, widespread scam detected as PDF/Fraud. Through these emails, scammers attempt to trick recipients into paying a large fee for their inclusion into a purported database of European business subjects.

Beyond the usual topics of malicious email subjects (such as payments, orders, and deliveries), which remained largely unchanged, there was a notable increase in malicious travel-themed emails in T1. These increased more than sevenfold compared to T3 2021, but still represented less than 1% of all identified malicious email messages.

As for the file types of malicious attachments detected in emails, executables remained the leading format, followed by script files and Office documents. While the share of executables was reduced in T1, script files and Office documents grew more prevalent. Office files doubled their share this period as a result of the aforementioned Emotet activity – but this trend is expected to be reversed in the following periods.

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



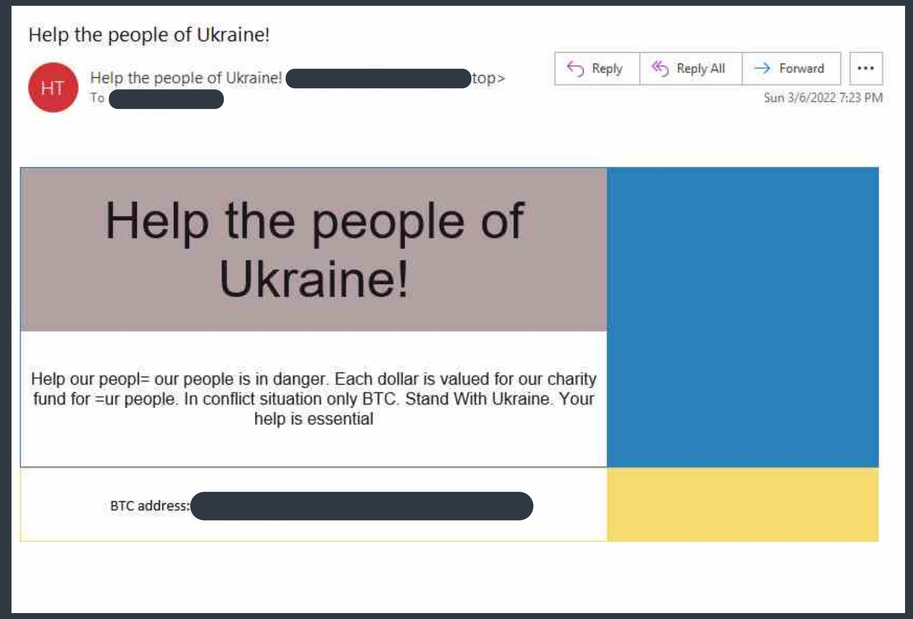
Global distribution of Email threat detections in T1 2022

Spam detections increased by 5.8% in T1, mostly due to two large spikes, the first on February 24 and the second on April 12. ESET telemetry recorded an overall increase in email messages scanned around these dates, but while the total numbers of emails scanned increased up only to 37% against the T1 average, spam levels jumped between two- and threefold. Other than these upticks, spam levels remained fairly steady over this period.

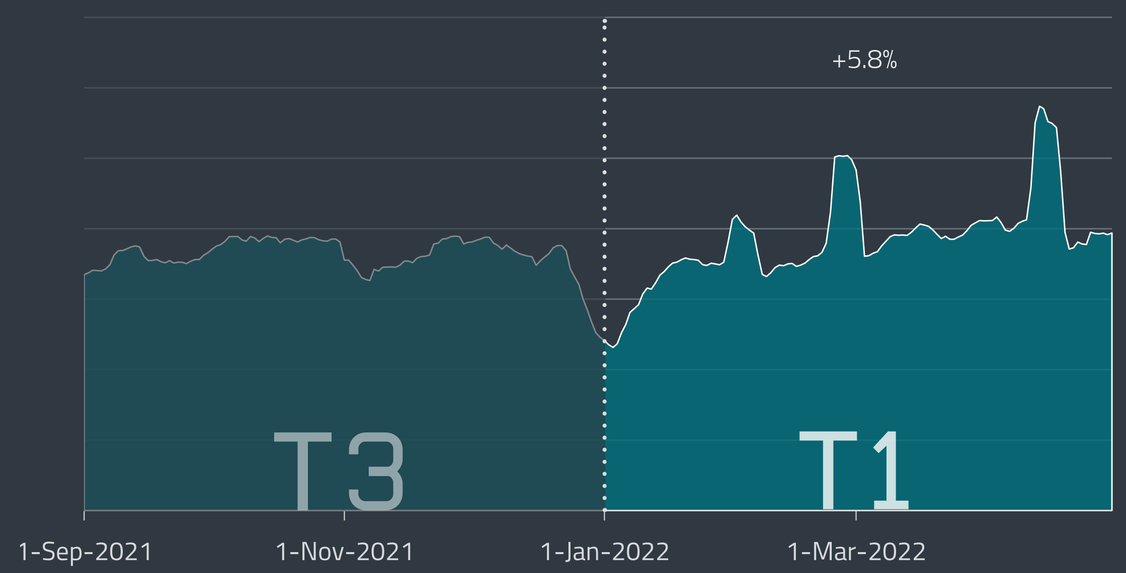
The February 24 spike coincides with the beginning of Russia's invasion of Ukraine. As noted in the *Web threats* section, scammers didn't shy away from exploiting the war and immediately started taking advantage of people trying to support Ukraine, using fictitious charities and fundraisers as lures.

Looking at the geographic distribution of spam sources according to ESET telemetry, 16% of spam emails detected in T1 originated from the United States, followed by China (13.2%), Japan (9.9%), Poland (6.5%), and France (5.7%) – the same top five countries as in the previous period. The share of spam in all emails sent was highest in China (66%), followed by Singapore, South Korea, Russia ,and Argentina, where between 23% and 34% 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.



Example of a spam email exploiting the war in Ukraine



Spam detection trend in T3 2021 – T1 2022, seven-day moving average

ANDROID THREATS

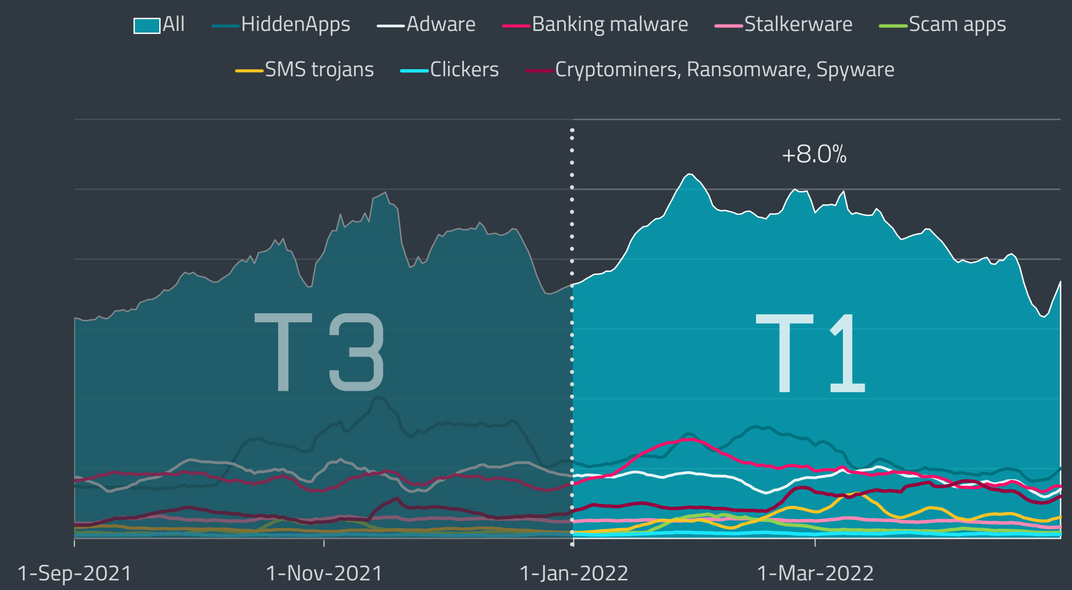
Android threat detections grew slightly in T1 2022; HiddenApps continued to be the most prevalent type of Android threat while Spyware experienced significant growth.

Compared to the last four months of 2021, Android detections saw a slight growth of 8% in T1 2022; however not all Android threat categories experienced increased numbers of detections.

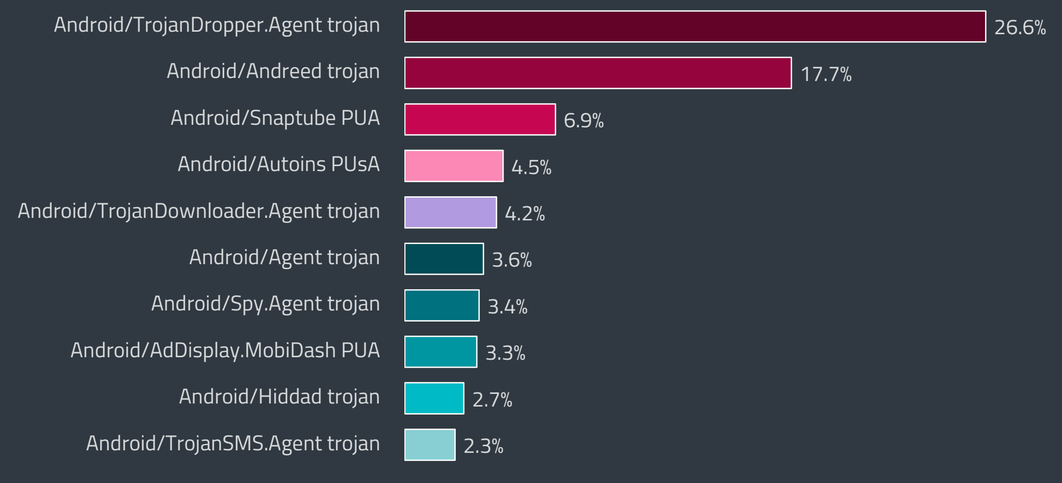
HiddenApps, deceptive apps that hide their own icons, continued to be the most prevalent type of Android threat according to ESET telemetry; although their detections decreased by 10.2% in T1.

Another Android category that experienced a decrease in detection numbers is Adware (-11%), continuing the trend started in T3 2021. Stalkerware detections also dropped compared to T3 2021, by 11.7%. ESET monitors this threat category separately and not as a part of Spyware, even though Stalkerware is a type of consumer-grade spyware.

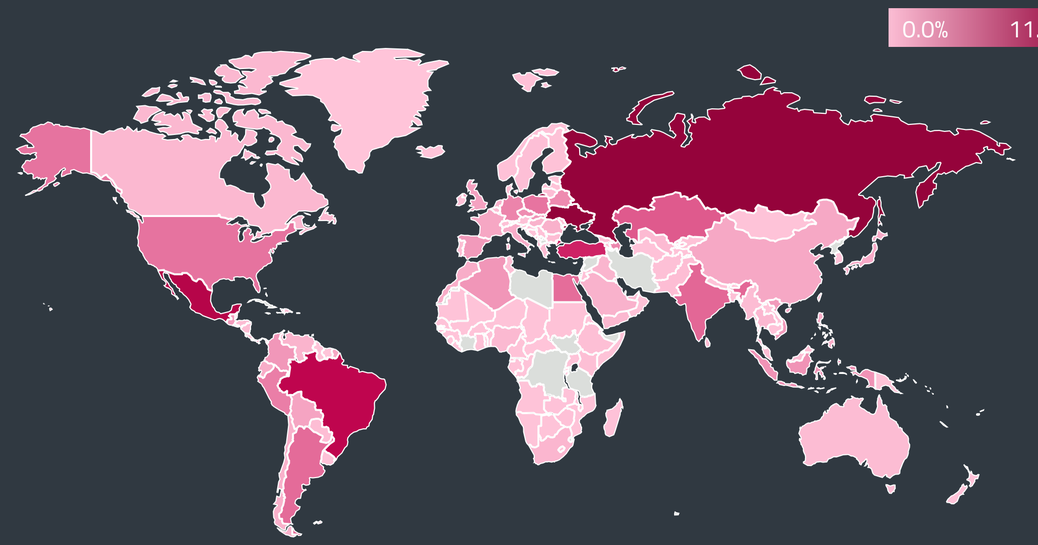
It is important to repeat the findings of ESET Research's *in-depth analysis of stalkerware* [93], because an investigation by TechCrunch revealed that some of the stalkerware apps identified in ESET's previous analysis are in fact controlled by one operator that is, *according to TechCrunch* [94], a



Detection trends of selected Android threat categories in T3 2021 – T1 2022, seven-day moving average



Top 10 Android threat detections in T1 2022 (% of Android threat detections)



Global distribution of Android threat detections in T1 2022

Vietnam-based company called 1Byte. Just as ESET Research showed, these stalkerware apps tend to be riddled with vulnerabilities, exposing not only the victim but also the buyer of these apps.

Android Ransomware also saw a significant fall in detections in T1 2022 (-49.3%). This drop can be explained by the high volatility of cryptocurrencies that are usually used as ransom payments, which means it is difficult to make any predictions about any threats using cryptocurrencies.

The category that saw the biggest growth was Spyware (170.2%). This type of threat can access a variety of smartphone functions, such as audio and video recordings, and the huge rise in its detections means that the attackers can find various ways to monetize personal or even company data accessible through an Android device. Researchers from *Lab52* [95] identified spyware that establishes complete control over the device and its contents if permissions of the malicious app are accepted by the user. ESET detects this threat as "a variant of Android/Spy.Agent trojan", which is number seven in the top 10 Android threat detection list.

Researchers Joel Reardon and Serge Egelman at *AppCensus* [96] discovered several apps available on Google Play that contained malicious code to harvest phone numbers, email addresses and location data. Some of them had been downloaded more than 10-million times before Google took them down. However, they later appeared again in the store, albeit without the software development kit (SDK) responsible for the data collection. The researchers connected these apps with a Panama-based company which is, according to the *Wall Street Journal* [97] (paywall), linked to a US defense contractor that provides cyberintelligence services.

Further, other spyware, installed thanks to a new distribution vector by more than 100,000 users, was described by *Pradeo* [98]. The Facestealer spyware was available on the Google Play store as a cartoon photo tool and used social engineering to steal Facebook credentials. Google later removed the malicious app from its store.

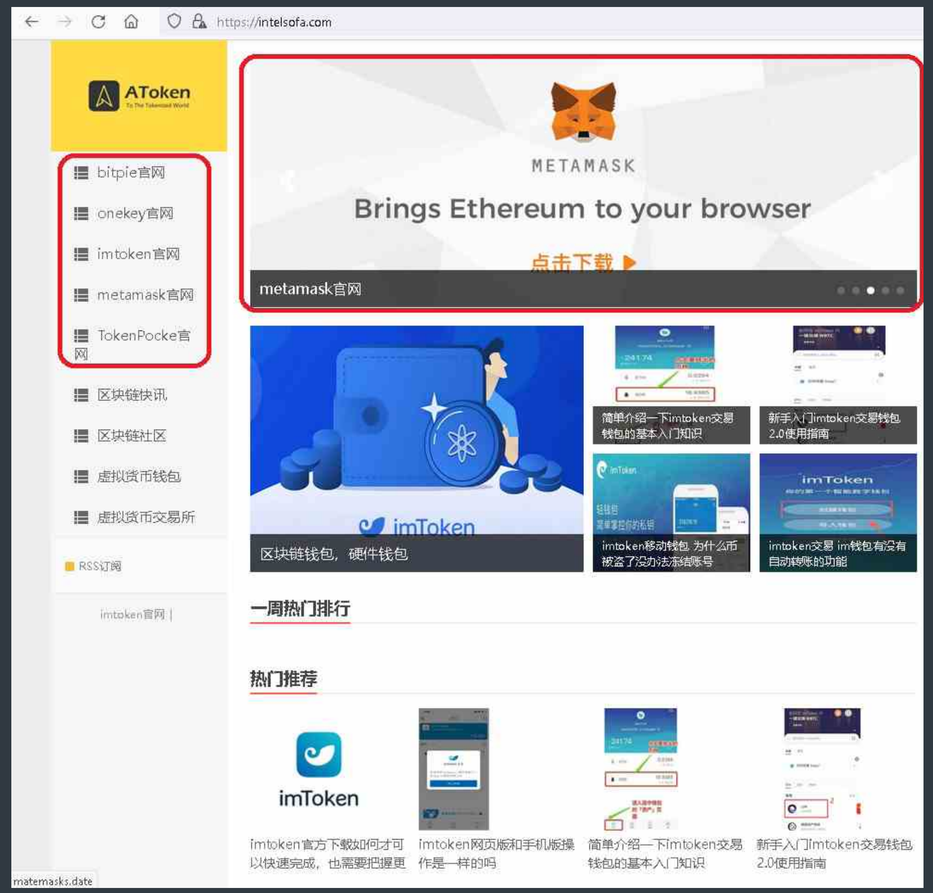
EXPERT COMMENT

Spyware does not directly steal money from its victims; instead, it steals as much sensitive data from the affected mobile device as possible. The attacker then aggregates a package with data from a large number of victims and sells it on the black market either to the highest bidder, or basically to anyone. The victims might then never know when their data will be abused and in many cases, they might be surprised years later and not be able to connect their personal identity theft to any action that might have led to this. Therefore, most people affected by this recent rise in spyware detections will not yet know they have become victims.

Lukáš Štefanko, ESET Malware Researcher

Other Android categories that experienced a significant rise in detections were Scam Apps (27.7%), Clickers (31.6%) presenting a form of ad fraud, and SMS trojans (145.20%). This threat, which is most visible on the mobile monthly bill of affected users, is represented in the top 10 Android threat list by Android/TrojanSMS.Agent.

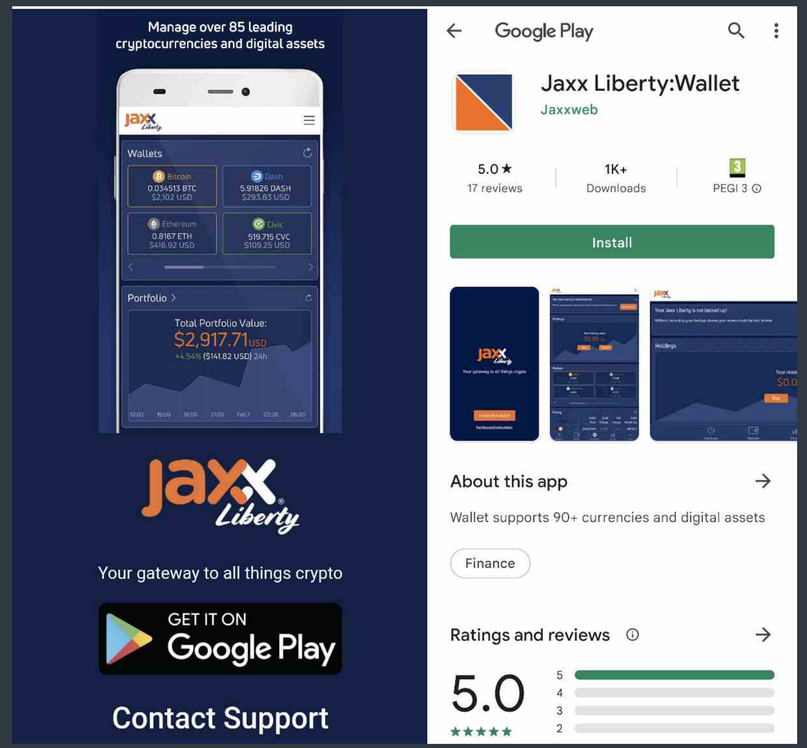
Detections of Android Cryptominers increased twofold in T1 2022, however, their overall numbers on the Android platform are too low to judge whether this growth is of any significance. As ESET researchers have pointed out many times in the past, crypto-threats are dependent on sometimes highly volatile currencies and when bitcoin appeared to be slowly regaining its value after several bad months, *ESET researchers uncovered* [33] a sophisticated scheme that distributes trojanized Android and iOS apps posing as popular cryptocurrency wallets.



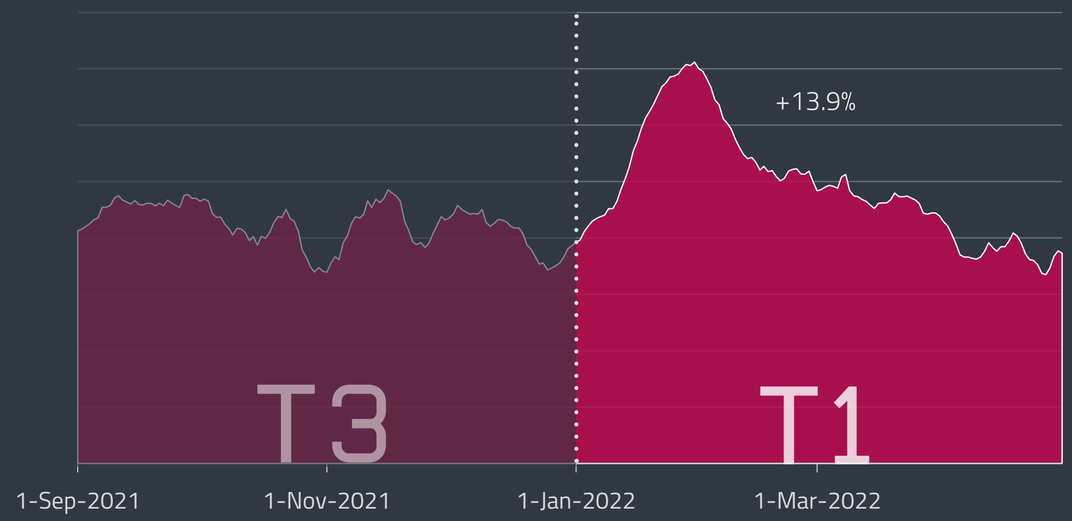
Page containing advertisement for fake wallets

These malicious apps are able to steal victims' secret seed phrases by impersonating Coinbase, imToken, MetaMask, Trust Wallet, Bitpie, TokenPocket, or OneKey. This is a sophisticated attack vector since the malware author carried out an in-depth analysis of the legitimate applications misused in this scheme, enabling the insertion of their own malicious code into places where it would be hard to detect while also making sure that such crafted apps had the same functionality as the originals. All of the dozens of trojanized cryptocurrency wallet apps detected by ESET were distributed through websites mimicking legitimate services. To make things worse, their source code was leaked online, which means it might attract other attackers.

ESET researchers also found malicious applications impersonating the legitimate Jaxx Liberty Wallet app in the Google Play store. One of the apps used a fake website mimicking Jaxx Liberty as a distribution vector. As the threat actor behind this malicious app managed to place it in the official Google Play store, the fake website redirected the user to download its mobile version from the Google Play store and didn't have to use a third-party app store as an intermediary. Google removed 13 of these apps from its store in January 2022.

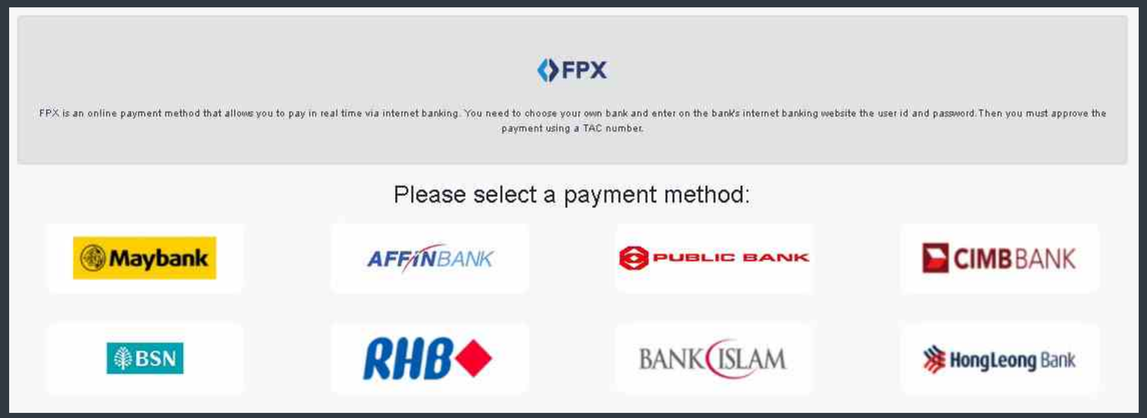


Fake website redirects the user to install the fake app from Google Play



Android Banking malware detection trend in T3 2021 – T1 2022, seven-day moving average

Android Banking malware grew by 13.9% in T1 2022, after experiencing a decline in T3 2021. In the Android top 10, it was represented by Android/TrojanDropper.Agent. One of the Android banking malware cases that ESET researchers analyzed in T1 was a campaign targeting the customers of *eight Malaysian banks* [31]. The malware is distributed via copycat websites of legitimate services with the majority being cleaning services available in Malaysia.



Malayan banks targeted by malicious apps

These copycat websites include buttons that claim to download apps from Google Play. However, these buttons do not actually lead to the Google Play store, but to malicious apps controlled by the attackers. The malicious apps pretend to offer goods and services for purchase while matching the interface of legitimate stores. At the payment step, victims are presented with a fake payment page and are asked to select one of eight Malaysian banks and then enter their online banking credentials.

Many other researchers also discovered new Android banking malware or new distribution vectors. *Check Point* [99] found Sharkbot disguised as security apps on the Google Play store, *Bitdefender* [100] identified new FluBot and TeaBot campaigns spreading through SMS messages asking "Is this you in this video?", while *Threat Fabric* [101] researchers analyzed another piece of Android banking malware – Medusa – that started a distribution scheme using the same SMS phishing service as FluBot. They *also* [102] discovered a new threat they dubbed Xenomorph, targeting users of 56 different European banks. All of the aforementioned threats are detected by ESET as variants of the Android/TrojanDropper.Agent trojan. According to ESET telemetry, countries with the biggest detections of this umbrella banking malware threat are Brazil, Mexico, Turkey, Argentina, and Ukraine.

And to show that Android can also suffer from high-impact vulnerabilities, *researchers at Tel-Aviv University* [103] discovered that Samsung phones were shipped with design flaws in Android's hardware-backed cryptographic key management services. The flaw affected millions of Samsung's flagship phones including the Galaxy S8, S9, S10, S20, and S21.

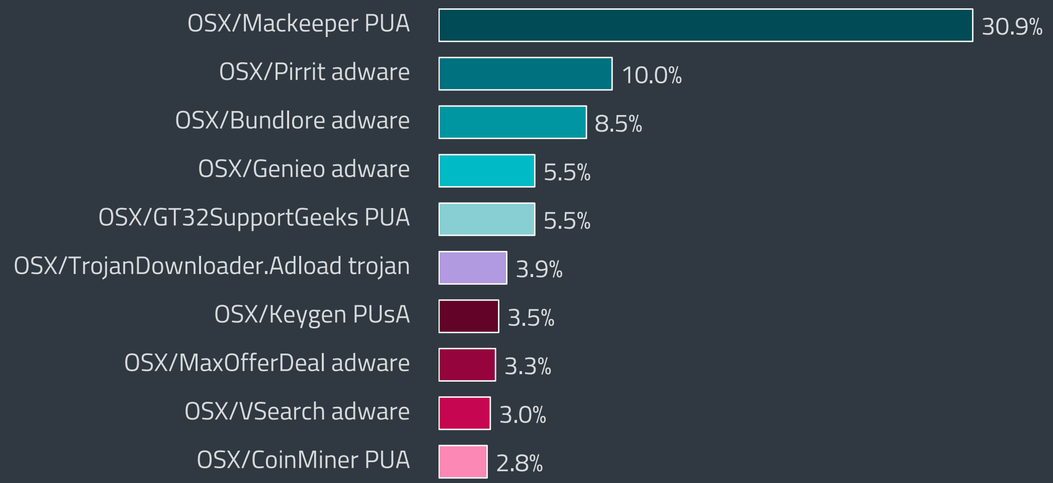
macOS AND iOS THREATS

macOS detection numbers saw a notable decline in T1 2022; compared to T3 2021 the biggest decrease was visible in the Trojans category.

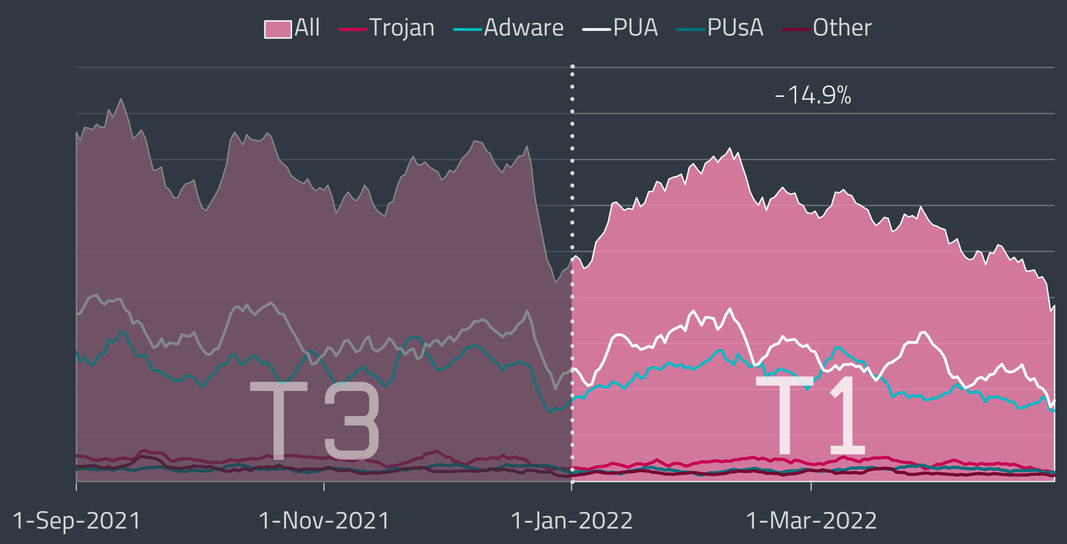
In T1 2022, detections of macOS threats saw a notable decline (14.9%) and, what's more, a notable decline was detected in all monitored macOS threat categories. Trojans experienced the biggest decline (-18.8%) compared to T3 2021, followed by Potentially unwanted applications (PUAs, -15.6%). This type of threat is the most widespread hazard targeting Mac systems; it accounted for around 47% of all macOS detections during the first four months of 2022, visible also in the top 10 macOS threats according to ESET telemetry. The number one macOS detection – OSX/Mackeeper PUA – has been the same since our Q1 2020 Threat Report, but now with higher prevalence. In T1 2022 it was responsible for more than 30% of all macOS threat detections. This PUA, displaying unsolicited ads, was most active in the United States and Japan.

Other examples of these types of apps – installed by users after being tricked by the description of an allegedly useful program – are OSX/GT32SupportGeeks PUA and OSX/CoinMiner PUA, which are number five and number ten on the top 10 macOS threat list. The first one is often presented as a macOS performance scanner that reports alleged issues on the system; the second one uses the system's resources to mine digital currency.

Adware (-13.8%) and Potentially unsafe applications (PUsAs, -12.7%) also declined in T1, with Adware being the second most prevalent macOS threat in T1 with 38% overall prevalence. In the top 10 macOS threat list, it is represented by OSX/Pirrit, OSX/Bundlore, OSX/Genieo, OSX/MaxOfferDeal, and OSX/VSearch. OXS/Bundlore is notoriously known for "bundling" adware applications with legitimate apps, while OSX/Genieo, OSX/MaxOfferDeal, and OSX/VSearch intercept internet searches. All of the above-mentioned adware apps display intrusive ads.



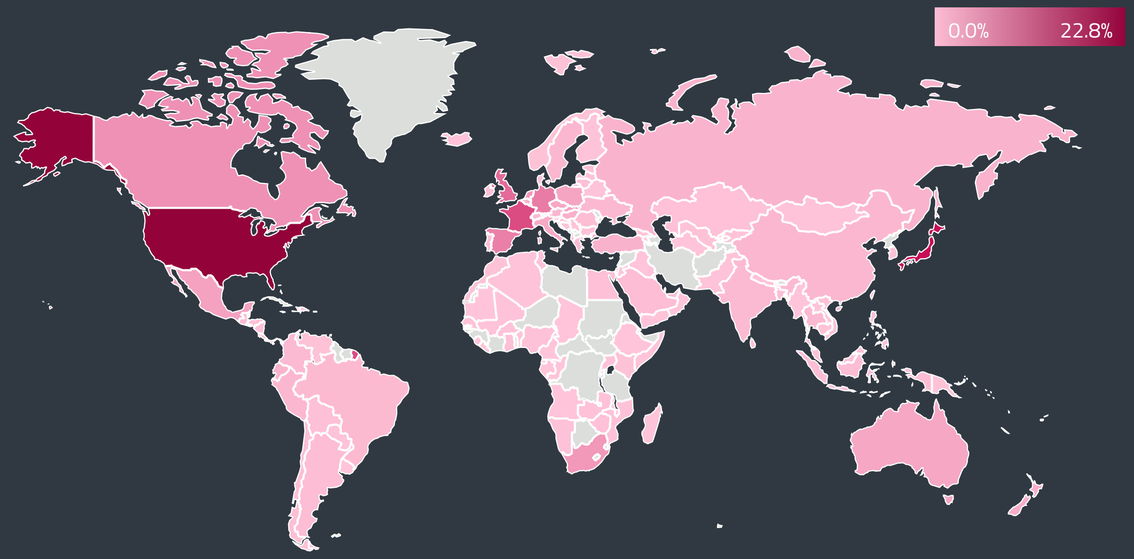
Top 10 macOS threat detections in T1 2022



macOS threat detection trend in T3 2021 – T1 2022, seven-day moving average

According to ESET telemetry, the most macOS detections in T1 2022 were found in the United States, with 21.6%, followed by Japan (12.8%), the United Kingdom (7.2%), South Africa (5.9%), and France (5%). The dip visible around the end of 2021 and the beginning of 2022 is similar to the one detected the year before, and could be attributed to this specific time of the year in which people around the world celebrate various religious and cultural festivities and simply don't use their computers that often.

It is important to note that, for the purposes of these Threat Reports, to describe and monitor threats faced by macOS systems in a more real-world way, we changed the methodology behind the analysis of macOS threat prevalence at the turn of the year. However, data from the previous period was also recalculated so that this report is able to analyze comparable data. And while the overall number of macOS detections is indeed decreasing, companies, organizations, and high-profile individuals should keep in mind that if a target is interesting enough, threat actors or APT groups will also deploy malware targeting non-Windows systems.



Global distribution of macOS threat detections in T1 2022

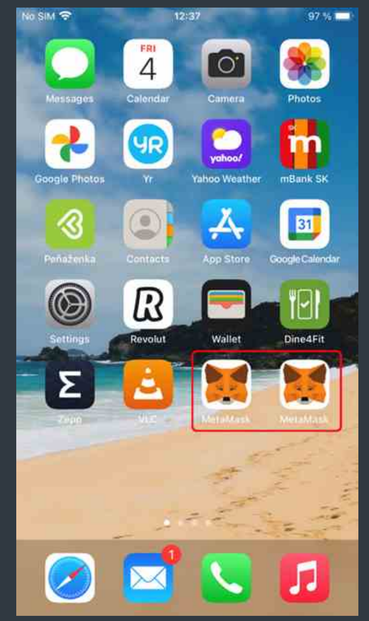
The latest ESET Research discovery of a case like this is a threat *compiled for both Intel and the newer Apple silicon processors* [104] used in the Mac lineup. This malware, detected by ESET as OSX/NukeSped.N, is an executable disguised as a job description document and ESET researchers think it is part of a campaign by the infamous Lazarus APT group, which has extensive experience in hiding malware in fake job lures.

At the beginning of the year, ESET researchers published their insights about a compromised Hong Kong pro-democracy radio station website that was serving a Safari exploit that installed cyberespionage malware on visitors' macOS devices. *DazzleSpy* [46], as it was dubbed by ESET, is macOS malware previously unseen by ESET telemetry. Its features include gathering information about the system; searching, downloading and uploading files; exfiltrating the macOS keychain; and providing access for the perpetrator via remote desktop. Comments in its code suggest it could also exploit iOS and PAC-enabled (Pointer Authentication Code) devices such as the iPhone XS and newer models. Given the complexity of the exploits used in this campaign, ESET researchers assess that the group behind this operation has strong technical capabilities.

Another example of a cross-platform threat was discovered by researchers at Intezer. Called *SysJoker* [105], the macOS version is described more thoroughly by *Objective-See* [106]. SysJoker masquerades as a system update and is part of an espionage campaign; Intezer assess this backdoor is after specific targets. ESET telemetry suggests the same – SysJoker has a low prevalence with detections mainly in Asia and the United States. *Volexity* [107] also discovered a new macOS variant of a feature-rich, multiplatform malware family, dubbed Gimmick. It uses public cloud hosting services (such as Google Drive) for command-and-control channels.

Despite their built-in security features, iOS devices are also targets of cyberthreats and targeted attacks. As is described in the *Android* section, ESET researchers discovered *maliciously patched cryptocurrency wallets* [33] targeting not only Android but also iOS devices to steal victims' seed phrases. These malicious apps are not available on Apple's App Store; they must be downloaded and installed using configuration profiles, which add an arbitrary trusted code-signing certificate. Using these profiles, it is possible to download applications that are not verified by Apple, from sources outside the App Store.

It means the weakest security link in such cases is the user, but not every threat can be detected by safe user behavior and security features…such as the Pegasus phone hacking tool mentioned in ESET Threat Reports several times in the past. As new revelations come to light about the latest victims of this NSO Group spyware tool, for instance the *Spanish prime minister* [108] and *Finnish diplomats* [109], Reuters *uncovered* [110] that a second Israeli spy firm – QuaDream – used exploits similar to those employed by NSO Group. Besides that, *Google's Project Zero* [111] published its own in-depth analysis of the ForcedEntry exploit that can remotely compromise an iOS device for the purpose of installing the Pegasus spyware. For a typical user, Pegasus is impossible to detect; however, Apple patched the underlying issues in September 2021. It means that updated devices should be secure, but the discovery of other vulnerabilities *shows* [112] that updating must be done on a regular basis, while hoping one will not be targeted by another zero-day exploit in the meantime.



Trojanized wallet successfully installed on iPhone

EXPERT COMMENT

Seeing macOS threats declining should be a positive sign for users. However, as is shown not only by our own research, companies and organizations should stay on the lookout for targeted macOS malware, protect their systems accordingly and try to increase employee awareness also about non-Windows-based threats. Companies simply don't have homogenous networks and it takes only one device to be compromised, regardless of its operating system.

Marc-Etienne M.Léveillé, ESET Senior Malware Researcher

IoT SECURITY

Mirai-based botnets still wreak havoc. Russia's war in Ukraine affects IoT.

In 2016, the noose around the necks of the authors of Mirai was tightening, yet before the police arrested them, they published the source code online. Six years later, researchers still track many IoT botnets that either use the original code or are built upon it. Gafgyt, BotenaGo, or Enemybot are only some of the names that fall within this category in ESET telemetry.

If we leave out the separately tracked Mozi and ZHtrap, Mirai-based botnets were responsible for close to 7.3 million attacks in T1 2022. Of those, 26% were aimed at the United States, 7% at the United Kingdom, and 6% at Germany. When focusing on the unique IPs facing these attacks, most were found in Germany (14%) and the US (12%). Japan, Mexico, and the UK each accounted for 5%.

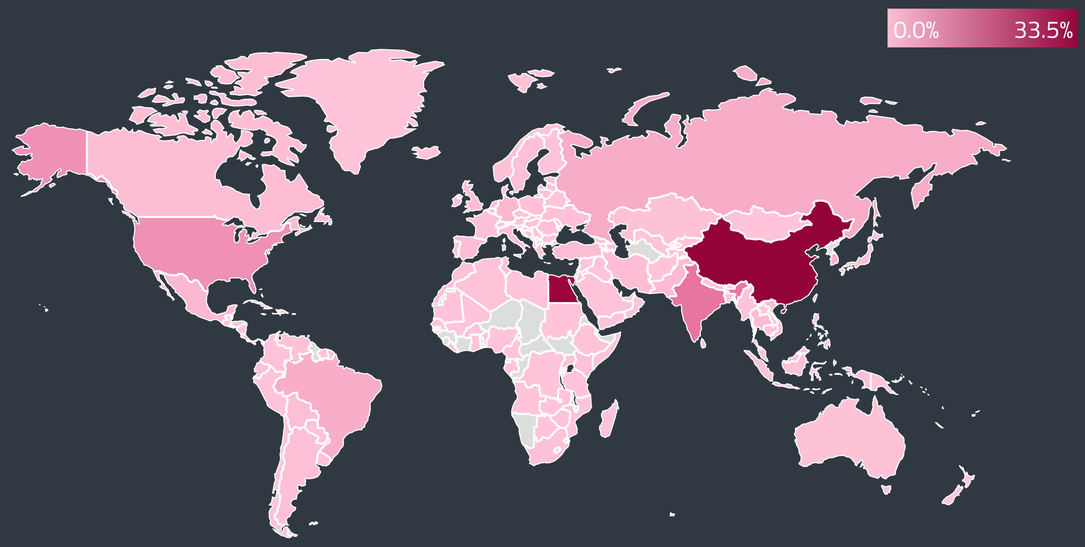
The origins of these attacks? The top three countries with the most *attackers' IPs* were China (33%), Egypt (30%), and India (7%). As for the largest amounts of malicious traffic produced, China leads the pack (22%), followed by Egypt (16%), South Korea (14%), and the US (14%). It's interesting that most of the 800+ payload servers – these being the servers delivering the final payload with their IPs embedded in the command injections in the exploits – were close to their victims, namely in the US (37%), the Netherlands (10%), and Germany (9%).

As for the spreading mechanism of Mirai-based botnets, the *ED 41471* [113] flaw – a shell command execution in MVPower DVR – was the most widespread, accounting for 84% of all attempts. A *Shodan search* [114] shows almost 67,000 such devices, although more than a third of them are tagged as honeypots. The second most exploited vulnerability was a 2017 command injection in ZyXEL P660HN routers (*CVE-2017-18368* [115]), amounting to 8% of attack attempts seen by ESET.

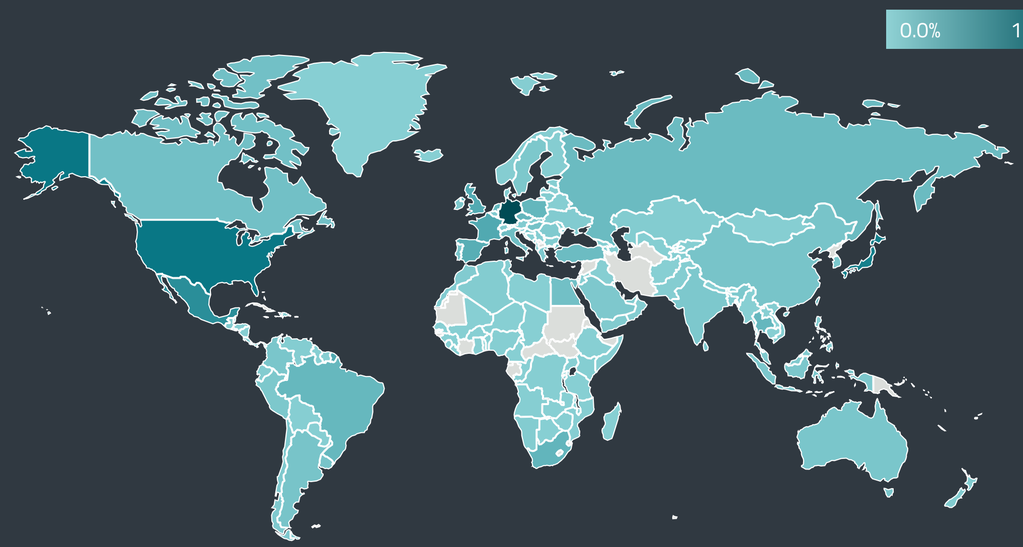
Another Mirai-based botnet tracked by ESET is ZHtrap. To broaden its ranks, its bots focused exclusively on *CVE-2015-2051* [116], a remote code execution flaw in the D-Link DIR-645 routers. ESET telemetry reported 106,000 attacks in T1 2022, a 9% increase in activity compared to T3 2021.

In T1 2022, ZHtrap's payload servers were most frequently seen in the Netherlands (41%), which is also the country where the highest number (29%) of the 106,000 detected attacks originated. The second most frequent source of malicious traffic was the US with 28%, followed by Romania with 12%, Germany with 11%, and Poland with 9%.

Although the US (13%), Germany (11%), and the UK (6%) led the list of unique IPs of ZHtrap targets, the biggest waves of the attacks made landfall in Taiwan (16%).



Global distribution of countries with IP addresses of Mirai-based bots in T1 2022



Global distribution of IP addresses targeted by Mozi botnet in T1 2022

EXPERT COMMENT

While Mirai started as a botnet targeting Minecraft infrastructure, it quickly evolved into a powerful botnet with global reach. The publication of its source code turned it into the basis of most new IoT botnets and gave birth to many mods, improvements, and additional features not seen in the original.

Mirai-based botnets also demonstrate why people need to patch their publicly accessible smart devices and systems. Devices past their ends-of-life and those that still sport patchable vulnerabilities are the prime targets enabling the continual spread of this threat.

Strong passwords and proper configuration are also key in preventing Mirai-like attacks, as the botnets themselves often brute-force their way into the weakly protected and exposed command line services such as Telnet and SSH.

Milan Fránik, ESET Malware Researcher

And then there is the biggest IoT botnet tracked by ESET, named Mozi. Its operators allegedly were *arrested* [117] by Chinese authorities in 2021, yet the botnet seems to survive and propagate further on its own – as any brain-eating zombie in a world full of vulnerable humans would.

In T1 2022, ESET detected close to 500,000 unique IPs compromised by Mozi, 11% less than in T3 2021. The geolocation of the attacker IPs was predominantly Chinese (59%) and Indian (30%). As for the targeted IPs, Germans were the most frequently hit with 17%, followed by victims in the US (8%) and Japan (7%).

If the number of attacks is considered, Mozi was detected 5.6 million times, a 6% growth compared to T3 2021. Close to a third of the attacks (30%) had to be fended off by the US.

The distribution of Mozi relied on the same intrusion vectors as in T3 2021, namely exploitation of vulnerabilities in Netgear DGN devices (EDB-25978), DASAN routers (CVE-2018-10562), D-Link routers (CVE-2015-2051), and Jaws web servers (EDB-41471). ESET data shows an increase in Mozi activity, detecting its attacks on 5.5 million occasions in T1 2022, a 6% growth vs. T3 2021.

In T1 2022, the number of router scans requested by customers as well as the number of unique-router checks remained almost identical to those in T3 2021 – oscillating around 270,000 and 164,000 respectively.

These scans also confirmed one positive trend seen in T2 and T3 2021, namely that use of weak or default passwords for routers is slowly declining. The latest checks found their ratio dropping by 7.5% compared to T3 2021. On a similarly positive note, the ratio of routers being vulnerable to one of the ESET-monitored flaws has also dropped, in this case by 15% between T3 2021 and T1 2022.

In April, reports of a new Enemybot botnet run by the Keksec group emerged. Fortinet researchers *described it* [118] as a potential update and rebrand of Gafgyt with additional features from Mirai. Its operators seem to have two main purposes in mind: DDoS and cryptomining. In contrast with other botnets mentioned in this category, Enemybot seems to use a wider set of vulnerabilities – including some very recent ones – to "recruit" bots among Seowon Intech, D-Link, and iRZ routers.

Around the same time, another new DDoS botnet called *Fodcha* [119] was observed by Qihoo 360's Network Security Research Lab. According to their findings, the main targets for its further spread are various routers, DVRs, and servers, with the number of daily live bots surpassing 50,000.

When IoT security is mentioned, most people think of weak passwords in routers or hijackable IP cameras. But more expensive "smart" devices are up for grabs too. Security researcher David Colombo *discovered* [120] that, by abusing a flaw in a third-party app, he could take control of multiple features on Tesla cars, including tracking them, opening their doors and windows, and starting their engines.

As shown by multiple stories related to the invasion of Ukraine, IoT security can become key in future conflicts. Among them was the hack and sabotage of *Viasat's KA-SAT network* [9]; a new variant of Cyclops Blink botnet (replacing VPNFilter) targeting network firewall devices by *WatchGuard* [121] and *ASUS* [122] routers, which was later *disrupted* [123] by the US authorities; and – although related only remotely – findings that vulnerable *MikroTik* [124] routers were abused in Glupteba and Trickbot campaigns. To find out more about attacks related to the war in Ukraine, read our *Featured story*.

EXPLOITS

RDP attacks dropped for the first time since the beginning of 2020; SQL and SMB followed.

Since the beginning of 2020, password-guessing attacks aimed at exposed RDP services had been constantly growing. After more than two years, this changed for the first time and the brute-force attempts have dropped by 41% between T3 2021 and T1 2022.

The shift came on January 10 as RDP attacks reached an all-time high. Since then, the detected attempts started to fall sharply. They reached the first low on January 15, then recovered partially only to drop again at the beginning of February. On February 20 – shortly before the Russian invasion of Ukraine – the password guesses fell again and oscillated at that level until the end of T1 2022.

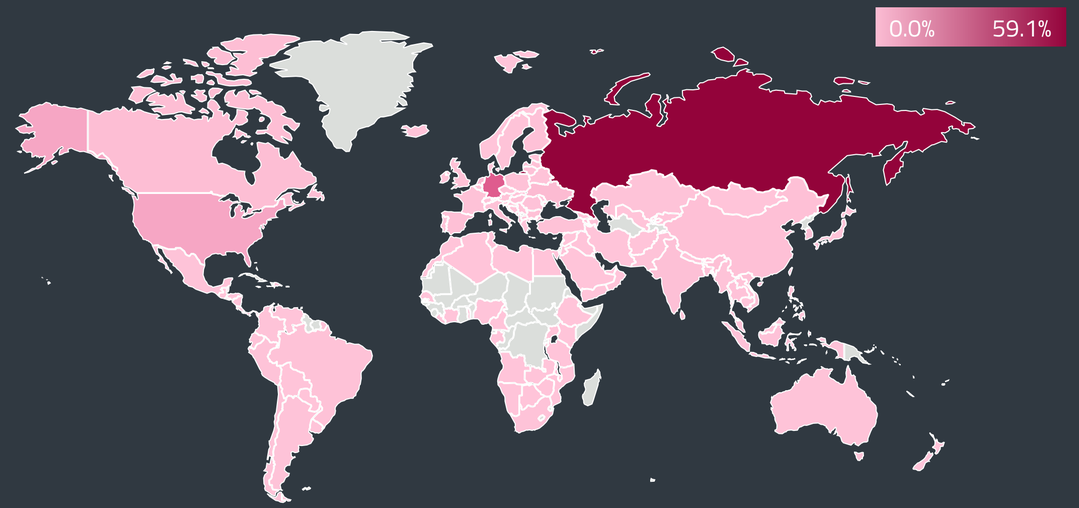
The number of unique clients reporting RDP attacks has followed a similar trajectory, dropping most notably at the turn of the year and overall, falling by 40% between T3 2021 and T1 2022. Consequentially, the average number of unique clients also decreased from 160,000 in T3 2021 to 97,000 in T1 2022.

Of the 121 billion RDP attack attempts seen in T1 2022, the top affected country was France (16%), followed by Spain (14%), Germany (8%), the United States (6%), and Italy (5%). Almost 60% of the incoming attacks came from Russia, followed in a distant second by Germany with 16% and the United States with 5%.

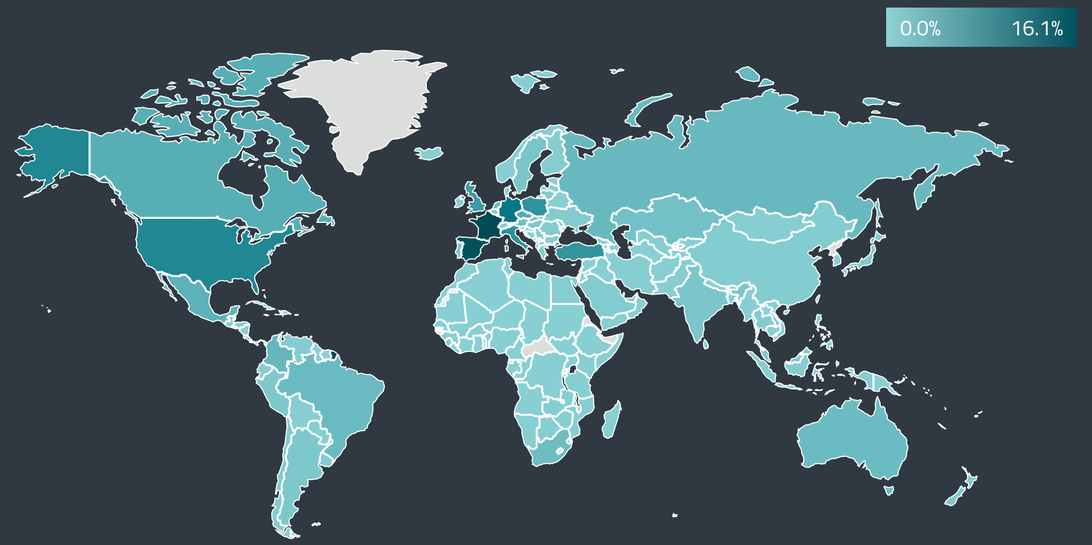
Interestingly, ESET telemetry shows an almost identical nosedive pattern for password guesses against exposed SQL services. As with RDP, SQL attack statistics reached an all-time high on January 10, followed by an extreme drop in the following days. In contrast to RDP, SQL numbers have not yet recovered. With 860 million attacks against SQL, T1 2022 saw a decline of 64% compared to T3 2021. The number of unique clients reporting malicious SQL connections decreased in the same period by 12%.

In the case of exposed SMB services, the decline started on January 9 and was slower and more gradual than in the case of RDP and SQL. Comparing T3 2021 with T1 2022, attacks targeting SMB dropped by 26%, and the number of unique clients went down by 6%.

As reported at the end of 2021, attackers also started using a new intrusion avenue – the critical ***Log4J vulnerability*** [125]. According to public reports, the beginning of 2022 only broadened the range of groups that adopted it into their toolkits, including ***Prophet Spider*** [126] and ***NightSky*** [78] ransomware on the criminal end and Magic Hound (also known as APT35, Charming Kitten, Phosphorus, TA453), ***Hafnium*** [127], ***Deep Panda*** [128], and ***TunnelVision*** [129] on the side of cyberespionage groups.



Global distribution of RDP password guessing attack attempt sources in T1 2022



Global distribution of RDP password guessing attack attempt targets in T1 2022

EXPERT COMMENT

There may be many reasons behind the decline in RDP attacks. First, the COVID-19 pandemic seems to be nearing its end and people are returning to offices. With less work being done remotely, there might be fewer interesting high-profile targets. Another factor that might have contributed to this positive development is increased awareness among IT departments and gradually improving security of corporate environments, removing exposed services and systems.

Russia's war against Ukraine has probably also played its part. Although the drop in RDP and SQL attacks started more than a month before the invasion, the physical and cyber-disruptions and the sanctions imposed after February 24 probably influenced the access to and availability of the infrastructure that was involved in the brute-force attacks.

Ladislav Janko, ESET Senior Malware Researcher

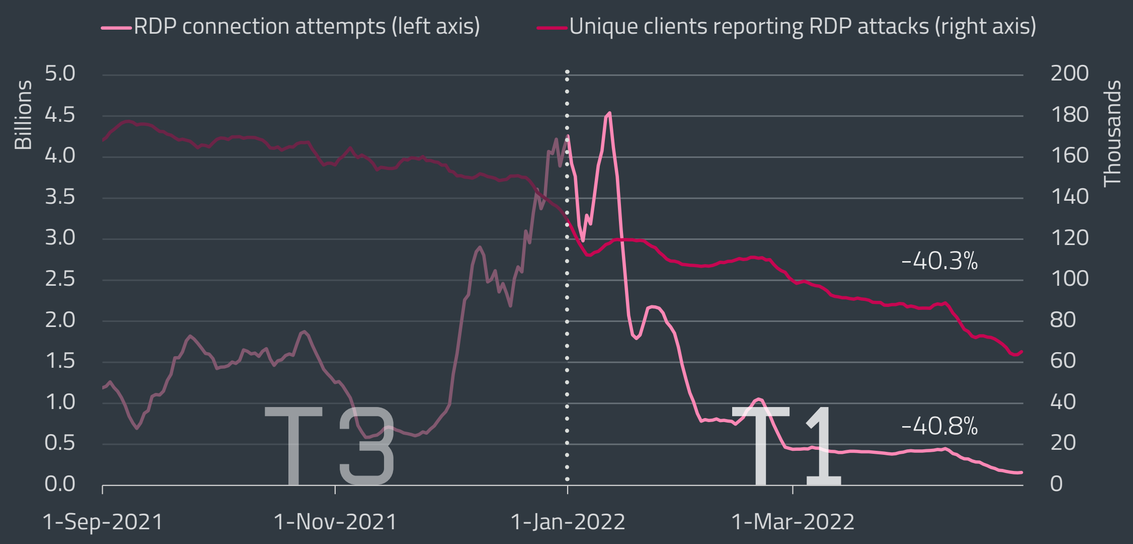
According to ESET telemetry, the number of Log4J exploitation attempts exploded after the vulnerability was published on December 10. Between January 1 and January 5, the numbers dropped from hundreds of thousands per day to tens of thousands per day, but it seems this was a short-lived holiday hiatus. After January 6, the activity of attackers – and probably also pentesters – jumped back to the levels from 2021.

Despite the gradual decline observable in our chart, Log4J isn't going away anytime soon as there are still many vulnerable applications in the wild. This has been confirmed by the Rezilion *report* [130], which identified *"over 90,000 potentially vulnerable internet-facing applications"*, acknowledging that this was probably only the tip of the iceberg.

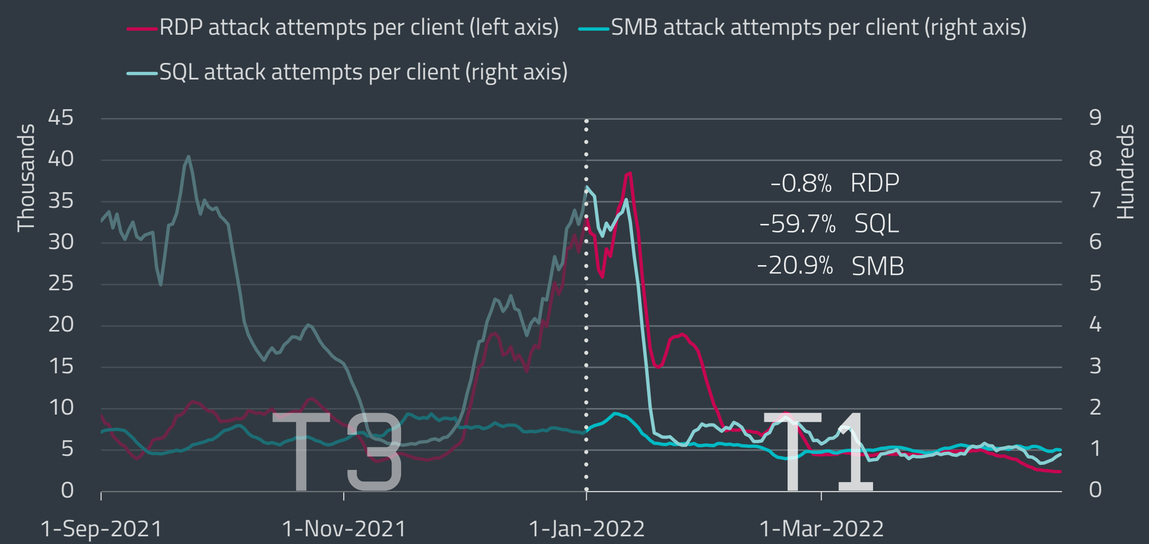
Another critical vulnerability appeared in April 2022, sporting a critical 9.8 CVSS score. The so-called Spring4Shell vulnerability (*CVE-2022-22965* [131]) has been found in the popular open-source VMWare Spring Core Java framework and allows the attackers to exploit the flaw for remote code execution (RCE) in all applications that run the unpatched version of the code.

Similar to Log4J, Spring4Shell can be exploited by sending a malicious query to the vulnerable server, allowing attackers to gain access to a broad range of the victims' data, credentials, and resources. While this makes Spring4Shell quite severe, the good news is that it is easier to identify and then to fix than Log4J.

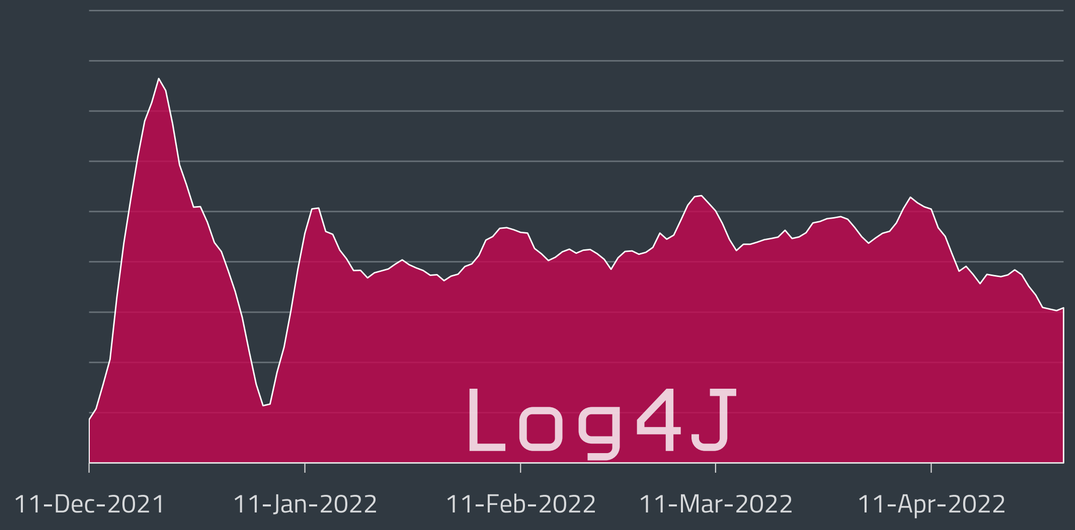
One month after its publication, ESET telemetry saw hundreds of thousands of attempts to exploit Spring4Shell. As in the Log4J case, we observed the biggest spike of activity shortly after the vulnerability was published.



Trends of RDP connection attempts and number of unique clients in T3 2021 – T1 2022, seven-day moving average

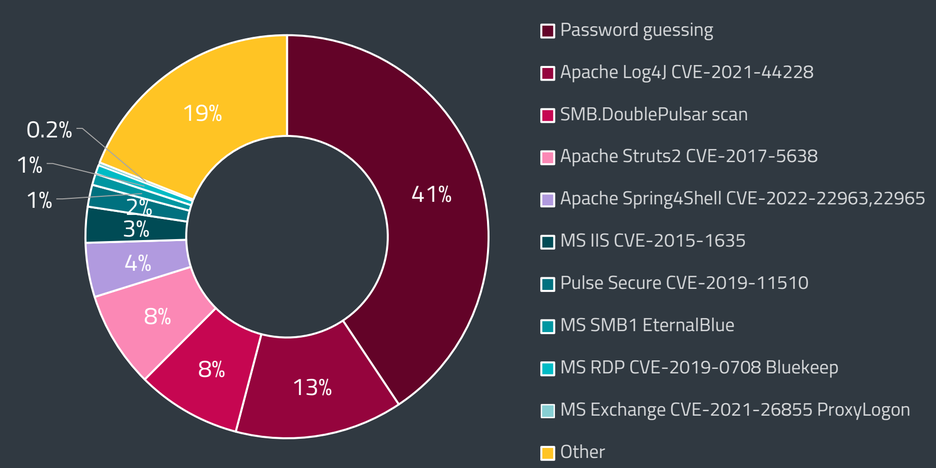


Trends of RDP, SMB and SQL attack attempts per client in T3 2021 – T1 2022, seven-day moving average

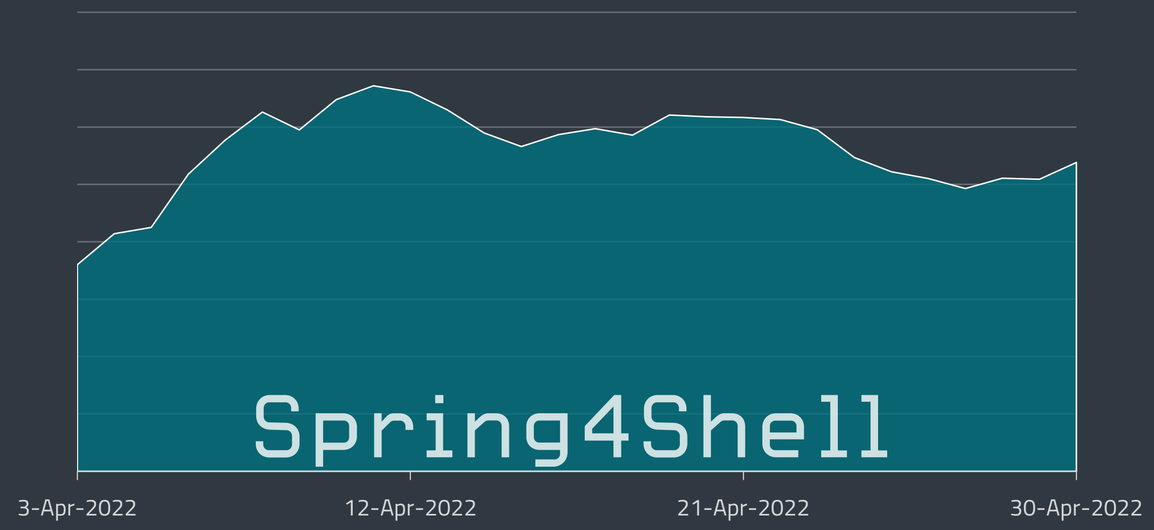


Log4J exploitation attempt trend, seven-day moving average

In the top 10 external network intrusion vectors, password guessing remains the most widespread. However, with 13%, Log4J became a solid number two in T1 2022, stealing most of the glory from *ProxyLogon* [132] – an RCE vulnerability chain in MS Exchange Servers. Our data suggests that ProxyLogon has become obsolete for offensive actors, since exploitation attempts targeting these flaws dropped from 14% in T3 2021 to less than 1% in T1 2022.



External network intrusion vectors reported by unique clients in T1 2022



Spring4Shell exploitation attempt trend in April 2022, seven-day moving average

Spring4Shell seems to be repeating Log4J's trajectory in the top 10 and despite being known only for a couple of weeks, it took fifth place, with 4% of detected exploitation attempts.

A new Linux vulnerability scoring 7.8 on the CVSS scale made noise in March. "Dirty Pipe" (*CVE-2022-0847* [133]) affects Linux kernel version 5.8 and later and was disclosed by security researcher Max Kellermann. According to his *public report* [134], the flaw makes "overwriting [of] data in arbitrary read-only files" possible. This allows attackers to inject their code into root processes and escalate their privileges on the victim's machine.

In T1 2022, Google Project Zero and Mandiant published summaries of their zero-day vulnerabilities findings in the previous year. *Google's team* [135] stated they found 58 previously unknown vulnerabilities; a two-fold jump compared to the 25 zero days uncovered in 2020. Researchers cited increased detection and disclosure as the possible reasons for the growth. Google also highlighted that only two of the 58 zero days stood out as novel, both related to a zero-click iMessage exploit FORCEDENTRY.

Mandiant's *findings* [136] are similar, although their list includes more zero days. In 2021, their researchers identified 80 new flaws, more than doubling the previous record of 32 from 2019. Mandiant also notes that the number of financially motivated actors deploying zero days is rising, mostly due to ransomware gangs utilizing them for initial access to environments of high-profile victims.

ESET RESEARCH CONTRIBUTIONS

Latest engagements and achievements of ESET Research experts

UPCOMING PRESENTATIONS

RSA Conference 2022

ESPecter: Showing the future of UEFI Threats [137]

In recent years, it has become clear that UEFI threats are real and have been deployed in the wild. UEFI implants such as LoJax and MosaicRegressor have used the lowest level of persistence, SPI flash, and the actors behind ESPecter bootkit think that compromising the bootloader is the way. This session by ESET director of threat research Jean-Ian Boutin and ESET malware researcher Martin Smolár will describe ESET's discovery of the aforementioned ESPecter – a previously undocumented real-world UEFI bootkit persisting on the EFI System Partition (ESP). This session raises awareness of UEFI threats affecting the ESP and provides guidance and resources for defenders to help secure their pre-OS environments. Boutin's and Smolár'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 discovery of ESPecter shows they are definitely not mere specters.

Black Hat USA 2022

Industroyer2: Sandworm's Cyberwarfare Targets Ukraine's Power Grid Again [138]

In this talk, ESET senior malware researcher Anton Cherepanov and ESET principal researcher Robert Lipovský will provide technical details of Industroyer2, a new version of the only malware to ever trigger electricity blackouts. Its latest variant was observed in Ukraine amidst the ongoing Russian invasion, aiming to cause a major electricity outage in a region with a population of more than two million, using components amplifying the impact. In the presentation, the researchers will show data linking this attack to the notorious Sandworm APT group and discuss why and how the attack was mostly unsuccessful. On top of that, actionable advice for defenders will be provided, including log entries to check; EDR rules to consider; configuration options to hamper Sandworm compromise and lateral movement; and detection/hunting rules for Snort and YARA.

Virus Bulletin 2022

Lazarus & BYOVD: Evil to the Windows core [139]

In this session, ESET senior malware researcher Peter Kálnai and ESET malware analyst Matěj Havránek will take a deep technical dive into a malicious component that was used in an attack by the Lazarus APT group in late 2021. Previously undocumented, this malware is a

sophisticated user-mode module that uses the Bring Your Own Vulnerable Driver (BYOVD) technique, leveraging a vulnerability in a legitimate, signed Dell driver. After gaining write access to kernel memory, the module's global goal is to blind security solutions and monitoring tools. This is tactically realized via several distinct mechanisms that target important kernel functions, structures, and variables of Windows systems from versions 7.1 up to Windows Server 2022. Kálnai and Havránek will shed more light on these mechanisms by demonstrating how they operate and what changes they make to system monitoring once the user-mode module is executed. Our researchers will also compare this Lazarus case to other APT groups abusing BYOVD, as it possesses a complex bundle of ways to disable monitoring interfaces not seen in the wild thus far.

REcon 2022

Under the hood of Wslink's multilayered virtual machine [140]

Wslink is a unique loader, linked to the Lazarus group, that ESET researchers discovered and documented at the end of last year. Most Wslink samples are packed and protected with an advanced virtual machine (VM) obfuscator; the samples contain no clear artifacts, such as specific section names, that easily link them to an already known and publicly described obfuscator. This VM additionally introduces several other obfuscation techniques such as insertion of junk code, encoding of virtual operands, duplication of virtual opcodes, opaque predicates, merging of virtual instructions, and a nested VM. In his presentation, ESET malware researcher Vladislav Hrčka analyzes the internals of the VM and describes ESET Research's semiautomated approach to seeing through the obfuscation techniques in a reasonable time. The approach is demonstrated on a few chunks of bytecode from a protected sample and the results are compared against a subsequently discovered non-obfuscated sample to confirm the validity of the method.

DELIVERED PRESENTATIONS

S4x22

Inside Industroyer2 and Sandworm's latest cyberattacks against Ukraine [141]

ESET's principal malware researcher Robert Lipovsky presented the work of the team that discovered Industroyer2, a new variant of Industroyer malware deployed by the infamous Sandworm group, that attempted to target a Ukrainian energy company after the outbreak of the war in Ukraine. Lipovsky talked about how the collaboration with CERT-UA mitigated this attack and compared it to the original Industroyer malware that switched off the lights in 2016. The presentation also looked at other recent Sandworm cyberattacks against Ukraine's critical infrastructure.

CARO Workshop 2022

Oil, water, and something fresh: Hunting Middle Eastern threat actors [142]

In this presentation, ESET's principal malware researcher Robert Lipovsky discussed hunting Middle Eastern threat actors OilRig, MuddyWater, and a new group ESET Research is calling FreshFeline. Based on the research of Adam Burgher, senior threat intelligence analyst at ESET, Lipovsky laid out the hunting methodology of ESET researchers and how it led to a newly discovered OilRig backdoor, several new campaigns from MuddyWater, and the backdoors and exploitation chain used by the FreshFeline group.

Behind the scenes of hunting InvisiMole [140]

Since ESETs discovery of this group in 2018, our researchers have been closely tracking activities of this highly targeted cyberespionage group. In this session, ESET senior malware researcher Anton Cherepanov and ESET malware researcher Zuzana Hromcová shared publicly unavailable information about hunting InvisiMole and discussed two previously undisclosed 2021 campaigns targeted at Ukraine and how the timing aligns with other geopolitical events in the region.

CARO Workshop 2022 Botconf 2022

TA410: APT10's distant cousin (CARO Workshop 2022) [140]

TA410: APT10's distant cousin (Botconf 2022) [143]

TA410 is a cyberespionage group first described in August 2019 and that shows interesting technical capabilities with its use of complex implants. TA410's activity shares some characteristics with past APT10 operations. As such, some public reports have misattributed TA410 activities to APT10. In this presentation, ESET malware researcher Alexandre Côté Cyr and senior malware researcher Matthieu Faou clarified what TA410 is and how its activities differ from the current activities of APT10. By leveraging ESET telemetry, they presented ESET Research's view of the main targets of TA410.

Botconf 2022 NorthSec

Jumping the air gap: 15 years of nation-state efforts (Botconf 2022) [144]

Jumping the air gap: 15 years of nation-state efforts (NorthSec) [145]

Air-gapping is used to protect the most sensitive of networks. In the first half of 2020 alone, four previously unknown malicious frameworks designed to breach air-gapped networks emerged, bringing the total, by ESET's count, to 17. ESET Research decided to revisit each framework known to date and to put them in perspective, side by side. This presentation by Alexis Dorais-Joncas, who leads the Canadian malware research team, and ESET security intelligence analyst Facundo Munõz, described how malware frameworks targeting air-gapped networks operate, and provided a side-by-side comparison of their most important TTPs.

Botconf 2022

ProxyChaos: a year-in-review of Microsoft Exchange exploitation [146]

Since the beginning of 2021, Exchange has been subject to several critical vulnerabilities, including the ProxyLogon and ProxyShell vulnerability chains, and their variations. ESET researchers have been closely monitoring malicious activities related to these vulnerabilities since they were made public and discovered multiple APT groups exploiting them. This presentation by ESET malware researcher Mathieu Tartare revisited the whole timeline of events and showed how attackers systematically exploited these vulnerabilities and for what purpose. For each vulnerability, the presentation gave an overview of the various groups that exploited it, including some yet undisclosed activities. Tartare also provided the attendees with a detailed timeline of the events and statistics from ESET telemetry, to show the wide scope of these attacks.

SeQCure

Disclosure of vulnerabilities: A challenge even in 2022 [147]

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, explained how malware research can lead to the discovery of vulnerabilities. Throughout the presentation of real-world case studies, our researchers detailed the different types of vulnerabilities that are most frequently discovered, how the disclosure process works, and the lessons that were learned.

ESET World

Worldwide aerospace and defense contractors under attack by Lazarus [148]

Advanced threat actors operating under the Lazarus umbrella have been relentlessly targeting worldwide defense contractors and aerospace companies for years. In this presentation, ESET's director of threat research Jean-Ian Boutin explained the details of the group's newest campaigns against this critical sector. While the opening lure is still the same – a fake job offer through social media like LinkedIn – the campaign's sophistication and diversity keeps increasing.

ESET European cybersecurity day SEMAFOR

Past and present cyberwar in Ukraine (ESET European cybersecurity day) [149]

Past and present cyberwar in Ukraine (SEMAFOR) [150]

With the brutal escalation of the war against Ukraine, ESET's principal malware researcher Robert Lipovsky took a closer look at the "cyber" part of it. What has been happening in Ukraine? Could the cyberwar spill over to other European countries? Should users be worried? Lipovsky explained to the attendees of these events the most important cyberattacks related to the armed conflict – in the past weeks, as well as in the past eight years.

ESET European Cybersecurity Day

Will machine learning improve or disrupt the cybersecurity equilibrium? [151]

Machine learning-based technologies increasingly help fight large-scale fraud, evaluate and optimize business processes, improve testing procedures, and develop new solutions to existing problems. Juraj Jánošík, the leader of ESET's automated threat detection and machine learning team, spoke

during his talk about how ESET recognized the potential of machine learning early on and employed it to improve malware detection starting over 20 years ago. Explaining that technological advances are not exclusively available to cybersecurity defenders, Jánošík also spoke about how cybercriminals do not hesitate to utilize machine learning-based technologies to make their malware and activities more efficient.

Zooming in on the current threatscape [152]

ESET security awareness specialist Ondrej Kubovič shared findings about the latest threats and trends detected in ESET telemetry during the last months of 2021. Among others, his presentation covered the hundreds of billions of password guesses aimed to break the protection of RDP remote access; the resurrection of Emotet, a threat described by Europol as the "most dangerous malware in the world"; and the over 400-fold increase in Android banking malware year-over-year.

WHITE PAPERS

Under the hood of Wslink's multilayered virtual machine [36]

ESET researchers recently described Wslink, a unique and previously undocumented malicious loader that runs as a server and that features a virtual-machine-based obfuscator. In this white paper, ESET malware researcher Vladislav Hrčka describes the structure of the virtual machine used in samples of Wslink and suggests a possible approach to see through the obfuscation techniques used in the samples analyzed. The virtual machine introduced a diverse arsenal of obfuscation techniques, which ESET researchers were able to overcome to reveal a part of the deobfuscated malicious code that is described in this document. This white paper also provides an overview of the internal structure of virtual machines in general, and introduces some important terms and frameworks used in our detailed analysis of the Wslink virtual machine.

ESET RESEARCH PODCAST

To increase the reach of ESET research among cybersecurity practitioners, administrators, researchers and the infosec community in general, we have decided to start our own podcast – the ESET Research podcast. New episodes are released every time we publish a major research story, which usually happens every few months.

The host of our podcast is ESET's Distinguished Researcher and infosec pioneer *Aryeh Goretsky* [153], who is talking to researchers, introducing them and their discoveries and offering the listeners a peek behind the curtain of how their research came to be.

You can listen to the latest episodes via the most popular podcast platforms including *Spotify* [154], *Google Podcasts* [155], *Apple Podcasts* [156] and *PodBean* [157].

MITRE ATT&CK CONTRIBUTIONS

ESET researchers regularly contribute to *MITRE ATT&CK®* [158] – a globally accessible knowledge base of adversary tactics and techniques. In T1 2022, ESETs *Process Injection: ListPlanting* [159] contribution was added to the ATT&CK knowledge base.

ListPlanting is a method of executing arbitrary code in the address space of a separate live process. Code executed via ListPlanting may also evade detection from security products since the execution is masked under a legitimate process. InvisiMole uses ListPlanting to inject code into a trusted process.

InvisiMole [160] is a modular spyware program that has been used by the InvisiMole APT group since at least 2013. The InvisiMole group also has two backdoor modules called RC2FM and RC2CL that are used to perform post-exploitation activities. It has been discovered on compromised victims in Ukraine and Russia. *Gamaredon group* [161] infrastructure has been used to download and execute the InvisiMole spyware against a small number of victims.

ESET has conducted extensive research into both of these APT groups. ESET researchers *revealed* [26] the modus operandi and extensive toolset of the elusive InvisiMole group, which targets military and diplomatic entities. Various tools used by Gamaredon are also *well known* [25] to ESET researchers and are frequently monitored and tracked by them.

The latest ATT&CK *v11 setlist* [162] also includes detections now paired with related Data Sources: Data Components, a beta version of sub-techniques for ATT&CK for Mobile, ATT&CK for ICS on *attack.mitre.org* [156], as well as regular updates and additions across Techniques, Software, and Groups.

MITRE ATT&CK EVALUATIONS

ESET participated in the latest round of MITRE ATT&CK evaluations that focused on tactics, techniques and procedures applied by the Wizard Spider and Sandworm nation-state APT groups: *Wizard Spider & Sandworm MITRE Engenuity ATT&CK evaluation* [163].

These evaluations are not a competitive analysis, as is stressed by *MITRE Engenuity* [164]. Some key parameters that the evaluations do not consider include performance and resource requirements, alerting strategy, noisiness (alert fatigue – any product could obtain a very high score on most of these results by producing alerts on every action recorded in the test environment), integration with endpoint security software, and ease of use. In ESET's case, this evaluation assessed *ESET Inspect* [165], our extended detection and response solution, which provides risk managers and incident responders with threat and system visibility.

The detection scenarios consisted of 19 steps (10 for Wizard Spider and 9 for Sandworm) spanning a spectrum of tactics listed in the ATT&CK framework, from initial access to lateral movement, collection, exfiltration, and so on. These steps are then broken down to a more granular level – a total of 109 sub-steps. ESET Inspect for Linux machines was not yet released at the time of the evaluation, so Linux-related steps and sub-steps were out of scope. That means 15 steps and 90 sub-steps were evaluated in ESET's case.

Out of the 15 applicable steps in the detection evaluation, ESET Inspect *detected all steps (100%)* [166]. Breaking the attack emulation down to a more granular level, out of the 90 applicable sub-steps in the emulation, ESET Inspect detected 75 sub-steps (83%) even without the modules present in ESET Inspect with Linux support. As the results indicate, ESET Inspect provides defenders excellent visibility of the attacker's actions on the compromised system throughout all attack stages. As already stated, ESET did not participate in the Linux part of the evaluation, but with the public launch of ESET Inspect with Linux support on March 30, 2022, the company's coverage of all major endpoint platforms, alongside Windows and macOS, is now complete.

To understand ESET's background, the company is a pioneer of research on Sandworm, with some of the most significant discoveries made about this threat group. ESET's outstanding visibility into this group is demonstrated by high-profile research, such as ESET's recent discovery of *Industroyer2* [14]. The discovery and cooperation with CERT-UA led to the prevention of the attack that was aimed at an energy provider in Ukraine. Other examples of ESET research analyzing Sandworm operations and tools include the *attacks against the Ukrainian power grid* [12], cyberattacks on *high-value targets in the Ukrainian financial sector* [167], the *supply-chain attacks against Ukraine* [168], and the devastating *NotPetya ransomware* [169], just to name a few.

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* [170]; however, it didn't take long and this infostealer was back in business with *new modules* [171].

OTHER CONTRIBUTIONS

ESET researchers discovered multiple vulnerabilities in various consumer Lenovo laptop models that allow an attacker with admin privileges to expose the user to firmware-level malware; they also identified an MSR vulnerability in the `AMDPowerProfiler.sys` kernel driver.

CVE-2021-26334 [172]

ESET researchers identified an MSR vulnerability in the `AMDPowerProfiler.sys` kernel driver, which is a part of *AMD μProf* [173] profiling software. Once the underlying software package is installed, the driver runs on every system boot. The unfiltered MSR IOCTL access combined with the lack of `FILE_DEVICE_SECURE_OPEN` flags and on-boot presence gives the attackers a good opportunity to exploit the driver even as an unprivileged user – this is an advantage compared to the BYOVD approach when the attackers need to load the driver themselves.

AMD *acknowledged* [174] the vulnerability and released a fix in its November 2021 *Patch Tuesday* [172] release. More information about malware that abuses vulnerabilities in kernel drivers is available in ESET Research's *blogpost* titled Signed kernel drivers – Unguarded gateway to Windows' core [30].

CVE-2021-3971 [37], *CVE-2021-3972* [38]

These two vulnerabilities affect UEFI firmware drivers originally meant to be used only during the manufacturing process of Lenovo consumer notebooks. Affected firmware drivers can be activated by an attacker to directly disable SPI flash protections (BIOS Control Register bits and Protected Range registers) or the UEFI Secure Boot feature from a privileged user-mode process during OS runtime. It means that exploitation of these vulnerabilities would allow attackers to deploy and successfully execute SPI flash or ESP implants, like *LoJax* [29] or ESET Research's latest UEFI malware discovery *ESPecter* [39], on the affected devices.

CVE-2021-3970 [40]

A third vulnerability – SMM memory corruption inside the SW SMI handler function – was discovered while ESET researchers investigated the aforementioned vulnerable drivers. This vulnerability allows

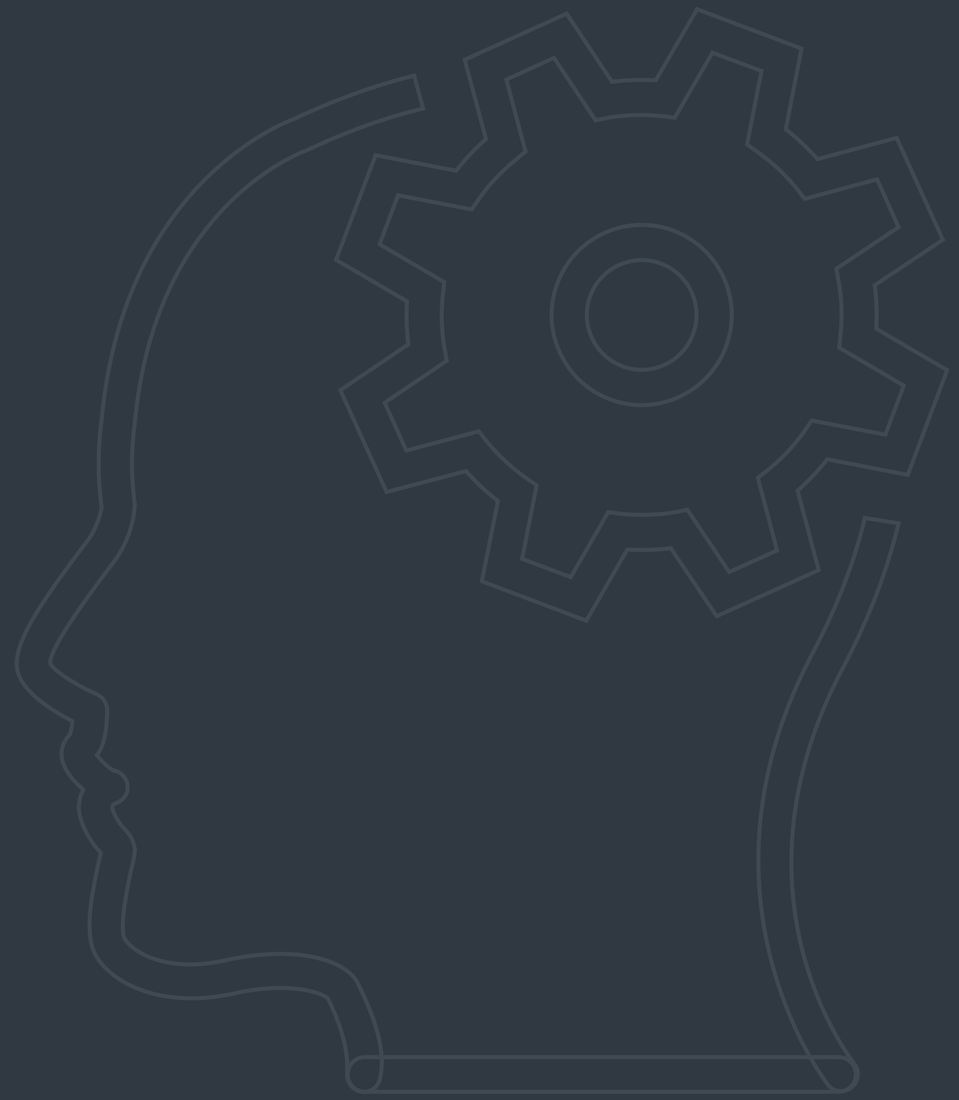
arbitrary read/write from/into SMRAM, which can lead to the execution of malicious code with SMM privileges and potentially lead to the deployment of an SPI flash implant.

Lenovo confirmed the vulnerabilities on November 17, 2021 and published an advisory on April 18, 2022. Altogether, the list of affected devices contains more than one hundred different consumer laptop models with millions of users worldwide, from affordable models like Ideapad-3 to more advanced ones like Legion 5 Pro-16ACH6 H or Yoga Slim 9-14ITL05. The full list of affected models with active development support is published in the ***Lenovo Advisory*** [41]. In addition to the models listed in the advisory, several other devices we reported to Lenovo are also affected, but won't be fixed due to them reaching End Of Development Support (EODS). More information is available in ESET Research's ***blogpost*** [42] titled "When 'secure' isn't secure at all: High-impact UEFI vulnerabilities discovered in Lenovo consumer laptops".

Frost & Sullivan's Insights for CISOs series: Participation in the panel about implications of the war in Ukraine [175]

The war in Ukraine changed geopolitics in Europe and the NATO alliance faster than anyone could have imagined. According to research and consulting firm Frost & Sullivan, one aspect of the war that is under-reported is the cybersecurity dimension and the question of whether sanctions and technology sales bans will drive new waves of ransomware attacks and cyber-economic espionage.

Cybersecurity executives from all over the world came together with Frost & Sullivan, to discuss the potential cybersecurity implications of the largest war in Europe since World War 2. Jean-Ian Boutin, ESET's director of threat research, shared the company's insights into various threats ESET Research detected in Ukraine, not only during the outbreak of the war but also those preceding it. He described 2022 as the year of WhisperGate, HermeticWiper, IsaacWiper and CaddyWiper from the perspective of CISOs, and outlined how the vendor community can ensure these attacks are mitigated. He also discussed diverse APT groups like Mustang Panda exploiting the Ukraine conflict as a bait for adversarial actions and what it means for CISOs and their evolving role.



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

Anton Cherepanov
Dušan Lacika
Igor Kabina
Jakub Souček
Jakub Tomanek
Ján Šugarek
Jean-Ian Boutin
Jiří Kropáč
Juraj Jánošík
Ladislav Janko
Lukáš Štefanko
Marc-Etienne M.Léveillé
Martin Červeň
Matthieu Faou
Michal Malík
Milan Fránik
Miroslav Legéň
Patrik Sučanský
Robert Kapp
Robert Lipovský
Vladimír Šimčák
Zuzana Legáthová

ABOUT THE DATA IN THIS REPORT

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

This data was processed with the honest intention to mitigate all known biases, in an effort to maximize the value of the information provided on the most significant in-the-wild threats.

Further, the data excludes detections of *potentially unwanted applications* [176], *potentially unsafe applications* [177] and *adware* [178], except where noted in the more detailed, platform-specific sections and in the Cryptocurrency threats section.

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

REFERENCES

[1] https://twitter.com/ESETresearch/status/1496581903205511181

[2] https://www.welivesecurity.com/2022/02/24/hermeticwiper-new-data-wiping-malware-hits-ukraine/

[3] https://twitter.com/ESETresearch/status/1496614321442459655

[4] https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/

[5] https://twitter.com/AvastThreatLabs/status/1496663206634344449

[6] https://www.welivesecurity.com/2022/03/15/caddywiper-new-wiper-malware-discovered-ukraine/

[7] https://www.welivesecurity.com/2017/06/27/new-ransomware-attack-hits-ukraine/

[8] https://cip.gov.ua/en/news/chergova-kiberataka-na-saiti-derzhavnikh-organiv-ta-banki

[9] https://www.viasat.com/about/newsroom/blog/ka-sat-network-cyber-attack-overview/

[10] https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/

[11] https://twitter.com/ESETresearch/status/1483161464106098689

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

[13] https://cert.gov.ua/article/39518

[14] https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/

[15] https://edition.cnn.com/2022/04/12/politics/gru-russia-hackers-ukraine-power-grid/index.html

[16] https://www.eset.com/int/ua-crisis/?utm_source=facebook&utm_medium=cpc&utm_campaign=ukraine-crisis&utm_term=eset-response-center&fbclid=IwAR2pu0PR2VThhA0GpRE0-Km9NmA3oELsHzsrR9I8DzNR_33I_2Sw0urrrD4#eset-helps

[17] https://www.welivesecurity.com/2022/03/23/mustang-panda-hodur-old-tricks-new-korplug-variant/

[18] https://www.welivesecurity.com/2022/02/27/beware-charity-scams-exploiting-war-ukraine/

[19] https://www.welivesecurity.com/2022/03/11/eset-research-webinar-apt-groups-ukraine-cyber-battlefield/

[20] https://www.welivesecurity.com/2014/09/22/back-in-blackenergy-2014/

[21] https://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/

[22] https://www.welivesecurity.com/2018/10/17/greyenergy-updated-arsenal-dangerous-threat-actors/

[23] https://www.welivesecurity.com/2017/07/04/analysis-of-telebots-cunning-backdoor/

[24] https://www.welivesecurity.com/2018/09/27/lojax-first-uefi-rootkit-found-wild-courtesy-sednit-group/

[25] https://www.welivesecurity.com/2020/06/11/gamaredon-group-grows-its-game/

[26] https://www.welivesecurity.com/2020/06/18/digging-up-invisimole-hidden-arsenal/

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

[28] https://www.welivesecurity.com/2019/07/11/buhtrap-zero-day-espionage-campaigns/

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

[30] https://www.welivesecurity.com/2022/01/11/signed-kernel-drivers-unguarded-gateway-windows-core/

[31] https://www.welivesecurity.com/2022/04/06/fake-eshops-prowl-banking-credentials-android-malware/

[32] https://appdefensealliance.dev/

[33] https://www.welivesecurity.com/2022/03/24/crypto-malware-patched-wallets-targeting-android-ios-devices/

[34] https://www.welivesecurity.com/2022/04/13/eset-takes-part-global-operation-disrupt-zloader-botnets/

[35] https://www.welivesecurity.com/2022/03/28/under-hood-wslink-multilayered-virtual-machine/

[36] https://www.welivesecurity.com/wp-content/uploads/2022/03/eset_wsliknkvm.pdf

[37] https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-3971

[38] https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-3972

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

[40] https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-3970

[41] https://support.lenovo.com/us/en/product_security/len-73440

[42] https://www.welivesecurity.com/2022/04/19/when-secure-isnt-secure-uefi-vulnerabilities-lenovo-consumer-laptops/

[43] https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2017-11882

[44] https://www.welivesecurity.com/2022/01/18/donot-go-do-not-respawn/

[45] https://www.trendmicro.com/en_us/research/20/c/operation-poisoned-news--hong-kong-users-targeted-with-mobile-ma.html

[46] https://www.welivesecurity.com/2022/01/25/watering-hole-deploys-new-macos-malware-dazzlespy-asia/

[47] https://unit42.paloaltonetworks.com/thor-plugx-variant/

[48] https://www.welivesecurity.com/2020/05/21/no-game-over-winnti-group/

[49] https://twitter.com/ESETresearch/status/1506904404225630210

[50] https://www.welivesecurity.com/2022/04/27/lookback-ta410-umbrella-cyberespionage-ttps-activity/

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

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

[53] https://www.bleepingcomputer.com/news/security/malicious-powerpoint-files-used-to-push-remote-access-trojans/

[54] https://thehackernews.com/2022/02/notorious-trickbot-malware-gang-shuts.html

[55] https://www.proofpoint.com/us/blog/threat-insight/bumblebee-is-still-transforming

[56] https://www.welivesecurity.com/2020/04/28/grandoreiro-how-engorged-can-exe-get/

[57] https://twitter.com/ESETresearch/status/1494249522301743105

[58] https://twitter.com/ESETresearch/status/1485660697044398081

[59] https://krebsonsecurity.com/2022/01/at-request-of-u-s-russia-rounds-up-14-revil-ransomware-affiliates/

[60] https://www.bleepingcomputer.com/news/security/revils-tor-sites-come-alive-to-redirect-to-new-ransomware-operation/

[61] https://www.bleepingcomputer.com/news/security/revil-ransomware-returns-new-malware-sample-confirms-gang-is-back/

[62] https://www.bleepingcomputer.com/news/security/hackers-use-contis-leaked-ransomware-to-attack-russian-companies/

[63] https://www.bleepingcomputer.com/news/security/oldgremlin-ransomware-gang-targets-russia-with-new-malware/

[64] https://edition.cnn.com/2022/03/30/politics/ukraine-hack-russian-ransomware-gang/index.html

[65] https://twitter.com/BrettCallow/status/1497249143663652865?s=20&t=NUaoFyINtpUfN4Vj2oxBEw

[66] https://twitter.com/contileaks

[67] https://www.washingtonpost.com/politics/2022/03/18/11-big-takeaways-conti-ransomware-leaks/

[68] https://twitter.com/uuallan/status/1498048260425977856?s=20&t=IiOyo7tgumTKIUnLqiermQ

[69] https://www.emsisoft.com/ransomware-decryption-tools/maze-sekhmet-egregor

[70] https://www.bleepingcomputer.com/news/security/free-decryptor-released-for-trickbot-gangs-diavol-ransomware/

[71] https://decoded.avast.io/threatresearch/decrypted-targetcompany-ransomware/

[72] https://www.bleepingcomputer.com/news/security/free-decryptor-released-for-yanluowang-ransomware-victims/

[73] https://decoded.avast.io/threatresearch/help-for-ukraine-free-decryptor-for-hermeticransom-ransomware/

[74] https://arxiv.org/abs/2202.08477

[75] https://krebsonsecurity.com/2022/03/estonian-tied-to-13-ransomware-attacks-gets-66-months-in-prison/

[76] https://www.bleepingcomputer.com/news/security/netwalker-ransomware-affiliate-sentenced-to-80-months-in-prison/

[77] https://www.bleepingcomputer.com/news/security/night-sky-is-the-latest-ransomware-targeting-corporate-networks/

[78] https://www.bleepingcomputer.com/news/security/

night-sky-ransomware-uses-log4j-bug-to-hack-vmware-horizon-servers/

[79] https://www.bleepingcomputer.com/news/security/qnap-warns-of-new-deadbolt-ransomware-encrypting-nas-devices/

[80] https://www.bleepingcomputer.com/news/security/a-look-at-the-new-sugar-ransomware-demanding-low-ransoms/

[81] https://www.bleepingcomputer.com/news/security/new-black-basta-ransomware-springs-into-action-with-a-dozen-breaches/

[82] https://www.bleepingcomputer.com/news/security/beware-onyx-ransomware-destroys-files-instead-of-encrypting-them/

[83] https://techcommunity.microsoft.com/t5/microsoft-365-blog/helping-users-stay-safe-blocking-internet-macros-by-default-in/ba-p/3071805

[84] https://www.bleepingcomputer.com/news/microsoft/microsoft-plans-to-kill-malware-delivery-via-office-macros/

[85] https://twitter.com/ESETresearch/status/1518923380782739458

[86] https://thehackernews.com/2022/04/emotet-testing-new-delivery-ideas-after.html

[87] https://thehackernews.com/2022/03/new-malware-loader-verblecon-infects.html

[88] https://time.com/nextadvisor/investing/cryptocurrency/bitcoin-crash-continues/

[89] https://www.vice.com/en/article/g5qj9j/cryptocom-says-incident-was-actually-dollar30-million-hack

[90] https://www.bleepingcomputer.com/news/cryptocurrency/wormhole-cryptocurrency-platform-hacked-to-steal-326-million/

[91] https://thehackernews.com/2022/02/hackers-steal-17-million-worth-of-nfts.html

[92] https://twitter.com/ESETresearch/status/1497194165561659394

[93] https://www.welivesecurity.com/2021/05/17/android-stalkerware-threatens-victims-further-exposes-snoopers-themselves/

[94] https://techcrunch.com/2022/02/22/stalkerware-network-spilling-data/

[95] https://lab52.io/blog/complete-dissection-of-an-apk-with-a-suspicious-c2-server/

[96] https://blog.appcensus.io/2022/04/06/the-curious-case-of-coulus-coelib/

[97] https://www.wsj.com/articles/apps-with-hidden-data-harvesting-software-are-banned-by-google-11649261181

[98] https://blog.pradeo.com/spyware-facestealer-google-play

[99] https://blog.checkpoint.com/2022/04/07/android-banking-stealer-dubbed-sharkbot-found-disguised-as-legitimate-anti-virus-apps-on-the-google-play-store/

[100] https://www.bitdefender.com/blog/labs/new-flubot-and-teabot-global-malware-campaigns-discovered

[101] https://www.threatfabric.com/blogs/partners-in-crime-medusa-cabassous.html

[102] https://www.threatfabric.com/blogs/xenomorph-a-newly-hatched-banking-trojan.html

[103] https://eprint.iacr.org/2022/208.pdf

[104] https://twitter.com/ESETresearch/status/1521735320852643840

[105] https://www.intezer.com/blog/malware-analysis/new-backdoor-sysjoker/

[106] https://objective-see.com/blog/blog_0x6C.html

[107] https://www.volexity.com/blog/2022/03/22/storm-cloud-on-the-horizon-gimmick-malware-strikes-at-macos/

[108] https://www.politico.eu/article/pegasus-hacking-spyware-spain-government-prime-minister-pedro-sanchez-margarita-robles-digital-espionage-crisis/

[109] https://www.bleepingcomputer.com/news/security/finnish-diplomats-phones-infected-with-nso-group-pegasus-spyware/

[110] https://www.reuters.com/technology/exclusive-iphone-flaw-exploited-by-second-israeli-spy-firm-sources-2022-02-03/

[111] https://googleprojectzero.blogspot.com/2022/03/forcedentry-sandbox-escape.html

[112] https://www.cvedetails.com/vulnerability-list/vendor_id-49/product_id-15556/Apple-Iphone-Os.html

[113] https://www.exploit-db.com/exploits/41471

[114] https://www.shodan.io/search/report?query=jaws%2F1.0

[115] https://nvd.nist.gov/vuln/detail/CVE-2017-18368

[116] https://nvd.nist.gov/vuln/detail/CVE-2015-2051

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

[118] https://thehackernews.com/2022/04/new-enemybot-ddos-botnet-borrows.html

[119] https://www.bleepingcomputer.com/news/security/new-fodcha-ddos-botnet-targets-over-100-victims-every-day/

[120] https://www.vice.com/en/article/akv7z5/how-a-hacker-controlled-dozens-of-teslas-using-a-flaw-in-third-party-app

[121] https://arstechnica.com/information-technology/2022/02/russias-most-cut-throat-hackers-infect-network-devices-with-new-botnet-malware/

[122] https://thehackernews.com/2022/03/new-variant-of-russian-cyclops-blink.html

[123] https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-botnet-controlled-russian-federation

[124] https://thehackernews.com/2022/03/over-200000-microtik-routers-worldwide.html

[125] https://www.welivesecurity.com/2021/12/13/log4shell-vulnerability-what-we-know-so-far/

[126] https://thehackernews.com/2022/01/initial-access-broker-involved-in.html

[127] https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/

[128] https://www.zdnet.com/article/chinese-hackers-deep-panda-return-with-log4shell-exploits-new-fire-chili-rootkit/

[129] https://securityaffairs.co/wordpress/128159/apt/tunnelvision-exploits-log4j-vulnerability.html

[130] https://www.rezilion.com/wp-content/uploads/2022/04/Log4Shell-4-Months-Later.pdf

[131] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22965

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

[133] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0847

[134] https://dirtypipe.cm4all.com/

[135] https://googleprojectzero.blogspot.com/2022/04/the-more-you-know-more-you-know-you.html

[136] https://www.mandiant.com/resources/zero-days-exploited-2021

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

[138] https://www.blackhat.com/us-22/briefings/schedule/#industroyer-sandworms-cyberwarfare-targets-ukraines-power-grid-again-27832

[139] https://www.virusbulletin.com/conference/vb2022/

[140] https://recon.cx/2022/conference.html

[141] https://whova.com/embedded/session/xfYtdNgvSv-eYXY1By4aWq606%4092h9NXnd7hwTzd-z4=/2292486/?widget=primary

[142] https://caro2022.org/agenda/

[143] https://botconf2022.sched.com/event/1199o/ta410-apt10s-distant-cousin

[144] https://botconf2022.sched.com/event/119AL/jumping-the-air-gap-15-years-of-nation-state-efforts

[145] https://nsec.io/speakers/

[146] https://botconf2022.sched.com/event/119A0/proxychaos-a-year-in-review-of-microsoft-exchange-exploitation

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

[148] https://www.esetworld.com/growth.protected/event-agenda/detail/157

[149] https://eecd.eset.com/agenda/detail/112

[150] https://www.computerworld.pl/event/semaforeng

[151] https://eecd.eset.com/agenda/detail/117

[152] https://eecd.eset.com/agenda/detail/120

[153] https://www.welivesecurity.com/author/goretsky/

[154] https://open.spotify.com/show/1WDjY2A3A3s5FKycrOVkhg

[155] https://podcasts.google.com/feed/aHR0cHM6Ly9mZWVkLnBvZGJlYW4uY29tL2VzZXRyZXNlYXJjaC9mZWVkLnhtbA

[156] https://podcasts.apple.com/us/podcast/eset-research-podcast/id1596306608

[157] https://esetresearch.podbean.com/

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

[159] https://attack.mitre.org/techniques/T1055/015/

[160] https://attack.mitre.org/software/S0260

[161] https://attack.mitre.org/groups/G0047

[162] https://attack.mitre.org/resources/updates/updates-april-2022/

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

[164] https://attackevals.mitre-engenuity.org/using-attack-evaluations/

[165] https://www.eset.com/int/business/solutions/xdr-extended-detection-and-response/

[166] https://www.eset.com/blog/awards-and-testing/hunting-down-sandworm-and-wizard-spider-how-eset-fared-in-the-attckr-evaluation/

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

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

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

[170] 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/

[171] https://twitter.com/ESETresearch/status/1409495354534473728

[172] https://github.com/eset/vulnerability-disclosures/commit/0b456d6fd13abb60407c2491904fd11613ead6c9

[173] https://developer.amd.com/amd-uprof/

[174] https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1016

[175] https://www.brighttalk.com/webcast/5567/537094

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

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

[178] https://help.eset.com/glossary/en-US/adware.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*.

Digital Security
Progress. Protected.

WeLiveSecurity.com
@ESETresearch
ESET GitHub