# THREAT REPORT T2 2022

WeLiveSecurity.com
@ESETresearch
ESET GitHub

# CONTENTS



# FOREWORD

*Welcome to the T2 2022 issue of the ESET Threat Report!*

The past four months were the time of summer vacations for many of us in the northern hemisphere. It appears that some malware operators also took this time as an opportunity to possibly rest, refocus, and reanalyze their current procedures and activities. According to our telemetry, August was a vacation month for the operators of Emotet, the most influential downloader strain. The gang behind it also adapted to Microsoft's decision to disable VBA macros in documents originating from the internet and focused on campaigns based on weaponized Microsoft Office files and LNK files.

In T2 2022, we saw the continuation of the sharp decline of Remote Desktop Protocol (RDP) attacks, which likely continued to lose their steam due to the Russia-Ukraine war, along with the post-COVID return to offices and overall improved security of corporate environments. Even with declining numbers, Russian IP addresses continued to be responsible for the largest portion of RDP attacks. In T1 2022, Russia was also the country that was most targeted by ransomware, with some of the attacks being politically or ideologically motivated by the war. However, as you will read on the following pages, this hacktivism wave has declined in T2, and ransomware operators turned their attention towards the United States, China, and Israel.

In terms of threats mostly impacting home users, we saw a sixfold increase in detections of shipping-themed phishing lures, most of the time presenting the victims with fake DHL and USPS requests to verify shipping addresses. A web skimmer known as Magecart, which saw a threefold increase in T1 2022, continued to be the leading threat going after online shoppers' credit card details. Plummeting cryptocurrency exchange rates also affected online threats – criminals turned to stealing cryptocurrencies instead of mining them, as seen in a twofold increase in cryptocurrency-themed phishing lures and rising numbers of cryptostealers.

The past four months were also interesting in research terms. Our researchers uncovered a previously unknown macOS backdoor and later attributed it to ScarCruft, discovered an updated version of the Sandworm APT group's ArguePatch malware loader, uncovered Lazarus payloads in trojanized apps, and analyzed an instance of the Lazarus Operation In(ter)ception campaign targeting macOS devices while spearphishing in crypto-waters. They also discovered buffer overflow vulnerabilities in Lenovo UEFI firmware and a new campaign using a fake Salesforce update as a lure.

During the past few months, we have continued to share our knowledge at the Virus Bulletin, Black Hat USA, RSA, CODE BLUE, SecTor, REcon, LABSCon, and BSides Montreal cybersecurity conferences, where we disclosed our findings about campaigns deployed by OilRig, APT35, Agrius, Sandworm, Lazarus, and POLONIUM. We also talked about the future of UEFI threats, dissected the unique loader we named Wslink, and explained how ESET Research does attribution of malicious threats and campaigns. For the upcoming months, we are happy to invite you to ESET talks at AVAR, Ekoparty, and many others.

I wish you an insightful read.

**Roman Kováč**
ESET Chief Research Officer

# EXECUTIVE SUMMARY

## FEATURED STORY

**I see what you did there: A look at the CloudMensis macOS spyware**

ESET researchers discovered CloudMensis, previously unknown macOS malware that uses cloud storage as its C&C channel and to exfiltrate documents, keystrokes, and screen captures from compromised Macs.

## NEWS FROM THE LAB

**Sandworm attacks Ukraine with new version of ArguePatch**

ESET Research discovered an updated version of the ArguePatch malware loader used by Sandworm. ArguePatch was previously used in the Industroyer2 attack against a Ukrainian energy provider, as well as in multiple attacks involving the data-wiping malware CaddyWiper.

**Operation In(ter)ception is open to crypto-opportunities**

ESET Research spotted an Operation In(ter)ception campaign for macOS, by Lazarus, in which the malware was disguised as a job description for the Coinbase cryptocurrency platform.

## STATISTICS & TRENDS

| Category | T1 2022/ T2 2022 | Key points in T2 2022 |
|---|---|---|
| **Overall threat detections** | -9.1% ↓ | Decrease in detections in almost all monitored categories |
| **Infostealers** | -14.3% ↓ | JS/Spy.Banker (aka Magecart) remains top banking malware |
| **Ransomware** | -24.1% ↓ | Politically motivated ransomware on the decline |
| **Downloaders** | -31.0% ↓ | Emotet continues activity, adapts distribution vectors |
| **Cryptocurrency threats** | -16.0% ↓ | Cryptostealers see first period of growth, at almost 50% |
| **Web threats** | -6.0% ↓ | Surge in shipping-themed phishing lures |
| **Email threats** | -10.2% ↓ | Office files double their share among malicious attachments |
| **Android** | +9.5% ↑ | Android spyware continues its growth from T1 |
| **macOS** | -15.1% ↓ | Decline in detections most prominent in the Adware category |
| **RDP attacks** | -89.4% ↓ | RDP attacks fall further, following sharp T1 decline |

# FEATURED STORY

# I see what you did there: A look at the CloudMensis macOS spyware

*Marc-Étienne M.Léveillé*

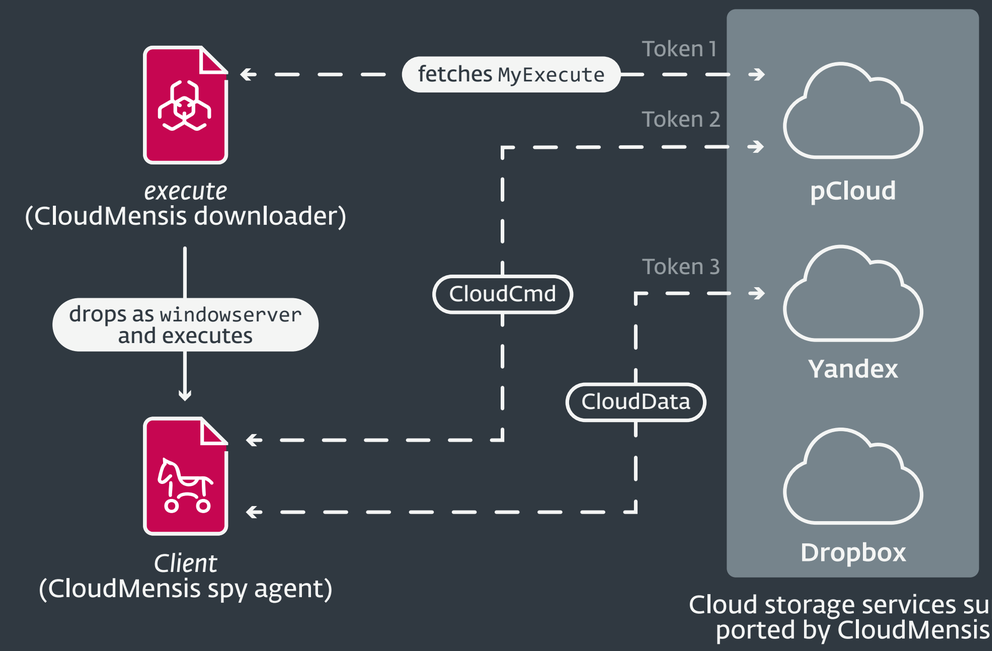
*ESET researchers discovered CloudMensis, previously unknown macOS malware that uses cloud storage as its C&C channel and to exfiltrate documents, keystrokes, and screen captures from compromised Macs.*

ESET researchers discovered a previously unknown macOS backdoor that they named CloudMensis. The malware uses public cloud storage services to communicate back and forth with its operators, and its capabilities clearly show that the intent of its operators is to gather information from the victims' Macs by exfiltrating documents, keystrokes, and screen captures.

CloudMensis is malware for macOS developed in Objective-C. The samples analyzed by ESET Research are compiled for both Intel and Apple silicon architectures.

It is not known how victims are initially compromised by this threat. Once CloudMensis gains code execution and administrative privileges, it runs first-stage malware that retrieves a more feature-rich second stage from a cloud storage service.

Interestingly, to retrieve its second stage from a cloud storage provider it doesn't use a publicly accessible link; it includes an access token to download the `MyExecute` file from the drive. In the sample analyzed, ***pCloud*** [1] was used to store and deliver the second stage.




Outline of how CloudMensis uses cloud storage services

## The spy agent component

The second stage of CloudMensis is a much larger component, packed with a number of features to collect information from the compromised Mac. The intention of the attackers here is clearly to exfiltrate documents, screenshots, email attachments, and other sensitive data.

CloudMensis uses cloud storage both for receiving commands from its operators and for exfiltrating files. It supports three different providers: pCloud, Yandex Disk, and Dropbox. The configuration included in the analyzed sample contains authentication tokens for pCloud and Yandex Disk.

One of the first things the CloudMensis spy agent does is load its configuration. The configuration contains the following:

- Which cloud storage providers to use and authentication tokens
- A randomly generated bot identifier
- Information about the Mac
- Paths to various directories used by CloudMensis
- File extensions that are of interest to the operators

The default list of file extensions found in the analyzed sample, pictured in the figure below, shows that operators are interested in documents, spreadsheets, audio recordings, pictures, and email messages from the victims' Macs. The most uncommon format is perhaps audio recordings using the Adaptive Multi-Rate codec (using the `.amr` and `.3ga` extensions), which is specifically designed for speech compression. Other interesting file extensions in this list are `.hwp` and `.hwpx` files, which are documents for *Hangul Office* [2] (now Hancom Office), a popular word processor among Korean speakers.

```
471 aDocDocxXlsXlsx db '*.doc;*.docx;*.xls;*.xlsx;*.ppt;*.pptx;*.hwp;*.hwpx;*.csv;*.pdf;*'
471                                     ; DATA XREF: __cfstring:cfstr_DocDocxXlsXlsx↓o
471                 db '.rtf;*.amr;*.3gp;*.m4a;*.txt;*.mp3;*.jpg;*.eml;*.emlx',0
1F8 aHwModel        db 'hw.model',0     ; DATA XREF: __cfstring:cfstr_HwModel↓o
```

File extensions found in the default configuration of CloudMensis

## Bypassing TCC

Since the release of macOS Mojave (10.14) in 2018, access to some sensitive inputs, such as screen captures, cameras, microphones and keyboard events, are protected by a system called TCC, which stands for Transparency, Consent, and Control. When an application tries to access certain functions, macOS prompts the user, who can grant or refuse access, whether the access request from the application is legitimate. Ultimately, TCC rules are saved into a database on the Mac. This database is protected by System Integrity Protection (SIP) to ensure that only the TCC daemon can make any changes.

CloudMensis uses two techniques to bypass TCC (thus avoiding prompting the user), thereby gaining access to the screen, being able to scan removable storage for documents of interest, and being able to log keyboard events. If SIP is disabled, the TCC database (`TCC.db`) is no longer protected against tampering. Thus, in this case CloudMensis adds entries to grant itself permissions before using sensitive inputs. If SIP is enabled but the Mac is running any version of macOS Catalina earlier than 10.15.6, CloudMensis will exploit a vulnerability to make the TCC daemon (tccd) load a database CloudMensis can write to. This vulnerability is known as *CVE-2020–9934* [3] and was *reported and described by Matt Shockley* [4] in 2020.

## Communication with the C&C server

To communicate with its operators, the CloudMensis configuration contains authentication tokens to multiple cloud service providers. Each entry in the configuration is used for a different purpose. All of them can use any provider supported by CloudMensis. In the analyzed sample, Dropbox, pCloud, and Yandex Disk are supported.

## Commands

There are 39 commands implemented in the analyzed CloudMensis sample. Some commands require additional arguments. Commands allow the operators to perform actions such as:

- Change values in the CloudMensis configuration: cloud storage providers and authentication tokens, file extensions deemed interesting, polling frequency of cloud storage, etc.
- List running processes
- Start a screen capture
- List email messages and attachments
- List files from removable storage
- Run shell commands and upload output to cloud storage
- Download and execute arbitrary files
- Metadata from cloud storage

Metadata from the cloud storages used by CloudMensis reveals interesting details about the operation. The figure on the next page shows the tree view of the storage used by CloudMensis to send the initial report and to transmit commands to the bots as of April 22, 2022.

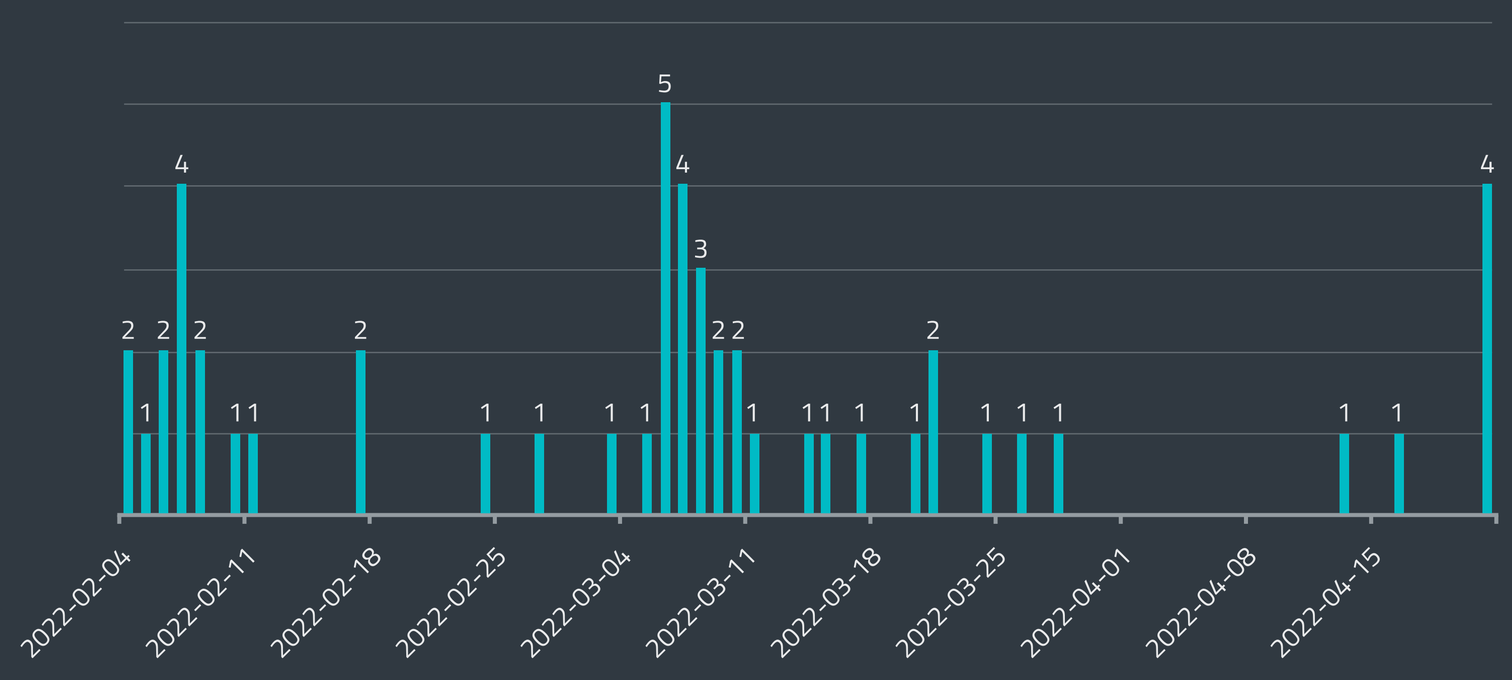
This metadata gave partial insight into the operation and helped draw a timeline. First, the pCloud accounts were created on January 19, 2022. The directory listing from April 22 shows that 51 unique bot identifiers created subdirectories in the cloud storage to receive commands. Because these directories are created when the malware is first launched, we can use their creation date to determine the date of the initial compromise, as seen in the chart on the next page.

The chart shows the first compromise was on February 4, with a spike of compromises in early March 2022. The last spike may be explained by sandboxes running CloudMensis, once it was uploaded to VirusTotal.

```
.
├── Febrary
│   ├── 04474A41
│   │   ├── August
│   │   ├── July
│   │   ├── June
│   │   └── May
│   │       ├── 48A5F94F97EC56E54C873A702E61A90C94EDCE38EBAAA2D7... (1 byte)
│   │       └── AC219DF1 (1 byte)
│   ├── 09ABA73E
│   │   ├── August
│   │   ├── July
│   │   ├── June
│   │   └── May
│   │       ├── 967B478B14EC54E947F76FE4BC28EC6CB0553DEA7AB3F264... (1 byte)
│   │       └── A72A96EF (276 bytes)
│   ├── 0E4401B2
│   └── ...
├── January
│   ├── AAKP1XUnvCalhdBdjF5kRaGttkD8H6ce (344 bytes)
│   ├── AbLH4ZlHoCn9DWvzy9pRV7Tv7NiiYgcH (344 bytes)
│   ├── B9yx2dNlSjXhDRIdMMjvxUIlOPTizVny (344 bytes)
│   ├── BoPgm0XkSF21NpIgC2Kbl6VtfsdyCZYj (344 bytes)
│   ├── C33OFX5yhS6uLgo3S2Kq7Nc7WYPx73QH (344 bytes)
│   ├── CEAYyDpgiTKJ2UTln7ExNyTiZVawyEO3 (344 bytes)
│   └── ...
├── My Videos
│   └── pCloud.mp4 (6,319,438 bytes)
├── My Music
│   └── ...
├── My Pictures
│   └── ...
├── Getting started with pCloud.pdf (16,371,465 bytes)
└── a.txt (6 bytes)

94 directories, 403 files
```

Tree view of the directory listing from the CloudCmd storage




Subdirectory creation dates under `/Febrary` (sic)

## Conclusion

CloudMensis is a threat to Mac users, but its very limited distribution suggests that it is used as part of a targeted operation. Operators of this malware family seem to deploy CloudMensis to specific targets that are of interest to them. Usage of vulnerabilities to work around macOS mitigations shows that the malware operators are actively trying to maximize the success of their spying operations. At the same time, no undisclosed vulnerabilities (zero-days) were found to be used by this group during ESET's research. Thus, running an up-to-date Mac is recommended to avoid, at least, the mitigation bypasses.

Apple recently acknowledged the presence of spyware targeting users of its products and is *previewing Lockdown Mode* [5] on iOS, iPadOS and macOS, which disables features that are frequently exploited to gain code execution and deploy malware.

*WeLiveSecurity blogpost* [6]

Following the publication of the CloudMensis blogpost, ESET Research found that the CloudMensis malware exhibits similar features and artifacts to Windows variants of the so-called *RokRAT* [7], attributed by Cisco Talos with high confidence to Group 123, also known as *ScarCruft* [8], APT37 and Reaper.

ESET researchers attribute RokRAT and CloudMensis to the ScarCruft APT group. ScarCruft has been operating since at least 2012 and is *suspected to be a North Korean espionage group* [9]. It primarily focuses on South Korea, but other Asian countries have also been targeted. The group's toolset contains a broad range of downloaders, exfiltration tools, and backdoors used for espionage.

The indicators that guided attribution include a matching list of favored file extensions, similarities in development artifacts such as paths left in malware samples, and shared use of cloud service providers for command and control.

*Attribution details on Twitter* [10]

The ScarCruft group is also the topic of an upcoming *ESET Research talk at AVAR 2022*.

# NEWS FROM THE LAB

Latest findings from ESET Research Labs across the world

## UEFI threats

### Buffer overflow vulnerabilities in Lenovo UEFI firmware

ESET researchers discovered three buffer overflow vulnerabilities in the UEFI firmware of multiple Lenovo notebook devices. More than 70 various models were affected, including several within the ThinkBook series. We reported all of these vulnerabilities to the manufacturer on February 18. Lenovo acknowledged them and released a *security advisory* [11] on June 12 with a list of affected devices and firmware update instructions.

More information on the topic can be found in the *ESET Research Contributions* section.

*Twitter thread* [12]

## macOS threats

### Fake Salesforce update deploys Sliver on macOS

ESET Research spotted a new campaign, which used a fake Salesforce update as a lure, to deploy the Sliver malware for macOS and Windows. Previously, SentinelOne *documented* [13] a COVID-19-themed campaign with a compromise chain that is very similar to the macOS one that we found.

Sliver is a framework similar to Cobalt Strike and is being used in more and more malicious campaigns. In this particular campaign, Sliver was deployed using an additional Go Mach-O executable that downloads and runs the Bash script. The Windows variant also uses a downloader written in the Go language.

As opposed to the script described by SentinelOne, the shell script that deploys Sliver on macOS doesn't include the "covid" malware and only installs the Sliver implant, which is sufficient to deploy additional malware if needed.

The fake Salesforce update download page included a link to a PDF with instructions on how to disable macOS security features. Additionally, it appears that the victim's Salesforce credentials were phished before landing on the download page.

*Twitter thread* [14]

## Sandworm

### Sandworm attacks Ukraine with new version of ArguePatch

The ESET research team found an updated version of the Sandworm APT group's ArguePatch malware loader. ArguePatch – named so by the Computer Emergency Response Team of Ukraine (CERT-UA) and detected by ESET products as Win32/Agent.AEGY – was previously used in the Industroyer2 attack against a Ukrainian energy provider, as well as in multiple attacks involving the data-wiping malware called CaddyWiper.

In order to stay under the radar during the Industroyer2 attack, ArguePatch used a patched version of the HexRays IDAPro remote debugging software. This was changed in the updated version, in which the malware operators switched to an ESET executable stripped of its signature.

The new variant of ArguePatch includes a feature to execute the next stage of an attack at a specified time. This bypasses the need for setting up a scheduled task in Windows and is likely intended to help the attackers stay under the radar.

This shows that Sandworm continues to update its arsenal for campaigns targeting Ukraine.

*Twitter thread* [15]

*WeLiveSecurity blogpost* [16]

## Lazarus

### Lazarus payloads hiding in trojanized apps

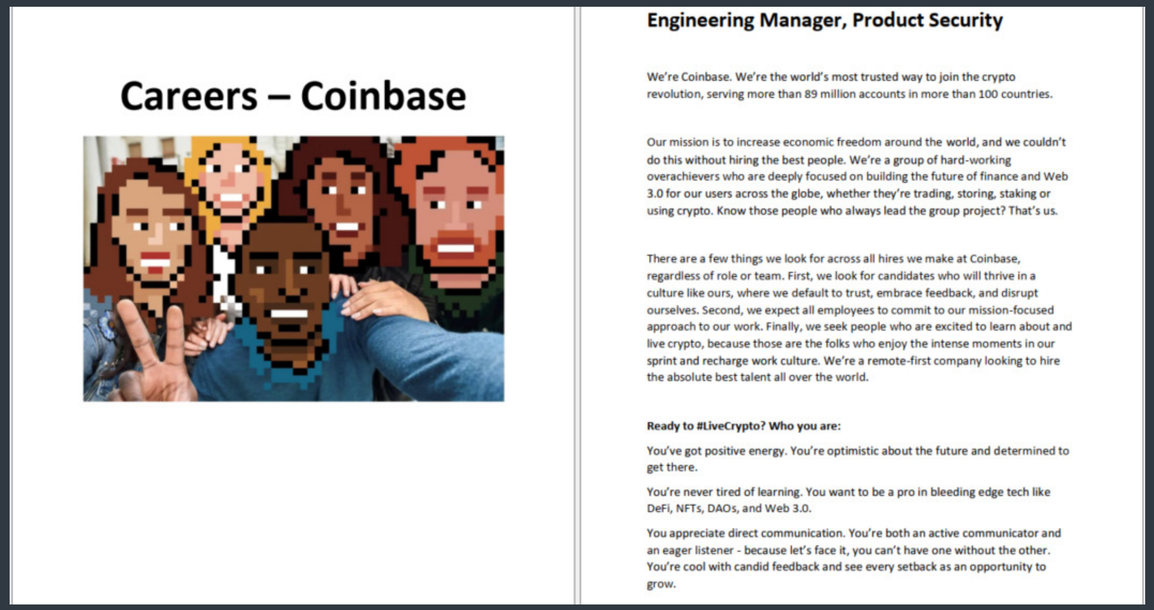
ESET researchers saw the Lazarus APT group using various trojanized, popular applications in May 2022. First, we tweeted about a Windows executable called `mozila.cpl`, which was submitted to VirusTotal in November 2020. The file is a trojanized sqlite v3.31.1 library with an embedded payload that exfiltrates RAR-compressed files from a victim's system.

Later that month, we reported that Lazarus had disguised one of its payloads as a well-known Windows activation tool by putting it into the KMSAuto folder. Since KMSAuto is a crack tool and its users typically exclude its location from their security products, it makes for a great hiding place for the Lazarus payload. The payload itself was a VMProtect-ed executable that, after dumping it from memory, turned out to be a RAT, delivered by a trojanized DeFi app.

*Twitter threads* [17] [18]

### Operation In(ter)ception is open to crypto-opportunities

ESET Research discovered an instance of the Operation In(ter)ception campaign for macOS, by Lazarus. We spotted that a signed Mach-O executable disguised as a job description for Coinbase had been uploaded to VirusTotal from Brazil. While targeting potential victims through LinkedIn and fake job offers is nothing new for Lazarus, they have not gone spearphishing in crypto-waters before.


Careers – Coinbase

Engineering Manager, Product Security

We're Coinbase. We're the world's most trusted way to join the crypto revolution, serving more than 89 million accounts in more than 100 countries.

Our mission is to increase economic freedom around the world, and we couldn't do this without hiring the best people. We're a group of hard-working overachievers who are deeply focused on building the future of finance and Web 3.0 for our users across the globe, whether they're trading, storing, staking or using crypto. Know those people who always lead the group project? That's us.

There are a few things we look for across all hires we make at Coinbase, regardless of role or team. First, we look for candidates who will thrive in a culture like ours, where we default to trust, embrace feedback, and disrupt ourselves. Second, we expect all employees to commit to our mission-focused approach to our work. Finally, we seek people who are excited to learn about and live crypto, because those are the folks who enjoy the intense moments in our sprint and recharge work culture. We're a remote-first company looking to hire the absolute best talent all over the world.

**Ready to #LiveCrypto? Who you are:**

You've got positive energy. You're optimistic about the future and determined to get there.

You're never tired of learning. You want to be a pro in bleeding edge tech like DeFi, NFTs, DAOs, and Web 3.0.

You appreciate direct communication. You're both an active communicator and an eager listener - because let's face it, you can't have one without the other. You're cool with candid feedback and see every setback as an opportunity to grow.

Fake Coinbase job description used in Operation In(ter)ception

Built as a fat Mach-O executable, supporting both Intel and Apple Silicon processors, this malware was similar to *another ESET discovery* [19] that we tentatively attributed to Lazarus at the time. This newer sample drops three files: a decoy PDF document, and two malicious executables; the first, `FinderFontsUpdater.app`, executes the second, `safarifontagent`, which is a downloader. The C&C server from which the downloader gets the next stage did not respond at the time we analyzed this threat.

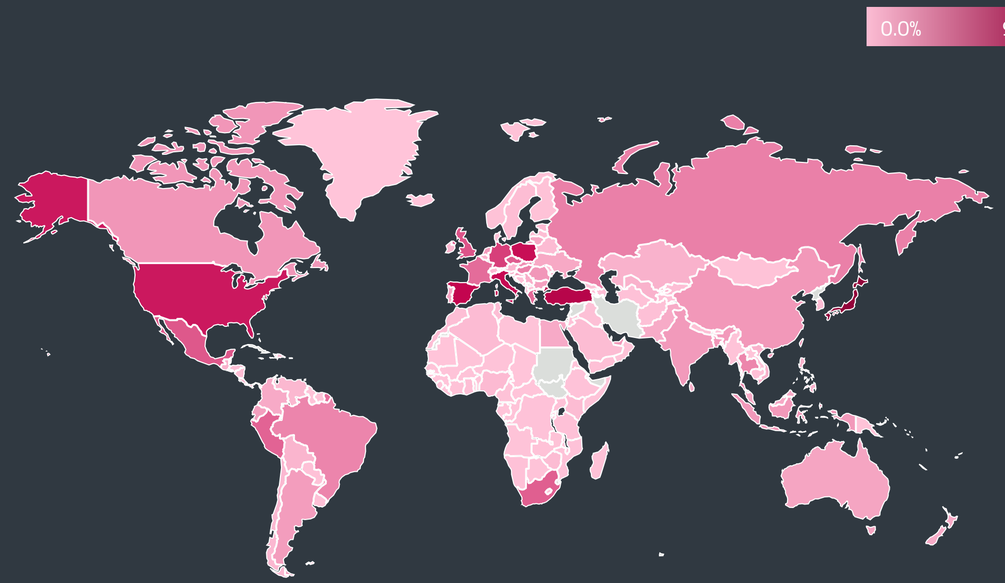
The bundle was signed using a certificate issued in February 2022 to a developer named Shankey Nohria. However, the application was not notarized and Apple revoked the certificate on August 12.

There is also a Windows counterpart to this threat that drops the same decoy document, which was *spotted* [20] by a researcher at Malwarebytes.

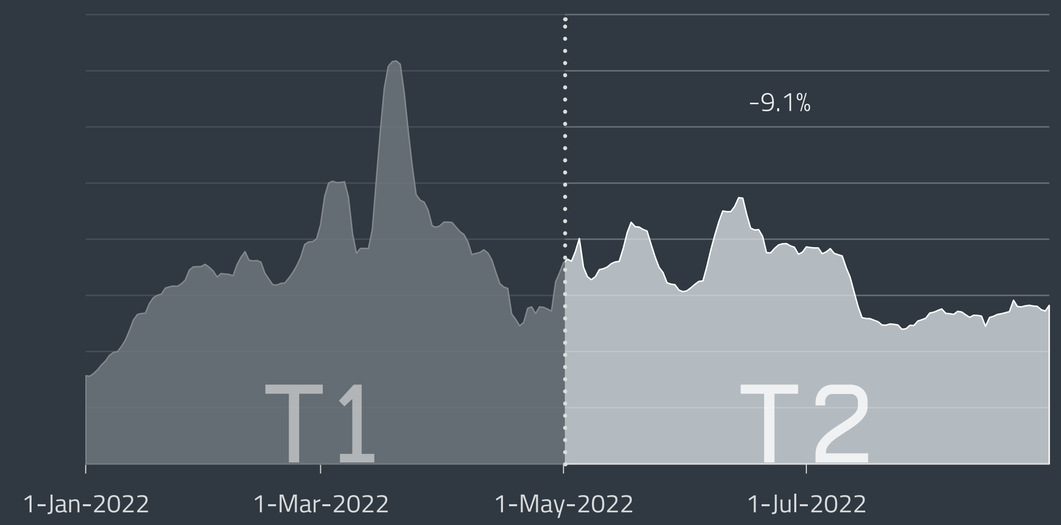
*Twitter thread* [21]

# STATISTICS & TRENDS

The threat landscape in T2 2022 as seen by ESET telemetry




Global distribution of malware detections in T2 2022




Overall threat detection trend in T1 2022 – T2 2022, seven-day moving average

# THREAT LANDSCAPE OVERVIEW

*A summary of the threat landscape developments in T2 2022.*

The threat landscape of T2 2022 was characterized by a decrease in almost all monitored categories, with an overall threat detection decline of 9.1%. Total threat numbers peaked on June 14, which was caused by DOC/TrojanDownloader.Agent, an Emotet malware family.

Speaking of Emotet, the ***Downloaders*** section specifies that while Emotet remained quite active in T2, its numbers were down by 31%. We also saw Emotet moving away from VBA macros in favor of DOC and LNK files.

There were also changes in the ***Exploits*** category, in which new exploits such as Log4Shell and Spring4Shell were on the rise while RDP attack attempts declined by 89%.

In what constitutes one of the largest declines in ***Ransomware*** numbers in the last two years, that category's detections dropped by 24%. Unlike T1, during which the most targeted country was Russia due to its invasion of Ukraine, this time ransomware operators turned their attention towards the US.

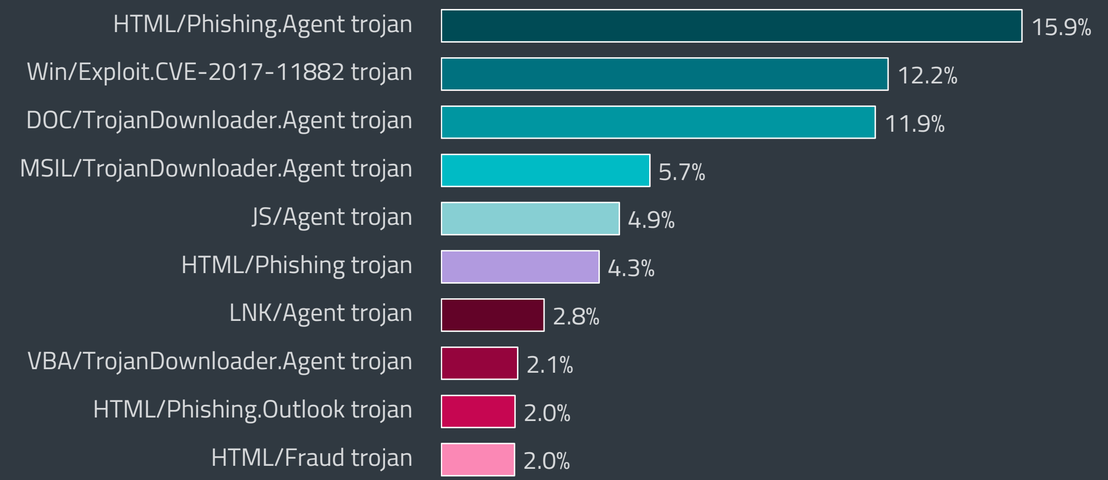
As was to be expected, ***Cryptocurrency threats*** went down, this time by 18.9%, along with the price of bitcoin. In a surprise twist, the continuously declining subcategory of Cryptostealers grew by almost 50% in T2.

While ***Web threats*** did not decrease as steeply as other categories, they were nevertheless on a downward trend in T2, with only unique phishing URLs experiencing growth this period. ESET phishing feeds showed a dramatic sixfold surge in shipping-themed phishing lures.

As opposed to T1, when ***Email threats*** experienced their largest increase to date, their numbers went down by 15% in T2. However, thanks to its rapid growth, HTML/Phishing.Outlook, one of the Email threat families, managed to get on to the overall top 10 most detected malware list for the first time.

Also on the decline, with a 14.3% decrease in detections this period, was the ***Infostealers*** category. The decrease was caused by a reduction in the number of detections of its strongest subcategory, Spyware, which went down by 21.7%.

Most of the ***macOS*** subcategories declined as well, coming to an overall 15.6% decrease in number. Almost half of the monitored detections were potentially unwanted applications (PUAs).




Top 10 malware detections in T2 2022 (% of malware detections)

Over in the ***IoT security*** category, you can see that the Mozi botnet lost some of its power in T2, slowing down by 23%. On the other hand, other Mirai-based botnets increased their activity by 61%

The ***Android*** category was the only one that registered an overall increase in the number of detections, which went up by 9.5%. Its fastest-growing subcategory was Spyware, but its highest numbers were reached by HiddenApps.

Several malware families in the top 10 malware detections list traded positions, moving up or down the list by a few places. The only major changes were MSIL/Spy.AgentTesla's disappearance from the list following a notable 29% decrease in detections, and the appearance of a newcomer among the top-detected threats, the HTML/Phishing.Outlook trojan. This fresh new member of the top 10 grew by 66.1% between T1 and T2 2022.

# TOP 10 MALWARE DETECTIONS

## → HTML/Phishing.Agent trojan

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

## ↗ Win/Exploit.CVE-2017-11882 trojan

This detection name stands for specially crafted documents exploiting the *CVE-2017-11882* [22] 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.

## ↘ DOC/TrojanDownloader.Agent trojan

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

## ↗ MSIL/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.

## ↘ JS/Agent trojan

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

## → HTML/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/Phishing.Outlook trojan

HTML/Phishing.Outlook is a detection name for phishing emails that harvest login information for Microsoft's outlook.com email service. Email messages falling under this detection typically contain HTML attachments posing as outlook.com login pages. Frequently, these phishing forms already come prefilled with the target's email addresses, probably making the target more likely to supply the rest of the information.

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

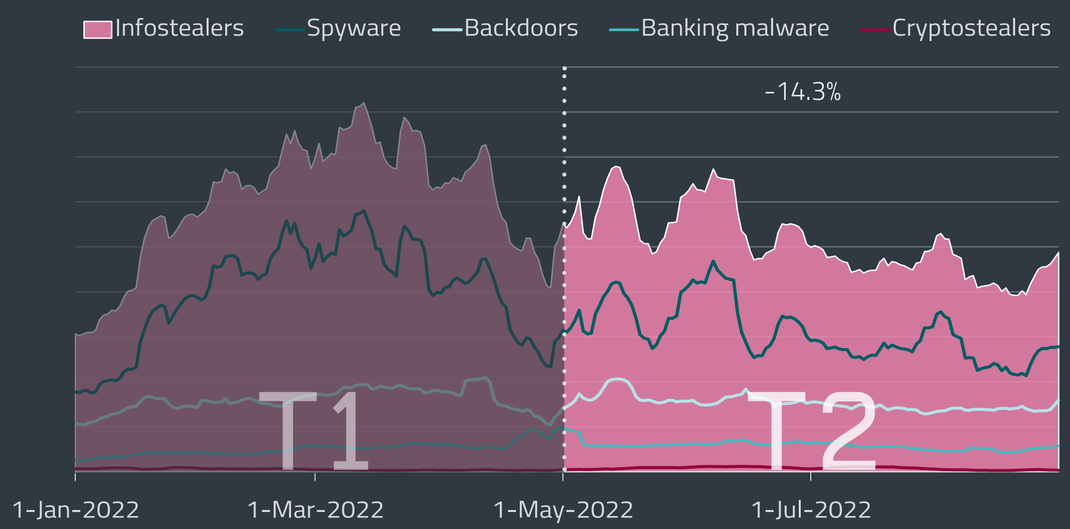
# INFOSTEALERS

*JS/Spy.Banker continued its reign in the Banking malware subcategory; Agent Tesla numbers dropped.*

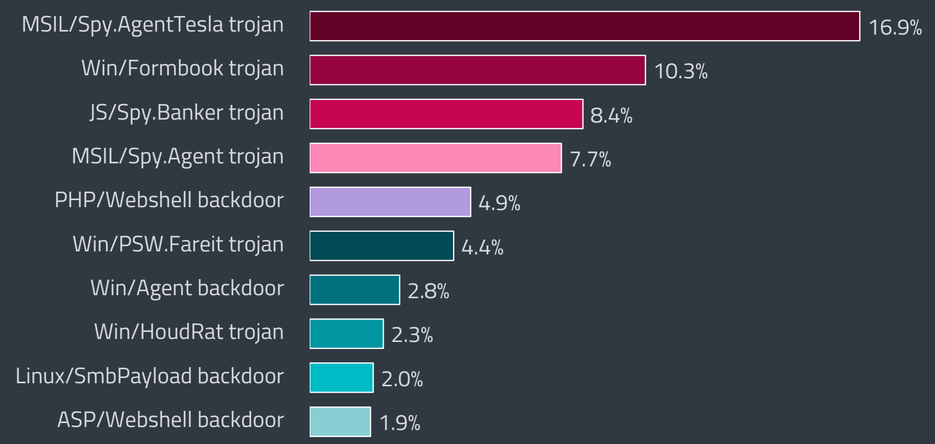
As is the case for most of our categories in T2 2022, the number of Infostealer detections decreased compared to T1. They went down by 14.3%, caused by a decline in their strongest subcategory, Spyware, which lost 21.7% in T2. Backdoors seem to have stabilized, for now, only having 2% fewer detections than in the previous period. Meanwhile, banking malware continued its growth from T1, this time increasing by 9.9%. Rather unexpectedly, the biggest growth among Infostealer subcategories was exhibited by the smallest one, Cryptostealers. In T2 2022, it managed an unprecedented gain of 49.7%.

Despite the substantial decrease in detections, Spyware was still the most prevalent Infostealer subcategory, responsible for 58.6% of detections in the category. Spyware's decline might have been helped by the drop in MSIL/Spy.AgentTesla detections, which were down by 24.6% in T2. We still registered a considerable spike in detections in this subcategory on June 6, caused by the aforementioned Agent Tesla alongside the Win/Formbook trojan. On that date, the highest number of attack attempts conducted by both malware families was seen in Turkey.

Looking at the chart of the top 10 Infostealer threats, half of them are in the Spyware subcategory. As usual, MSIL/Spy.AgentTesla was in the lead with 16.9% of all Infostealers and 28% of Spyware – even the drop in numbers did not succeed in dethroning it as the most prevalent there. It introduced a new distribution method in T2 when it started ***spreading*** [24] via weaponized Windows compiled




Infostealer detection trend in T1 2022 – T2 2022, seven-day moving average




Top 10 infostealer families in T2 2022 (% of Infostealer detections)

HTML Help files, which use the `.chm` extension, attached to phishing emails impersonating the shipping company DHL.

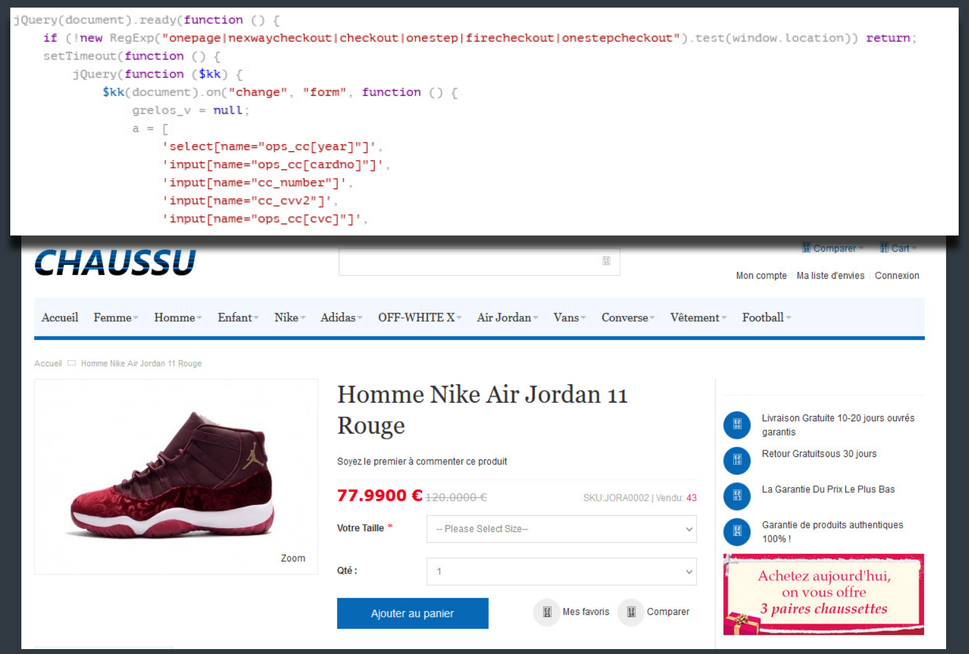
The Win/Formbook trojan also managed to keep its second place despite losing an even higher percentage of its detections than Agent Tesla (36.7%, to be precise). It constituted 10.3% of Infostealer detections and 17.1% of Spyware detections. The MSIL/Spy.Agent trojan actually grew by 14.4%, but still remained the third most detected spyware, with 12.8%, and the overall fourth most detected in the Infostealer category, with 7.7%.

In addition to somewhat recovering from their decline, the Backdoor subcategory increased its overall share of Infostealer detections, going from 25.5% in T1 to 29.1% in T2. Backdoor numbers peaked on May 12 when we saw increased activity from the Win32/Agent.TJS backdoor, caught mostly in the Czech Republic.

This time, four backdoors managed to claim places in the Infostealer top 10, as opposed to three in T1. PHP/Webshell kept a steady trend and remained the most prevalent backdoor with 16.5%, which is 5% of all Infostealers. Even a 7.2% decrease could not budge the Win/Agent family from its second place in the subcategory, which it earned with 9.2% (2.8% of Infostealers). T1's third-place holder, ASP/Webshell, was fourth this time, narrowly replaced by the Linux/SmbPayload backdoor with 6.5% of Backdoor and 2% of Infostealer detections.

While the rates of banking malware detections increased by 9.9% in T2, they showed a clear, albeit gentle, downward trend across the period. Detections in this subcategory constituted 10.8% of the Infostealer category. Banking malware detections peaked on June 9, with the largest amount of hits recorded in the United States and attributed to JS/Spy.Banker. The second most detected malware family on that day was the notorious Qbot, which also had its T2 peak at that time.

JS/Spy.Banker's dominance from T1 continued in T2. This web skimmer, better known as Magecart, constituted three-fourths of all Banking malware detections, leaving far behind the rest of the families in the subcategory. *From January up until almost the end of May* [25], Magecart led a very successful campaign, during which it compromised more than 300 restaurants, stealing at least 50,000 credit card records in the process. It was also the third most detected among the Infostealers, with 8.4%, and the only banking malware to get into the overall top 10.




Website compromised by JS/Spy.Banker and the malicious skimmer code linked to the page

However, it is important to note that web skimmers such as JS/Spy.Banker are distributed and detected in a different way from most of the Infostealer top 10. Since they constitute online scripts that are lying in wait on hacked or unpatched websites (mostly hosted on WordPress and Magento), their detection statistics are based on the number of visits to these websites and might not reflect the actual level to which the skimmers in question have spread. The only other members of the Infostealer top 10 that work similarly to JS/Spy.Banker are PHP/Webshell and ASP/Webshell. The rest of the most-detected families are distributed via email attachments or as downloader payloads.

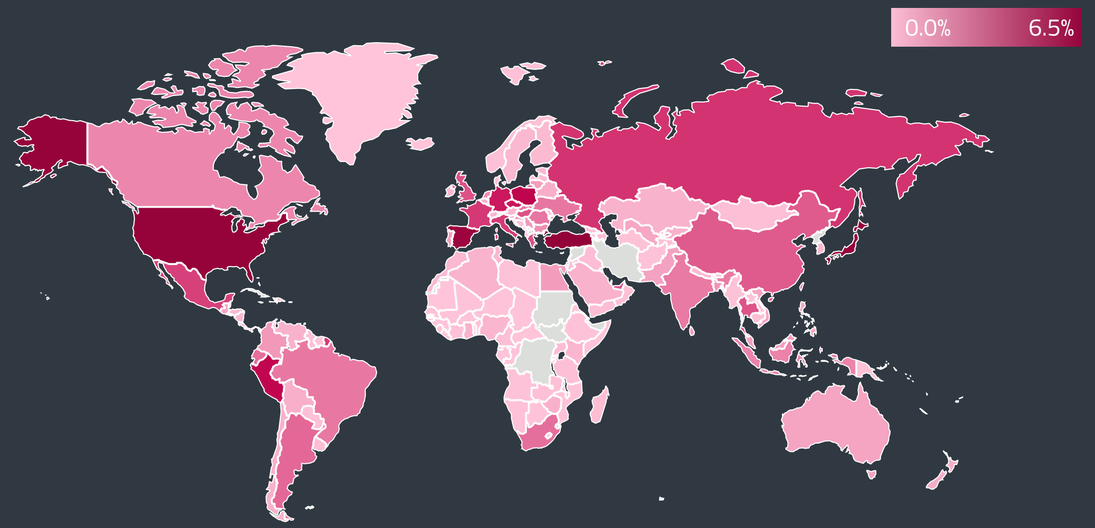
## EXPERT COMMENT

The most prevalent variant of JS/Spy.Banker was JS/Spy.Banker.KJ. It is quite an interesting piece of malware because the part of the code that downloads the skimmer itself is rather short, uses only a handful of common JavaScript functions, and mostly does not use complex obfuscation. This means the malicious code blends in with the original code quite seamlessly, making the infested web page appear safe. This posed a challenge in differentiating between a legitimate site and a skimmer-infested site, showing the resourcefulness of the malware's creators.

**Radim Raszka, ESET Detection Engineer**

As we already mentioned in the opening paragraph, the Cryptostealers subcategory unexpectedly grew by 49.7% in T2. This development was caused by a staggering increase in PowerShell/PSW. Coinstealer detections, which gained a new variant in T2. More details regarding Cryptostealers can be found in the *Cryptocurrency threats* chapter of this report.

Concerning the geographical distribution of Infostealer detections, the top three countries in the list faced almost the same amount of attack attempts: Turkey 6.5%, and both Japan and the United States 6.3%.




Global distribution of Infostealer detections in T2 2022

# RANSOMWARE

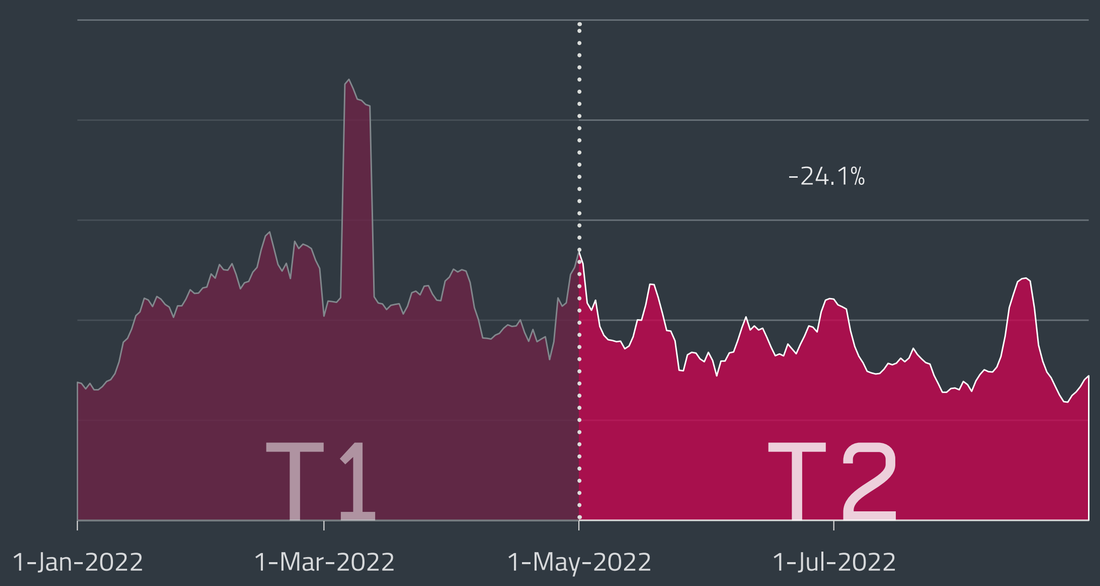
*Ransomware detections dropped by a quarter in T2 2022. Politically loaded messages related to the Russian war against Ukraine receded in new variants.*

The Ransomware category dropped by more than 24% in T2 2022, which is the most significant decrease since the beginning of 2021 when ransomware detections declined by 27%.

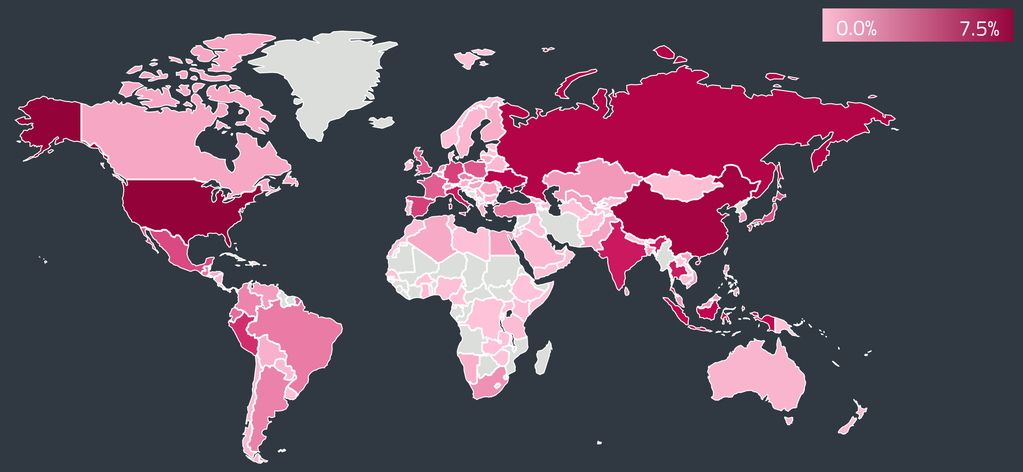
This detection trend shows several upticks, first on May 18, caused by Lockbit attacks in Guatemala, accounting for 59% of all detections on that day. Another peak in telemetry appeared on June 28 due to the spread of Win/Filecoder.WannaCryptor.D (24%) in Peru and the distribution of multiple old variants of MSIL/Filecoder (16.5%) in Ukraine. The last and the largest spike was observed on August 12, caused primarily by well-known variants of Win/Filecoder and MSIL/Filecoder, with 45% of detections that day coming from the United States.

Russia was replaced by the United States in being the country most targeted by ransomware in T2 2022, reporting 7.5% of all such attacks. It was followed by China with 6% and Israel with 5.5%.

Coming in at fourth and fifth place were Russia and Ukraine; both faced roughly the same number of ransomware attacks. The difference compared to T1 2022 was the decreased number of attacks with politically loaded messages. Russia was most commonly targeted by years-old Win/Filecoder variants and ransomware families that lock victims' screens. In contrast, Ukraine was hit mostly by derivatives of HiddenTear, the first open-source ransomware, detected by ESET as AK and Y variants of MSIL/Filecoder.




Ransomware detection trend in T1 2022 – T2 2022, seven-day moving average



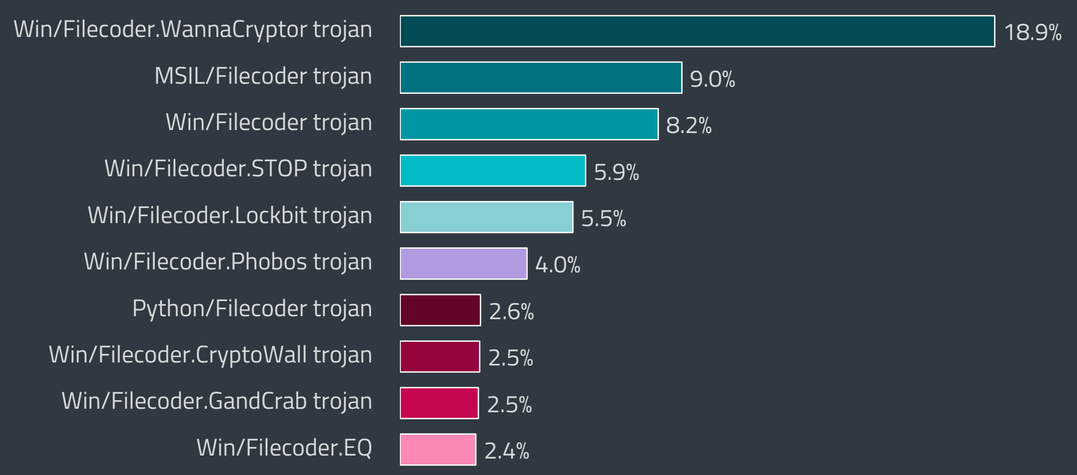

Global distribution of Ransomware detections in T2 2022

In the Ransomware top 10, the most interesting change was probably the increased prevalence of Python/Filecoder. While in T1 2022 it ranked tenth, in T2 2022 it moved up to seventh place, accounting for 2.5% of all detections in the category. The detection covers amateurish attempts to create ransomware. Names such as `test.pyc` used for some of the recently seen binaries and the use of hardcoded private keys such as `1881**ANARCHY_rtxDATA__ANARCHY1881***` support this hypothesis.

```
privkey = "1881**ANARCHY_rtxDATA__ANARCHY1881***"
enc_key = hashlib.md5(privkey.encode("utf-8")).hexdigest()
enc_key = enc_key.encode("utf-8")
```

Hardcoded private key as seen in some amateurish Python/Filecoder variants

T2 2022 brought several new trends to the ransomware scene. Lockbit (3.0) started the first ever *ransomware bug bounty* [26] program, offering researchers and (un)ethical hackers anything between USD 1000 and USD 1 million in Monero for findings related to their operation. The sought-after items include flaws in malware, vulnerabilities in the leak site, or "brilliant ideas" for improvements. The highest sum is reserved for anyone who can identify the person running Lockbit's affiliate program, currently known by the nickname *"LockBitSupp"*. In an interesting turn of events, it was this actor who *publicly claimed* [27] that one of the gang's victims – Entrust – was behind the DDoS attacks that were hitting Lockbit's leak sites.




Top 10 ransomware families in T2 2022 (% of Ransomware detections)

Another trend observed in T2 2022 is the shift of skilled ransomware writers towards the Rust programming language. The first to make the move were the *BlackCat* [28] creators, followed by *Hive* [29]. The latest addition to this currently exclusive club is the T2 newcomer *Luna* [30]. Using Rust offers malware operators several advantages, including improved evasion of security solutions and improved *error resistance* [31].

In the past couple of years, one of the most prevalent red team tools (ab)used by the ransomware gangs has been Cobalt Strike. However, in T2 2022 some of the ransomware groups switched to *Brute Ratel* [32] because of its lower detection rates by EDR and security solutions.

The last four months saw some curious ransomware-related cases. For example, a victim in the automotive industry experienced what it meant to have initial access to their network sold on the black market. Its systems were hit by *three different ransomware gangs* [33] in just two weeks. Another uncommon approach has been seen in cases caused by a new ransomware family called Zeppelin. *CISA and the FBI* [34] warned that victims targeted by this gang could see their data encrypted several times during a single compromise.

But ransomware actors are also facing increased pressure from authorities. Due to ransomware attracting so much attention, new regulations are being passed, sanctions imposed, and the willingness of victims to pay the ransom decreasing. A mixture of these factors is forcing the threat actors to refocus from high-profile victims to mid-sized organizations and to lower the demanded *ransoms* [35]. A new *report* [36] by the British think tank RUSI even suggests that increased attention on ransomware is pushing perpetrators to look for new hunting grounds, primarily in the Global South, where attacks are less laborious and the risk of prosecution is lower.

An illustrative case of making the life of ransomware gangs harder is the *USD 10 million reward* [37] offered for information about *"individual(s) who hold a key leadership position in the Conti ransomware... group"*. But even victims may not come out unscathed, as shown by the *Colonial Pipeline* [38] case. The US regulator has proposed to fine the company nearly USD 1 million for *"control room management failures"* that complicated recovery from the 2021 ransomware compromise.

Despite the growing law-enforcement and regulatory activity, many new ransomware actors appeared on the scene in T2 2022. Reminding the world of the 2017 WannaCryptor (aka WannaCry) incident, *CISA and the FBI* [39] warned that North Korean threat actors cooked up a new ransomware family called Maui. About a week later Microsoft attributed another newcomer *H0lyGh0st* [40] to hackers from the same country. QNAP NAS devices have another threat to worry about too, namely *Checkmate* [41]. A new free-to-use ransomware builder *Redeemer* [42] (version 2.0) may also worsen the situation as it opens the doors for unskilled actors who want to try their luck in the game.

There were also some "rebrands" during this period. Chaos ransomware builder has been used to create another family called *Yashma* [43]. And we have to mention Conti, which after catastrophic leaks saw its minions *dissolved* [44] into several other gangs, including Hive, BlackBasta, BlackCat, and BlackByte.

The list of high-profile victims in T2 2022 is also quite long. It includes a *Foxconn factory in Mexico* [45] hit by Lockbit, the *government of Costa Rica* [46] that saw its systems attacked by Conti, building materials manufacturer *Knauf Group* [47] hit by Black Basta, and the already mentioned security giant *Entrust* [48].

In the happy corner, there were multiple families that ceased their activity or actors behind them were arrested. In the case of *Thanos* [49], its creator, seller and also operator – a Venezuelan doctor – was arrested by the authorities. *AstraLocker* [50] closed up shop with decryptors now available. Victims of the newcomer *Yashma* [51] can also decrypt their files using a new decryptor.

The final bit of good news comes from the *No More Ransom* [52] initiative – where ESET is an associate partner – which in its six years of existence has helped 1.5 million ransomware victims to decrypt their files and save around USD 1.5 billion.

## EXPERT COMMENT

The growing proportion of Python ransomware families can have multiple explanations. First, Python is easy to use even for unskilled malware writers. As a scripting language, it also allows threat actors to obfuscate and change their code and create new variants that can evade detection. Second, technically advanced ransomware actors are abandoning the mass-spreading model mostly tracked by our telemetry and are increasingly focusing on big-game hunting and RaaS schemes, letting the rookies claim a bigger portion of their former market. Last but not least, there are very many "test" projects related to encryption on GitHub that can be easily reused as part of a new ransomware strain.

**Igor Kabina, ESET Senior Detection Engineer**

# DOWNLOADERS

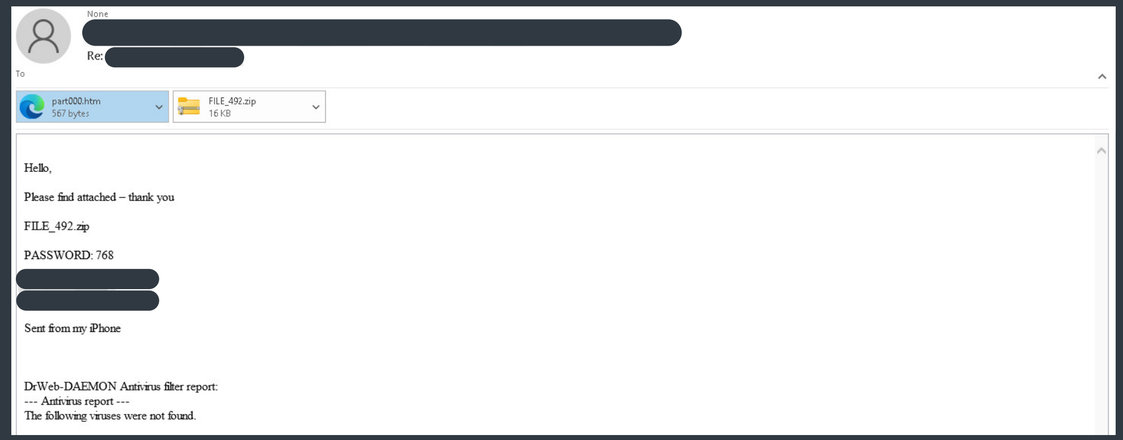
*In T2 2022, Emotet operators took their foot off the gas but remained the dominant force in the Downloaders category.*

A hundredfold increase in activity and looking for new compromise vectors – that is where we left Emotet at the end of T1 2022. In T2 2022, the number of its attacks headed in the opposite direction – although not as dramatically – and dropped by over 31%.

As for the new vectors, Emotet's operators have abandoned VBA macros in response to ***Microsoft disabling them*** [53] in documents originating from the internet. Instead, Emotet has moved to campaigns based on weaponized Microsoft Office files (91%) and LNK files (9%). Both arrive in email inboxes in the form of password-protected ZIP files.

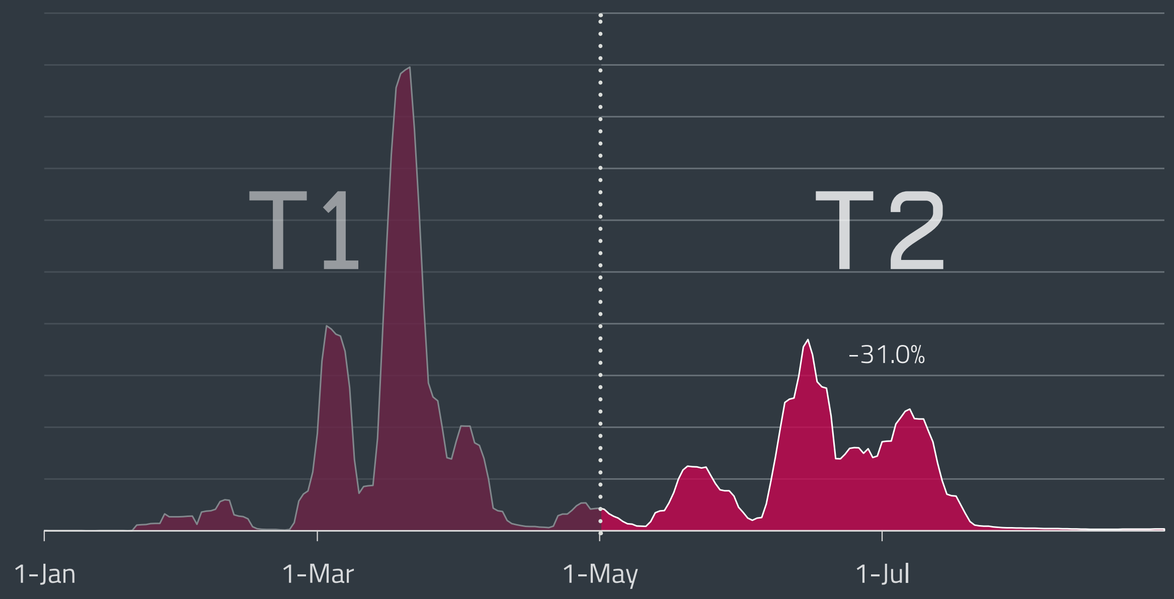
The only significant campaign built on LNK files was detected on May 18, aimed primarily at inboxes in Japan and Italy. All the other upticks visible in the trend chart between June and mid-July were caused by waves of malspam containing weaponized documents and spreadsheets (DOC), aiming at the same regions.

According to ESET telemetry data, August was a vacation month for Emotet operators. Regarding new features first seen in T2 2022, Emotet operators added the Google Chrome CC stealer ***module*** [54] that extracts credit card information from that browser and sends it to the command and control server. They have also returned to some of the earlier modules, namely the years-old Spreader.




An email from one of Emotet's malspam campaigns that spread malware via attached password-protected ZIP files

In the T2 2022 Downloader top 10, Emotet remained the most influential malware family. Its malicious DOC and LNK files were responsible for almost half of all detections in the category, which declined by 16% in overall detections. The only other notable player in the top 10 list was MSIL/TrojanDownloader.Agent with 21% of detections, mostly attacking devices in Turkey and Spain.

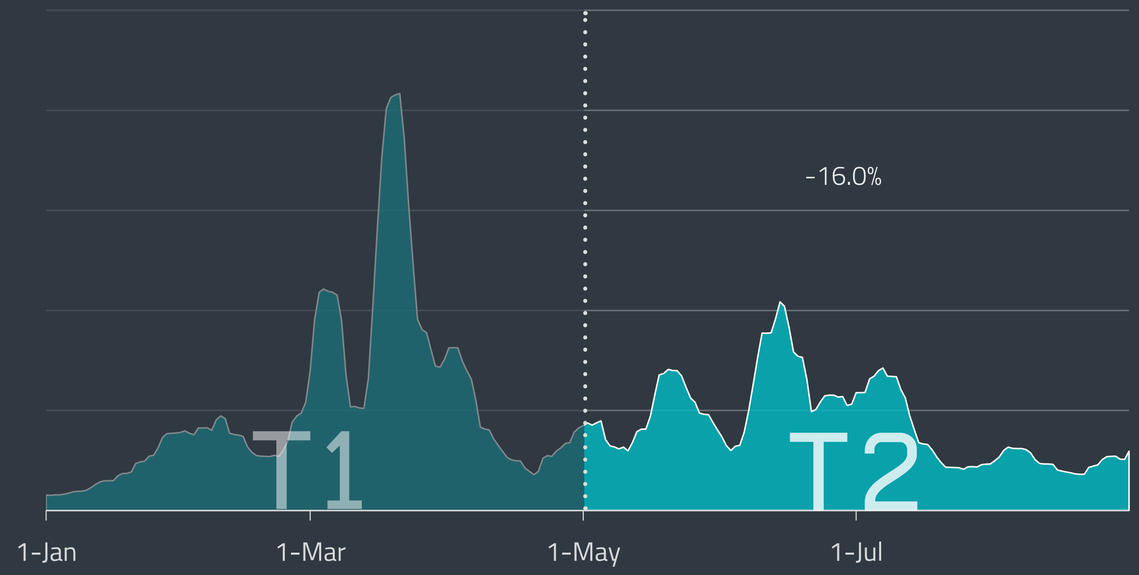



Emotet detection trend in T1 2022 – T2 2022, seven-day moving average

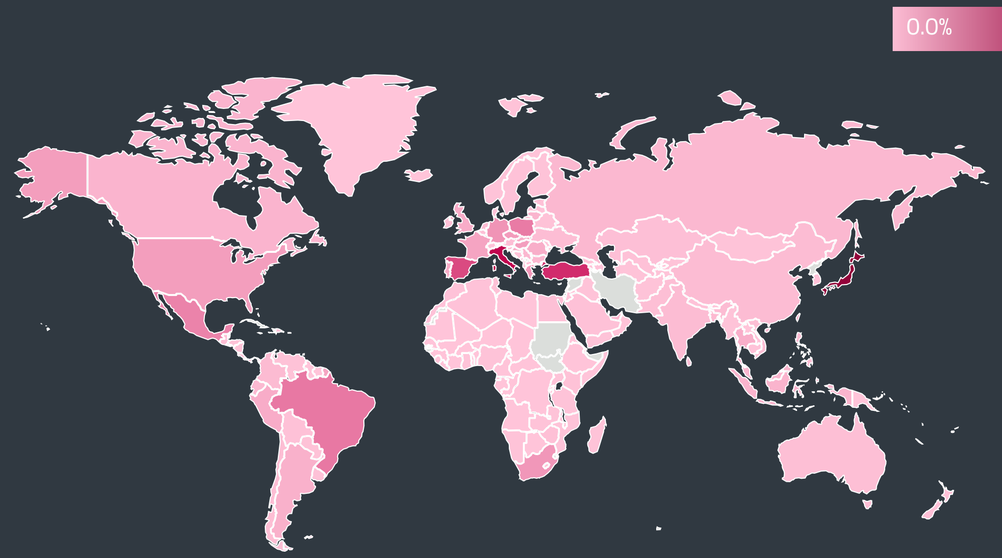
## EXPERT COMMENT

In June, we saw Emotet operators reintroduce the old Spreader module, which they used for lateral movement before the January 2021 takedown. Its main goal is to gain remote access to other devices in the network by brute force, using a hardcoded list of usernames and passwords. If successful, the spreader copies the main Emotet binary to the compromised system and executes it as a service.

**Zoltán Rusnák, ESET Malware Researcher**

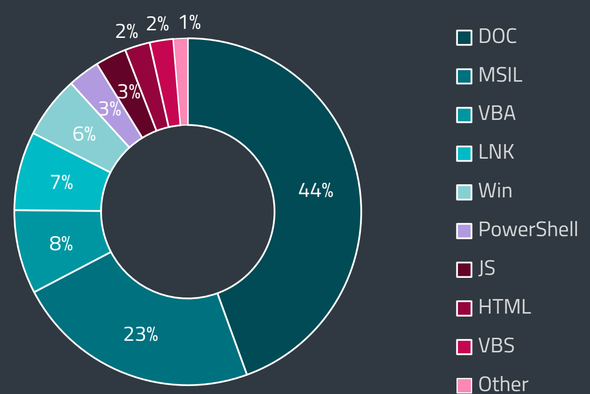



Downloader detection trend in T1 2022 – T2 2022, seven-day moving average




Global distribution of Downloader detections in T2 2022

MSIL's variants JDM, MVU, and MRS used the already documented approach of downloading two binaries: an EXE file, and a DLL tool to execute it, leading to a compromise by either Agent Tesla, Fareit, or the MSIL/Agent.CFQ trojan. The KXQ and MFV variants opted for a modified tactic: downloading an encrypted DLL injector posing as a JPG or BMP file that, if executed, delivered the same final payloads.




Downloader detections per detection type in T2 2022

Another downloader family in the top 10 that ditched VBA macros as an initial vector was PowerShell/TrojanDownlader.Agent. Its variants FSW and FSV – responsible for every fifth detection of this family in T2 – were part of campaigns spreading weaponized Windows compiled HTML Help files, which use the `.chm` extension.

If such file is executed, a regular Windows Help window is opened to mask that HTML code is run in the background. That in turn downloads PowerShell script with two built-in binaries: a loader that injects a running process with the second binary and the final payload – MSIL/Spy.AgentTesla.E.

Emotet and this campaign confirmed the trend seen in T1 2022, namely the abandonment of VBA macros as the initial compromise avenue. Since the beginning of the pandemic, it was the unopposed number one vector for several malware families including Emotet, Trickbot, and Qbot. But at the beginning of 2022, VBA-based downloaders started declining, with weaponized Office files (DOC) and MSIL detections taking the lead. In T2, VBA placed third, closely followed by the LNK platform.

One of the factors that contributed to this trend was Microsoft's February 2022 announcement that VBA macros in documents downloaded from the internet would be disabled by default. Despite the *flurry* [53] of rollbacks and re-announcements of this step by Microsoft in T2 2022, it seems that VBA macros have already lost their appeal to cybercriminals, who are testing new ways to compromise their victims – such as the LNK and CHM files.

# CRYPTOCURRENCY THREATS

*Cryptostealers were on the rise while cryptocurrency exchange rates plunged.*

T2 2022 brought a steep decline in cryptocurrency exchange rates, including the price of bitcoin dipping below USD 20,000 for the first time since late 2020. It seems that, for now, cryptocurrencies, NFTs, and other blockchain-related ventures have lost much of their shine. Looking at the Cryptocurrency threats trend chart, this is true for cybercriminals to a degree, with the T2 detection numbers continuing the decrease started in T1, this time going down by 18.9%.

However, the threat posed by cryptocurrency-related malicious activities was far from gone, as recent headlines were rife with stories of various criminal feats, from NFTs stolen in a ***Discord phishing scam*** [55] to an ***exploit*** [56] allowing hackers to steal bitcoin from ATMs. Law enforcement is also staying vigilant: the US Securities and Exchange Commission (SEC) ***announced*** [57] in May that it plans to increase the size of its cybersecurity unit to protect investors in cryptocurrency markets.

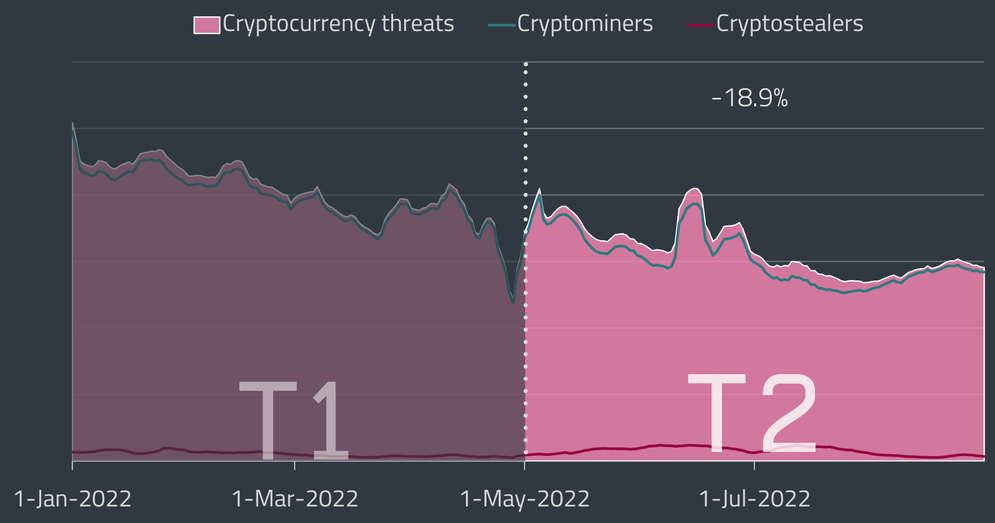
In T2 2022, the Cryptominers subcategory continued its decline from T1, going down by a further 20.7%. Cryptominers still experienced a strong detection peak, which occurred on June 11 and was caused by the AH variant of the MSIL/CoinMiner potentially unwanted application (PUA).

An interesting development in the coinminer threat landscape was the emergence of a new piece of malware based on the ESET-discovered ***KryptoCibule*** [58]. First documented by researchers at ***Symantec*** [59], who named it ClipMiner, this new coinminer, with the ability to scan clipboard content for wallet addresses, has made its operators at least USD 1.7 million. ESET tracks ClipMiner as two detections, MSIL/Agent_AGen.UG, and MSIL/Agent_AGen.UL. Our telemetry shows that both of them were on an upward trend in T2 2022.

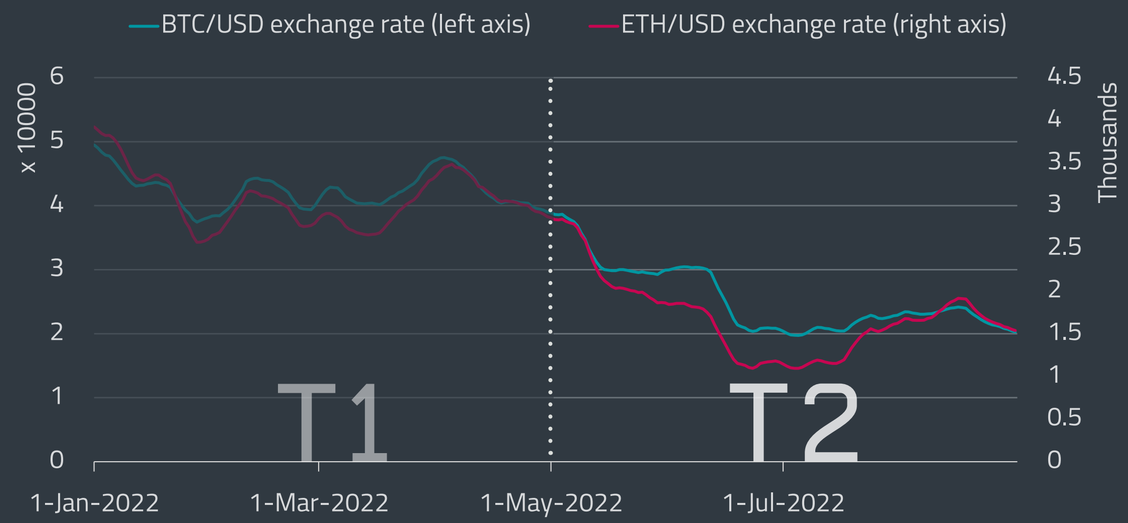
The top three coinminer detections – as usual – continued to be occupied by the same families. Despite a significant decrease in numbers between T1 and T2 2022 (32.8%), the Win/CoinMiner PUA was first with 41.7%. The JS/CoinMiner PUA with 13.8% declined by 7.6%, the smallest drop among the top three. This allowed it to claim second place from its long-time holder, the Win/CoinMiner trojan, which had 12% of Cryptominer detections in T2 after its numbers decreased by 22.9% compared to T1.

Even though PUAs boasted the two most-detected cryptominers, their overall proportion shrunk slightly in the Trojan:PUA ratio, making it 33% (Trojans) to 67% (PUAs) this time, continuing the trend that started in T1. Similarly, the amount of in-browser detections increased relative to desktop detections: in T1, it was 13% to 87%, compared to T2's 17% to 83%.

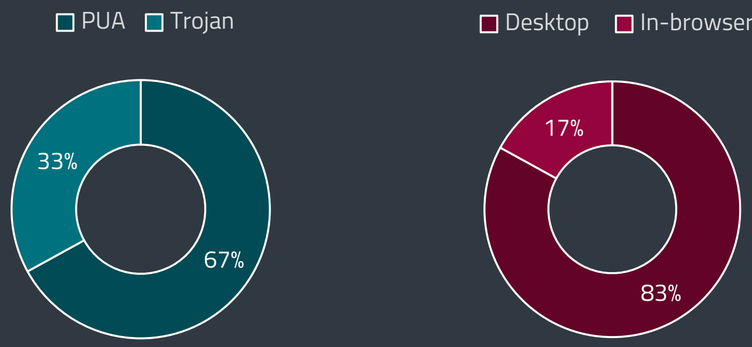
Related to the increase of in-browser detections, the number of cryptojacking domain visits grew by 16.4% in T2. If you want to avoid having your computer used against your will for mining, we advise you to steer clear of free streaming websites or torrent sites.




Cryptocurrency threat detection trend in T1 2022 – T2 2022, seven-day moving average




Bitcoin and Ethereum/USD exchange rates in T1 2022 – T2 2022, seven-day moving average




Trojan:PUA and desktop:in-browser ratio of cryptominer detections in T2 2022

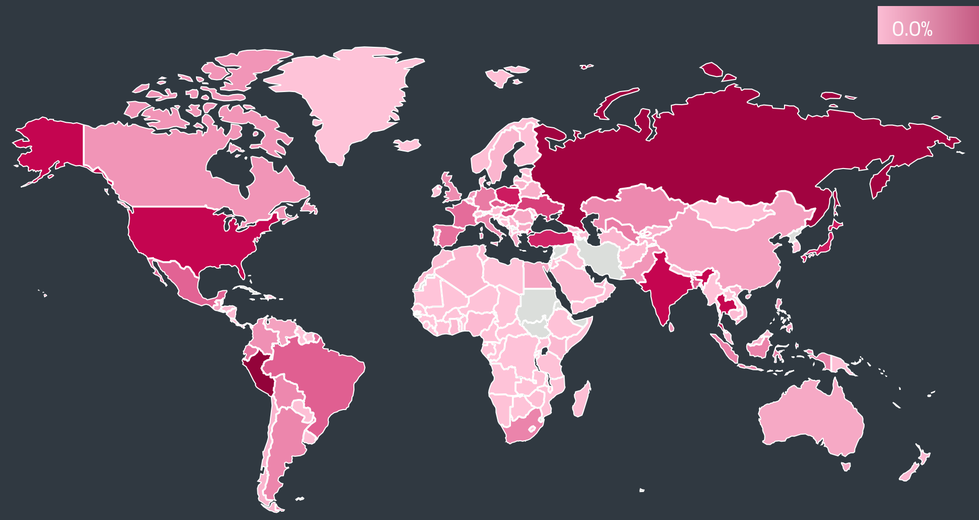
In a surprise twist, the Cryptostealers subcategory did not decline this time. Even more surprisingly, not only did they not decrease in number, they actually experienced rather significant growth of almost 50%. This can be almost single-handedly attributed to the meteoric rise of the PowerShell/PSW.CoinStealer trojan, a malware family that did not have many detections in the past, but managed to become the second most detected cryptostealer in T2 thanks to a new variant added to its arsenal, PowerShell/PSW.CoinStealer.D.

Threats belonging to this malware family search for installed cryptocurrency browser extensions such as Metamask, Binance, or Coinomi. They then exfiltrate this information for nefarious purposes, for example changing the target cryptocurrency addresses in memory to effectively transfer their ownership from the target to the cybercriminal.

We saw see two spikes in the Cryptostealers detection trend. The first, on June 13, was caused by Win/Spy.Agent, mainly registered in Peru. The second spike, which occurred on July 8, was due to PowerShell/PSW.CoinStealer, with the highest number of attempted attacks registered in India and the United States.

| | T1 2022 | T2 2022 |
|---|---|---|
| 1 | webminepool[.]com | webminepool[.]com |
| 2 | dl-x[.]com | mainevnap[.]com |
| 3 | wypracowanie.edu[.]pl | dl-x[.]com |
| 4 | slovolam[.]sk | gsgazete[.]com |
| 5 | carrierecalciatori [.]it | mituus[.]com |
| 6 | arafifblues[.]com | slovolam[.]sk |
| 7 | kaizoku-ehime[.]jp | wypracowanie.edu[.]pl |
| 8 | mainevnap[.]com | monerominer[.]rocks |
| 9 | mituus[.]com | arafifblues[.]com |
| 10 | monerominer[.]rocks | geotimes[.]com.ge |

Top 10 most visited cryptojacking domains in T1 2022 and T2 2022




Global distribution of Cryptocurrency threat detections in T2 2022

As in T1 2022, the Win/Spy.Agent trojan was the most-detected cryptostealer with 30.8%. However, the aforementioned heavy hitter of T2, PowerShell/PSW.CoinStealer, was close behind. Accounting for 27.9% of all cryptostealers, it beat the Win/PSW.Agent trojan, which ended up third and registered 20.7% of cryptostealer detections.

As opposed to the leading coinminers, all the families in the top three cryptostealers experienced growth in T2, paradoxically with Win/Spy.Agent growing the least out of the three, by 14.8%. Since PowerShell/PSW.CoinStealer was, according to our telemetry, mostly dormant in T1, it increased by more than a thousandfold in T2. Meanwhile, Win/PSW.Agent doubled its number of detections, going up by 102.1%.

ESET telemetry registered the highest number of cryptocurrency threat detections in Peru (8.3%), with Russia (7.2%) and the United States (4.3%) in second and third places, respectively.

## EXPERT COMMENT

Soaring energy prices negatively influence cryptocurrency exchange rates and the willingness to trade or mine cryptocoins. Malware authors now increasingly find it more profitable to steal cryptocurrencies than to illicitly mine them. Additionally, free streaming websites and torrenting sites are capitalizing on the trend of releasing films straight to streaming platforms that started during the height of the pandemic, and in-browser coinminers are taking advantage of that. With the continuing energy crisis, we anticipate that the growth of cryptostealers accompanied by the rise of in-browser coinminers will continue.

**Igor Kabina, ESET Senior Detection Engineer**

# WEB THREATS

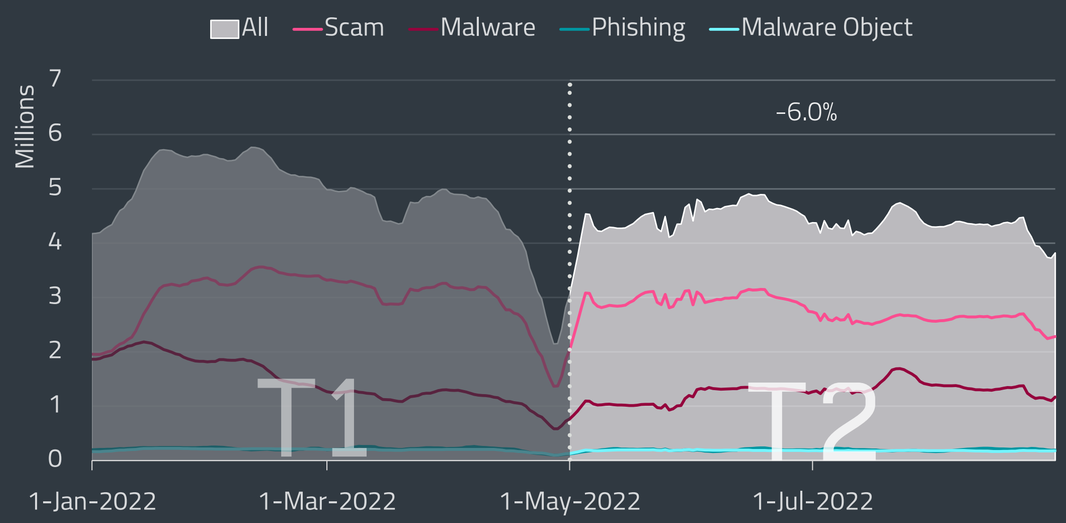
*Shipping-themed phishing lures skyrocketed while most web threats stagnated.*

Web threats did not experience as extensive a decrease in T2 2022 as other monitored categories, but nevertheless started exhibiting a slight downward trend. Overall blocks decreased by 6% and the decline was somewhat more pronounced when it came to the number of unique URLs blocked, which went down by 10.3%. All of the web threat subcategories followed this trend too, the only exception being unique phishing URL detections – those increased by 28.3%.

The number of unique phishing URLs that ESET products blocked reached almost 4.7 million in T2. On average, we blocked 38,000 of these a day. Interestingly, despite the significant uptick in unique URLs, the overall number of detected phishing websites remained relatively stable, only decreasing by 3.9%.

As in T1, of all of the Web threat subcategories, Malware blocks declined the most. The total number of malware-distributing website blocks went down by 9.8%, while the number of unique URLs our products blocked diminished by a quarter. On the other hand, the number of legitimate websites hosting malware, labeled Malware objects in the accompanying charts, stayed stable, with only a 3% decrease in both all blocks and unique blocks.

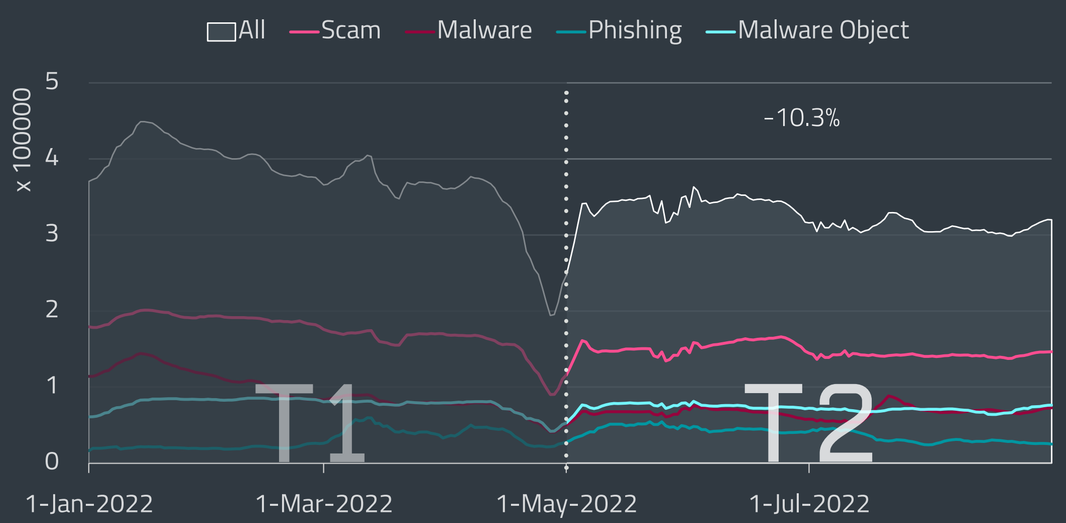
Scam site detections did not change drastically (4.5% decrease) and remained the most prevalent form of web threat, with over 340 million overall blocks and 18 million unique blocks. Their numbers



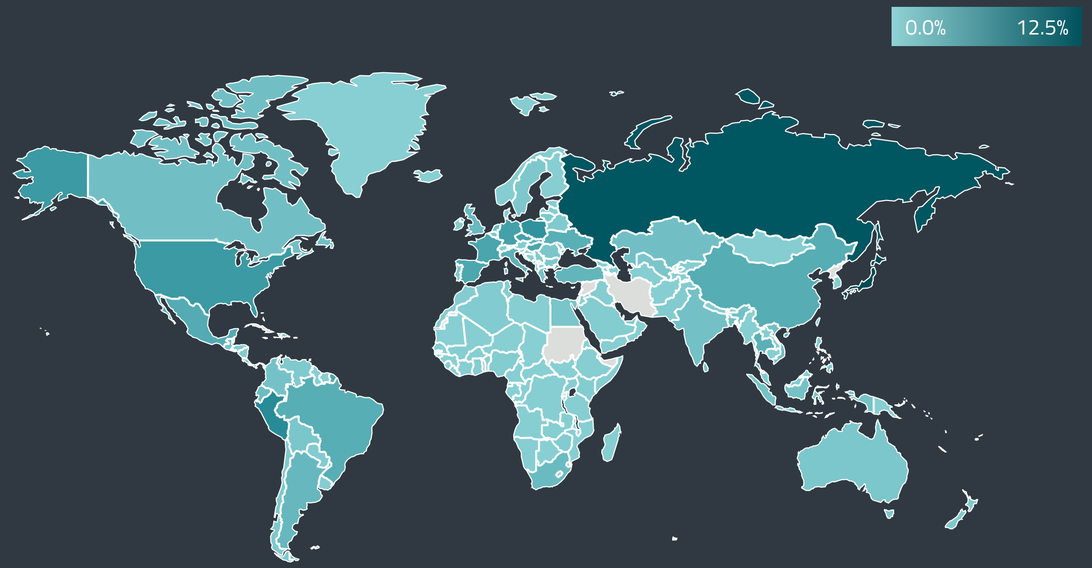

Web threat block trend in T1 2022 – T2 2022, seven-day moving average

| | Malware | Scam | Phishing |
|---|---|---|---|
| 1 | freychang[.]fun | survey-smiles[.]com | propu[.]sh |
| 2 | aj2396[.]online | s.sarafan[.]fun | mrproddisup[.]com |
| 3 | jecromaha[.]info | v.vfghe[.]com | foreign-movies.baby-supernode[.]xyz |
| 4 | www.hostingcloud[.]racing | mybetterck[.]com | thecred[.]info |
| 5 | iclickcdn[.]com | newrrb[.]bid | watchvideoplayer[.]com |
| 6 | webanalyser[.]org | bwukxn[.]com | www--bancosantafe--com-- ar.insuit[.]net |
| 7 | d1ywb8dvwodsnl.cloudfront[.]net | serch07[.]biz | tech4-you[.]com |
| 8 | vk-online[.]xyz | cellar.z5h64q92x9[.]net | tabledownstairsprovocative[.]com* |
| 9 | broworker1s[.]com | loft.z5h64q92x9[.]net | gtorra[.]pw |
| 10 | buikolered[.]com | hilarion-lar[.]com* | google-qa[.]net |

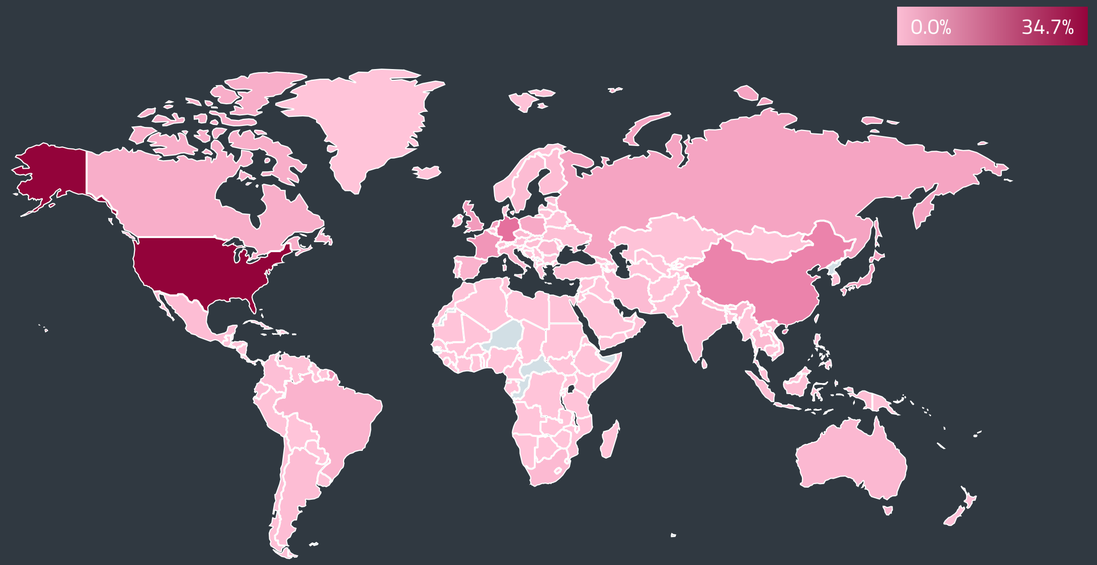
Top 10 blocked Malware, Scam and Phishing domains in T2 2022; domains first detected in this period are marked with *




Unique URL block trend in T1 2022 – T2 2022, seven-day moving average



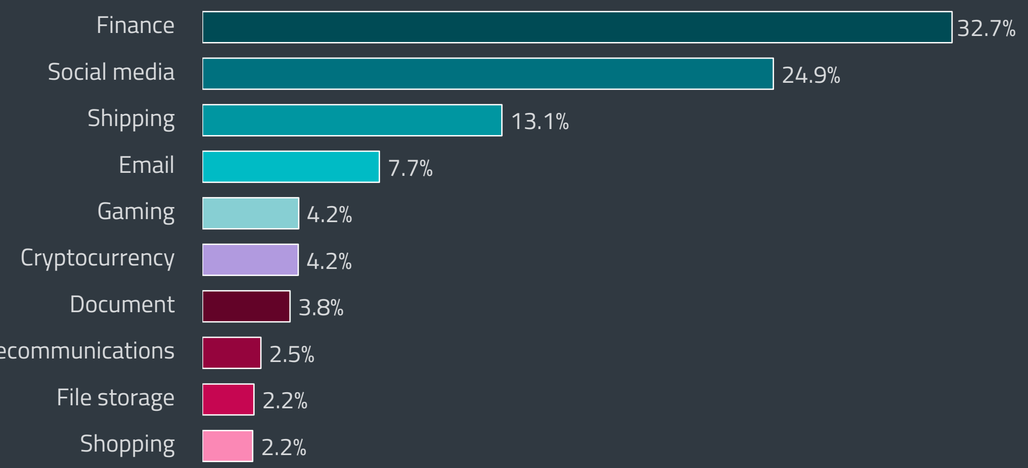

Global distribution of Web threat blocks in T2 2022




Global distribution of blocked domain hosting in T2 2022

peaked on May 25, when we registered 5 million scam website blocks, almost double the daily average amount. Unique scam URL blocks were down by 12.1%, with the largest number of unique blocked scam URLs on July 4, coming to almost 210,000.

Based on GeoIP tracking, the US remained the country hosting the largest proportion of detected Web threats, being the virtual home to more than a third of them (34.7%). Apart from that, the threats were slightly more spread out among other countries, where their shares did not reach double digits, with Germany in second place hosting 7.6% of web threats, followed by China with 5.9%. Conversely, the countries that found themselves on the receiving end of web threat attack attempts the most often were Japan (12.5%), Russia (10.6%), and Peru (4.4%).

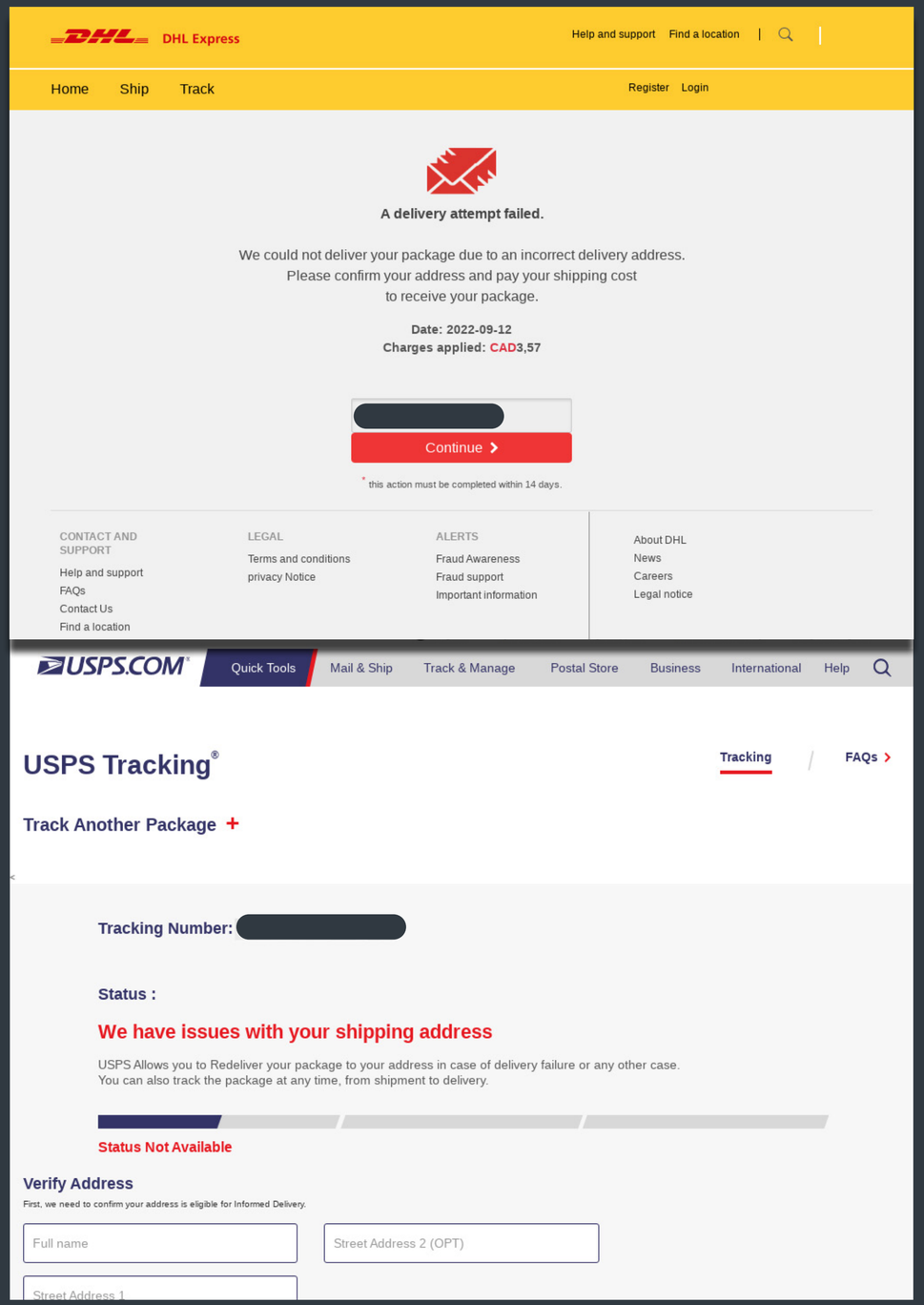



Top 10 phishing website categories in T2 2022 by number of unique URLs

ESET phishing feeds show that the Finance category remained the go-to sector when it comes to phishing websites, making up almost a third of the recorded unique phishing URLs in T2 2022[1]. It was followed by the Social media category, which in turn took up one-fourth of detections. That comes as no surprise considering that, according to our data, Facebook was the most impersonated among companies and services. Starting in 2021 and culminating at the beginning of T2 2022, Facebook and Messenger were used as lures in a *large-scale phishing operation* [60] that generated its operators significant advertising revenue.

Of note is also the sixfold increase in detections that catapulted the Shipping category into third place among phishing categories, where it now resides with 13.1%. This category was mostly represented by fake DHL and USPS requests to verify shipping addresses.

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




Phishing websites impersonating DHL and USPS and claiming issues with shipping addresses

Though cryptocurrency-themed lures accounted for basically the same percentage of phishing websites as in T1, their actual numbers almost doubled. This is an interesting development at a time when cryptocurrency exchange rates are plummeting. Notably, the increase in these websites is happening alongside the rising number of cryptostealers and in-browser coinminers caused by criminals turning to stealing cryptocurrencies instead of mining them (for more details, see the *Cryptocurrency threats* section.

After being reduced by almost half in T1, the number of homoglyph blocks remained practically the same in T2. Hotmail remained the most impersonated service, while T1's second-most targeted, Eastman Credit Union, disappeared from our telemetry completely in T2.

The list of the 10 most targeted services and domains featured two newcomers: the first was a domain that impersonated the Canadian internet-only bank Tangerine at tạngerlne[.]com – note the a changed into ạ and i written as l; the other targeted the global finance group ING using the domain ingdirẹct[.]com, switching e to ẹ. Both of them were inaccessible at the time of writing.


Top 10 brands and domain names targeted with homoglyph attacks in T2 2022

# EMAIL THREATS

*Emotet's weaponized Office file attachments again doubled their proportion of detections. Outlook was the brand most abused by phishers in T2 2022.*

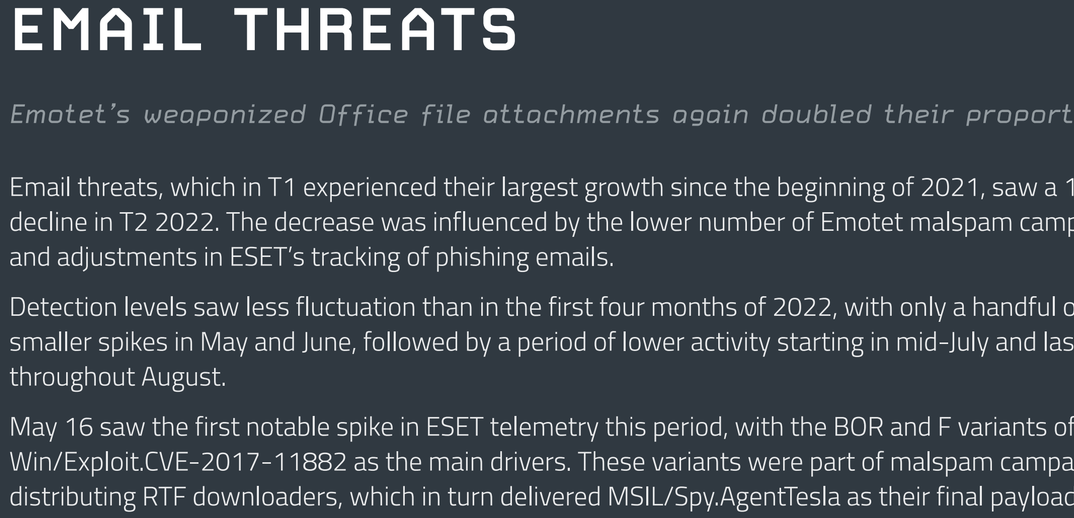
Email threats, which in T1 experienced their largest growth since the beginning of 2021, saw a 10% decline in T2 2022. The decrease was influenced by the lower number of Emotet malspam campaigns and adjustments in ESET's tracking of phishing emails.

Detection levels saw less fluctuation than in the first four months of 2022, with only a handful of smaller spikes in May and June, followed by a period of lower activity starting in mid-July and lasting throughout August.

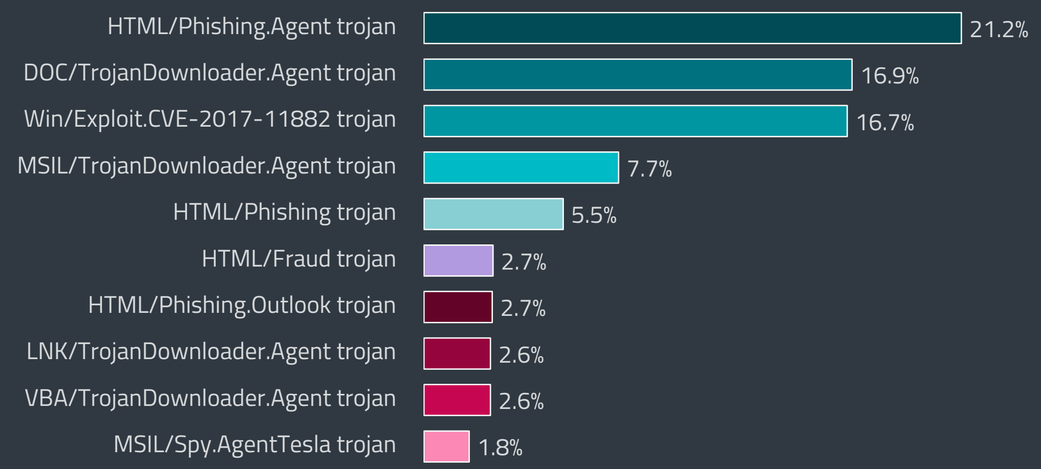
May 16 saw the first notable spike in ESET telemetry this period, with the BOR and F variants of Win/Exploit.CVE-2017-11882 as the main drivers. These variants were part of malspam campaigns distributing RTF downloaders, which in turn delivered MSIL/Spy.AgentTesla as their final payloads.

The recipients of these emails were typically lured into opening attachments that appeared to be DOC files containing a jumble of characters. To hide the malicious nature of the documents, attackers masked them as invoices or purchase lists.

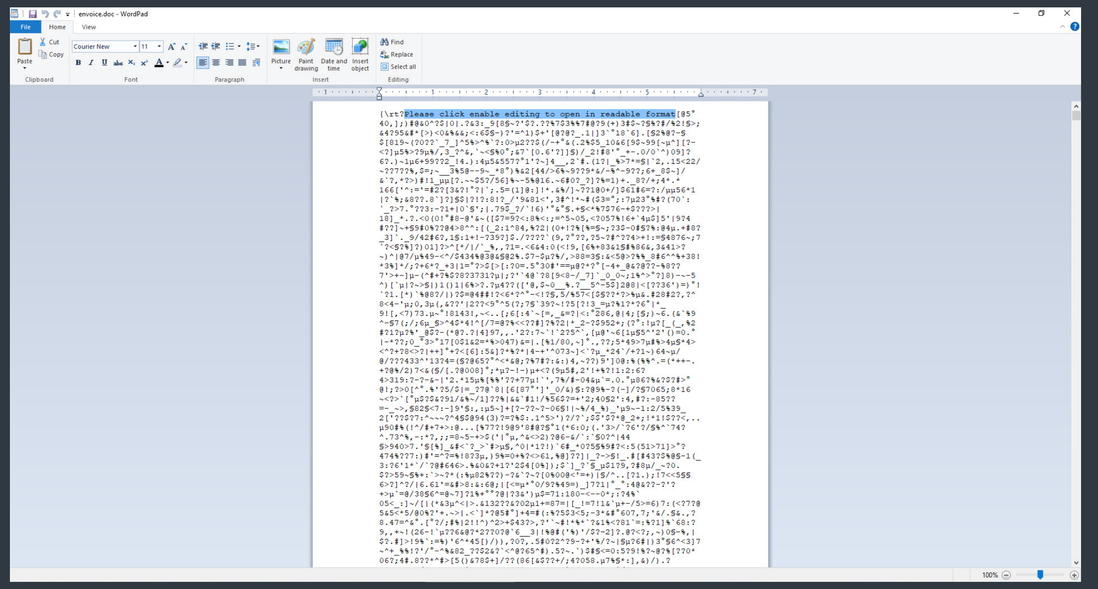
Another wave of the same campaign was seen on June 14, contributing to the largest T2 2022 uptick. However, it wasn't the only wave of malspam that wreaked havoc on that day. The Emotet botnet was flooding inboxes in Japan and Italy with messages carrying weaponized Office files – typically




Malicious email detection trend in T1 2022 – T2 2022, seven-day moving average




Top 10 threats detected in emails in T2 2022




Documents used in a malspam campaign that spread variants of MSIL/Spy.AgentTesla

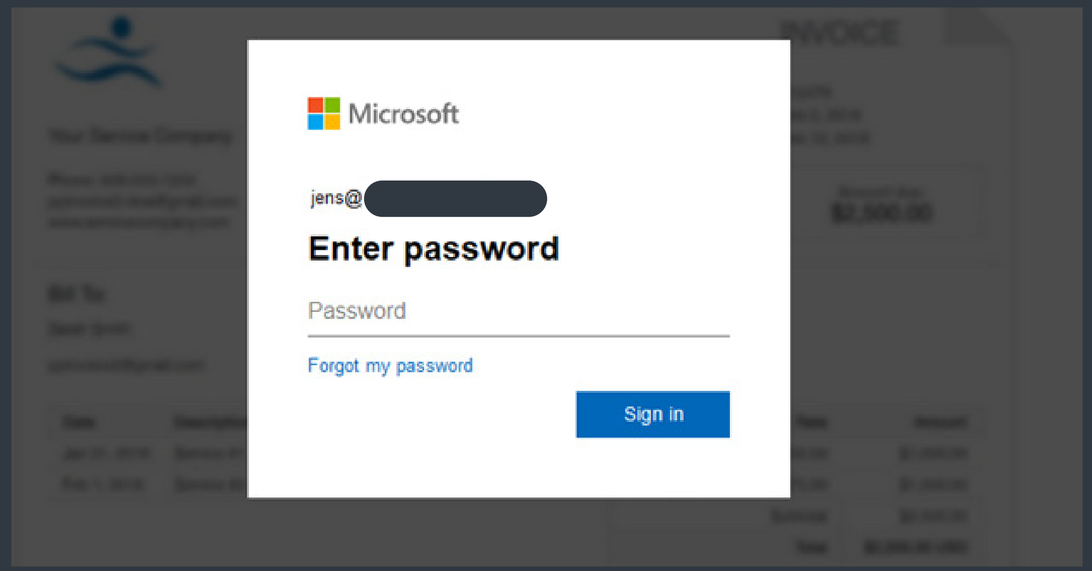
Microsoft Excel spreadsheets – triggering the DOC/TrojanDownlader.Agent.EAR and .DOV detections. The latter also contributed to spikes in the detection trend on June 22 and July 7.

Among the top 10 Email threats, HTML/Phishing.Agent kept its lead with 21%. Its overall numbers declined by 20% between T1 and T2, partially due to an adjustment in ESET telemetry that separated it from emails spreading fraudulent pharmaceutical offers.

The second most prevalent threat, DOC/TrojanDownloader.Agent triggered by Emotet campaigns, also saw a drop of 31%, diminishing its share in the T2 Email threats category to 17%. With this botnet shifting away from VBA macros, VBA/TrojanDownloader.Agent detections are slowly but surely sliding down the top 10, descending from the leading position to ninth place in just one year.

A noteworthy addition to the top 10 was HTML/Phishing.Outlook – a threat that tries to lure its victims to open an HTML file attached to an email, presenting them with a fake Outlook login page and attempting to steal their passwords. Its numbers were already growing in T1, and it further increased its share by 54% in T2, moving up from eleventh to seventh place. Countries that faced the biggest portion of these attacks were the United Kingdom and New Zealand.

While keeping similar detection levels as in T1, Microsoft became the number two among abused brands, being used to target victims in the United States and in the UK. HTML/Phishing.DHL emails, which were wildly popular during the 2020 and 2021 pandemic lockdowns, declined by 55% between T1 and T2 2022, descending to the third position among branded phishing threats.




Example of a fake login form displayed by HTML/Phishing.Outlook

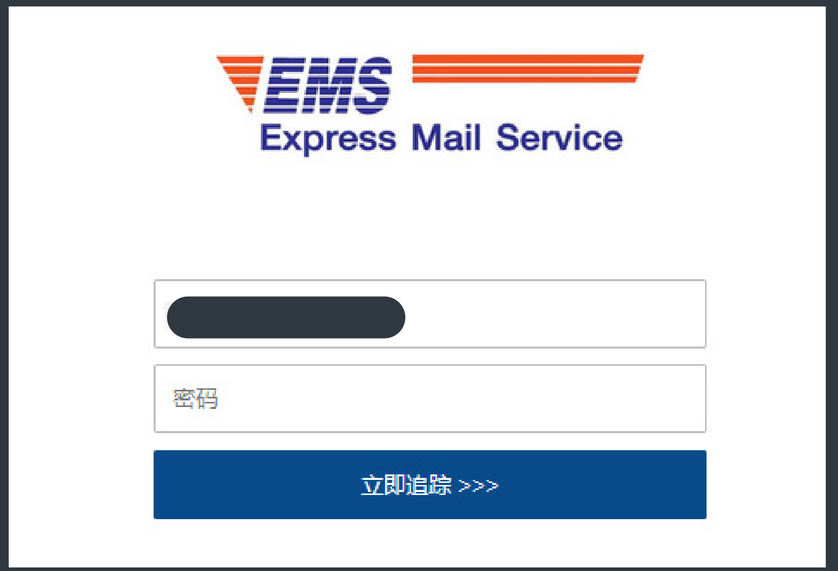
## EXPERT COMMENT

The phishing forms found in HTML/Phishing.Outlook email attachments typically come pre-filled with email addresses, probably in an attempt to appear more trustworthy. This might make the targeted user more likely to insert the rest of the requested information, thus making the operation more effective for the phishers.

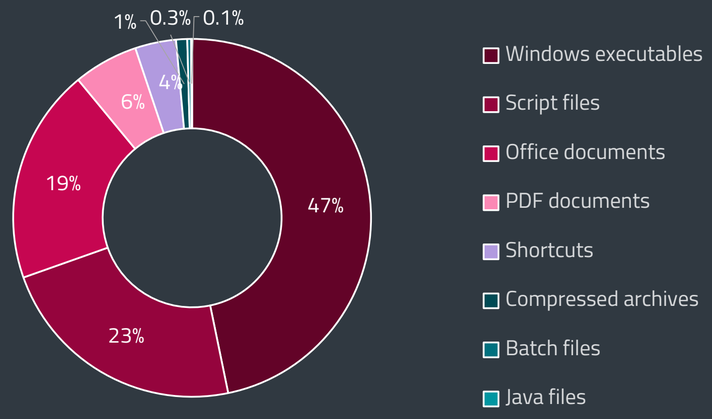
**Jiří Kropáč, ESET Director of Threat Detection**

The organization whose logo and name saw the biggest jump in abuse between T1 and T2 2022 was Express Mail Service (or EMS). Moving up from fourteenth place to sixth, its detections were 33 times more prevalent than in the previous four months, with most of its targets in the Asia-Pacific region.

Being generic in the subject line presumably pays off, considering that "Re:", "RE", and "Fwd:" were the highest-ranking subject lines reported by ESET telemetry in T2 2022. As for broader subject topics used, hoping to dupe victims into opening the email, the "payment" theme – including invoices, orders and purchases – outran its competition, being used in 46% of malicious emails. The "Bank message" theme was the second most prevalent, being the topic of a quarter (24.7%) of the encountered malevolent messages.



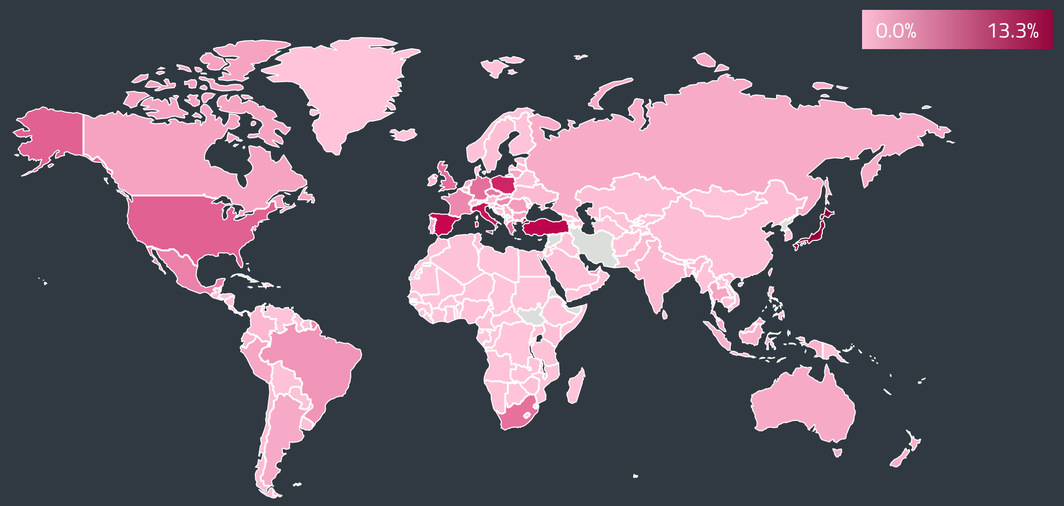

A phishing page posing as an EMS form and spread as an email attachment, detected as HTML/Phishing.EMS




Top malicious email attachment types[2] in T2 2022

As COVID-19 is becoming endemic, it apparently loses its appeal as a lure. Emails that used the disease in the subject line in T2 were only half as frequent as in T1 2022, reaching a 0.19% share – the lowest level since the beginning of 2021. Going in the opposite direction, "travel" topics were 70% more frequent in T2 than in T1, being the subject line in 1.4% of detected emails.

`EU-BusinessRegister.pdf` remained the most prevalent name of blocked attachments seen in T2, fueling the well-known subscription scam. Another popular filename among attached files – `198_Invoice_#15427.html` – might sound generic, yet is presumably effective, as it triggers the already mentioned and booming HTML/Phishing.Outlook detection.




Global distribution of Email threat detections in T2 2022

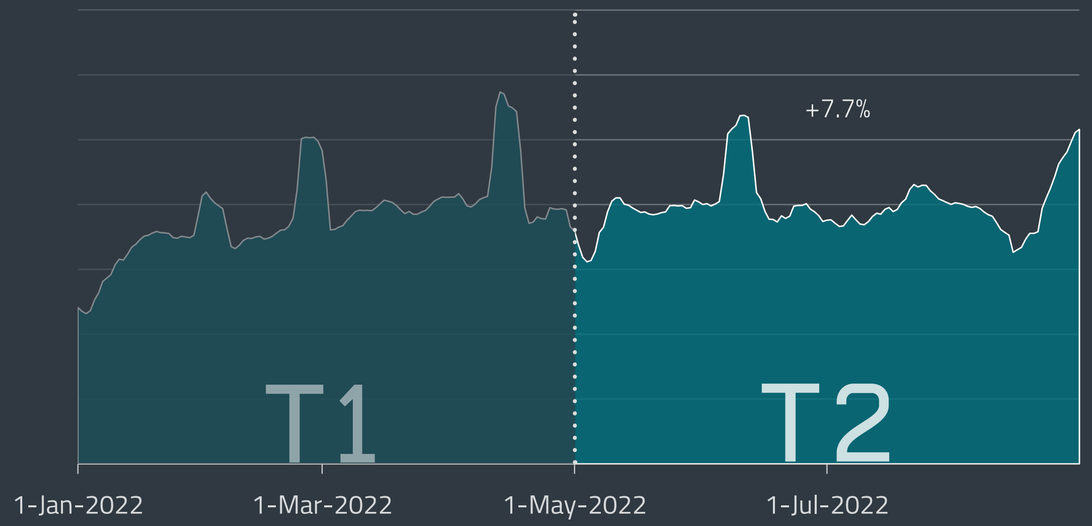
At 47%, Windows executables were the most prevalent malicious attachment type in T2 2022. Although losing eight percentage points relative to T1, this file format kept its distance from the 23% reached by the second-place contender, script files. As in T1 2022, compromised Office files almost doubled their share, going from 10% in T1 2022 to 19% in T2 2022. The reason for the uptick is identical to the previous four months, namely Emotet "promoting" Office files other than VBA-macro-containing ones to its main intrusion vector, instead of those with VBA macros.

Spam emails kept a steady upward pace between T1 and T2 2022, increasing by 8%. There were two short-lived spikes in ESET data: one around June 6, with numbers reaching approximately double the volume of a regular day, and a second one in the last days of August, probably driven by the end of the holiday season.

If the geographic distribution is considered, the top five countries remained the same, but some of them switched places. The United States remained the biggest source of spam, spewing out 20.5% of the global volume. The second most prolific spam producer was China with 14.6%, followed by Poland with 11%, France with 9.4%, and Japan with 8.8%.

Looking at the spam portion in all emails, China has the worst ratio, with 76% of sent messages falling into the unsolicited category. Singapore is second with 41.3% and Russia third with close to 30%.

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.




Spam detection trend in T1 2022 – T2 2022, seven-day moving average

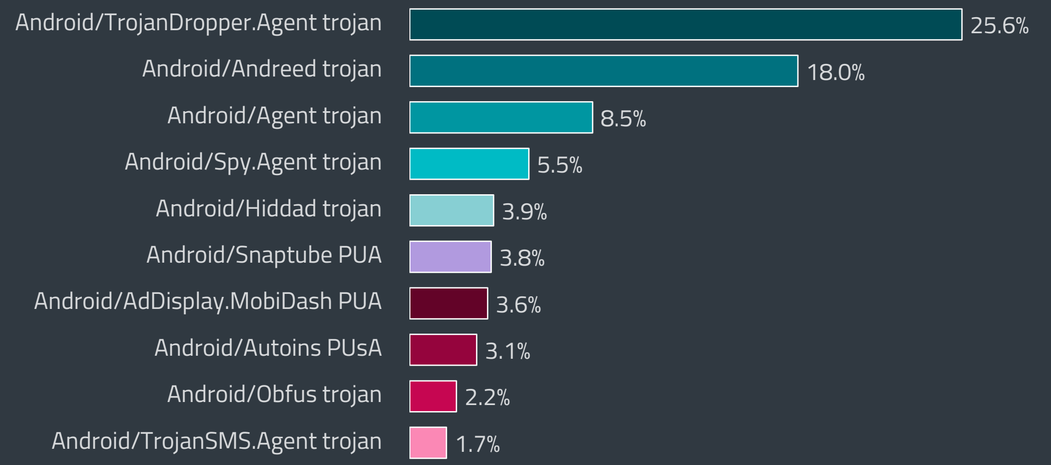
[2] The statistic is based on a selection of well-known extensions.

# ANDROID

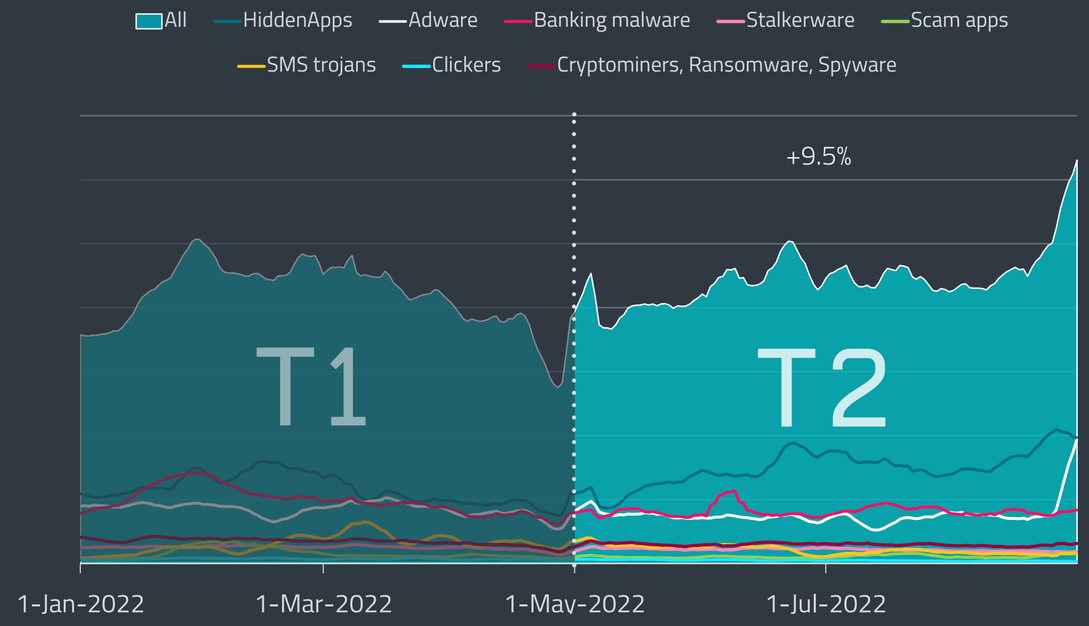
*For over a year, Android detections have continued to grow – in T2 2022 by 9.5%. The most significant growth was seen in the Spyware category.*

For 16 months now ESET telemetry has exposed continuous but leisurely growth of Android detections, most recently at 9.5% in T2 2022. The category that experienced the biggest growth was again Spyware (109%), represented by Android/Spy.Agent trojan, which is number three in the top 10 Android detection list. Compared to T1 2022, this threat has jumped four places from number seven. Malicious apps falling under this detection name have a wide range of spying capabilities including recording audio and video.

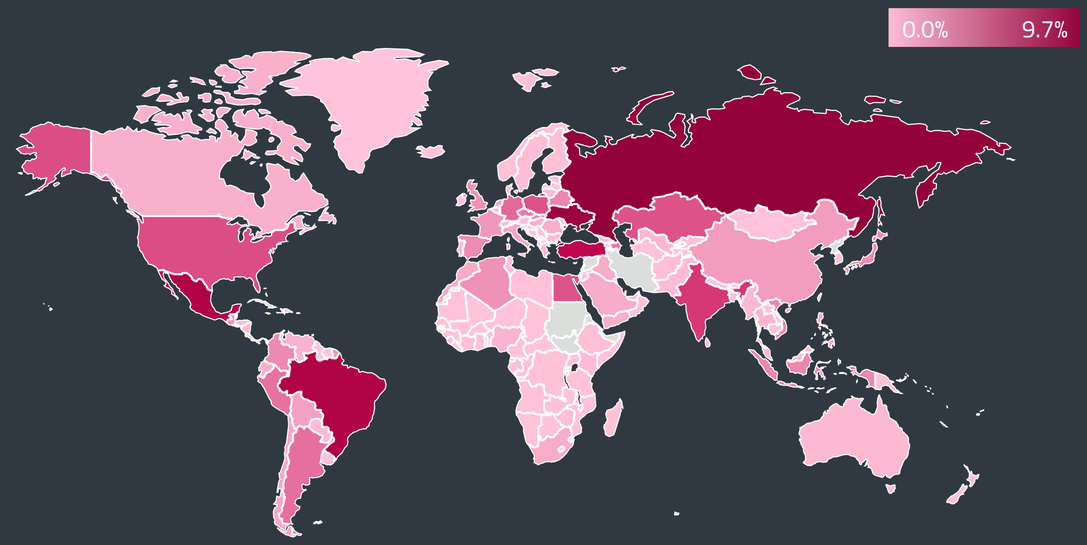
Behind a large portion of Android/Spy.Agent detections recognized in ESET telemetry is "GB WhatsApp" – a popular but cloned (and therefore unofficial) third-party version of WhatsApp with additional features. However, the cloned app is not available on Google Play; there are no security checks in place compared with the legitimate WhatsApp and versions available on various download websites are riddled with malware. WhatsApp is even *temporarily banning* [61] accounts that use such unsupported apps and if these accounts continue to use them, they are permanently banned from accessing WhatsApp. Most of these detections in T2 were seen in Egypt, Brazil, India, and Peru.




Top 10 Android detections in T2 2022 (% of Android detections)




Detection trends of selected Android detection categories in T1 2022 – T2 2022, seven-day moving average




Global distribution of Android detections in T2 2022

## EXPERT COMMENT

Behind the growth of Spyware are mainly easy-to-access, off-the-shelf Android spyware kits available on various online forums. In many cases, amateur attackers can find working and reliable remote access trojans (RATs) online for free. In comparison, the successful deployment of other types of Android malware, such as banking malware, requires at least some level of technical skill.

**Lukáš Štefanko, ESET Malware Researcher**

Another Spyware variant, detected by ESET as Android/Spy.Facestealer trojan, was spotted on Google Play by *Trend Micro* [62]. Facestealer disguises itself as various useful applications and changes its code frequently, therefore it repeatedly manages to enter the digital marketplace. In its beginnings, the spyware would steal people's Facebook login credentials (hence the name); however, currently, it can also exfiltrate various other user credentials and even private keys to cryptocurrency wallets.

The *macOS and iOS* section mentions vulnerabilities in iOS that have been exploited by commercial surveillance companies. *Google's Threat Analysis Group* [63] revealed that it found commercial surveillance software developer Cytrox packaging exploits for several zero-day vulnerabilities, with one of them affecting Android. High-profile and carefully chosen victims are first served with the Alien trojan, which then loads the Predator spyware onto their Android devices to exfiltrate their data and spy on their activities. Google claims that Cytrox sold these zero-day attacks to various government-backed threat actors.

Even with this growth, Spyware didn't come close to reaching the detection numbers of HiddenApps – deceptive apps that hide their own icons, then stealthily display ads – or Adware. HiddenApps also experienced growth in T2 2022, increasing by 32.4%. In the top 10, this category is represented by Android/Hiddad in fifth place.

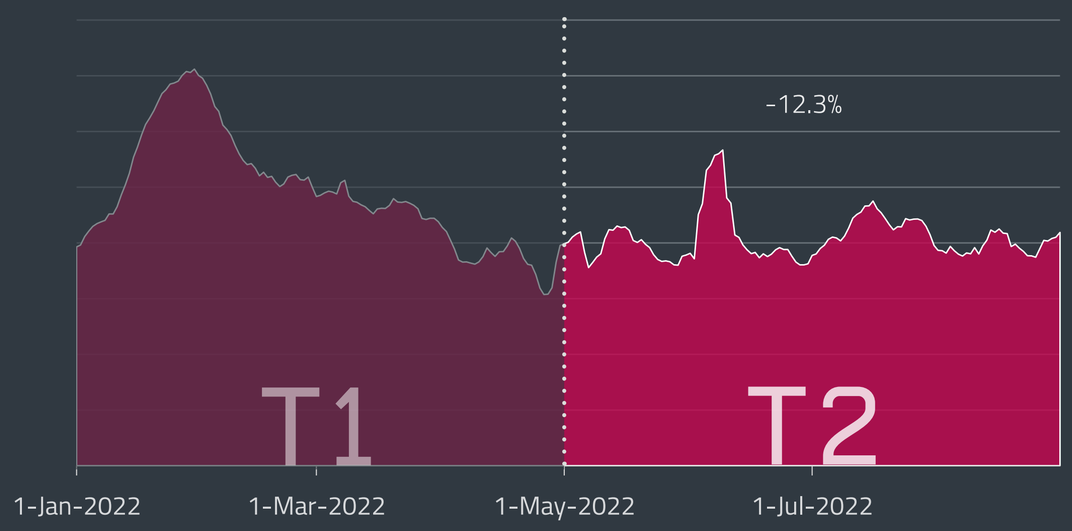
As is visible in the trend chart, Adware detections saw a steep increase towards the end of T2 2022, even though the category experienced a mild overall decline of 4.2%. In terms of functionality, Adware is similar to HiddenApps, but typically doesn't have the stealthy features made to avoid discovery on the affected device. Behind the growth of this category towards the end of T2 was Android/AdDisplay.Fyben PUA. This detection covers modded apps – reworked copies of original apps – that have malicious code injected into the `com.android.app.Activity` package, which is responsible for the display of unwanted ads. For obvious reasons, these apps are not available on Google Play.

Even though the official versions of these apps are available in official stores, some people still resort to downloading modded versions from unofficial download sites. One reason is that the desired app is not compatible with the device that the person is currently using and modded apps are sometimes recompiled to work even on device models that the original does not support. Another reason is that the developer has not made the app available in certain regions. Due to sanctions following Russia's invasion of Ukraine, people in Russia and Belarus can *no longer download or update* [64] paid apps from Google Play. Sanctions also mean that developers from those countries can no longer place their paid apps on the platform.

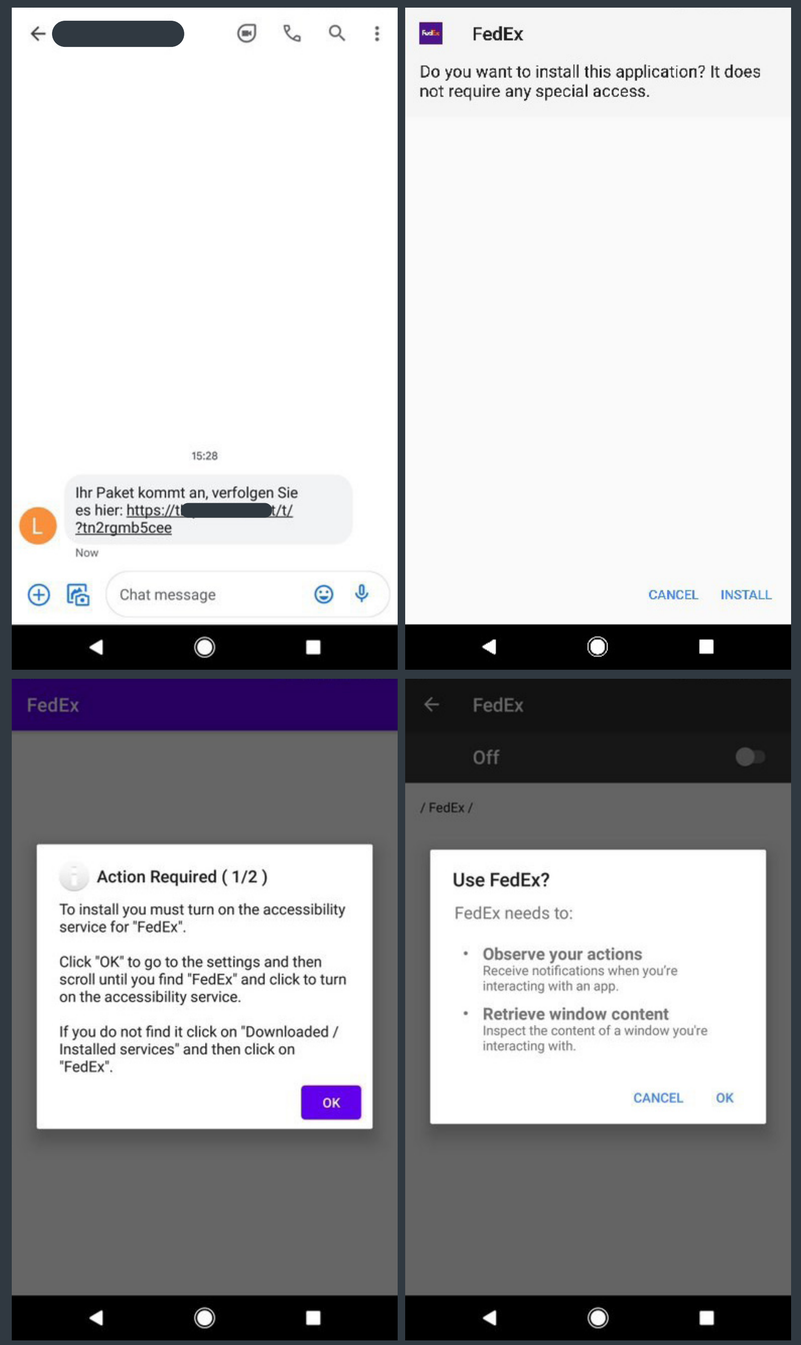
In Russia, this has led to the launch of NashStore (meaning Our Store), which offers apps for the owners of Android devices in Russia, Kazakhstan, Belarus, Kyrgyzstan, and Armenia. The above-mentioned reasons may explain why ESET telemetry saw most Android/AdDisplay.Fyben PUA detections in Ukraine, Mexico, Russia, Turkey, and Poland.

All of the other Android detection categories monitored by ESET experienced a decline in T2 2022 – Ransomware decreased by 8%, Stalkerware by 10%, Clickers by 30%, SMS Trojans by 32%, and Cryptominers by 48.5%.

Even banking malware saw a decrease of 17%; this category had experienced relatively steady and sometimes very strong growth in the past, with the exception of T3 2021. Ultimately, this decrease has put the T2 Android banking malware detections on a similar level as they were at the end of 2021. The global *law enforcement takedown* [65] of the notorious *FluBot Android banking malware* [66] is partially behind the decrease in detection numbers in this category. ESET detects this threat as several variants of the Android/TrojanDropper.Agent trojan.




Android Banking malware detection trend in T1 2022 – T2 2022, seven-day moving average

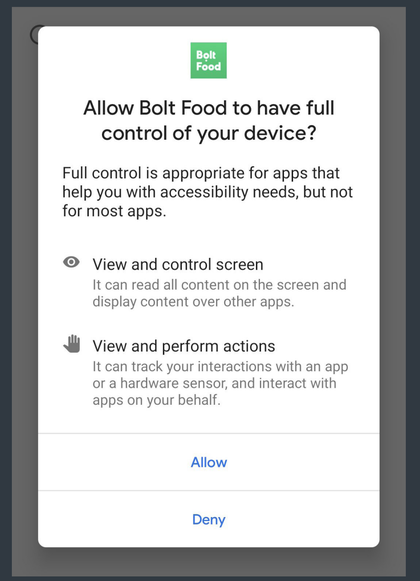



One of many FluBot examples detected by ESET: this one was spreading in Germany and impersonating the FedEx app

The FluBot banking malware had been wreaking havoc in many European countries and in the US, attacking the customers of various banks and aggressively spreading through SMS. Its infrastructure was successfully disrupted in May by the Dutch Police and the investigators are now trying to identify the individuals behind this Android threat. Even with this takedown, ESET still detects many unrelated Android banking malware variants that can exfiltrate online banking credentials and immediately access the victim's finances. Vigilance is therefore always necessary.

In Poland, *ESET researchers detected* [67] new Android banking malware called ERMAC 2.0; it impersonates the popular food delivery app Bolt Food. Since March 2022, the ERMAC 2.0 banking trojan has been available for rent on underground forums for USD 5,000 a month and its purpose is to steal victims' credentials for various financial and cryptocurrency apps. The list of targeted apps is received from the attacker's C&C server and is based on the apps installed on the device. ESET detects this threat as a variant of Android/TrojanDropper.Agent trojan, which has been number one on the top 10 Android detection list not only in T2 2022 but also during the last 12 months.

*Cleafy* [68] found newer versions of the SOVA (owl in Russian) Android banking malware with the functionality to intercept multifactor authentication codes. Additionally, this trojan served as a base for another Android banking trojan described by *F5 Labs* [69] that they named MaliBot. Both of these Android banking trojans are detected by ESET as different variants of Android/TrojanDropper.Agent. *Trend Micro* [70] also detected several apps on Google Play that, after installing, download additional banking malware onto the compromised Android device. As such, ESET detects these malicious apps as variants of Android/TrojanDownloader.Agent.



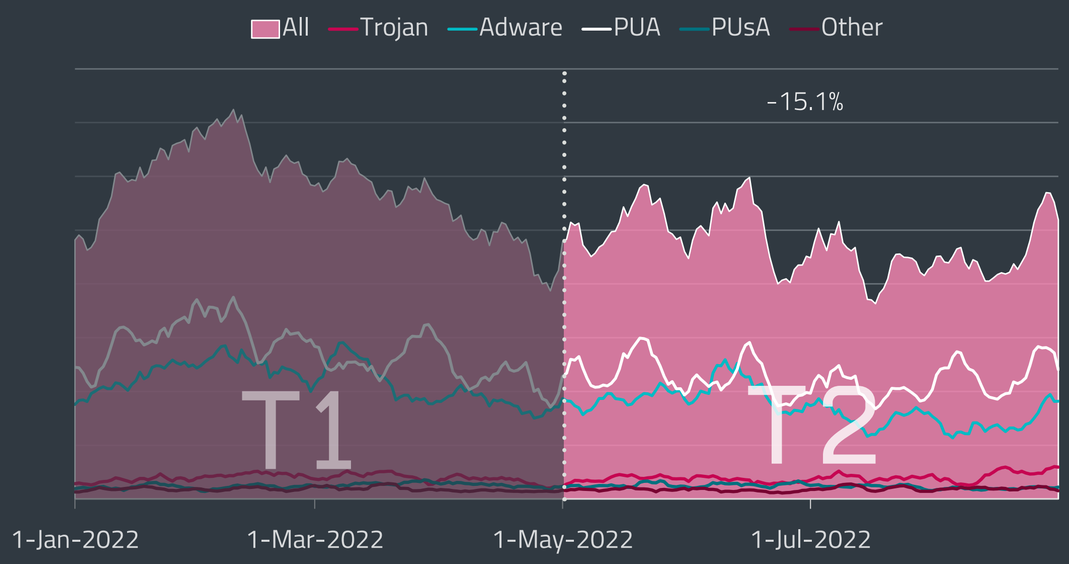

ERMAC 2.0 impersonating the popular food delivery app Bolt Food

# macOS AND iOS

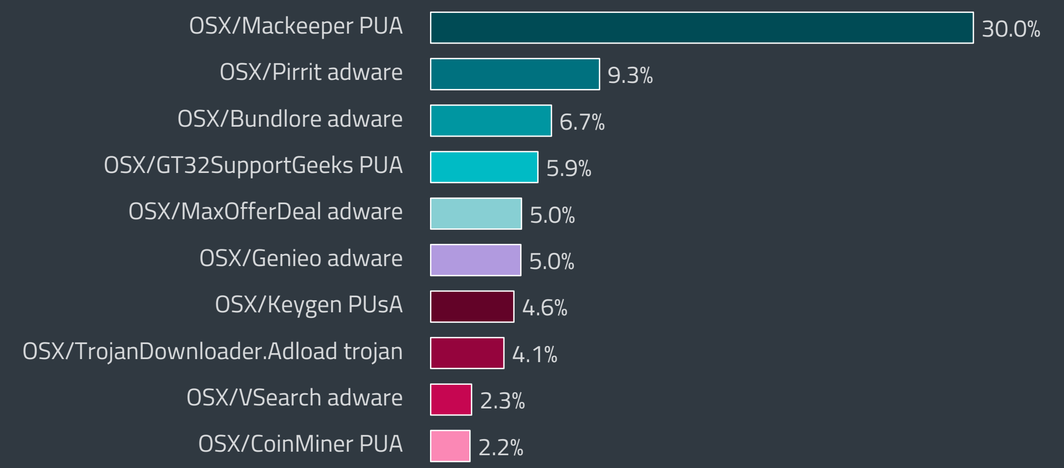
*macOS detections continued to decline throughout T2 2022, with the Adware category losing one-fifth of its detection numbers.*

In T2 2022, macOS detections saw a decline of 15.1%, with the Adware category experiencing the largest decrease in detection numbers (20.3%). This type of detection covers programs that display unsolicited ads, and is represented in the top 10 macOS detection list by OSX/Pirrit, OSX/Bundlore, OSX/MaxOfferDeal, OSX/Genieo, and OSX/VSearch. All of these adware families saw decreasing numbers of detections, with the exception of OSX/MaxOfferDeal – compared to T1 its detections increased by 30% in T2. OSX/MaxOfferDeal displays unwanted online ads and redirects users to websites that can be riddled with malicious links; ESET products detected it in T2 mainly in the United States and France.

Even though their numbers also declined (by 15.7%), Potentially Unwanted Applications (PUAs) continued to be the most widespread type of macOS detection. In T2 2022, PUAs accounted for 44% of all macOS detections and were represented in the top 10 by OSX/Mackeeper, which has the potential to mislead users into unnecessary purchases, OSX/GT32SupportGeeks, which is often presented as a macOS performance scanner reporting alleged issues, and OSX/Coinminer, which uses the system's resources to mine digital currency.




macOS detection trend in T1 2022 – T2 2022, seven-day moving average

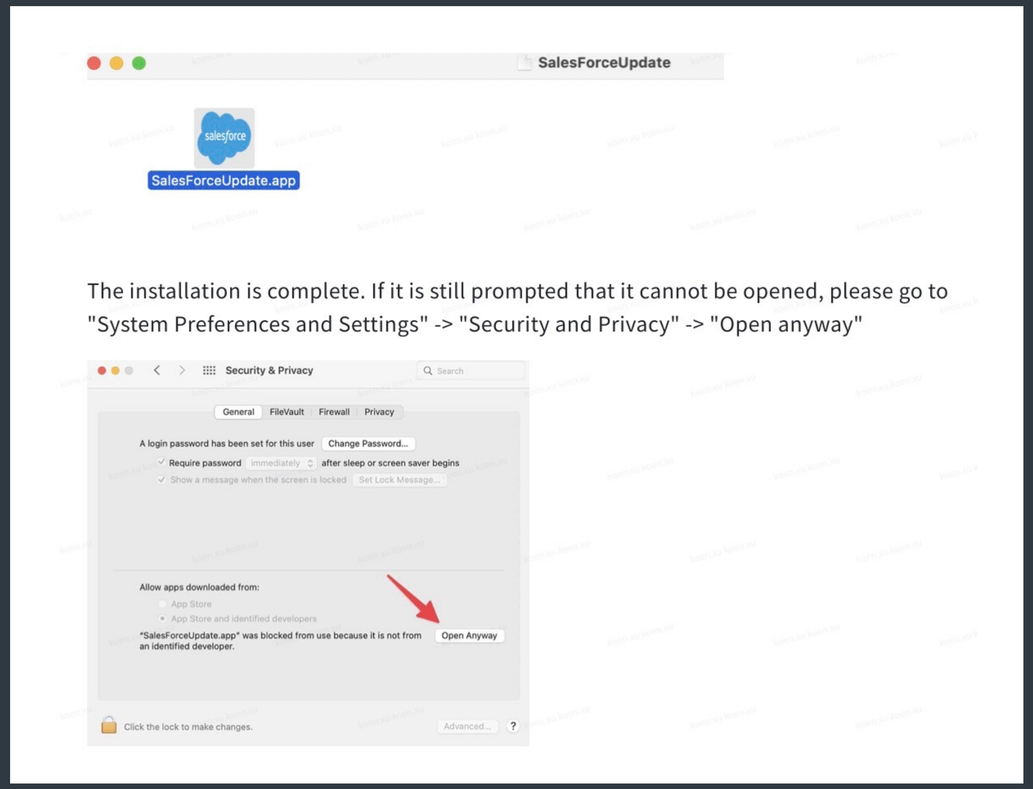



Top 10 macOS detections in T2 2022

Potentially Unsafe Applications (PUsAs) also declined by just a smidge (-1.2%) and the only category that experienced a very minor increase in numbers was Trojans (2.6%), represented by OSX/TrojanDownloader.Adload, which is currently number eight on the top 10 macOS detection list.

In July, *ESET researchers* [14] warned about a new campaign using a fake update of the Salesforce customer relationship management (CRM) software. Its goal was to deploy the *Sliver* [71] malware to macOS and Windows systems. The macOS compromise chain is very similar to a COVID-19-themed campaign previously documented by *SentinelOne* [13]; however, this newer campaign didn't include the "covid" malware and only installed the Sliver implant, which has sufficient functionality to deploy additional malware if needed. The download page included a link to a PDF document that contains instructions on how to install the file – one of the instructions basically guides the victim into disabling macOS security features. ESET products detect this threat as variants of the aforementioned OSX/TrojanDownloader.Adload trojan.

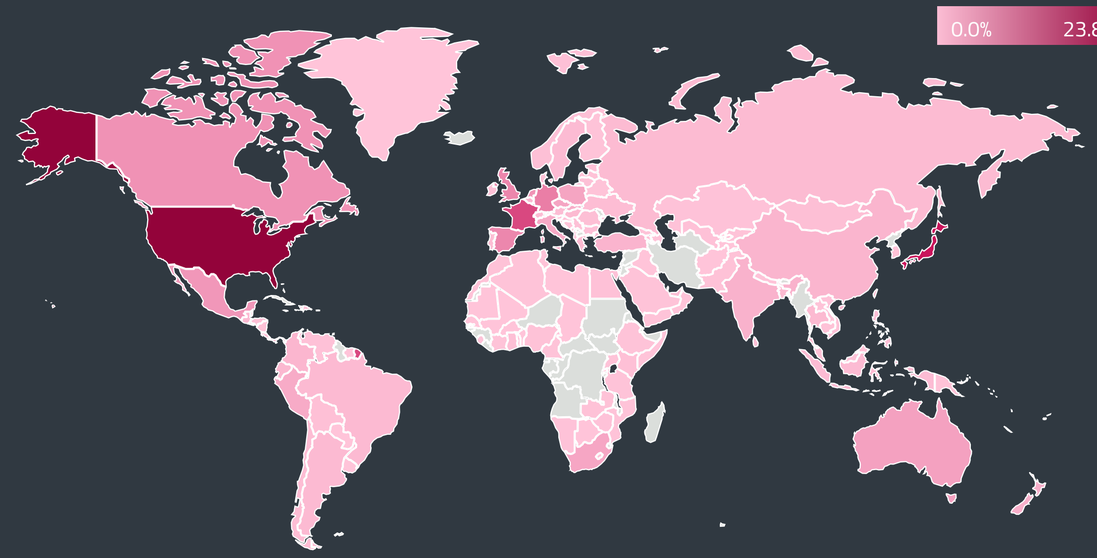
ESET telemetry registered the most macOS detections in T2 2022 in the United States (23.8%), Japan (11%), France (7.8%), Germany (4.4), and the United Kingdom (3.9%). The macOS detection numbers in all of these countries saw decreasing numbers, with the United Kingdom experiencing the biggest drop among this group, by 38.5%.




PDF document navigating the victim into disabling macOS security features

Even though the overall macOS detection numbers are decreasing, ESET researchers continue to discover new threats to the users of this platform being deployed by various APT groups. As described in the *Featured story*, ESET researchers discovered a previously unknown macOS backdoor, which they dubbed *CloudMensis* [6], that spies on users of macOS systems and exclusively uses public cloud storage services to communicate back and forth with its operators. The limited distribution of OSX/CloudMensis.A suggested to the researchers that it is used as part of a targeted operation. Later on, this hypothesis was corroborated – ESET researchers were able to attribute CloudMensis to the ScarCruft APT group.

In previous issues, the ESET Threat Report has extensively covered the topic of Pegasus, the commercial phone hacking tool developed by the NSO Group. In T2 it *was revealed* [72] that the tool was used by at least five member states of the European Union. And to show that it is not the only commercial-grade spyware targeting high-profile individuals, Google's *Threat Analysis Group (TAG)* [73] informed the public about the iOS version of another commercial-grade spyware called Hermit, spying on users in Italy and Kazakhstan.




Global distribution of macOS detections in T2 2022

To address the security issues related to iOS spyware, such as Pegasus and Hermit, Apple included a new security feature in iOS 16, which was released in September 2022. The feature is called Lockdown Mode: it limits certain functions of the iPhone and some of its apps that can be vulnerable to an attack. For instance, it blocks attachments in messages (except for pictures), FaceTime calls if the iPhone has not called that contact before, incoming invitations, configuration profiles, and wired connections to a computer or an accessory. This function also blocks attempts to enroll the iPhone into mobile device management software. Lockdown Mode will also be part of macOS Ventura scheduled to be released in October. According to ESET researchers, protecting against the aforementioned CloudMensis malware may be one of the reasons some users would want to enable this additional feature on their Apple devices. Another new security feature of iOS 16 is that security updates no longer require a full iOS update and can be installed automatically: this option has to be enabled manually via Settings → General → Software Update.

Vulnerabilities tied to Pegasus are, however, not the only ones that Apple device owners should be concerned about. In August, Apple released patches for two new zero-day vulnerabilities (*CVE-2022-32893* [74] and *CVE-2022-32894* [75]) that *may have been actively exploited* [76], according to Apple. The first vulnerability was found in Apple's WebKit (HTML rendering software) and allows a malicious website to trick iPhones, iPads, and Macs into running unauthorized software. The second vulnerability then allows the attacker, who has already exploited the WebKit vulnerability, to gain control of the operating system kernel, which would allow the attacker to take over control of the whole device. An update is therefore highly advised.

# IoT SECURITY

*While zombie botnet Mozi started losing steam, other Mirai-based botnets used T2 2022 to expand while updating the list of vulnerabilities they exploit.*

Is Mozi, the biggest zombie IoT botnet monitored by ESET research, finally dying? Our telemetry data suggests just that, as the number of bots dropped by 23%, falling from 500,000 compromised devices in T1 to 383,000 in T2. The number of attacks took the same downward path, plunging from 5.6 million in T1 to 4.3 million in T2, meaning an equal decline of 23%. Most of these attacks were aimed at machines in the US (30.4%).

As in the previous periods, the largest portion of the botnet was geolocated in China (53%) and India (35%). Of the approximately 94,000 targeted IPs, most were in Germany (17%), the United States (8%), and Japan (7%).

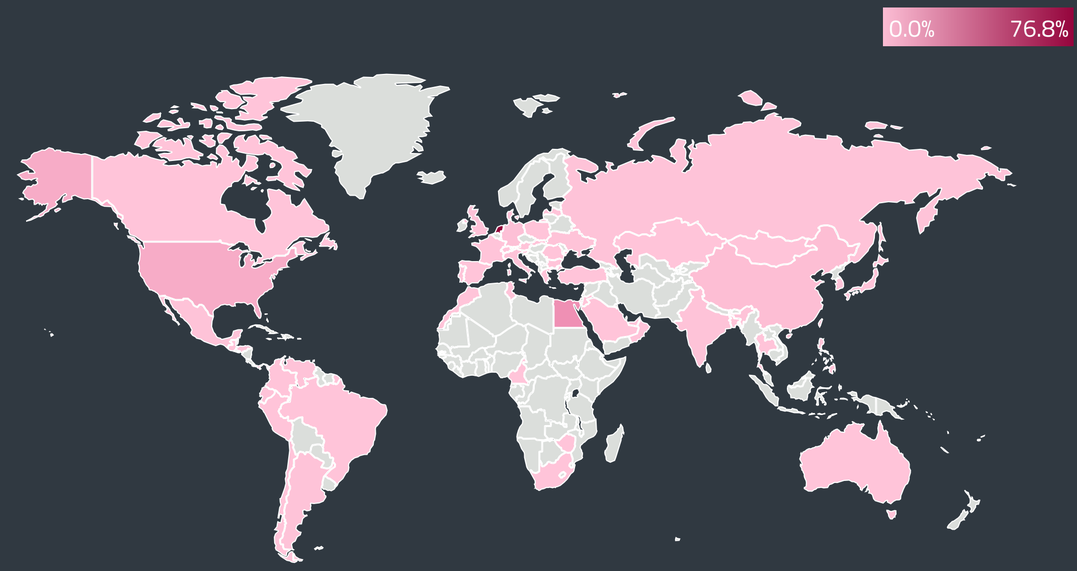
Most of these statistics confirm the assumption that the Mozi botnet is on autopilot, running without human supervision since its reputed author was ***arrested*** [77] in 2021. Subsequently, the distribution of both attacker IPs and target IPs as well as the share of individual countries have hardly changed. There was also no change in the list of vulnerabilities abused to spread Mozi malware and the share of attacks caused by each one of them.

However, that's not the case for other botnets monitored by ESET researchers, with the ZHtrap botnet being a prime example. The number and distribution of its bots have changed dramatically between T1 and T2 2022.

While the number of ZHtrap attacks dropped from 106,000 to 58,000 – taking a 45% dip – the geolocations of its bots changed massively. Almost 77% of attacks caused by this botnet in T2 2022 came from the Netherlands, an increase of 48 percentage points compared to T1. The second largest ZHtrap bot activity was seen in Egypt, growing from nonexistent in T1 to a 10% share in T2 2022, pushing the United States down to the third place with 5% (-23 percentage points).

While the operators didn't seem interested in the US as the location of their bot farm, they moved most of their *payload* servers there, growing their share to 53% in T2 versus 9% in T1. In contrast, ZHtrap shut down a large part of its payload servers in the Netherlands, its share dropping from 41% in T1 to 16% in T2.

In stark contrast to Mozi, the list of vulnerabilities used to spread ZHtrap has also changed dynamically. In T1 2022, it was spreading almost exclusively (99.5%) via the old ***CVE-2015-2051*** [78] in D-Link routers. In T2, this weakness remained the number one choice but was used in "only" 80% of attacks,

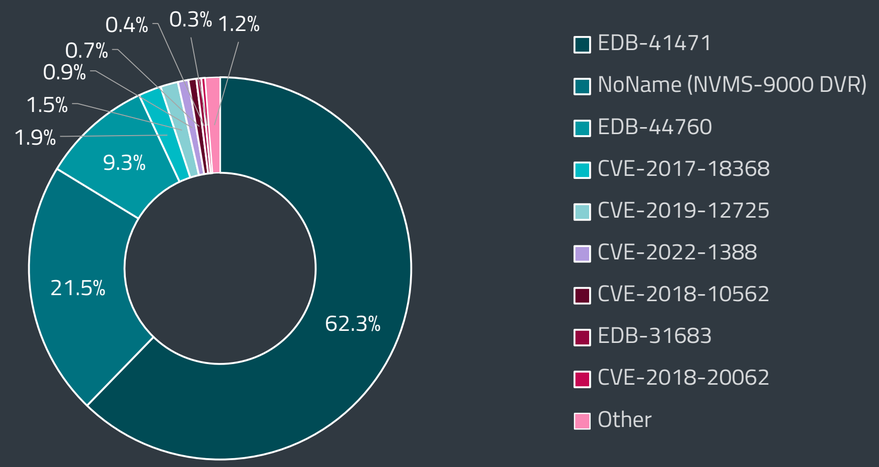



Global distribution of ZHtrap bot activity in T2 2022

followed by the ***EDB-41471*** [79] bug in MVPower DVR devices with 13%. Also, two recently reported flaws – one in Confluence servers (***CVE-2022-26134*** [80]) and another in Zyxel devices (***CVE-2022-30525*** [81]) – were at least tested by the operators as a distribution vector.

Of course, ZHtrap and Mozi aren't the only two botnets that used Mirai's leaked source code to build their own malware. Gafgyt, BotenaGo, Dofloo, and Tsunami are just a few of the most prominent names that ESET labels with one umbrella name – "Mirai-based botnets". This diverse group cumulatively accounted for 11.7 million attacks in T2 2022, a 61% increase compared to T1 2022.

What significantly influenced these figures was our recent addition of detection for attacks against a patched 2019 flaw in ***NVMS-9000 Digital Video Recorders*** [82]. Despite this vulnerability not having a CVE or EDB entry, it has become quite prevalent in T2 2022 and is now the second most "popular" attack vector, accounting for 21% of attempts caused by Mirai-based botnets.




Vulnerabilities most exploited by Mirai-based botnets in T2 2022

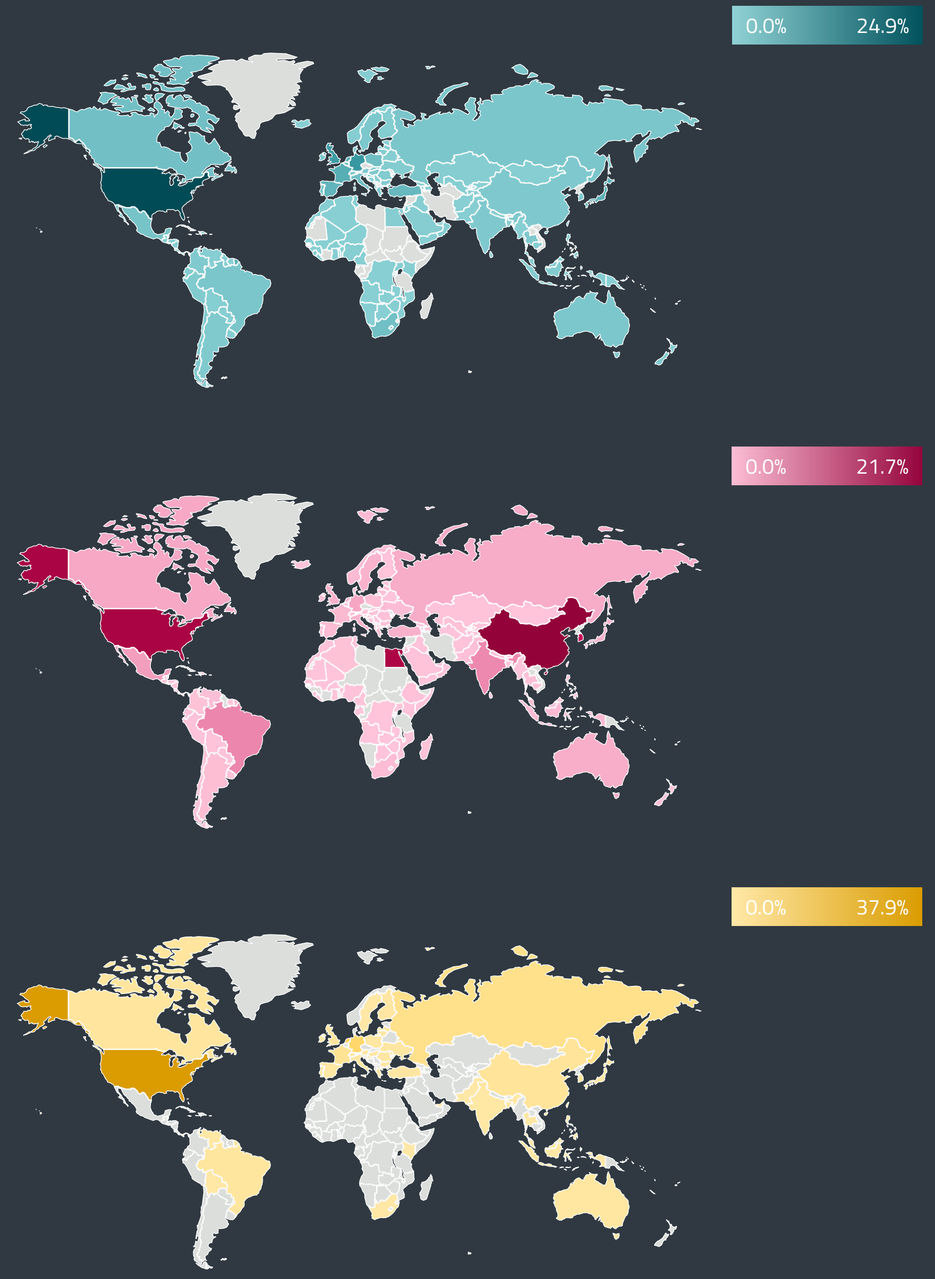
Another strong contributor to the same 11.7 million attacks was the vulnerability found in D-Link routers *EDB-44760* [83]. Between T1 and T2 2022, its detection numbers grew more than twenty-fold, making it the third most exploited flaw, with 9.3%. However, both previously mentioned vulnerabilities are still dwarfed by the *EDB-41471* [79] bug in MVPower DVR devices, which claimed a 62.3% share of the Mirai-based detection pie.

From a geographic point of view, the United States withstood 25% of attacks by the Mirai-based botnets – not counting Mozi and ZHtrap – followed by Germany with 7.1% and the United Kingdom with 6.6%. Considering only the targeted IP addresses, Germany (16%) led the pack, followed by the US (9%) and Japan (6%).

Regarding the infrastructure of Mirai-based botnets, 8% of their payload servers disappeared between T1 and T2 2022. Most of those remaining were detected in the US (38%), Netherlands (11%), and Germany (9%). As for bots, these were most prevalent in China (21%), the US (16%) and Egypt (15%).

Moving away from the botnets, the number of user-requested router scans in ESET security products fell by 17%, with the number of tested routers falling by 21%. Due to a smaller scan base, the number of devices that were using easy-to-guess passwords declined proportionately, dropping by 25%. The dip in the T2 data was probably caused by the Northern Hemisphere summer vacations and lower overall activity in July and August.

With IoT devices, even basic vulnerabilities can be a major issue, since patching them is seldom as straightforward as with computers, phones, and tablets. But when a critical CVSS 9.8 flaw hits the




Global distribution of Mirai-based attacks, bots and payload servers (from top to bottom) in T2 2022

market, threat actors don't wait long to start exploiting it. This was the case with *CVE 2022-1388* [84] found in F5 Big-IP network devices. It allowed an unauthenticated attacker to gain full control of victims' devices – and based on news stories there were a few occasions where it was even used to *wipe them* [85].

In T2 2022, ESET telemetry reported over 100,000 exploitation attempts targeting CVE 2022-1388 in F5 devices. If not blocked, the established connections would have been used to drop and run a Linux shell script that would then download a Mirai binary from a predefined list of URL links. Several Mirai-based botnets exploited this vulnerability to expand their bot network.

The last four months were rife with experiments that showed how vulnerable the IoT-powered world can become. Manufacturers including *Honda* [86], *Hyundai/Kia* [87], and *Tesla* [88] saw their products broken into by researchers, who not only gained access but started and even drove off in them.

In T2 2022, Forescout researchers also presented *proof-of-concept ransomware* [89] that can target IoT, IT, and operational technology (OT). Not exactly a new idea, as this type of threat has been *predicted for years* [90], but certainly one worth keeping in mind as more PoCs like this are being published.

In T1 2022, we mentioned the sabotage of Viasat's *KA-SAT satellite network* [91], which caused major disruptions to communications and forced the company to distribute 30,000 replacement modems. In T2, Ukraine, the European Union, and the Five Eyes nations all *attributed the incident to Russia* [92].

## EXPERT COMMENT

According to expectations, the zombie-like Mozi botnet is slowly starting to lose steam, which opens up the field to other Mirai-based botnets. And as our data shows, these are becoming increasingly powerful and widespread, experimenting with vulnerabilities both old and new, including those from popular vendors. What this means for organizations and users is that patching is of the utmost importance, especially in developed countries, which are still the main targets of most IoT threats monitored by our systems.

**Milan Fránik, ESET Malware Researcher**

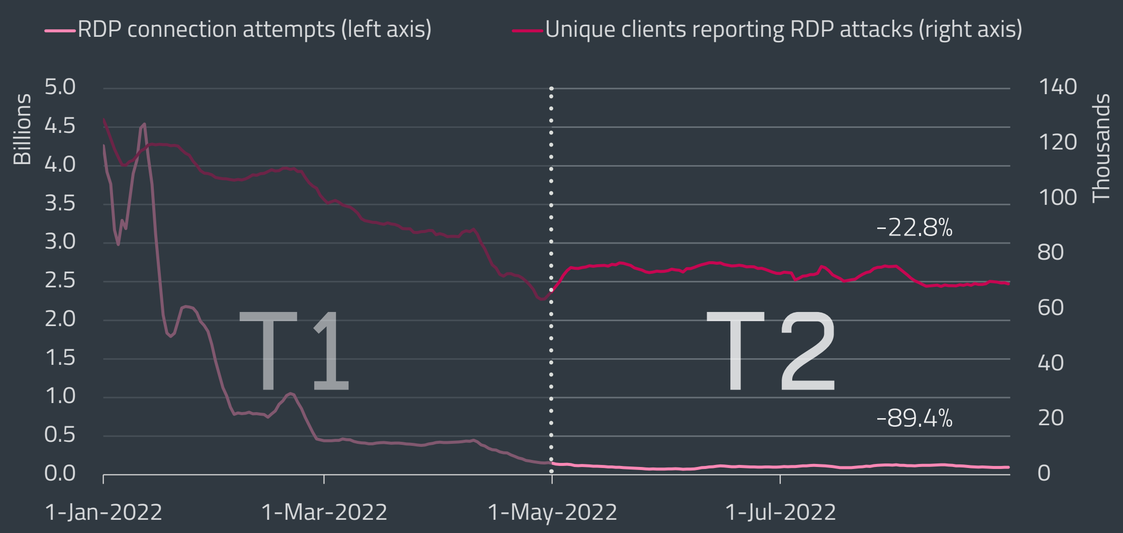
# EXPLOITS

*While attack attempts against RDP, SQL and SMB followed a downward spiral in T2 2022, new exploits like Log4Shell and Spring4Shell grew in popularity.*

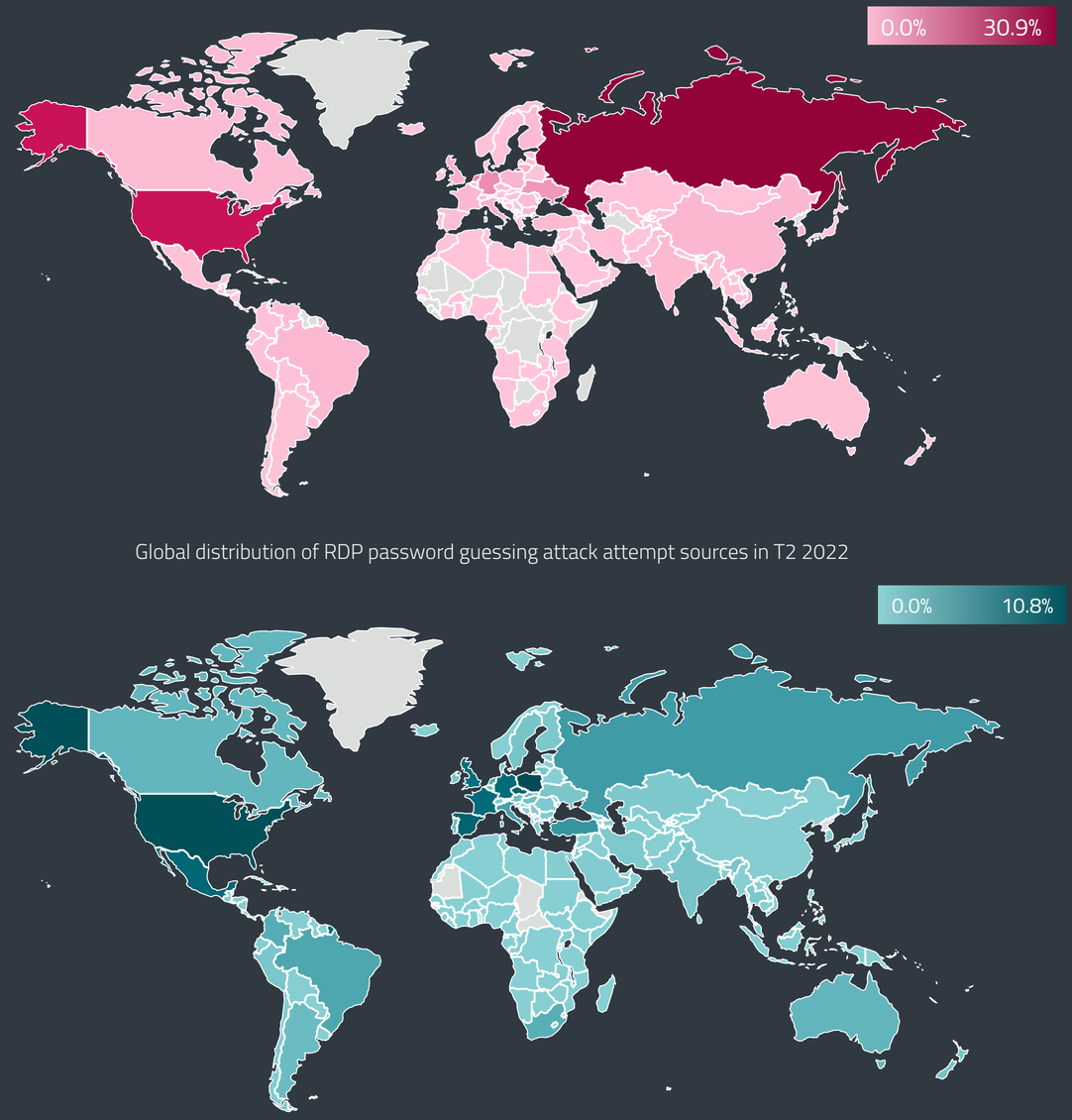
After an unprecedented drop in RDP password-guessing attacks in T1 2022, the detection trend did not recover and stayed down at levels not seen since 2020. The decrease between the two periods was still a whopping 89.4%, going from 123 billion detections to 13 billion; however, this difference was mostly caused by the high volumes of blocked attempts in the first days of January 2022. On an average day in T2 2022, 104 million RDP connection attempts were blocked compared to 1 billion in T1 2022.

The trend of unique clients reporting an RDP attack attempt declined at a much slower pace, going down by 22.8% between T1 and T2, stabilizing in May. The average number of unique clients facing an RDP attack attempt in May through August 2022 receded from 102,000 to 73,000 devices.

The reasons for the decline remain the same as in T1: less remote work, better countermeasures implemented by security and IT departments, and Russia's war with Ukraine, which seems to have impacted portions of the attacking infrastructure. Another factor that might cause further drops in RDP attacks is the ***default protection*** [93] in Windows 11 against brute-force attacks. However, its effects will probably become apparent only after more organizations have adopted the newest version of that operating system.




Trends of RDP connection attempts and number of unique clients in T1 2022 – T2 2022, seven-day moving average




Global distribution of RDP password guessing attack attempt sources in T2 2022



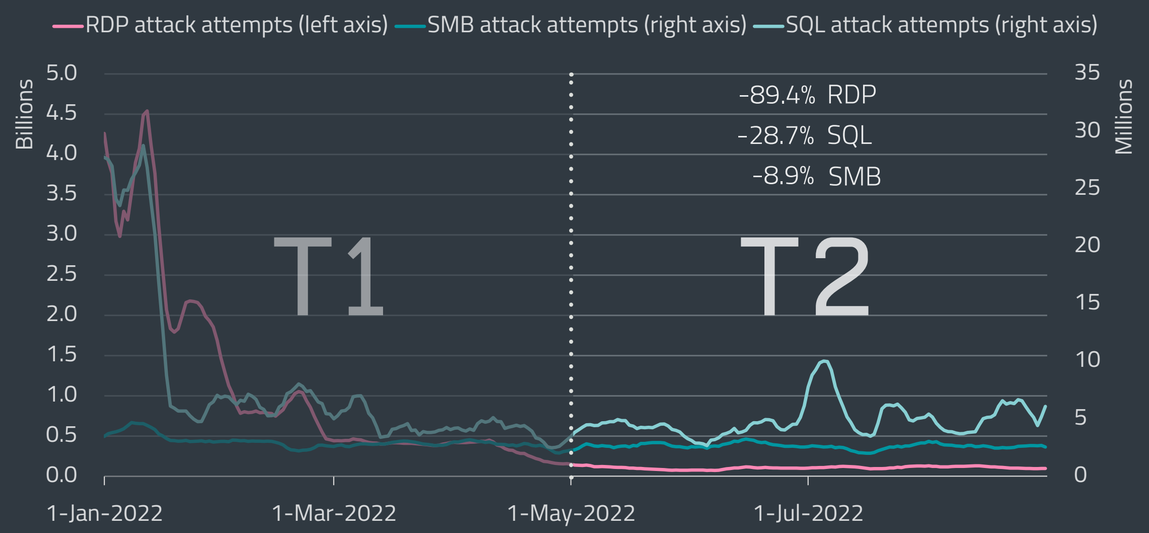

Global distribution of RDP password guessing attack attempt targets in T2 2022

From a geographical standpoint, most of the 13 billion blocked RDP attacks in T2 2022 were aimed at Poland (10.8%), the United States (10.2%), and Spain (7.3%). Keeping a distant lead, Russian IP addresses were responsible for the largest portion of the attacks (31%), followed by IPs in the US (14%) and Panama (8%). It is important to note that the use of VPNs and proxy services might influence these statistics.

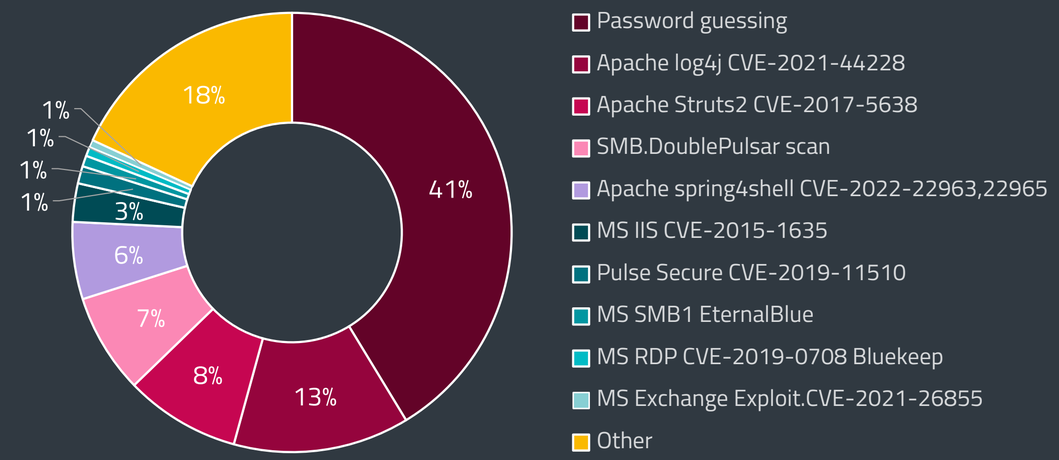
In comparison to RDP, attacks against public-facing SQL services only saw one sharp drop in January after which detection numbers found steady ground. Attack attempts declined from 859 million in T1 to 612 million in T2 2022, meaning a 29% reduction. The number of unique clients closed T2 2022 with a negligible 1.8% decline. On an average day in May through August 2022, SQL services had to withstand 4.9 million attack attempts.

Geographically, the country that saw the most attacks against SQL services in T2 was Turkey. Threat actors hit it especially hard on July 1 and July 20, causing peaks in our data that accounted for 65% and 61% of SQL attack detections on those days. The last uptick in SQL data occurred on August 31, with the United Kingdom facing 49% of SQL attacks on that day, followed by Austria with 19%.

In contrast with SQL and RDP, the trend of attacks targeting SMB services kept its balance. Blocked connection attempts went from 356 million in T1 to 324 million in T2 2022, accounting for a minor decline of only 9%. The number of unique clients reporting such incidents remained steady, losing only 0.7%. On an average day in T2 2022, ESET's brute-force attack protection blocked 2.6 million malicious SMB connection attempts.




Trends of RDP, SMB and SQL attack attempts per client in T1 2022 – T2 2022, seven-day moving average




External network intrusion vectors reported by unique clients in T2 2022

The country facing the biggest portion of the attacks aimed at SMB was Mexico with 35%, followed by France with 16% and the US with 9%.

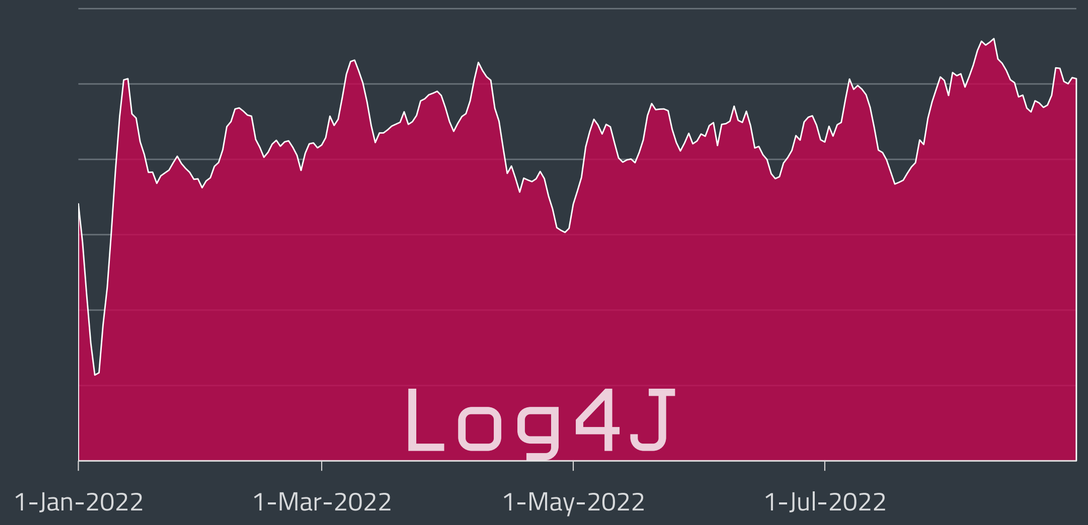
Regarding the most prevalent network intrusion vectors in T2 2022, password guessing kept its lead with 41% of the detection pie – identical to its share in T1.

The second most favored vector was the critical Log4J vulnerability, with 13%, which became increasingly popular among threat actors. T2 2022 data showed a 14% growth in exploitation attempts correlating with news reports of *ransomware gangs* [94] and sophisticated groups such as *Mercury* [95] and *Lazarus* [96] abusing the vulnerability. Despite a patch being available, it seems Log4J isn't going away anytime soon – with CISA's Cyber Safety Review Board calling it *endemic* [97].

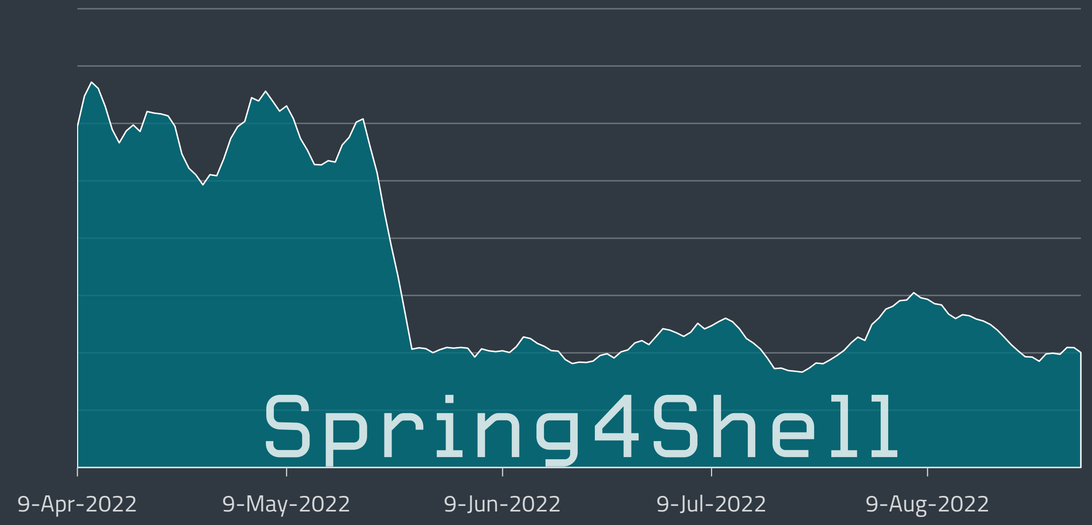
In T1 2022, another high-profile vulnerability called Spring4Shell came to light and started to gain traction. Despite having potentially less severe consequences than Log4J, it followed a similar trajectory, demonstrating the potential to become one of the top network attack vectors. After T2 2022, we can say that scenario did not materialize, at least not yet.

Spring4Shell remained fifth among the top 10 network intrusion vectors, but its share grew from 4% in T1 to 6% in T2 2022. Its overall detections in May through August also went up by 113%; however, the trendline showed a major drop of activity around May 20.

Last but not least, a new zero-day vulnerability surfaced in T2 2022. The now-patched *CVE-2022-30190* [98] – also known as Follina – affects Microsoft's Support Diagnostic Tool and enables an




Detection trend of Log4J exploitation attempts in T1 and T2 2022, seven-day moving average




Detection trend of Spring4Shell exploitation attempts in April through August 2022, seven-day moving average

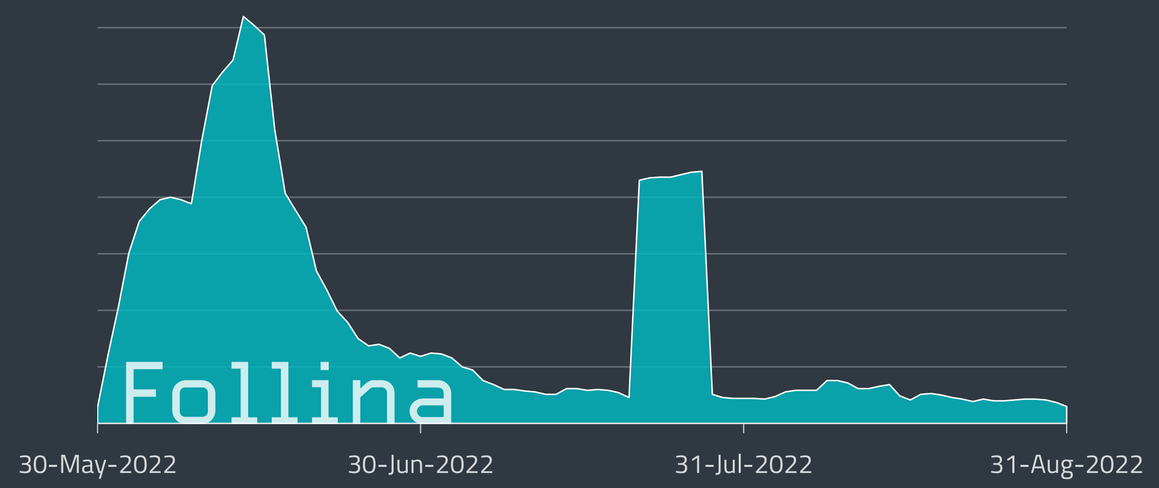
attacker to take control of a victim's device. The bug also made ***headlines*** [99] because it has been used by state-backed threat actors targeting EU and US organizations. CERT-UA even pointed its finger at ***APT28*** [100] as the possible culprit.

ESET telemetry reported hundreds of attempts to exploit Follina, demonstrated by several spikes in our detection data. The countries facing most of the attacks were Spain (20%), the US (7.5%) and the United Arab Emirates (7.3%).

## EXPERT COMMENT

A likely explanation for the sudden drop in Spring4Shell detections is that a group of threat actors tested the vulnerability as an intrusion vector and decided to drop it due to unsatisfactory performance. Another is that they decided to use a different attack avenue for the time being.

**Ladislav Janko, ESET Senior Malware Researcher**




Detection trend of attack attempts targeting the Follina vulnerability in T2 2022, seven-day moving average

# ESET RESEARCH CONTRIBUTIONS

Latest engagements and achievements of ESET Research experts

## UPCOMING PRESENTATIONS

### AVAR 2022

*Lazarus declares war on Windows system monitoring* [101]

Since late 2021, Lazarus group malware authors have been improving new malware that is able to turn off as many Windows monitoring features as possible, effectively blinding most monitoring tools, security solutions, and event logging. In their presentation, ESET senior malware researcher Peter Kálnai and ESET malware analyst Matěj Havránek will focus on the most recent version of this malicious module, discovered in summer 2022 and containing newly added blinding features. They will demonstrate how these mechanisms operate and what changes the malware makes to the system once the module is executed. For developers of security products, the contents of this session should provide the impetus to reevaluate their implementations and to increase their solutions' self-protection.

*Who's swimming in South Korean waters? Meet ScarCruft's Dolphin* [101]

ScarCruft, also known as APT37 and Reaper, is an espionage group that has been operating since at least 2012 and primarily focuses on South Korea. Last year, ScarCruft conducted a watering-hole attack on a South Korean newspaper site. This attack was previously publicly described as having the BLUELIGHT backdoor as its final payload. However, as ESET malware researcher Filip Jurčacko will explain in his presentation, ESET Research discovered a second, more sophisticated backdoor called Dolphin that was deployed on selected compromised machines via BLUELIGHT. In his talk, Jurčacko will present a technical description of the Dolphin backdoor and its capabilities, provide useful information for threat hunters looking to track ScarCruft activity, and show the evolution of multiple Dolphin versions that ESET researchers observed after their initial discovery.

*Behind the MirrorFace mask: LODEINFO malware interfering with Japanese elections* [101]

In the weeks leading up to the Japanese House of Councillors election in July 2022, the APT group that ESET researchers track as MirrorFace launched a spearphishing campaign against Japanese political entities. Once the victims opened the malicious attachments, LODEINFO malware – in use since 2019 and exclusively against Japanese entities – was executed, opening the door for the threat actor to move to the next stage of the attack. In his presentation, ESET malware researcher Dominik Breitenbacher will introduce the audience to the MirrorFace APT group, a threat actor exclusively targeting Japanese entities with the LODEINFO malware, and will then provide a detailed description of the campaign against Japanese political entities. In the process, Breitenbacher will unearth MirrorFace tactics and procedures that haven't been published in detail before. The presentation will close by describing the evolution of the LODEINFO malware over the past few years.

*SparklingElf, recent supplies to SparklingGoblin's Linux malware arsenal, new ties to APT41* [101]

ESET researchers Thibaut Passilly and Vladislav Hrčka will present the discovery of a Linux variant of SideWalk, a modular Windows backdoor belonging to the SparklingGoblin APT group, that was originally named StageClient. The researchers also discovered that the backdoor exhibits a huge functionality overlap with the Specter IoT botnet malware, a modular Linux RAT, that creates an all but indisputable link between the malware authors, meaning that these tools come from the same threat actor. During their presentation, the ESET researchers will explain the connections between StageClient and Specter, introduce the SparklingGoblin APT group to the audience, and describe the code similarities between StageClient and SideWalk. Lastly, they will describe how the Linux userland rootkit, discovered alongside StageClient, injects itself into processes and hides its files and network connections to achieve stealthiness.

### Ekoparty 2022

*Ukraine's past and present cyberwar* [102]

For the past eight years, Ukraine has been the target of enormous cyber-aggression by numerous APT groups. ESET principal malware researcher Robert Lipovsky will walk attendees through the most notable attacks, including those against the country's power grid with a special focus on the latest attempt: Industroyer2. This new version of the only malware specifically designed to trigger electricity blackouts was deployed in Ukraine amidst the ongoing Russian invasion. As in 2016 with the original Industroyer, the aim of this cyberattack was to cause a major power outage – but this time the attackers failed. Lipovsky will outline how the attack unfolded, why it was unsuccessful, and reverse engineer the samples, showing how the code evolved since the first version. The presentation will also focus on the evolution of disruptive wiper campaigns of the Sandworm APT group – from the infamous NotPetya worm, through the HermeticWiper campaign that ESET discovered on February 23, 2022, only a few hours before the invasion, and on to CaddyWiper. It will also disclose how the attackers have recently been trolling ESET.

## DELIVERED PRESENTATIONS

### BSides Montreal

*Clustering malware activity: How we do attribution* [103]

In this presentation, ESET malware researcher Alexandre Côté Cyr explained how ESET Research does attribution using technical artifacts (such as code similarity), infrastructure, TTPs, and socio-political factors like victimology. Concrete examples from previous research were showcased to illustrate how these indicators can be used, or misused, to cluster activity. The relative merits and reliability of these indicators were discussed, along with how they can be combined to arrive at a more accurate conclusion. Attendees were also presented with the pitfalls associated with each of them, with examples of how we can get it wrong. This part of the presentation also brought up other obstacles encountered when doing attribution, including the varying definitions of certain APT groups among various researchers, along with tool sharing and so-called "umbrella groups" that encapsulate multiple subgroups.

### LABSCon

*Phosphorescent Connections and Shifting Oil Reserves: Overlap in Middle Eastern Threat Actors* [104]

In his presentation, ESET senior threat intelligence analyst Adam Burgher revealed insights into recent campaigns deployed by Middle Eastern threat actors OilRig, APT35 (aka Phosphorus), and Agrius. Attendees learned about a new OilRig campaign and the group's shift in C&C methodology; a sharp APT35 pivot from public vulnerability exploitation to a low-key custom backdoor campaign that is ongoing; and an Agrius wiping campaign called Fantasy Vacation that targets the diamond industry and has ties to APT35.

### Black Hat USA 2022

*Industroyer2: Sandworm's Cyberwarfare Targets Ukraine's Power Grid Again* [105]

ESET senior malware researcher Anton Cherepanov and ESET principal researcher Robert Lipovsky provided technical details on Industroyer2, a new version of the only malware specifically designed to trigger electricity blackouts. Its latest observed variant was detected in Ukraine amidst the ongoing

war, aiming to cause a major electricity outage in a region with a population of more than two million, using components amplifying the impact. Joining the presentation was Deputy Director of Ukraine's State Service of Special Communications and Information Protection, Victor Zhora. This is the first time that a Ukrainian governmental representative has taken part in such a high-profile cybersecurity conference. The Industroyer2 attack was thwarted thanks to the swift response of Ukrainian defenders and CERT-UA. ESET Research provided the Ukrainian side with crucial analysis of this threat. In the presentation, the researchers showed data linking this attack to the notorious Sandworm APT group and discussed why and how the attack was mostly unsuccessful. On top of that, the attendees were provided with actionable advice for defenders, including log entries, EDR rules, and detection/hunting rules for Snort and YARA.

## Virus Bulletin 2022

*Lazarus & BYOVD: Evil to the Windows core* [106]

In their session, ESET malware researcher Peter Kálnai and ESET malware analyst Matěj Havránek took 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 explained these mechanisms by demonstrating how they operate and what changes they make to system monitoring once the user-mode module is executed. Our researchers also compared 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.

*Creepy things that glow in the dark: a deep look at POLONIUM's undocumented tools* [107]

POLONIUM is a threat actor that was first publicly documented in June 2022 by Microsoft researchers. While public visibility of the group's activities is very limited, ESET telemetry shows that POLONIUM has in fact been active since at least September 2021, continuously developing new tools and improving its existing ones. The presentation explained and exposed various components of POLONIUM's toolset – the findings of ESET malware researcher Matias Porolli, presented by ESET principal researcher Robert Lipovsky, show that the group uses four previously undocumented backdoors, and several in-house-developed tools, including custom keyloggers and a tool to capture snapshots from the webcam. Lipovsky also shared insights about how the group operates, its victimology, network infrastructure, the tricks that POLONIUM operators use to try to evade detection, and how they abuse cloud storage services for command and control. The presentation concluded with a showcase of possible overlaps with other APT groups.

## RSA Conference 2022

*ESPecter: Showing the Future of UEFI Threats* [108]

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, but the actors behind the ESPecter bootkit think that compromising the bootloader is the way. This session by ESET head of threat research Jean-Ian Boutin and ESET malware researcher Martin Smolár described ESET's discovery of the aforementioned ESPecter – a previously undocumented real-world UEFI bootkit persisting on the EFI System Partition (ESP). This session raised awareness of UEFI threats affecting the ESP and provided guidance and resources for defenders to help secure their pre-OS environments. Boutin and Smolár's analysis of this previously unknown, real-world UEFI ESP bootkit helped 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.

## CODE BLUE 2022 REcon 2022 SecTor 2022

*Under the hood of Wslink's multilayered virtual machine* (CODE BLUE 2022) [109]

*Under the hood of Wslink's multilayered virtual machine* (REcon 2022) [110]

*Under the hood of Wslink's multilayered virtual machine* (SecTor 2022) [111]

Wslink is a unique loader, linked to the Lazarus group, that ESET researchers discovered and documented at the end of 2021. 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 analyzed the internals of the VM and described ESET Research's semiautomated approach to seeing through the obfuscation techniques in a reasonable time. The approach was demonstrated on a few chunks of bytecode from a protected sample and the results were compared against a subsequently discovered non-obfuscated sample to confirm the validity of the method.

# MITRE ATT&CK CONTRIBUTIONS

ESET will be participating in the next round of *MITRE Engenuity ATT&CK* [112] evaluations that will focus on tactics, techniques, and procedures (TTPs) applied by the Turla APT group. Turla is a cyber-espionage group that has been active for more than 12 years. It has compromised many governments, especially diplomatic entities, all around the world, operating a large malware arsenal that ESET Research *has documented over the last* few *years* [113] [114] [115] [116] [117]. Besides our research, we also made several *contributions* [118] to the MITRE ATT&CK Enterprise Matrix related to the *Turla Group* [119].

ESET's research into APT groups like Turla has directly or indirectly helped many organizations and nation-states successfully thwart potential attacks by providing much-needed visibility into TTPs used by those very same groups for economic, espionage, geopolitical, or criminal purposes. ESET will again participate in both the Detection and the Protection evaluation rounds; results are to be expected during the second quarter of 2023.

# OTHER CONTRIBUTIONS

ESET researchers discovered three buffer overflow vulnerabilities in the UEFI firmware of several Lenovo Notebook devices, affecting more than 70 various models, including several within the ThinkBook series. All of these vulnerabilities were reported to the manufacturer on February 18. Lenovo acknowledged them, and released a *security advisory* [11] on June 12 containing a list of affected devices and firmware update instructions.

*CVE-2022-1890* [120]

UEFI BIOS images of several Lenovo laptop models contained a buffer overflow vulnerability leading to arbitrary code execution while processing the `System` NVRAM variable inside the ReadyBootDxe driver.

*CVE-2022-1891* [121]

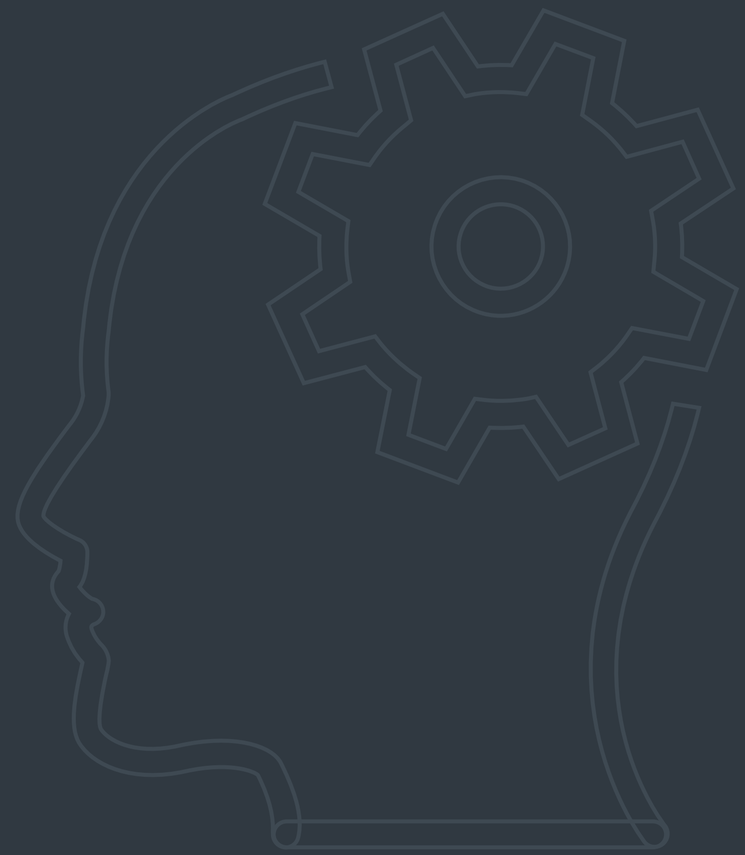
UEFI BIOS images of several Lenovo laptop models contained a buffer overflow vulnerability leading to arbitrary code execution while processing the `System` NVRAM variable inside the SystemLoadDefaultDxe driver.

*CVE-2022-1892* [122]

UEFI BIOS images of several Lenovo laptop models contained a buffer overflow vulnerability leading to arbitrary code execution while processing the `OilSetup` NVRAM variable inside the SystemBootManagerDxe driver.

The vulnerabilities can be exploited to achieve arbitrary code execution in the early phases of the platform boot, possibly allowing the attackers to hijack the OS execution flow and disable some important security features. These vulnerabilities were caused by insufficient validation of the `DataSize` parameter passed to the UEFI Runtime Services function `GetVariable`. An attacker could create a specially crafted NVRAM variable, causing buffer overflow of the data buffer in the second `GetVariable` call.

It's a typical UEFI "double `GetVariable`" vulnerability that can be identified in the firmware code by the IDA plugin efiXplorer. However, the vulnerabilities we found *were not covered* [123] by this plugin at the time of discovery. To help fellow researchers discover similar vulnerabilities and improve overall real-world UEFI firmware security, we submitted our improvements to the *efiXplorer repository* [124].



# 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

Dušan Lacika
Igor Kabina
Ján Šugarek
Jean-Ian Boutin
Jiří Kropáč
Juraj Jánošík
Ladislav Janko
Lukáš Štefanko
Marc-Étienne M.Léveillé
Martin Červeň
Michal Malík
Milan Fránik
Miroslav Balúž
Miroslav Legéň
Patrik Sučanský
Peter Kálnai
Radim Raszka
Robert Kapp
Vladimír Šimčák
Zuzana Legáthová
Zoltán Rusnák

# ABOUT THE DATA IN THIS REPORT

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

Further, the data excludes detections of *potentially unwanted applications* [125], *potentially unsafe applications* [126] and *adware* [127], except where noted in the more detailed, platform-specific sections and in the Cryptocurrency threats section.

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

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

# REFERENCES


[1] https://www.pcloud.com/

[2] https://office.hancom.com/

[3] https://nvd.nist.gov/vuln/detail/CVE-2020-9934

[4] https://medium.com/@mattshockl/cve-2020-9934-bypassing-the-os-x-transparency-consent-and-control-tcc-framework-for-4e14806f1de8

[5] https://www.apple.com/newsroom/2022/07/apple-expands-commitment-to-protect-users-from-mercenary-spyware/

[6] https://www.welivesecurity.com/2022/07/19/i-see-what-you-did-there-look-cloudmensis-macos-spyware/

[7] https://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html

[8] https://malpedia.caad.fkie.fraunhofer.de/actor/apt37

[9] https://attack.mitre.org/groups/G0067/

[10] https://twitter.com/ESETresearch/status/1575103839115804672

[11] https://support.lenovo.com/us/en/product_security/len-91369

[12] https://twitter.com/ESETresearch/status/1547166334651334657

[13] https://www.sentinelone.com/blog/from-the-front-lines-new-macos-covid-malware-masquerades-as-apple-wears-face-of-apt/

[14] https://twitter.com/ESETresearch/status/1547943014860894210

[15] https://twitter.com/ESETresearch/status/1527531726905409536

[16] https://www.welivesecurity.com/2022/05/20/sandworm-ukraine-new-version-arguepatch-malware-loader/

[17] https://twitter.com/ESETresearch/status/1524731829139476480

[18] https://twitter.com/ESETresearch/status/1526183746524876802

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

[20] https://twitter.com/h2jazi/status/1555205042331947011

[21] https://twitter.com/ESETresearch/status/1559553324998955010

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

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

[24] https://asec.ahnlab.com/en/34793/

[25] https://www.recordedfuture.com/amid-rising-magecart-attacks-online-ordering-platforms

[26] https://www.bleepingcomputer.com/news/security/lockbit-30-introduces-the-first-ransomware-bug-bounty-program/

[27] https://twitter.com/vxunderground/status/1561262483448512513

[28] https://www.microsoft.com/security/blog/2022/06/13/the-many-lives-of-blackcat-ransomware/

[29] https://www.microsoft.com/security/blog/2022/07/05/hive-ransomware-gets-upgrades-in-rust/

[30] https://thehackernews.com/2022/07/new-rust-based-ransomware-family.html

[31] https://www.lpalmieri.com/posts/error-handling-rust/

[32] https://www.bleepingcomputer.com/news/security/ransomware-hacking-groups-move-from-cobalt-strike-to-brute-ratel/

[33] https://www.bleepingcomputer.com/news/security/automotive-supplier-breached-by-3-ransomware-gangs-in-2-weeks/

[34] https://www.bleepingcomputer.com/news/security/fbi-zeppelin-ransomware-may-encrypt-devices-multiple-times-in-attacks/

[35] https://www.coveware.com/blog/2022/7/27/fewer-ransomware-victims-pay-as-medium-ransom-falls-in-q2-2022

[36] https://rusi.org/explore-our-research/publications/commentary/ransomware-now-threatens-global-south

[37] https://www.state.gov/reward-offers-for-information-to-bring-conti-ransomware-variant-co-conspirators-to-justice/

[38] https://www.phmsa.dot.gov/news/phmsa-issues-proposed-civil-penalty-nearly-1-million-colonial-pipeline-company-control-room

[39] https://www.cisa.gov/uscert/ncas/alerts/aa22-187a

[40] https://www.microsoft.com/security/blog/2022/07/14/north-korean-threat-actor-targets-small-and-midsize-businesses-with-h0lygh0st-ransomware/

[41] https://www.qnap.com/en/security-advisory/QSA-22-21

[42] https://www.bleepingcomputer.com/news/security/new-redeemer-ransomware-version-promoted-on-hacker-forums/

[43] https://blogs.blackberry.com/en/2022/05/yashma-ransomware-tracing-the-chaos-family-tree

[44] https://www.bleepingcomputer.com/news/security/conti-ransomware-shuts-down-operation-rebrands-into-smaller-units/

[45] https://www.bleepingcomputer.com/news/security/foxconn-confirms-ransomware-attack-disrupted-production-in-mexico/

[46] https://www.darkreading.com/attacks-breaches/costa-rica-declares-state-of-emergency-under-sustained-conti-cyberattacks

[47] https://www.bleepingcomputer.com/news/security/building-materials-giant-knauf-hit-by-black-basta-ransomware-gang/

[48] https://www.bleepingcomputer.com/news/security/lockbit-claims-ransomware-attack-on-security-giant-entrust-leaks-data/

[49] https://thehackernews.com/2022/05/us-charges-venezuelan-doctor-for-using.html

[50] https://www.bleepingcomputer.com/news/security/astralocker-ransomware-shuts-down-and-releases-decryptors/

[51] https://www.bleepingcomputer.com/news/security/free-decryptor-released-for-astralocker-yashma-ransomware-victims/

[52] https://www.europol.europa.eu/media-press/newsroom/news/hit-ransomware-no-more-ransom-now-offers-136-free-tools-to-rescue-your-files

[53] https://techcommunity.microsoft.com/t5/microsoft-365-blog/helping-users-stay-safe-blocking-internet-macros-by-default-in/bc-p/3566717/highlight/true#M4281

[54] https://thehackernews.com/2022/06/new-emotet-variant-stealing-users.html

[55] https://www.bleepingcomputer.com/news/security/bored-ape-yacht-club-otherside-nfts-stolen-in-discord-server-hack/

[56] https://thehackernews.com/2022/08/hackers-stole-crypto-from-bitcoin-atms.html

[57] https://www.sec.gov/news/press-release/2022-78

[58] https://www.welivesecurity.com/2020/09/02/kryptocibule-multitasking-multicurrency-cryptostealer/

[59] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/clipminer-bitcoin-mining-hijacking

[60] https://www.bleepingcomputer.com/news/security/massive-facebook-messenger-phishing-operation-generates-millions/

[61] https://faq.whatsapp.com/824303528016260/?locale=en_US

[62] https://www.trendmicro.com/en_us/research/22/e/fake-mobile-apps-steal-facebook-credentials--crypto-related-keys.html

[63] https://blog.google/threat-analysis-group/protecting-android-users-from-0-day-attacks/

[64] https://support.google.com/googleplay/android-developer/answer/11950272?hl=en

[65] https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-sms-based-flubot-spyware-infecting-android-phones?

[66] https://www.welivesecurity.com/2021/05/17/take-action-now-flubot-malware-may-be-on-its-way/

[67] https://twitter.com/ESETresearch/status/1526897310231322630

[68] https://www.cleafy.com/cleafy-labs/sova-malware-is-back-and-is-evolving-rapidly

[69] https://www.f5.com/labs/articles/threat-intelligence/f5-labs-investigates-malibot

[70] https://www.trendmicro.com/en_us/research/22/g/examining-new-dawdropper-banking-dropper-and-daas-on-the-dark-we.html

[71] https://github.com/BishopFox/sliver

[72] https://www.politico.eu/article/pegasus-use-5-eu-countries-nso-group-admit/

[73] https://blog.google/threat-analysis-group/italian-spyware-vendor-targets-users-in-italy-and-kazakhstan/

[74] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32893

[75] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32894

[76] https://www.theguardian.com/technology/2022/aug/18/apple-security-flaw-hack-iphone-ipad-macs

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

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

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

[80] https://nvd.nist.gov/vuln/detail/CVE-2022-26134

[81] https://nvd.nist.gov/vuln/detail/CVE-2022-30525

[82] https://isc.sans.edu/diary/Scanning+Activity+for+NVMS-9000+Digital+Video+Recorder/25434

[83] https://www.exploit-db.com/exploits/44760

[84] https://nvd.nist.gov/vuln/detail/CVE-2022-1388

[85] https://www.bleepingcomputer.com/news/security/critical-f5-big-ip-vulnerability-exploited-to-wipe-devices/

[86] https://www.thedrive.com/tech/i-tried-the-honda-keyfob-hack-on-my-own-car-it-totally-worked

[87] https://www.thedrive.com/news/how-thieves-are-stealing-hyundais-and-kias-with-just-a-usb-cable

[88] https://arstechnica.com/information-technology/2022/06/hackers-out-to-steal-a-tesla-can-create-their-very-own-personal-key/

[89] https://thehackernews.com/2022/06/researchers-demonstrate-ransomware-for.html

[90] https://www.welivesecurity.com/2017/01/25/rot-ransomware-things/

[91] https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview

[92] https://thehackernews.com/2022/05/eu-blames-russia-for-cyberattack-on-ka.html

[93] https://thehackernews.com/2022/07/microsoft-adds-default-protection.html

[94] https://thehackernews.com/2022/05/avoslocker-ransomware-variant-using-new.html

[95] https://www.microsoft.com/security/blog/2022/08/25/mercury-leveraging-log4j-2-vulnerabilities-in-unpatched-systems-to-target-israeli-organizations/

[96] https://www.bleepingcomputer.com/news/security/lazarus-hackers-target-vmware-servers-with-log4shell-exploits/

[97] https://www.cisa.gov/sites/default/files/publications/CSRB-Report-on-Log4-July-11-2022_508.pdf

[98] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30190

[99] https://www.wired.com/story/microsoft-follina-vulnerability-windows-office-365/

[100] https://cert.gov.ua/article/341128

[101] https://aavar.org/cybersecurity-conference/index.php/agenda/

[102] https://www.ekoparty.org/en_US/

[103] https://bsidesmtl.ca/bsides-montreal-2022-september-10-2022/program-2022/

[104] https://www.labscon.io/speakers/adam-burgher/

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

[106] https://www.virusbulletin.com/conference/vb2022/abstracts/lazarus-byovd-evil-windows-core/

[107] https://www.virusbulletin.com/conference/vb2022/abstracts/creepy-things-glow-dark-deep-look-poloniums-undocumented-tools/

[108] https://www.rsaconference.com/library/presentation/usa/2022/especter%20first%20real-world%20uefi%20bootkit%20persisting%20on%20esp

[109] https://codeblue.jp/2022/en/talks/?content=talks_21

[110] https://cfp.recon.cx/2022/talk/7EQPJX/

[111] https://sector.ca/sessions/under-the-hood-of-wslinks-multilayered-virtual-machine/

[112] https://attackevals.mitre-engenuity.org/enterprise/turla/

[113] https://www.welivesecurity.com/wp-content/uploads/2017/08/eset-gazer.pdf

[114] https://www.welivesecurity.com/wp-content/uploads/2018/01/ESET_Turla_Mosquito.pdf

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

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

[117] https://www.welivesecurity.com/2020/05/26/agentbtz-comratv4-ten-year-journey/

[118] https://attack.mitre.org/software/S0126/

[119] https://attack.mitre.org/groups/G0010/

[120] https://github.com/eset/vulnerability-disclosures/commit/b7db546f7b58dc88509898d77bfdc8959b929eb0#diff-1b088545db98018b1b6c3909d4e879c0033325f4c3762a4afcb55a819c5cddb8

[121] https://github.com/eset/vulnerability-disclosures/commit/b7db546f7b58dc88509898d77bfdc8959b929eb0#diff-da115c7f06d6e27f4d388104dc64d82b1a101d13ed7339cdd3c5e94fd7d3056d

[122] https://github.com/eset/vulnerability-disclosures/commit/b7db546f7b58dc88509898d77bfdc8959b929eb0#diff-c0af4b8268b4ec4c292409326bfcf5e982993cf5275bcf0d2aa85ef18876a551

[123] https://i.blackhat.com/eu-20/Wednesday/eu-20-Labunets-efiXplorer-Hunting-For-UEFI-Firmware-Vulnerabilities-At-Scale-With-Automated-Static-Analysis.pdf

[124] https://github.com/binarly-io/efiXplorer/commit/6bccee7b6817c8af6a737c24c25e88435a85a3f0

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

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

[127] 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