THREAT REPORT T3 2022

WeLiveSecurity.com

@ESETresearch

ESET GitHub

Digital Security
Progress. Protected.

CONTENTS

FOREWORD

Welcome to the T3 2022 issue of the ESET Threat Report!

In 2022, an unprovoked and unjustified attack on Ukraine shocked the world, bringing devastating effects on the country and its population. The war continues to impact everything from energy prices and inflation to cyberspace, which ESET researchers and analysts have monitored extensively throughout the year.

Among the effects seen in cyberspace, the ransomware scene experienced some of the biggest shifts. From the beginning of the invasion, we've seen a divide among ransomware operators, with some supporting and others opposing this aggression. The attackers have also been using increasingly destructive tactics, such as deploying wipers that mimic ransomware and encrypt the victim's data with no intention of providing the decryption key.

The war also affected brute-force attacks against exposed RDP services, with these attacks nose-diving in 2022. Other factors that might have contributed to this slump, besides the war, are a decline in remote work, improved setup and countermeasures by company IT departments, and a new brute-force blocking feature built into Windows 11. Most of the RDP attacks detected in 2022 originated from Russian IP addresses.

Even with the decline in RDP attacks, password guessing was still the most favored network attack vector in T3 2022. And despite remedies being available for the Log4J vulnerability since December 2021, it still placed second in the external intrusion vector ranking.

Various crypto-threats were impacted by plummeting cryptocurrency exchange rates on one side and soaring energy prices on the other. While traditional crimeware such as cryptostealers and cryptominers declined, cryptocurrency-related scams have been going through a renaissance: cryptocurrency-themed phishing websites blocked by ESET products increased by 62% in T3, and the FBI recently issued a warning about a surge in new crypto-investment schemes.

Numerous holidays celebrated in December led to increased phishing activity impersonating online shops, as people buying gifts online represent a very lucrative target for cybercrooks. And when mobile game developers rolled out new releases before the Christmas season, attackers exploited the hype by uploading their modified malicious versions to third-party app stores. In turn, we've observed a significant increase in Android adware detections in T3 2022.

The Android platform also saw an increase in spyware throughout the year, due to easy-to-access spyware kits available on various online forums and used by amateur attackers. And although overall infostealer detections trended down in both T3 and the whole of 2022, banking malware was an exception, with detections doubling in a year-on-year comparison.

The final months of 2022 were bustling with interesting ESET research findings. Our researchers discovered a MirrorFace spearphishing campaign against high-profile Japanese political entities, and new ransomware named RansomBoggs that targets multiple organizations in Ukraine and has Sandworm's fingerprints all over it. ESET researchers also discovered a campaign conducted by the infamous Lazarus group that targets its victims with spearphishing emails containing documents with fake job offers; one of the lures was sent to an aerospace company employee. As for supply-chain attacks, we found a new wiper and its execution tool, both of which we attribute to the Agrius APT group, aiming at users of an Israeli software suite used in the diamond industry.

As always, ESET researchers took multiple opportunities to share their expertise at various conferences, appearing at AVAR, Ekoparty and others, where they took deep dives into technical aspects of most of the aforementioned ESET Research discoveries. For the upcoming months, we are happy to invite you to ESET talks at Botconf, RSA Conference and others.

I wish you an insightful read.

Roman Kováč
ESET Chief Research Officer

EXECUTIVE SUMMARY

FEATURED STORY

Unmasking MirrorFace: Operation LiberalFace targeting Japanese political entities

ESET researchers discovered a spearphishing campaign targeting Japanese political entities a few weeks before the House of Councillors elections, and in the process uncovered a previously undescribed MirrorFace credential stealer.

NEWS FROM THE LAB

RansomBoggs: New ransomware targeting Ukraine

ESET researchers spotted RansomBoggs, new ransomware targeting Ukraine, with the campaign sharing many traits with the infamous Sandworm APT group.

Fantasy: A new Agrius wiper deployed through a supply-chain attack

ESET researchers analyzed a supply-chain attack abusing an Israeli software developer to deploy Fantasy, Agrius's new wiper, with victims including the diamond industry.

STATISTICS & TRENDS

Category	T2 2022/ T3 2022	Key points in T3 2022
Overall threat detections	-13.2% ↓	Decrease in detections in most monitored categories
Infostealers	-11.9% ↓	Banking malware detections double year-on-year
Ransomware	-1.9% ↓	Ransomware-mimicking wipers target Ukraine
Downloaders	-44.8% ↓	MSIL downloaders take the lead, Emotet largely quiet
Cryptocurrency threats	-24.8% ↓	Cryptocurrency malware declines further, scams flourish
Web threats	-10.0% ↓	Cryptocurrency-themed phishing lures on the rise
Email threats	-17.4% ↓	30% year-over-year growth despite T3 decline
Android	+56.5% ↑	Ad-driven Android threats grow significantly
macOS	-5.5% ↓	Decline across detection categories except PUAs
RDP attacks	-15.9% ↓	RDP attacks remain down at 89 mil. daily average attacks

FEATURED STORY

Unmasking MirrorFace: Operation LiberalFace targeting Japanese political entities

Dominik Breitenbacher

ESET researchers discovered a spearphishing campaign targeting Japanese political entities a few weeks before the House of Councillors elections, and in the process uncovered a previously undescribed MirrorFace credential stealer.

Just weeks before the *Japanese House of Councillors election* [1] in July 2022, ESET researchers noticed a spearphishing campaign targeting candidates in that election. ESET Research tracks the APT group responsible for this activity as MirrorFace, and we named this campaign Operation LiberalFace. Our investigation revealed that the members of a specific political party were of particular focus in this campaign.

MirrorFace is a Chinese-speaking threat actor targeting companies and organizations based in Japan. While there is some speculation that this threat actor might be related to APT10, ESET is unable to attribute it to any known APT group. Therefore, we track it as a separate entity that we've named MirrorFace. In particular, MirrorFace and LODEINFO, its proprietary malware used exclusively against targets in Japan, have been *reported* [2] as targeting media, defense-related companies, think tanks, diplomatic organizations, and academic institutions. The goal of MirrorFace is espionage and exfiltration of files of interest.

We attribute Operation LiberalFace to MirrorFace based on these indicators:

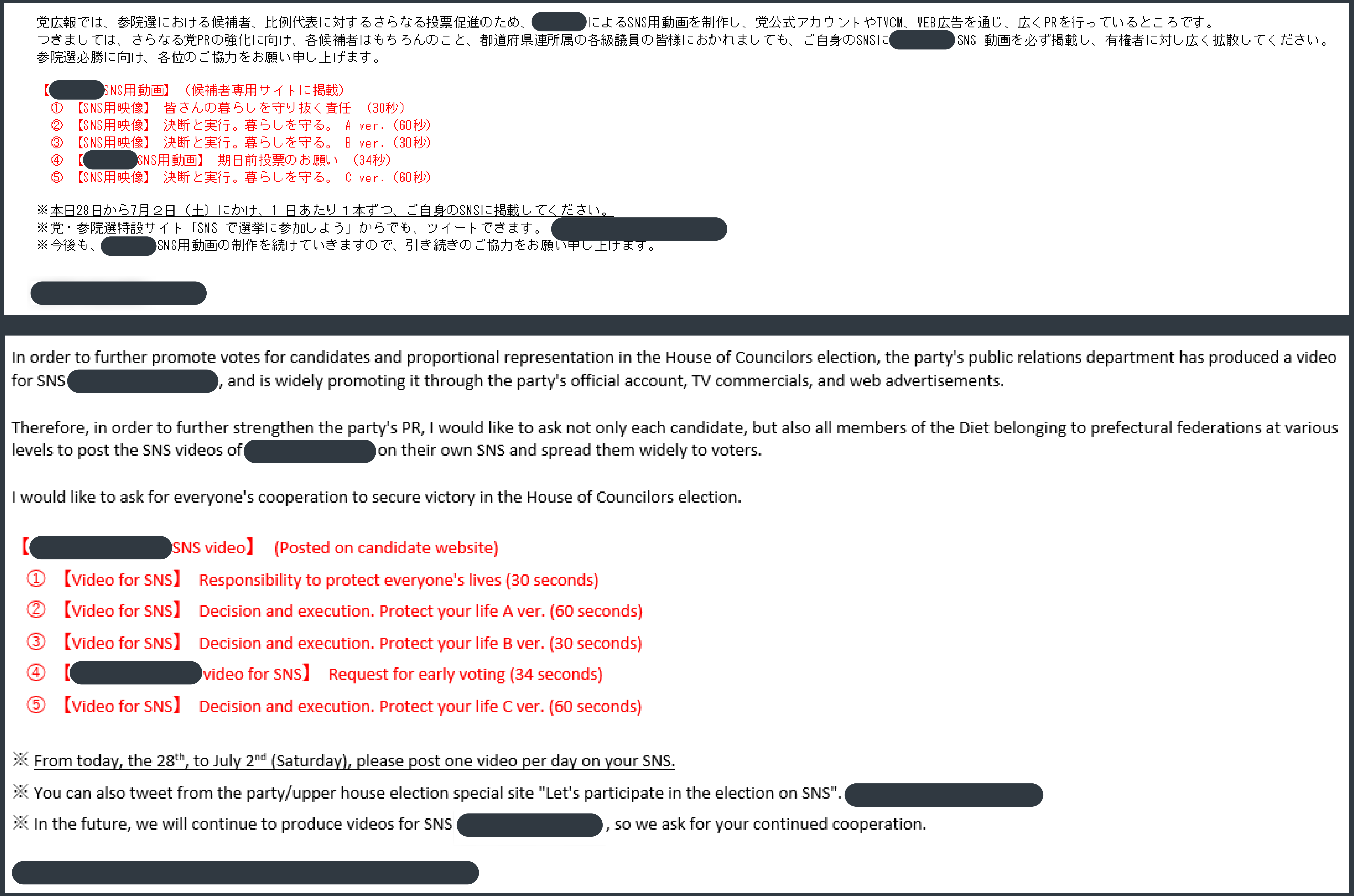
- To the best of our knowledge, LODEINFO malware is exclusively used by MirrorFace.
- The targets of Operation LiberalFace align with traditional MirrorFace targeting.
- A second-stage LODEINFO malware sample contacted a C&C server that we track internally as part of MirrorFace infrastructure.

One of the spearphishing emails sent in Operation LiberalFace posed as an official communication from the PR department of a specific Japanese political party, containing a request related to the House of Councillors elections, and was purportedly sent on behalf of a prominent politician. MirrorFace started the attack on June 29, 2022; the subject of the spearphishing email containing a malicious attachment was <redacted>SNS用動画　拡散のお願い (machine translation: [Important] <redacted> Request for spreading videos for SNS).

The malicious email asked the recipients to distribute the attached videos on their own social media profiles (SNS – Social Network Service) to further strengthen the party's PR and to secure victory in the election. Furthermore, the email provides clear instructions on the videos' publication strategy.

Since the House of Councillors election was held on July 10, 2022, this email clearly indicates that MirrorFace sought the opportunity to attack political entities. Also, specific content in the email indicates that members of a particular political party were targeted.

MirrorFace also used another spearphishing email in the campaign, where the attachment was titled 【参考】220628<redacted>発・<redacted>選挙管理委員会宛文書（添書分）.exe (machine translation: [Reference] 220628 Documents from



党広報では、参院選における候補者、比例代表に対するさらなる投票促進のため、[redacted]によるSNS用動画を制作し、党公式アカウントやTVCM、WEB広告を通じ、広くPRを行っているところです。
つきましては、さらなる党PRの強化に向け、各候補者はもちろんのこと、都道府県連所属の各級議員の皆様におかれましても、ご自身のSNSに[redacted]SNS 動画を必ず掲載し、有権者に対し広く拡散してください。
参院選必勝に向け、各位のご協力をお願い申し上げます。

【[redacted]SNS用動画】（候補者専用サイトに掲載）
① 【SNS用映像】 皆さんの暮らしを守り抜く責任 （30秒）
② 【SNS用映像】 決断と実行。暮らしを守る。 A ver.（60秒）
③ 【SNS用映像】 決断と実行。暮らしを守る。 B ver.（30秒）
④ 【[redacted]SNS用動画】 期日前投票のお願い （34秒）
⑤ 【SNS用映像】 決断と実行。暮らしを守る。 C ver.（60秒）

※本日28日から7月２日（土）にかけ、１日あたり１本ずつ、ご自身のSNSに掲載してください。
※党・参院選特設サイト「SNS で選挙に参加しよう」からでも、ツイートできます。[redacted]
※今後も、[redacted]SNS用動画の制作を続けていきますので、引き続きのご協力をお願い申し上げます。

[redacted]

In order to further promote votes for candidates and proportional representation in the House of Councilors election, the party's public relations department has produced a video for SNS [redacted], and is widely promoting it through the party's official account, TV commercials, and web advertisements.

Therefore, in order to further strengthen the party's PR, I would like to ask not only each candidate, but also all members of the Diet belonging to prefectural federations at various levels to post the SNS videos of [redacted] on their own SNS and spread them widely to voters.

I would like to ask for everyone's cooperation to secure victory in the House of Councilors election.

【[redacted]SNS video】 (Posted on candidate website)
① 【Video for SNS】 Responsibility to protect everyone's lives (30 seconds)
② 【Video for SNS】 Decision and execution. Protect your life A ver. (60 seconds)
③ 【Video for SNS】 Decision and execution. Protect your life B ver. (30 seconds)
④ 【[redacted]video for SNS】 Request for early voting (34 seconds)
⑤ 【Video for SNS】 Decision and execution. Protect your life C ver. (60 seconds)

※ From today, the 28th, to July 2nd (Saturday), please post one video per day on your SNS.
※ You can also tweet from the party/upper house election special site "Let's participate in the election on SNS". [redacted]
※ In the future, we will continue to produce videos for SNS [redacted], so we ask for your continued cooperation.

[redacted]

Original text of the email (above) and translated version (below)

`the Ministry of <redacted> to <redacted> election administration committee (appendix).exe`. The attached decoy document references the House of Councillors election as well.

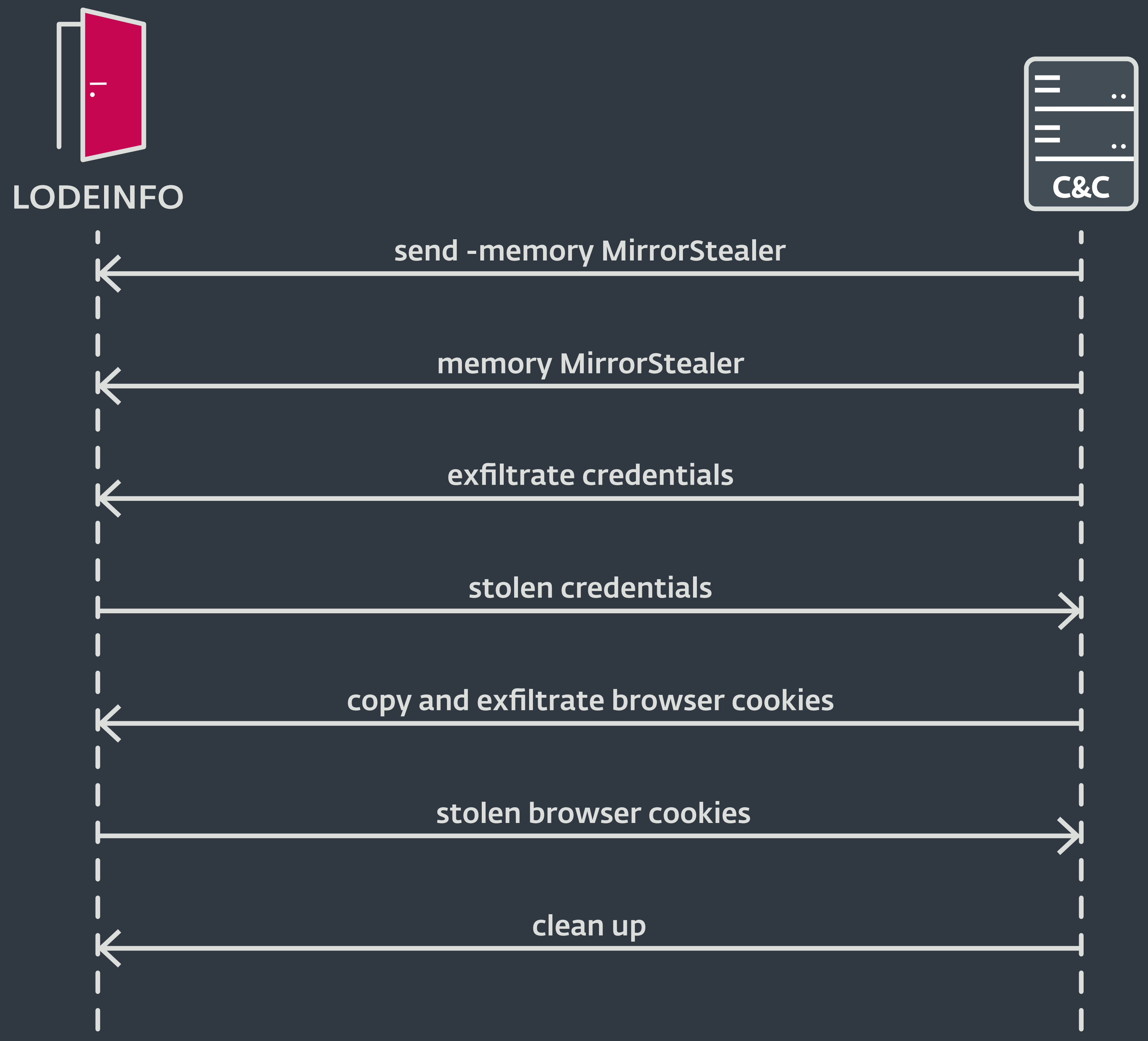
All spearphishing emails analyzed by ESET Research contained a malicious attachment that opened a decoy document to deceive the target and to appear benign, and also deployed LODEINFO on the compromised machine. LODEINFO is a MirrorFace backdoor that is under continual development. JPCERT/CC *reported about the first version* [3] of LODEINFO (v0.1.2), which appeared around December 2019; its functionality allows capturing screenshots, keylogging, killing processes, exfiltrating files, and executing additional files and commands. Since then, we have observed several changes introduced to each of its versions.

Besides detecting LODEINFO, we also discovered that MirrorFace has used previously undocumented malware, which we have named MirrorStealer, to pilfer its target's credentials. We believe our research presents the first case in which this malware has been publicly described. MirrorStealer is a credential stealer: it steals credentials from various applications such as browsers and email clients. Interestingly, one of the targeted applications is *Becky!* [4], an email client that is currently only available in Japan. Since MirrorStealer doesn't have the capability to exfiltrate the stolen data, it depends on other malware to do it.

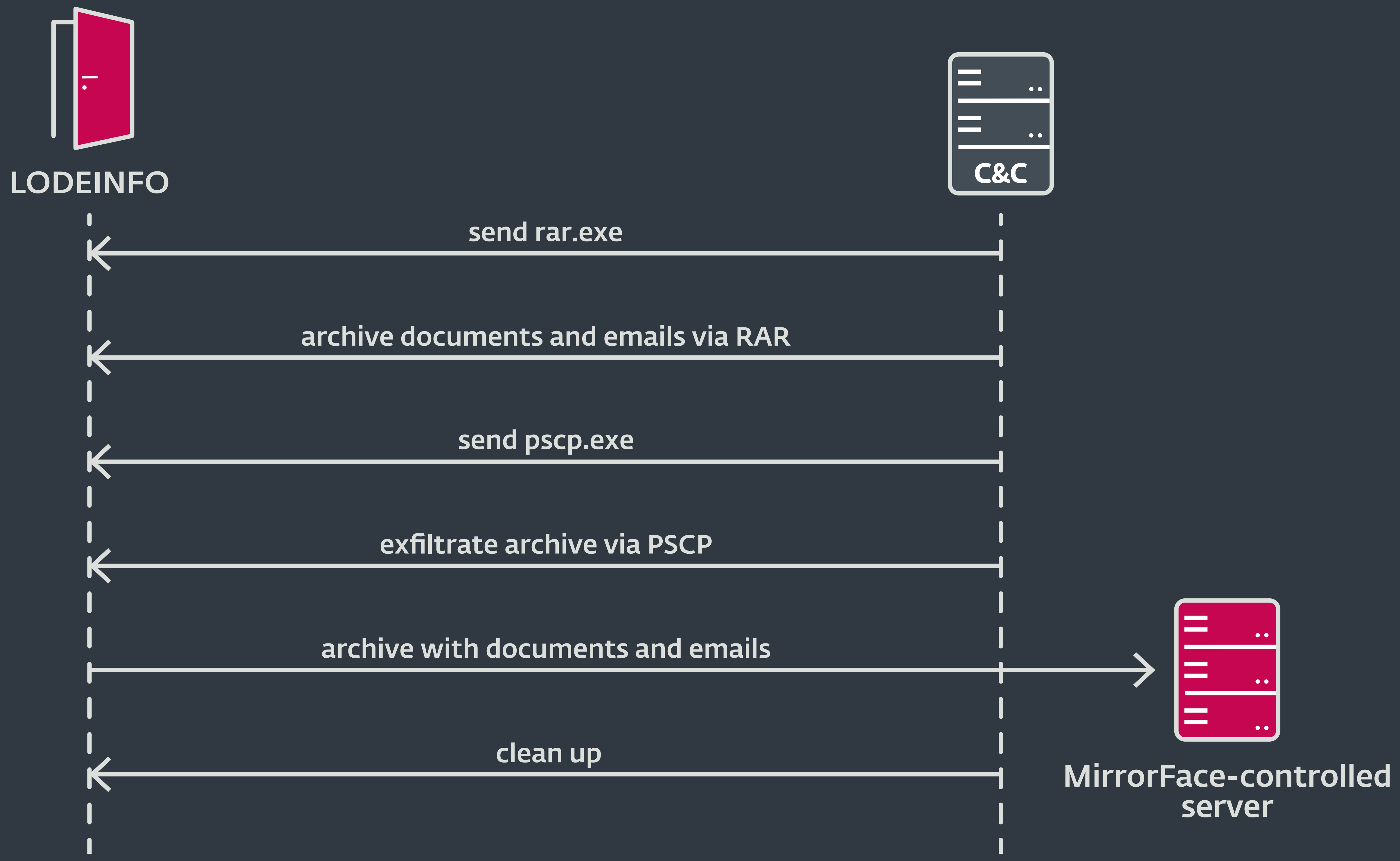
MirrorFace operators used LODEINFO commands to capture the screen of the compromised machine, obtained the list of computers connected to the network, and the list of available domains. LODEINFO was also used by the operators to exfiltrate credentials collected by MirrorStealer, and the victim's browser cookies.

Documents of various kinds as well as stored emails (`.eml` files) were also exfiltrated from the affected machine. The operator was interested in common document types, such as files with the extensions `.doc*`, `.ppt*`, `.xls*`, and `.*xps`. It is important to note that MirrorFace was also interested in files with the `.jtd` extension; this represents documents of the Japanese word processor *Ichitaro* [5] developed by JustSystems.

The last step we observed was delivering the second-stage LODEINFO. The operator delivered several binaries to the compromised machine; one of them was `JsSchHlp.exe`. The original `JsSchHlp.exe` is a benign application signed by JUSTSYSTEMS CORPORATION, the makers of the previously mentioned Japanese word processor Ichitaro. However, in this case, the MirrorFace operators abused a known Microsoft digital signature verification *issue* [6] and appended RC4 encrypted data to the `JsSchHlp.exe` digital signature. Because of the mentioned issue, Windows still considers the modified `JsSchHlp.exe` to be validly signed.



Flow of instructions sent to LODEINFO to deploy credential stealer, collect credentials and browser cookies, and to exfiltrate them to the C&C server



LODEINFO
C&C
send rar.exe
archive documents and emails via RAR
send pscp.exe
exfiltrate archive via PSCP
archive with documents and emails
clean up
MirrorFace-controlled server

Flow of the instructions sent to LODEINFO to exfiltrate files of interest

`JsSchHlp.exe` is also susceptible to DLL search-order hijacking. Therefore, upon execution, a DLL also delivered to the compromised machine is loaded. This malicious loader then reads the appended payload from `JsSchHlp.exe`, decrypts and runs it. The payload is the second-stage LODEINFO; however, it appears to us that the operator didn't manage to make the second-stage LODEINFO communicate properly with its C&C server. Therefore, any further steps of the operators while utilizing the second-stage LODEINFO remain unknown to us.

Based on certain activities performed on the affected machine, we think that the MirrorFace operators issued commands to LODEINFO in a manual or semi-manual manner, but in a somewhat careless way, leaving traces and making various mistakes. For instance, the operators made a few errors and typos when issuing commands to LODEINFO – they sent the string

```
cmd /c dir "c:\use\"
```

to LODEINFO, which most likely was supposed to be

```
cmd /c dir "c:\users\"
```

Our next observation is that even though they performed a few cleanups to remove traces of the compromise, they forgot to delete `%temp%\31558.txt` – the log containing the stolen credentials. Thus, at least this trace remained on the compromised machine, and it shows us that the operators were not thorough in the cleanup process.

ESET Research first unmasked details about this campaign and the APT group behind it at the *AVAR 2022 conference* [7] in December.

WeLiveSecurity blogpost [8]

NEWS FROM THE LAB

Latest findings from ESET Research Labs across the world

Worok

Worok: The big picture

ESET researchers have discovered a previously unknown cyberespionage group that they named Worok. Active since at least 2020, the group carries out targeted attacks against various high-profile companies and local governments mostly in Asia. Thus, we believe that the main goal of the operators is information theft.

In addition to leveraging existing tools to compromise its targets, Worok also develops its own. Those include two loaders, CLRLoad and PNGLoad, and the PowHeartBeat backdoor.

CLRLoad is a first-stage loader written in C++ that was used in 2021 – in 2022 it was replaced, in most cases, by PowHeartBeat. PNGLoad is a second-stage loader, this time written in C#, that uses steganography to reconstruct malicious payloads hidden in PNG images.

PowHeartBeat is a full-featured backdoor written in PowerShell, obfuscated using various techniques such as compression, encoding, and encryption. This backdoor has various capabilities, including command/process execution and file manipulation.

WeLiveSecurity blogpost [9]

SparklingGoblin

You never walk alone: The SideWalk backdoor gets a Linux variant

ESET Research discovered a Linux variant of the SideWalk backdoor, one of the multiple custom implants used by the SparklingGoblin APT group. SparklingGoblin targets mostly East and Southeast Asia, with a particular focus on the academic sector.

We first saw the Linux variant of SideWalk in action in February 2021 when it was deployed against a Hong Kong university that had already been targeted by SparklingGoblin in the past. SideWalk Linux exhibits several similarities with its Windows counterpart, along with some technical novelties. The similarities include the same customized ChaCha20 encryption algorithm, software architecture, configuration, and dead-drop resolver implementation. As opposed to SideWalk Windows, the Linux variant contains debugging symbols and leaves some unique authentication keys and other artifacts unencrypted, which makes its detection and analysis significantly easier.

WeLiveSecurity blogpost [10]

APT-C-50

Domestic Kitten campaign spying on Iranian citizens with new FurBall malware

ESET researchers identified a new version of the Android malware FurBall being used in the Domestic Kitten campaign carried out by the APT-C-50 group. The Domestic Kitten campaign is known to conduct mobile surveillance operations against Iranian citizens, and this new FurBall version is no different in its targeting.

This malicious Android application is delivered via a fake website mimicking a legitimate site that provides articles and books translated from English to Persian. The purpose of the copycat site is to offer an Android app for download after clicking on a button that says, in Persian, "Download the application". The button has the Google Play logo, but this app is not available from the Google Play store; it is downloaded directly from the attacker's server.

This version of FurBall has the same surveillance functionality as previous versions; however, the threat actors slightly obfuscated class and method names, strings, logs, and server URIs. Since the functionality of this variant hasn't changed, the main purpose of this update appears to be to avoid detection by security software. The malware requests only one intrusive permission – to access contacts – most likely to stay under the radar and not to attract the suspicion of potential victims during the installation process. This also might be the first stage of gathering contacts that could be followed by spearphishing via text messages.

WeLiveSecurity blogpost [11]

Bahamut

Bahamut cybermercenary group targets Android users with fake VPN apps

ESET researchers discovered a campaign, conducted by the Bahamut APT group, that targeted Android users. Active since January 2022, this campaign distributed trojanized versions of two legitimate VPN apps through a fake Secure VPN website. We found at least eight versions of the Bahamut spyware.

The malware is able to exfiltrate sensitive data such as contacts, SMS messages, call logs, device location, and recorded phone calls. It can also actively spy on chat messages exchanged through very popular messaging apps including Signal, Viber, WhatsApp, Telegram, and Facebook Messenger.

We found that the spyware code, and hence its functionality, is the same as in previous Bahamut Android campaigns, including collecting data in a local database before exfiltrating it to the operators' server, a tactic rarely seen in mobile cyberespionage apps.

This campaign tries to keep a low profile – the website URL is most likely delivered to potential victims with an activation key, which is not provided on the website. Unfortunately, we were not able to obtain a working key. In addition to that, we have seen no instances of the campaign in our telemetry data, and thus believe this campaign is highly targeted.

WeLiveSecurity blogpost [12]

ScarCruft

Who's swimming in South Korean waters? Meet ScarCruft's Dolphin

The ESET Research team analyzed a previously unreported backdoor used by ScarCruft, an APT group that focuses primarily on government and military organizations in South Korea. This backdoor, which we named Dolphin, has a wide range of spying capabilities, including monitoring drives and portable devices, exfiltrating files of interest, keylogging and taking screenshots, and stealing credentials from browsers.

In 2021, ScarCruft conducted a watering-hole attack, hosted on a South Korean online newspaper site that focuses on North Korea. Victims were compromised with multiple components, among them a backdoor named BLUELIGHT (reported by *Volexity* [13] and *Kaspersky* [14]). While at the time BLUELIGHT was considered to be the attack's final payload, we discovered another, more sophisticated backdoor, deployed on selected victims via BLUELIGHT. We named this backdoor Dolphin, based on text in the PDB path found in the executable.

After being deployed on selected targets, Dolphin searches the drives of compromised systems for interesting files and exfiltrates them to Google Drive. One unusual capability found in Dolphin's prior versions is the ability to modify the settings of victims' Google and Gmail accounts to lower their security, presumably to maintain Gmail account access for the threat actors.

WeLiveSecurity blogpost [15]

Lazarus

Amazon-themed Lazarus campaigns in the Netherlands and Belgium

ESET Research analyzed a set of malicious tools that were used by the Lazarus APT group in a spearphishing campaign against targets in the Netherlands and Belgium. The campaign, which took place in late 2021, targeted an employee of an aerospace company in the Netherlands and a political journalist in Belgium with spearphishing emails containing malicious Amazon-themed documents.

Both targets were presented with job offers – the employee in the Netherlands received an attachment via LinkedIn Messaging, and the journalist in Belgium received a document via email. Attacks started after these documents were opened. Several malicious tools were deployed on the system, including droppers, loaders, fully featured HTTP(S) backdoors, and HTTP(S) uploaders.

The most notable tool delivered by the attackers was a user-mode module that gained the ability to read and write kernel memory due to exploiting the CVE-2021-21551 vulnerability in a legitimate Dell driver. This vulnerability affects Dell DBUtil drivers; Dell provided a security update in May 2021. This is the first ever recorded abuse of this vulnerability in the wild.

WeLiveSecurity blogpost [16]

POLONIUM

POLONIUM targets Israel with Creepy malware

ESET researchers analyzed previously undocumented custom backdoors and cyberespionage tools deployed in Israel by the POLONIUM APT group. POLONIUM is a cyberespionage group first documented by *Microsoft* [17] in June 2022. According to Microsoft, the group is based in Lebanon and coordinates its activities with other actors affiliated with Iran's Ministry of Intelligence and Security.

POLONIUM's toolset consists of seven custom backdoors: CreepyDrive, which abuses OneDrive and Dropbox cloud services for C&C; CreepySnail, which executes commands received from the attackers' own infrastructure; DeepCreep and MegaCreep, which make use of Dropbox and Mega file storage services, respectively; and FlipCreep, TechnoCreep, and PapaCreep, which receive commands from attackers' servers. The group has also developed several custom modules to spy on its targets by taking screenshots, logging keystrokes, spying via the webcam, opening reverse shells, exfiltrating files, and more.

The numerous versions and changes POLONIUM introduced into its custom tools show a continuous and long-term effort to spy on the group's targets. We can infer from its toolset that POLONIUM is interested in collecting confidential data. The group doesn't seem to engage in any sabotage or ransomware actions.

WeLiveSecurity blogpost [18]

Sandworm

RansomBoggs: New ransomware targeting Ukraine

ESET researchers spotted a new wave of ransomware attacks targeting multiple organizations in Ukraine, with the campaign sharing many traits with the APT group Sandworm. We named this malware, which is developed in the .NET framework, RansomBoggs. Even though it is new, the way it is deployed bears close resemblance to some past attacks attributed to Sandworm.

Once RansomBoggs infiltrates the victim's machine, it generates a random key and encrypts files using AES-256 in CBC mode, then appends the `.chsch` extension to the encrypted files. The key is then RSA encrypted and written to `aes.bin`. Since the operators are not asking for money in exchange for data decryption, this is a case of file coder being used as a wiper.

RansomBoggs was distributed from the victims' domain controllers via a PowerShell script that was almost identical to the one used in both the CaddyWiper and Industroyer2 attacks in Ukraine, both of which were carried out by Sandworm.

WeLiveSecurity blogpost [19]

Twitter thread [20]

Agrius

Fantasy: a new Agrius wiper deployed through a supply-chain attack

ESET Research discovered a new wiper and its execution tool, both attributed to the Agrius APT group. We believe that Agrius operators conducted a supply-chain attack abusing an Israeli software developer to deploy the group's new wiper, Fantasy, and a new lateral movement and Fantasy execution tool, Sandals. Fantasy targeted victims in South Africa, Israel, and Hong Kong.

In this campaign, Agrius first deployed credential-harvesting tools at an organization in the diamond industry in South Africa. A few weeks later, it launched the wiping attack using Fantasy and Sandals, striking first the South African target, continuing with the targets in Israel, and finishing in Hong Kong. The campaign lasted less than three hours and within that timeframe ESET customers were already protected with detections identifying Fantasy as a wiper and blocking its execution.

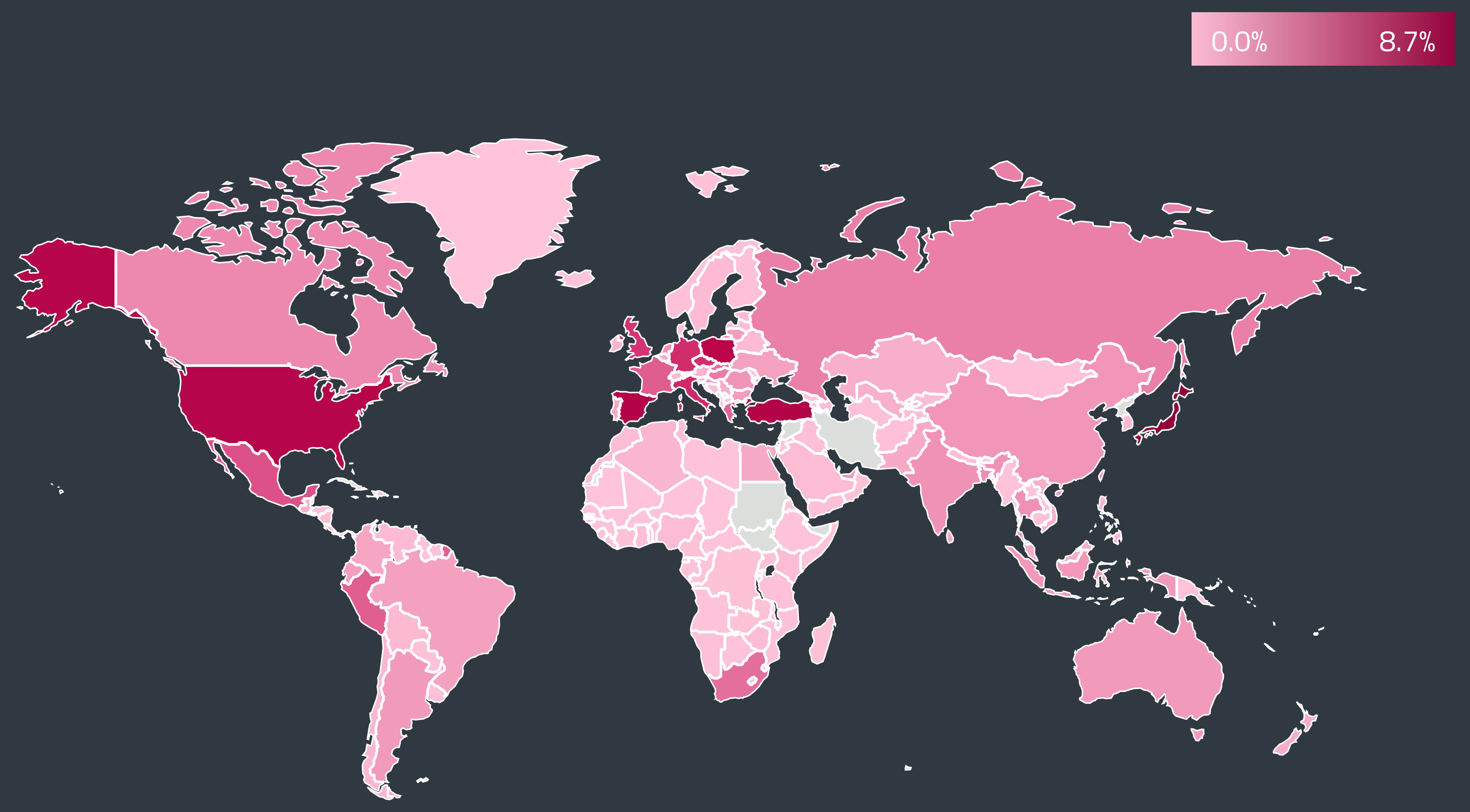
Sandals is a 32-bit Windows executable written in C#/.NET used to connect to systems in the same network via SMB, to write a batch file to disk that executes the Fantasy wiper, and then run that batch file via PsExec.

The Fantasy wiper is also a 32-bit Windows executable written in C#/.NET, so named for its filenames: `fantasy45.exe` and `fantasy35.exe`, respectively. It is similar in many respects to the previous Agrius wiper, Apostle, that initially masqueraded as ransomware before being rewritten to be actual ransomware. Fantasy makes no effort to disguise itself as ransomware.

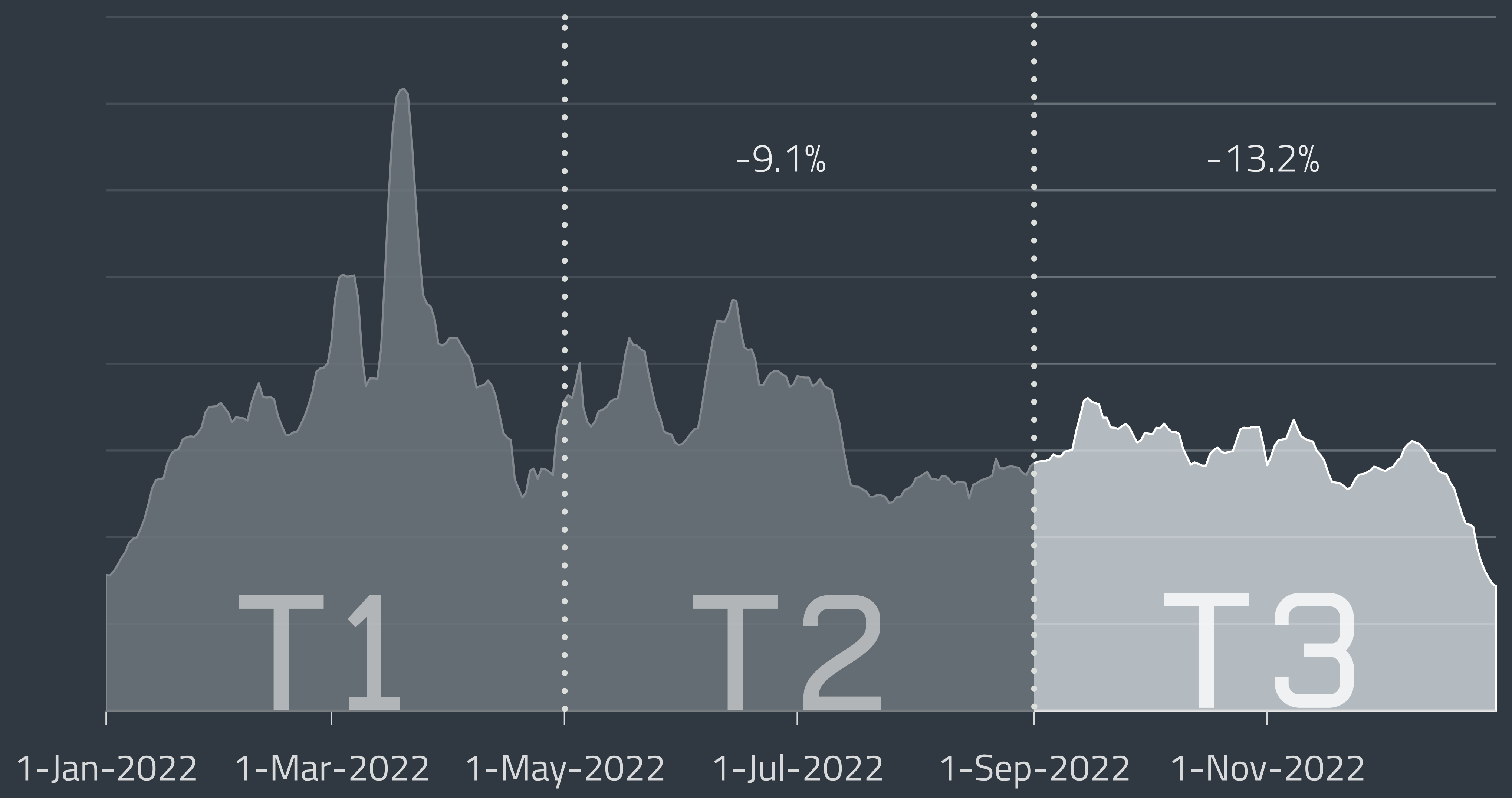
WeLiveSecurity blogpost [21]

STATISTICS & TRENDS

The threat landscape in T3 2022 as seen by ESET telemetry



Global distribution of malware detections in T3 2022



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

THREAT LANDSCAPE OVERVIEW

A summary of the threat landscape developments in T3 2022.

T3 2022 was, similar to T2, marked by a general decrease across the threat landscape. ESET telemetry registered an overall 13.2% reduction in threat detections, the trend chart showing just one small spike on September 14, caused by an increase in activity of HTML/Phishing.Agent. However, data for the whole year reveals that while we might have seen a momentary drop in numbers, total detections actually increased year-on-year, going up by 13%.

Even in T3, there was one category that thrived: The *Android* category registered a remarkable growth of 57% in detections. This was driven by a 163% increase in Adware and an 83% increase in HiddenApps detections.

In some other categories, there was a similar phenomenon to that observed in overall threat detections – while the number of detections in these categories decreased in T3, they registered a yearly increase. For instance, the *Downloaders* category saw 71% growth between 2021 and 2022. On the other hand, Emotet detections experienced a steep decline of 84% in T3, falling considerably silent apart from a campaign in Japan, and the addition of a new info-gathering module.

Similarly, while *Infostealer* detections decreased by 12% in T3, Banking malware detections continued their yearlong growth, increasing by more than 100% between 2021 and 2022.

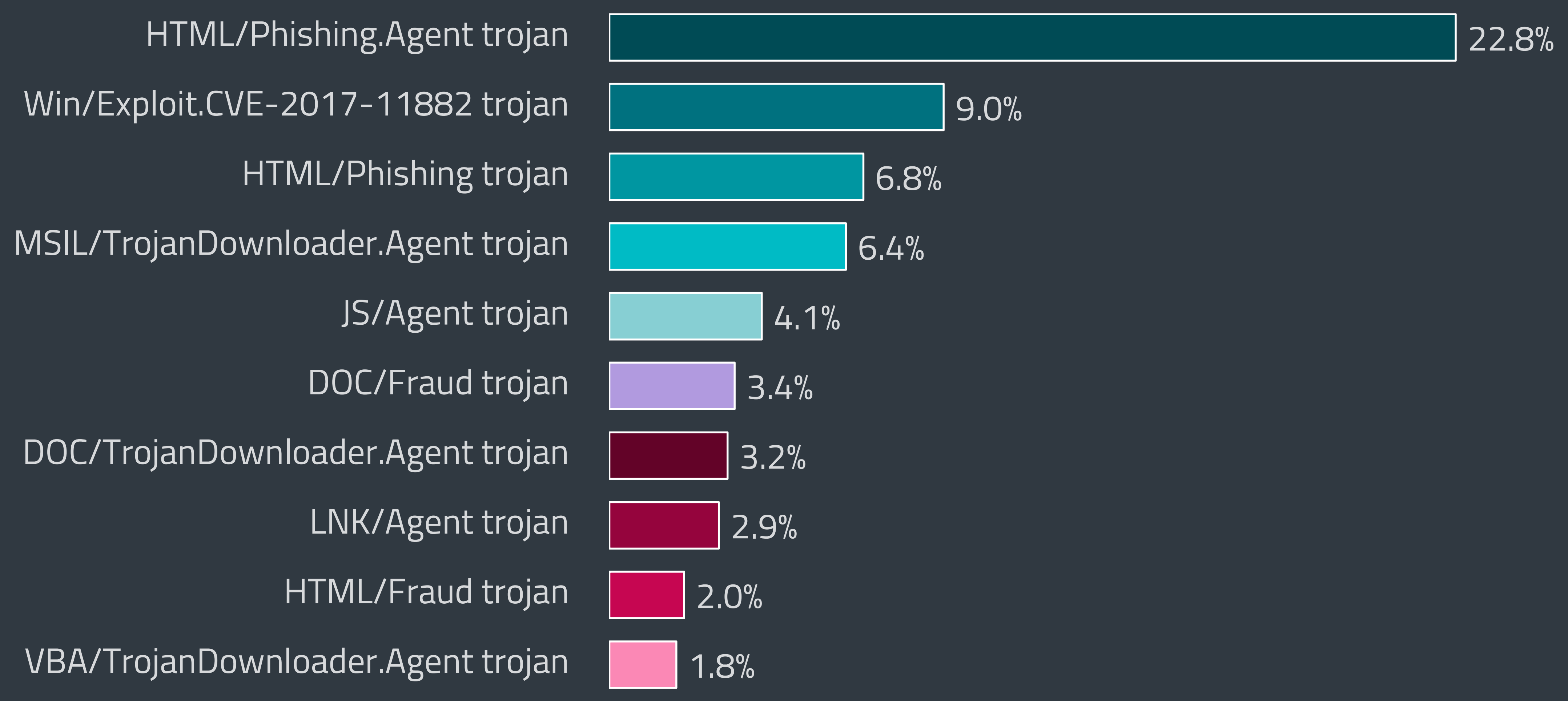
Circling back to Emotet, its massive campaigns in T1 2022 led to a 30% year-on-year increase in *Email threats*, a category that otherwise declined by 17% in T3.

Despite overall *Web threat* detections decreasing by 10.6% between 2021 and 2022, its Phishing subcategory was the only one to grow in T3, with the number of phishing website blocks up by 115% compared to T2.

Over in the *macOS* category, ESET telemetry registered only a slight, 5.5%, decline. Potentially unwanted applications (PUAs) made up 52% of these detections, growing by 3% compared to T2.

There was no yearly growth when it comes to *Ransomware* detections, which dropped by 20% between 2021 and 2022. However, in T3 2022, we saw increased use of ransomware-mimicking wipers related to the Russia-Ukraine war, such as Azov ransomware, Somnia wiper, and CryWiper.

In the *Exploits* category, RDP password-guessing attacks – once a bustling contributor in 2021 – dropped by 49% in 2022. The daily averages of attack attempts oscillated around 1 billion in T1, plummeting to around 100 million in T3. In contrast, SQL attacks reversed their course, growing by 9% in T3.



Top 10 malware detections in T3 2022 (% of malware detections)

As has now become expected, *Cryptocurrency threat* detections continued their downward spiral, decreasing by 45% from 2021 to 2022. While crimeware rates fell, cryptocurrency-related scams were on the rise.

In the area of *IoT security* threats, we saw shifts among IoT botnets: the number of new bots that joined the Mozi botnet decreased by 25%, the ZHtrap botnet died suddenly, and Mirai-based bots grew by 11%, although 6% fewer attacks were detected.

Apart from some position reshuffling, no dramatic changes occurred in the list of top ten malware detections. HTML/Phishing.Agent reigned supreme both in T3 and in 2022 overall. Only one family, HTML/Phishing.Outlook, left the most-detected club in T3, falling from ninth to sixteenth place. The empty spot in the list was, in turn, claimed by the DOC/Fraud trojan, which climbed into sixth place from its fourteenth position in T2.

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.

↗ 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 blocklisted URL, it triggers an HTML/Phishing.Gen detection.

→ 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.

↗ DOC/Fraud trojan

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

↘ 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.

↘ 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.

→ 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".

↘ 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.

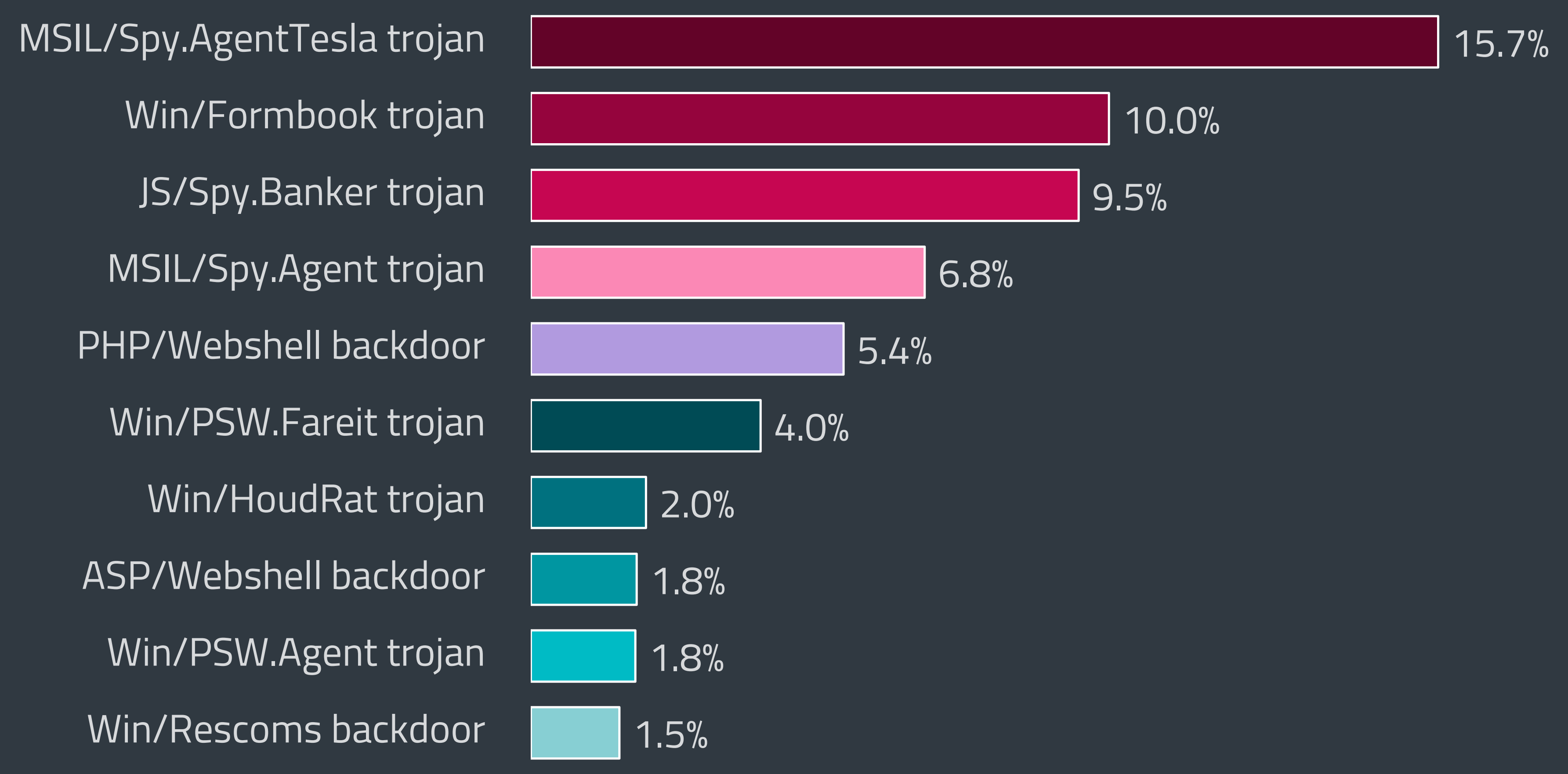
INFOSTEALERS

Banking malware detections doubled in 2022.

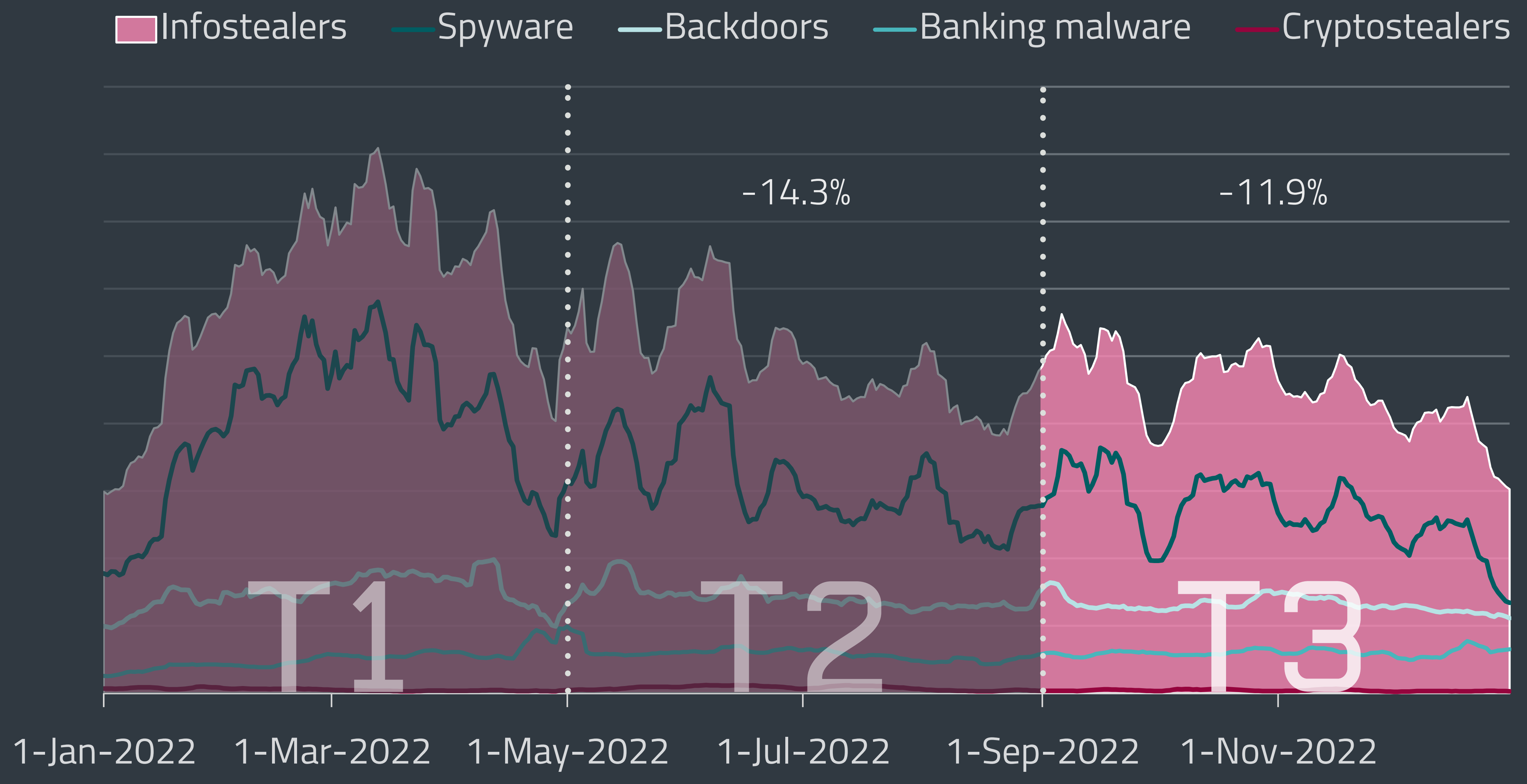
Our T3 2022 telemetry data is characterized by a decline across most monitored categories. Infostealers are no exception: their T3 decrease was close to 12%, and their 2022 overall numbers went down by almost 10% compared to 2021. Infostealers trended steadily, albeit gently, downward throughout the whole of T3, with no dramatic detection spikes or drops.

The one Infostealer subcategory that did not experience a decline in this reporting period was Banking malware: its T3 numbers stayed practically identical to those of T2. Even so, its year-on-year detections more than doubled, going up by 107%.

This phenomenon was caused by the prevalence of the web skimmer JS/Spy.Banker, also known as Magecart. It made up the overwhelming majority of banking malware detections in 2022: throughout the year, this malware family consistently accounted for about three-fourths of banking malware detections. JS/Spy.Banker also ended up being the third most detected infostealer, both in T3 (9.5%) and for the whole of 2022 (8%), and the only banking malware to get into the overall top ten infostealer list. It has to be noted, though, that the detections of this online script hiding on hacked websites are based on the number of unique visits to said websites, so it can shoot up much higher in our telemetry than most other malware in the Infostealer category, which is distributed as downloader payloads or via email attachments.



Top 10 infostealer families in T3 2022 (% of Infostealer detections)



Infostealer detection trend in 2022, seven-day moving average

Win/ClipBanker, the second-place holder, grew by 8.6% and accounted for 4.7% of banking malware registered by ESET telemetry in T3 2022.

The third-most detected banking malware family was the Latin American banking trojan Grandoreiro, with 4% of banking malware detections. While this percentage share might not look that impressive when compared to the likes of JS/Spy.Banker, Win/Spy.Grandoreiro experienced quite a growth spurt in 2022 – compared to 2021, its numbers were almost six times higher. In T3, it also continued its expansion outside Latin America, with the majority of its detections coming from Spain.

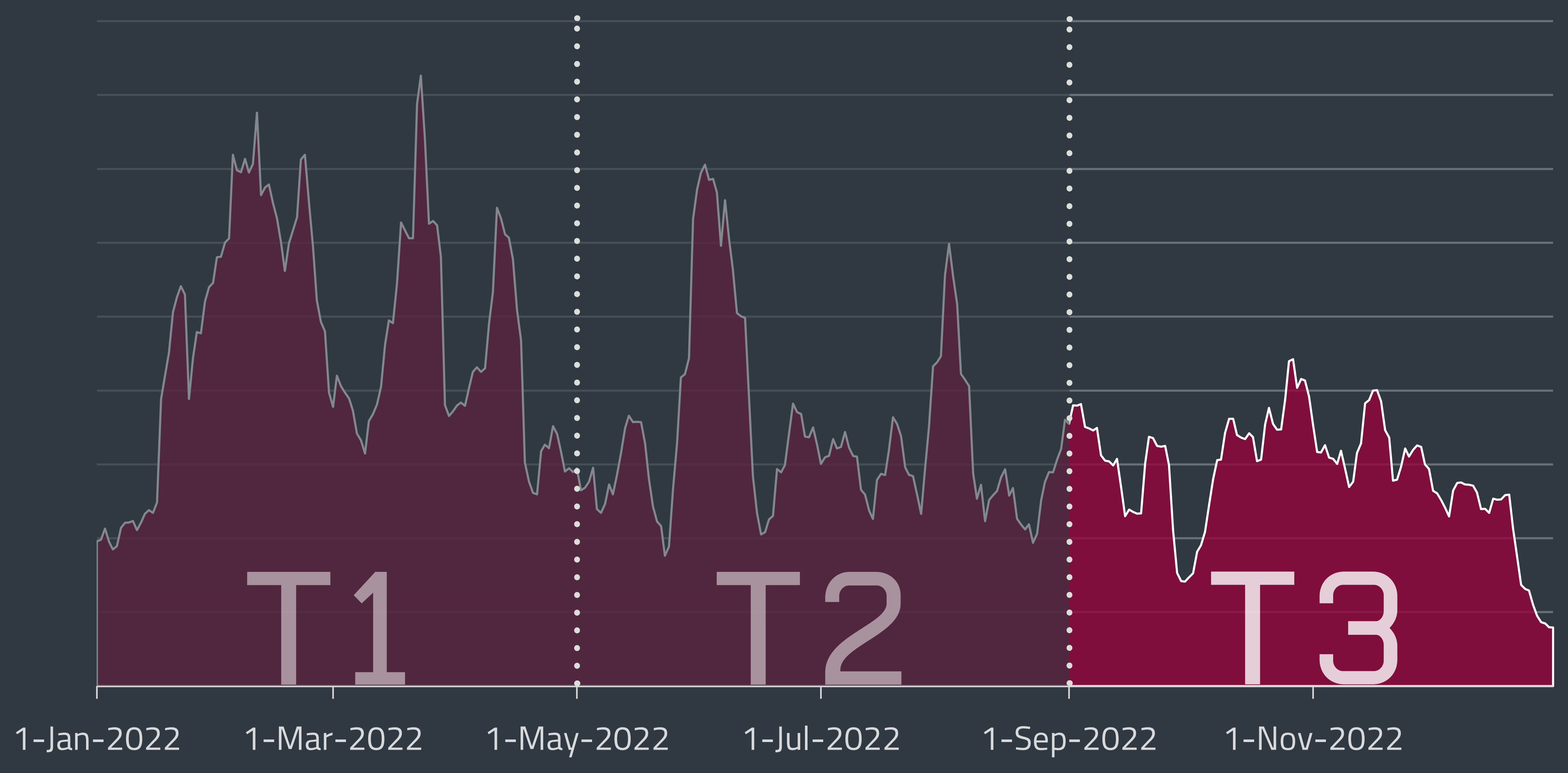
Speaking of *LATAM banking trojans* [24], many of them had quite a strong end of the year. The detections of not only Grandoreiro, but also several others such as Casbaneiro, Mispadu, and Mekotio, spiked in November and December of 2022. We could see a shift from script to Delphi downloaders in the most prevalent among these trojans, likely to improve their detection evasion. When using Delphi executables, the threat actors heavily utilized VMProtect and Themida, which offer very good code protection compared to what are usually very simple and custom-made script obfuscations.

While Banking malware was the only Infostealer subcategory not to decline in T3, the subcategory of Cryptostealers was the one that dropped the most, by 48.7%. This only further underlines the continuous decline of the "traditional" cryptocurrency crimeware threats, as opposed to scams and phishing.

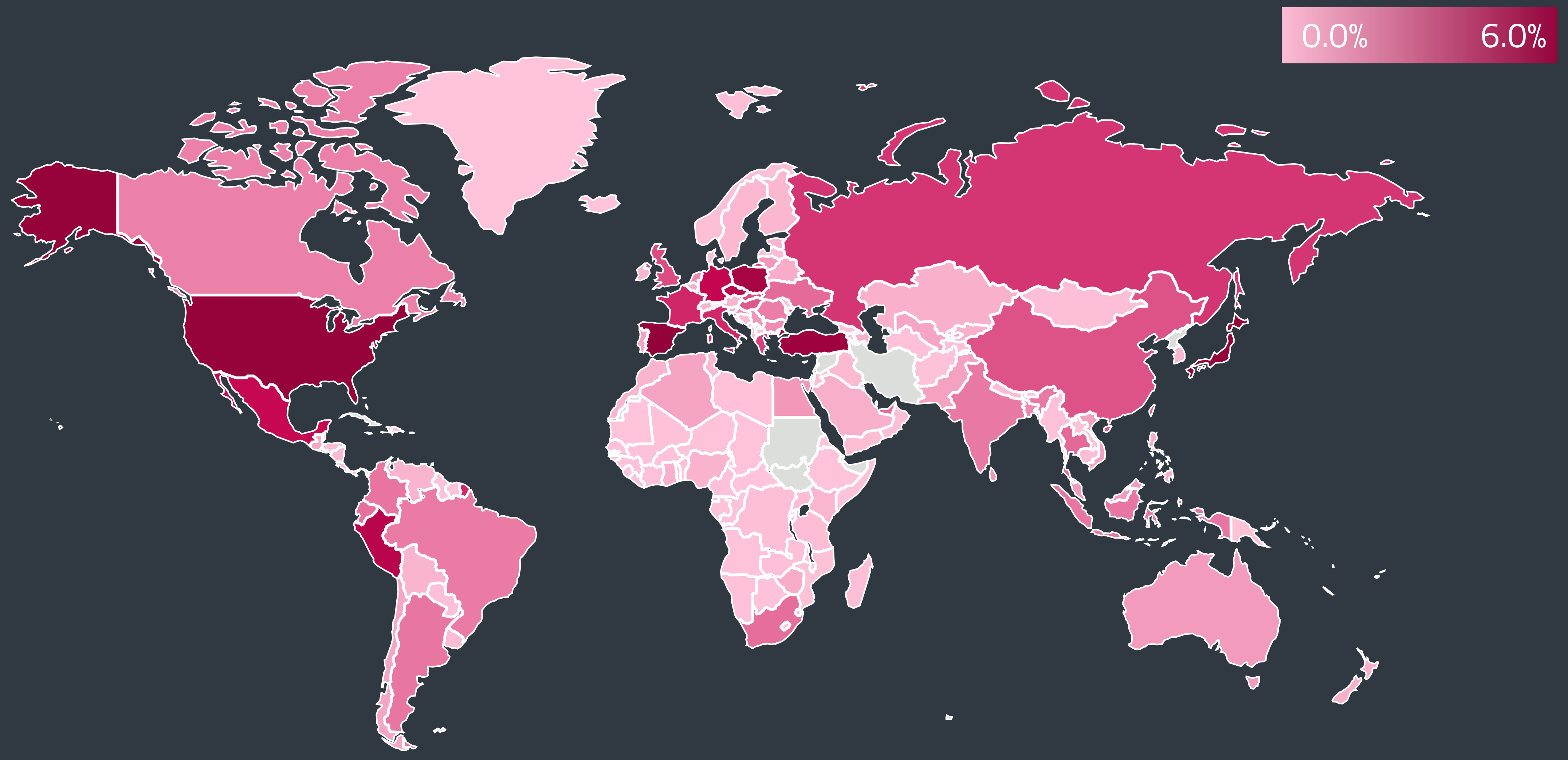
After appearing in our telemetry in T2 2022, PowerShell/PSW.Coinstealer managed to become the most detected cryptostealer in T3 with 31.5%. Win/PSW.Delf was in second place with 24.5%, and Win/Spy.Agent was third with 22.2%. More information about Cryptostealers can be found in the *Cryptocurrency threats* section.

The Spyware subcategory, which accounts for the majority of Infostealers in our telemetry, continued its downward trend in T3 with a 14.3% decrease. Its 2022 detections also declined compared to the year 2021, in total by 15%.

Despite the decrease in numbers, spyware continued to be a very common type of malware, especially due to the ready availability of many of its families online. The notorious Agent Tesla, known in our telemetry as MSIL/Spy.AgentTesla, is not the only spyware-as-a-service to be used widely. Recently, RedLine Stealer, another one of these families, made the news multiple times. In September, it was *reported* [25] that this malware had hit the video game publisher 2K Games, targeting its customers with fake support emails that contained malicious executables. In another video-game-related *campaign* [26], RedLine was part of a malware bundle that could self-spread through malicious YouTube videos, going after fans of games such as Final Fantasy, FIFA, and Lego Star Wars. According to our telemetry data, most RedLine detections were from Peru, Poland, and Turkey.



MSIL/Spy.AgentTesla detection trend in 2022, seven-day moving average



Global distribution of Infostealer detections in T3 2022

Spyware detections peaked at the beginning of T3, on September 6, when we registered an increased number of attack attempts in Turkey and the Czech Republic. The most detections on this day belonged to Win/Formbook, followed by Win/Spy.Weecnaw.L. Win/Spy.Weecnaw is a remote access trojan that experienced quite significant growth in T3, going up by 151.4%. The L variant of this trojan was being distributed via emails as an executable file disguised as a PDF invoice document.

The two spyware families with the most detections in T3, as well as in 2022 as a whole, were the usual suspects: MSIL/Spy.AgentTesla and Win/Formbook. They were also the top-detected infostealers, again both in T3 and in 2022. Agent Tesla constituted 26.1% of spyware in T3 (15.7% of infostealers), while the Win/Formbook trojan amounted to 16.7% of spyware (10% of infostealers). Both of these families were on a downward detection trend throughout the year.

While we could be tempted to say that after its decline in T2 and T3, the days of Agent Tesla are numbered, its long-term trend has been more-or-less stable overall. The momentary decrease in detections can be explained by a change in its distribution vector: it used to be spread mostly by email, but now it's being distributed more and more as a downloader payload.

The third place among Spyware and the fourth place in the Infostealer top list belonged to MSIL/Spy.Agent, which garnered 11.3% of spyware and 6.8% of infostealer detections. This malware family also trended downward in T3 and experienced a 24% decrease when compared to T2.

Backdoors, which constituted over 28% of infostealer detections, went down by 9.6% in T3 2022, their trend chart showing no significant spikes. Backdoors' year-on-year decline was similar, if slightly lower, to that of Spyware: 13% as compared to 14.3%.

There were only three backdoor families that managed to get into the infostealer top 10 in T3. The highest ranking among them was PHP/Webshell with 5.4% (18.4% of backdoors). Even though its detections declined in T3 by 5.8%, it had 7.6% more detections in 2022 than in 2021. ASP/Webshell, the second-most detected backdoor family with 6.2%, decreased in both T3 and 2022, by 15.6% and 27%, respectively. In T3, that meant eighth place overall in the top 10 infostealer list with 1.8%.

Closing out both the infostealer top 10 with 1.5% and the backdoor top 3 with 5.2% of detections was the Win/Rescoms backdoor. Its Win32/Rescoms.B variant spiked on October 24, when most of its attack attempts were captured in Turkey.

The country where we registered the most infostealer attack attempts in T3 2022 was the US with 6%, closely followed by Spain with 5.9% and Japan with 5.8%. When taking data for the entire year 2022 into account, the unenviable victory belongs to Spain (6.6%), with Japan in second place at 6.5%, and Turkey with 6.4% in third place.

TRENDS & OUTLOOK

Malware such as Agent Tesla, Magecart, Fareit, and Formbook will keep going strong in 2023. All of these families can be categorized as sophisticated infostealers with authors who are strongly motivated to keep updating their products in order to make a profit. The core of these applications is more or less stable; their development is now mostly centered around new and advanced code obfuscation and detection-avoidance techniques, which is a trend that will continue.

Spyware such as Agent Tesla and Fareit will try to propagate as much as possible to increase its chance of success. When it comes to banking malware, though, it is not guaranteed that its growth will continue, since multifactor authentication and other means of securing financial transactions have been making it harder to steal money straight from bank accounts. Cybercriminals might resort to cryptostealing, since it is easier to do and the transactions are harder to trace. However, with the volatility of the cryptocurrency market, it remains to be seen whether these attempts will bear fruit.

Jiří Kropáč, ESET Director of Threat Detection

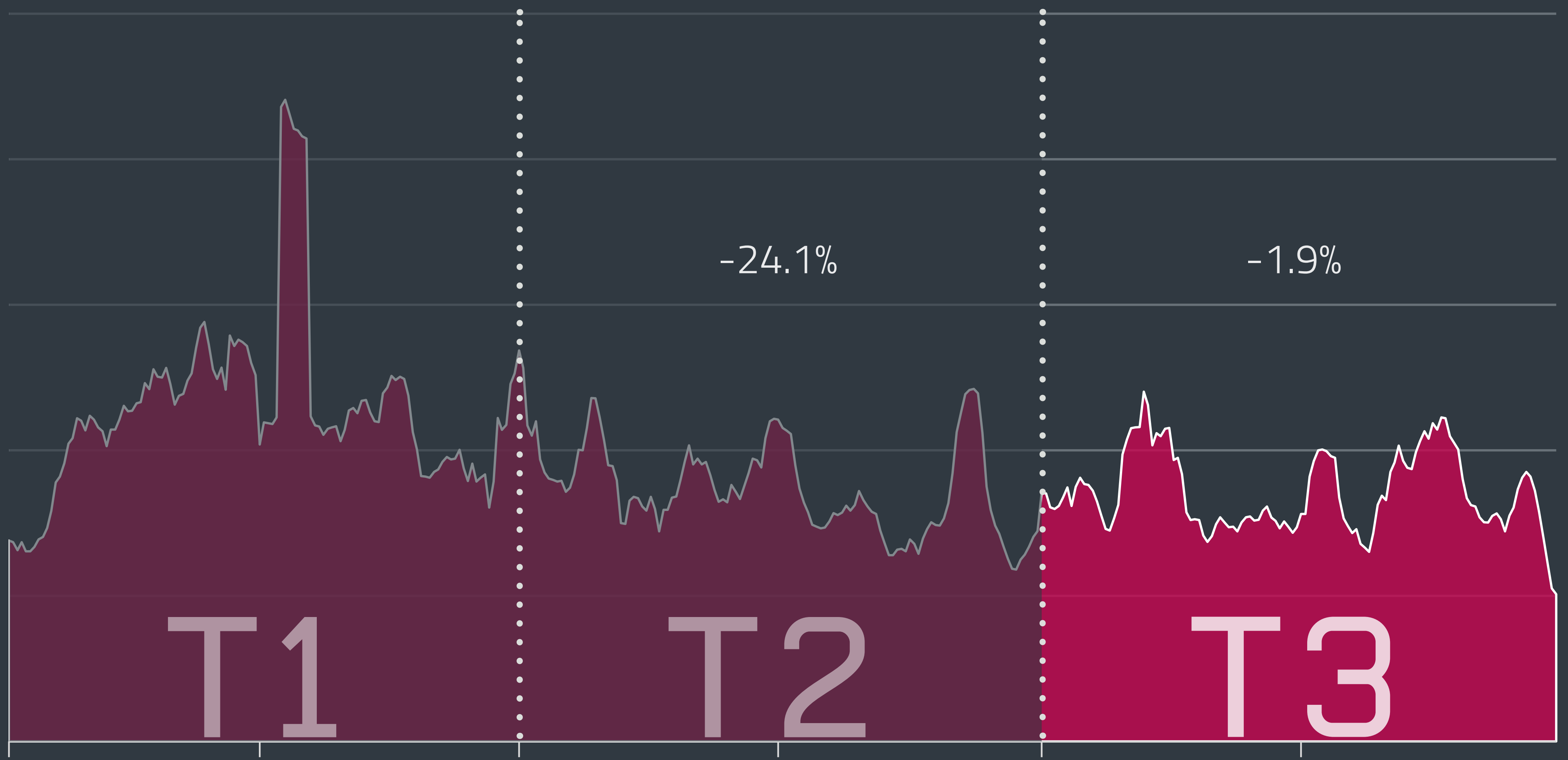
RANSOMWARE

While detection numbers stagnated, several ransomware-mimicking wipers appeared in connection with the Russia-Ukraine war.

In the last few years, ransomware has become widespread due to its profitability. However, the Russian invasion of Ukraine also highlighted its destructive potential, as threat actors on both sides of the conflict have used ransomware variants to attack their adversaries' organizations and effectively wipe their data by encrypting it with no intention of providing the decryption key.

In T3 2022, several new strains fit into this "wiper mimicking ransomware" category or were at least at its edge. In October, a wiper called *Azov Ransomware* [27] started spreading. It overwrote 666-byte chunks of data at a time, with no chance of recovery. Azov also backdoored most of the 64-bit executables it could find, increasing the risk of it being spread further. In the ransom note, its creators criticized the lack of Western help for Ukraine and sent political messages to the western public asking them to start protests, yet the malware did not target Russian organizations, so it's possibly a false flag operation.

In November, several organizations in Ukraine were hit with *Somnia wiper* [28]. CERT-UA attributed the malware to a group known as From Russia with Love. Supporting this view is an image dropped by Somnia's first-stage executable, displaying the name of the group and the letter Z – famously used as a symbol of Russian aggression against its neighbor.



Ransomware detection trend in 2022, seven-day moving average

FRWL
Z
FROM RUSSIA WITH LOVE

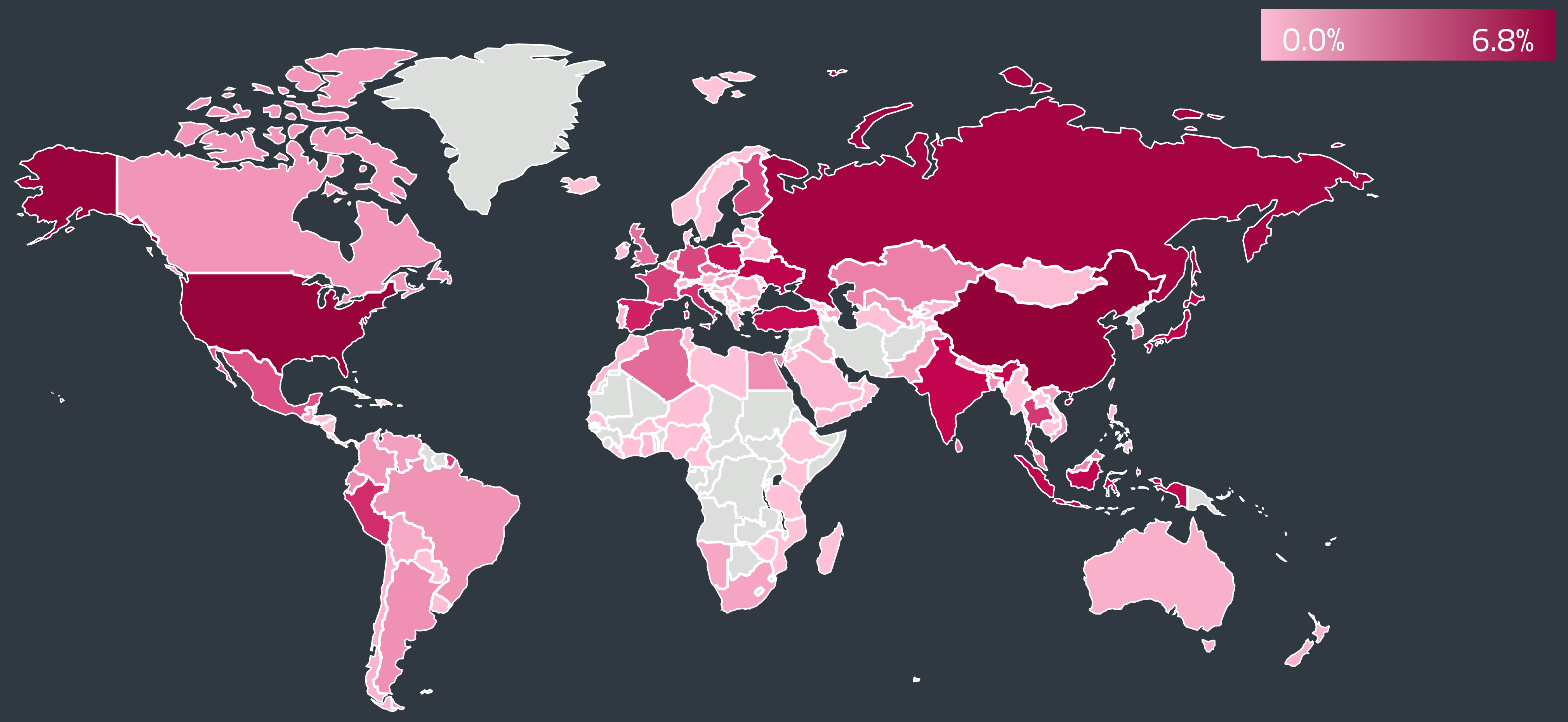
Image dropped during Somnia wiper attacks, displaying the name From Russia with Love and the letter Z

In December – probably in retaliation for the Somnia attacks – *CryWiper* [29] was launched at Russian governmental agencies and courts, destroying their data and systems. CryWiper is only the second destructive malware targeting Russia since the war broke out, with *RURansom* [30] in March 2022 being its only predecessor.

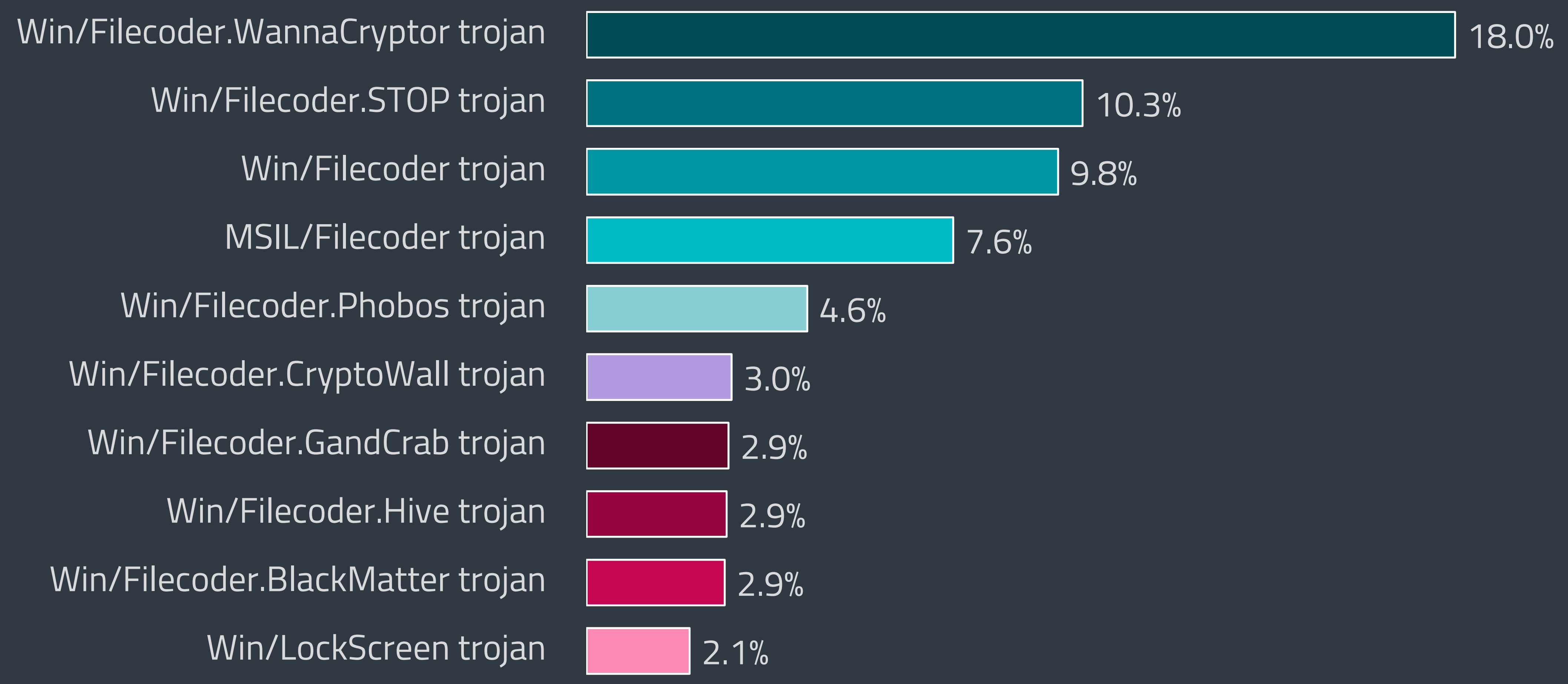
ESET research also found a new .NET ransomware in T3 2022 called *RansomBoggs* [20], targeting organizations in Ukraine. It landed at the edge of the wiper category, as its early versions did have a decryption function, but it wasn't called. However, its authors added the call later, but the attribution to Sandworm – a particularly ruthless Russia-aligned APT group – suggests its victims are unlikely to be helped by the malware's operators. We base this attribution on an almost identical POWERGAP PowerShell script used to distribute RansomBoggs and earlier Sandworm malware *CaddyWiper* [31], both deployed via *Active Directory Group Policy* [32].

Prestige ransomware, another malware from this category, was detected targeting logistics companies in Ukraine and Poland, as also mentioned in ESET's latest *APT Activity Report* [33].

As for the general trends in ransomware, the number of detections remained steady in T3, dropping only by 2% compared to T2 2022. The year-over-year detection trend was considerably more dynamic, dropping by 20% between 2021 and 2022. Several factors could have contributed, including



Global distribution of Ransomware detections in T3 2022



Top 10 ransomware families in T3 2022 (% of Ransomware detections)

increased international law enforcement cooperation and activity, disruptions caused by the war in Ukraine, and increased regulation limiting ransom payments and thus diminishing the financial return for the attackers.

Looking at geographical distribution in T3 2022, China saw the largest number of incidents, followed by the US, Russia, Ukraine, and Japan. The yearly data, however, showed Russia in the lead with 8%, followed by the US with less than 7%, and the fourth-placed Ukraine less than 4%, of all 2022 ransomware attacks.

Looking at the top 10 in T3 2022, some of the most notable strains were Win/Filecoder.STOP and Win/Filecoder.Hive. The former spiked in several countries simultaneously on September 20 and November 3; the latter attempted to infiltrate organizations in Namibia and the United States on September 1 and aimed at the US on November 3. The last ransomware spike in our telemetry occurred on November 29, due to attack attempts by Win/Filecoder.AvosLocker in Peru.

T3 2022 also saw a plethora of MSIL/Filecoder variants based on the publicly available HiddenTear code. These are typically injected into clean software, which was also the case of the AGP variant, whose authors used the classic Snake videogame to hide their code's nefarious purpose.

But the last four months of 2022 also brought good news to some ransomware victims. Those hit by *LockerGoga* [34], *RanHassan* [35], and *Zeppelin* [36] ransomware now all have a decryptor at their disposal. The Dutch police – together with a partner from the private sector – *tricked* [37] the NAS-targeting gang known as Deadbolt into handing over decryption keys, helping as many as 90% of the Dutch victims who reported the crime to the authorities.

T3 2022 also saw several ransomware affiliates arrested. A Ukrainian affiliate of the REvil gang was *detained and charged* [38] with involvement in several attacks, including the Kaseya case. Along with him, two other actors tied to the group were arrested in Romania. Another *successful apprehension* [39] was aimed at a Russian-Canadian national with ties to the LockBit gang. In the case of a *Netwalker affiliate* [40] arrested in Canada and extradited to the US, a sentence has been passed, sending him to prison for the next 20 years.

Despite all the decryption tools and growing law-enforcement activity, ransomware still poses a financially attractive model for criminals. The CISA-published estimates of ransom payments to *Cuba* [41] and *Hive* [42] ransomware operators amounted to USD 60 million from 101 victims in the former and as much as USD 100 million from 1,300 victims in the latter case.

The US Financial Crimes Enforcement Network (FinCEN) published its *report* [43] looking at the statistics from 2021, which documented over 1,200 ransomware-related incidents with USD 886 million in damages. Its data analysis also shows that 75% of the recorded attacks had a nexus to Russia, its proxies, or someone acting on its behalf.

Potentially astronomic incomes work like a magnet for criminals, which led them to kickstart numerous new ransomware families in T3 2022. The list includes a Linux version of *DarkAngels* [44], Conti's doppelganger *MONTI* [45], a new variant of MountLocker called *DagonLocker* [46], and *Vohuk, ScareCrow, and AERST* [47].

Regarding ransomware trends, there were a few things worth noting in T3 2022. An increasing number of gangs switched to *intermittent encryption* [48] – a process that only affects parts of the targeted files, still rendering them unrecoverable without a decryptor and decryption key. The reason for this change is that it speeds up the encryption process, shrinking the window for detection and prevention.

In the APT universe, planting false evidence that points to other threat actors or countries is nothing new. Yet in the crimeware arena, this approach isn't as frequent. Digging through *Yanlouwang ransomware* [49] gang's leaked communications, researchers found details about the criminal operation and also were able to prove that its operators are Russian-speaking, not China-aligned as previously thought.

In our past reports, we mentioned one of the few ransomware gangs that did not shy away from targeting Russian organizations and extorting them for hefty sums – *OldGremlin* [50]. Further attacks by this group on several industries have been documented throughout 2022, setting a new record in extorted ransoms of USD 16.9 million.

TRENDS & OUTLOOK

The Russian invasion of Ukraine in 2022 drove a wedge between actors in the ransomware scene, dividing them into supporters and opponents of the aggression. While the rift led to catastrophic leaks, in some cases including source code and private conversations of the gang members, it also motivated the attackers to deploy increasingly aggressive methods, to insult their victims, and sometimes even to destroy their data.

Yet, these ideological fights did not influence day-to-day ransomware developments much. Most threat actors continued with the double-extortion scheme and compromised any company and organization that could afford to pay a ransom. Regular users remained mostly uninteresting for the ransomware scene, with the only exception being the owners of NAS devices. As for the amateurish ransomware attempts, 2022 was rife with these, with a large chunk of them being written in Python.

In 2023, we expect the saturated ransomware scene to become even more feisty and competitive, with tensions building between individual ransomware gangs – part of it due to ideological differences and disagreements. As defenders, we hope those clashes will lead to threat actors losing their focus and making mistakes that can be leveraged to create decryptors or, in the best-case scenario, lead to their arrest and prosecution.

Igor Kabina, ESET Senior Detection Engineer

DOWNLOADERS

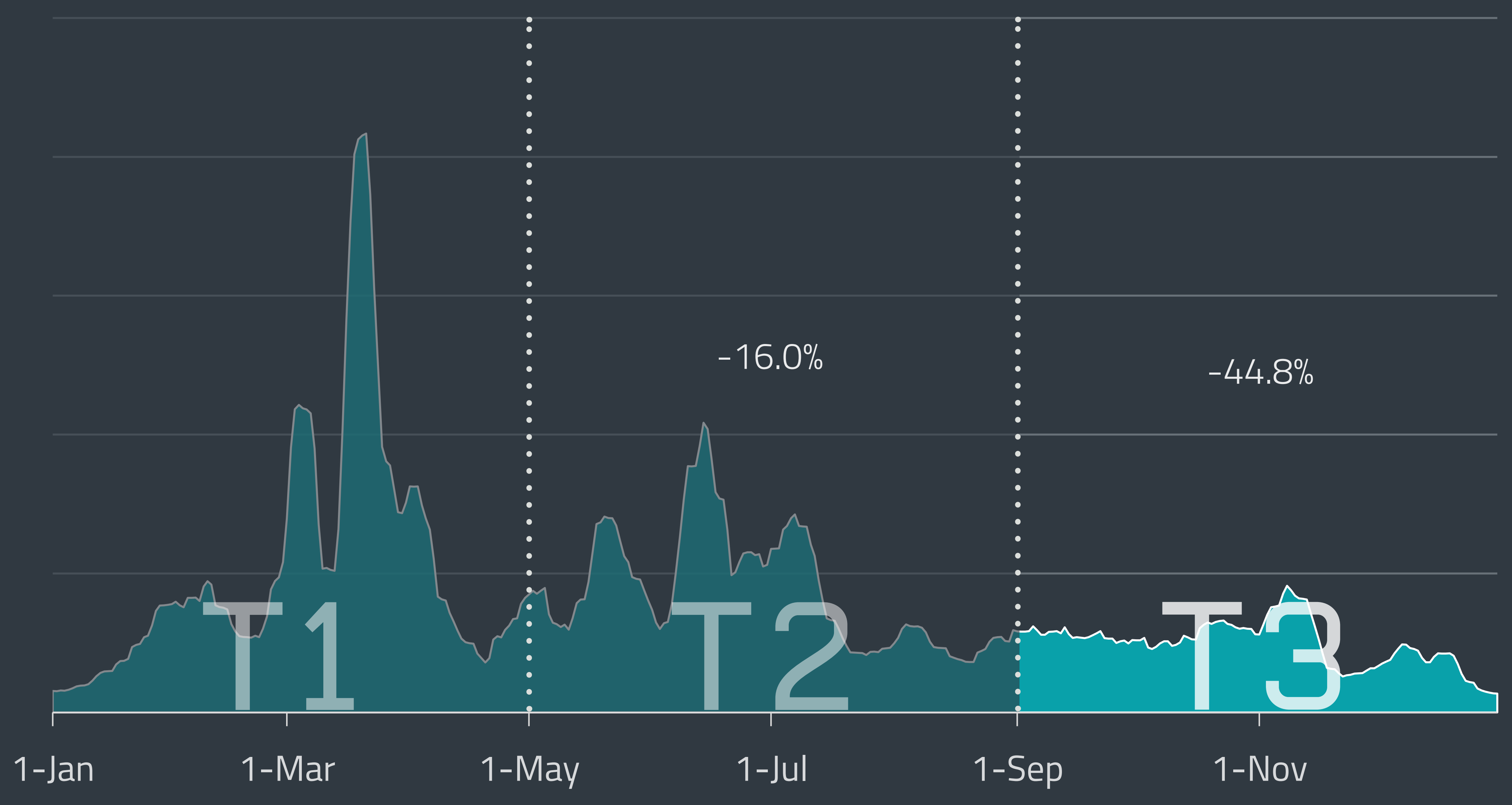
As Emotet sank to a whisper in T3 2022, dropping by 84%, MSIL downloaders took the lead.

T3 2022 in the Downloaders category brought an interesting flip. In T1 and T2, Emotet was the trend-setting malware family, responsible for most of the detections in ESET telemetry. However, this time around, it was the variants of MSIL/TrojanDownloader.Agent that led the pack with 37% of detections. Their activity was quite constant throughout T3, with the only visible slowdowns documented in November and in the last week of December.

The most prevalent variant of MSIL/TrojanDownloader.Agent was NKC, representing a downloader of Agent Tesla; this notorious spyware-for-hire allows its operators to exfiltrate victims' data and sensitive information, log their keystrokes, and control their cameras and microphones. Most of this activity was detected in mid September and at the beginning of October in Japan (14%), Turkey (14%) and Spain (10%).

The other major variants that followed – namely OFZ, NDX, OHG, OFQ and NHO – were collectively responsible for over 10% of this family's detections seen in T3 2022. These variants were key players in several malicious campaigns that downloaded an encrypted DLL injector (which posed as a JPG or BMP file) that led to a compromise by Agent Tesla, Fareit, or the MSIL/Agent.CFQ trojan. Most of this activity was observed in September and December in Japan (14%), the Czech Republic (14%), and Turkey (11%).

Emotet didn't go completely silent either, with an *update* [51] adding a new module that the infosec community named "hwinfo". It is designed to harvest additional information about the compromised device, enabling Emotet operators to vet the potential bot candidate before another data-harvesting module "systeminfo" is delivered. If both modules return satisfactory data, other Emotet modules can be downloaded. Based on the gathered information, botnet operators can be more precise in victim targeting, and also improve their detection of bots implanted by security researchers.



Downloader detection trend in 2022, seven-day moving average

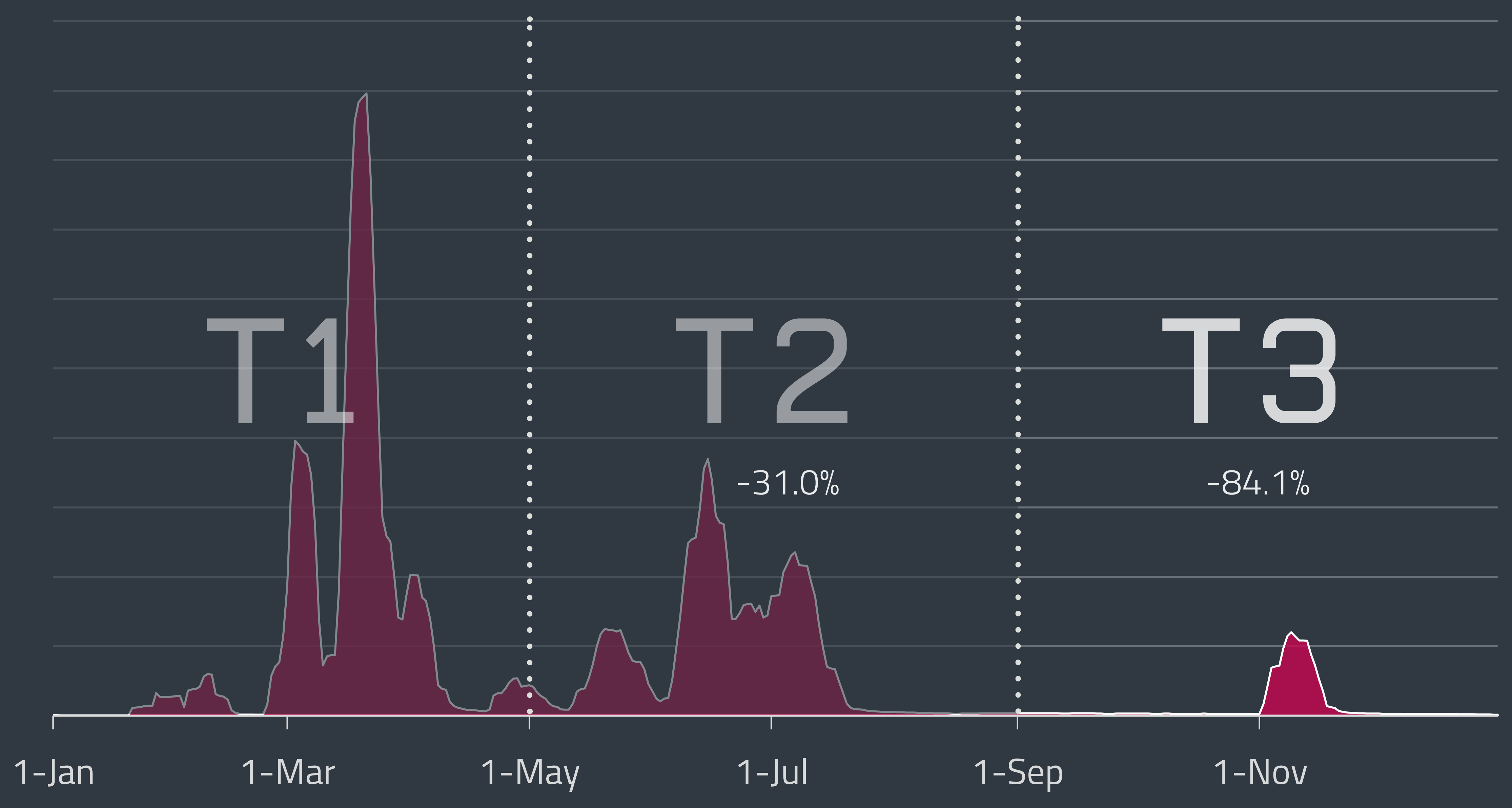
TRENDS & OUTLOOK

In 2022, Emotet came back in full force with large waves of malspam, mostly in the first half of the year. What soured its comeback was Microsoft's move to disable by default VBA macros from the internet. Cutting Emotet's favorite attack vector made its operators look for new ways to compromise their targets; their tests including LNK and XLL files. Based on their latest campaigns, they decided to go for weaponized Office files, most prominently spreadsheets.

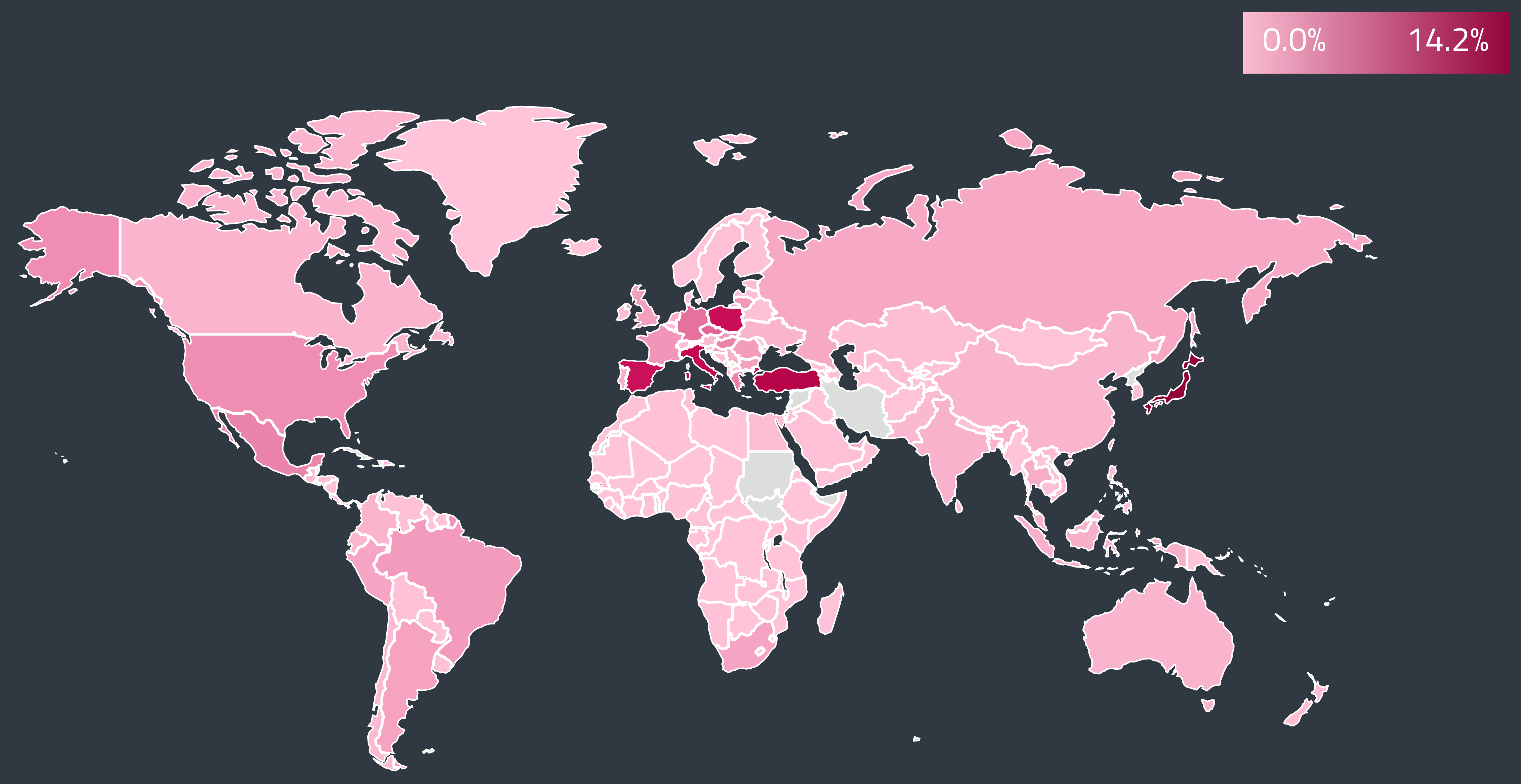
While the second half of 2022 saw only a single Emotet campaign, in November, it brought several updates to the malware itself. In T2, its authors added a new stealer module that can exfiltrate credit card details stored in Google Chrome, and returned an older spreader module. Another improvement came in October, when the new "hwinfo" module started harvesting additional information about the compromised machine, helping the operators to vet it before sending additional modules.

This shows that Emotet is still actively being developed by its authors, who would probably not invest so much time in a project they don't see a future for in 2023. This, however, doesn't necessarily mean it is going to be them who will keep control, especially if one is to believe rumors from social media that another threat group is trying to buy or has already bought Emotet and its infrastructure.

Jakub Kaloč, ESET Malware Researcher



Emotet detection trend in 2022, seven-day moving average

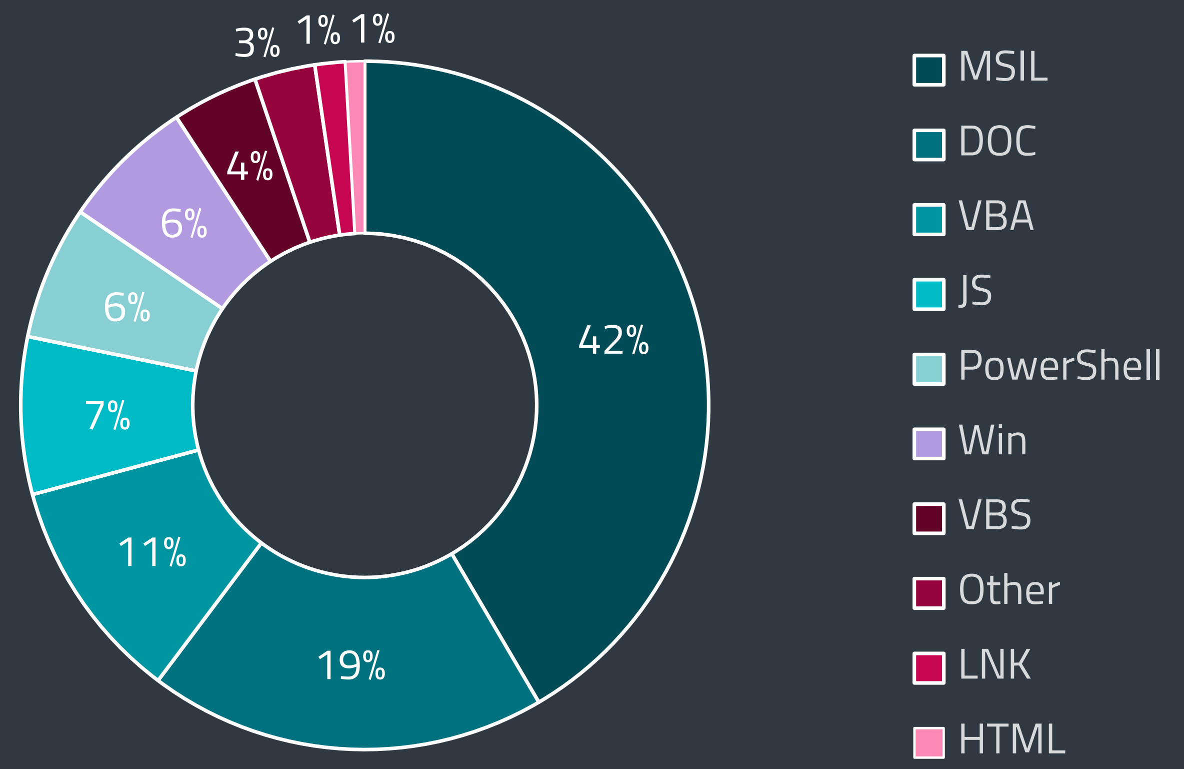


Global distribution of Downloader detections in T3 2022

While Emotet ramped up its activity in the first four months of 2022, it lost around 30% of its power in T2, and this trend continued into T3 2022, when it dropped by a further 84%. The only notable campaign that caused an uptick in ESET telemetry in this reporting period occurred between November 2 and November 14, with Japan (41%), Italy (7%), and Brazil (5%) being the top three targets facing most of the attacks.

These attacks used almost exclusively weaponized documents and spreadsheets attached to spam emails. Use of other intrusion vectors such as malicious LNK files – tested by Emotet operators in T1 and T2 2022 – and VBA macros, was negligible throughout T3 2022. As for final payloads, after Conti's demise, Emotet became the go-to delivery mechanism for several ransomware-as-a-service gangs, including *Quantum and BlackCat* [52].

Emotet's low activity in the last four months of 2022 has left its mark also on the types of detected downloaders. With a 42% share, MSIL detections were the most frequent type in T3 2022, a notable 19 percentage point jump compared to T2 2022. The second most prevalent type of downloader was weaponized Office files (DOC) – used almost exclusively by Emotet – accounting for 19% of blocked incidents, a drop of 25 percentage points. The once-leading VBA macros remained third but went up by 3 percentage points to 11%.



Downloader detections per detection type in T3 2022

CRYPTOCURRENCY THREATS

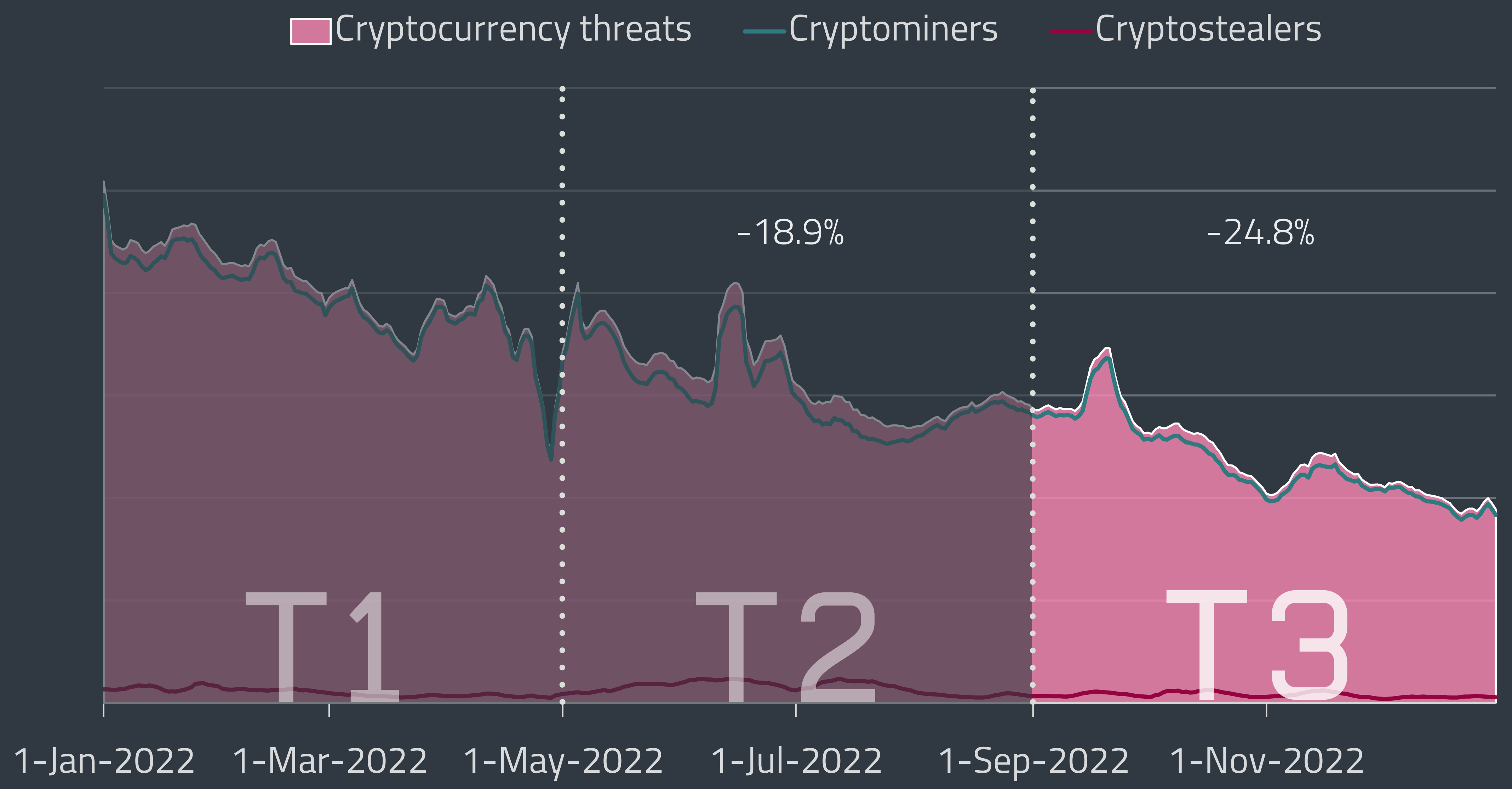
Bitcoin exchange rates, which are in a prolonged freefall, continued to drag cryptocurrency threat detections down with them.

Cryptocurrency threats finished 2022 the same way they started it: in a double-digit decline. The subcategory of Cryptominers, which went down by 23.6% in T3 2022, was impacted by plummeting cryptocurrency exchange rates on one side and soaring energy prices on the other. Even with their brief surge in T2 2022, Cryptostealers did not fare any better and registered a 48.7% decrease. Altogether, Cryptocurrency threats went down by 24.8% in T3 2022, their numbers falling almost by half when compared to 2021 (a 45.3% decline).

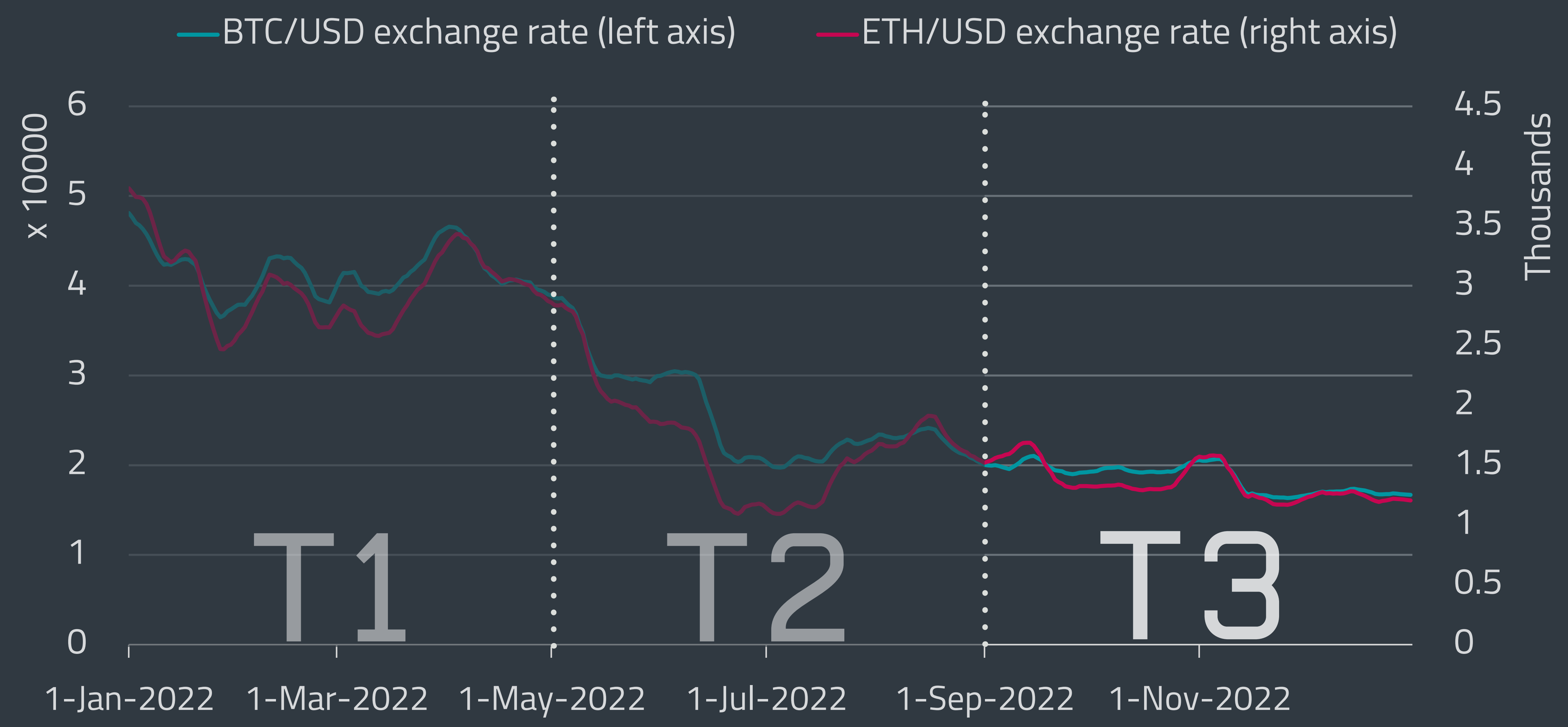
While the crimeware part of cryptocurrency-related threats looks to be way past its prime, cryptocurrency giveaway scams are rapidly gaining in popularity. As *revealed* [53] by Group-IB, just in the first half of 2022, the number of these scams tripled compared to the whole of 2021. In addition to that, the FBI *issued* [54] a public service announcement on October 3 warning of the rise in so-called pig butchering cryptocurrency investment scams. These schemes involve the fraudster gaining the victim's (i.e., the "pig's") trust and then enticing them into making regular deposits into crypto-investment accounts. Victims can usually track their investments on fake websites and apps that display dizzying growth. The operators of the scheme later proceed to the "butchering" part, which means cutting contact with the victim and disappearing with their cryptocurrency.

Looking at the Cryptominer threat detection trend in T3 2022, its journey downhill was nevertheless accompanied by a detection peak. It occurred on September 15 and was caused by a spike in the activity of several variants of the potentially unwanted application Win/CoinMiner. According to our telemetry data, the most prominent variants on that date were the IZ, QG, and RH variants, respectively, of the Win64/CoinMiner family. This family was generally active mainly in Russia, which was also the case on the day of the spike.

As before, the Win/CoinMiner PUA was the most detected cryptominer family in T3, despite experiencing a 23.3% decrease. Since potentially unwanted miners also cover software that users install on their machines willingly in order to obtain cryptocurrencies, this decrease is tied to the diminishing popularity of cryptomining among the general public.



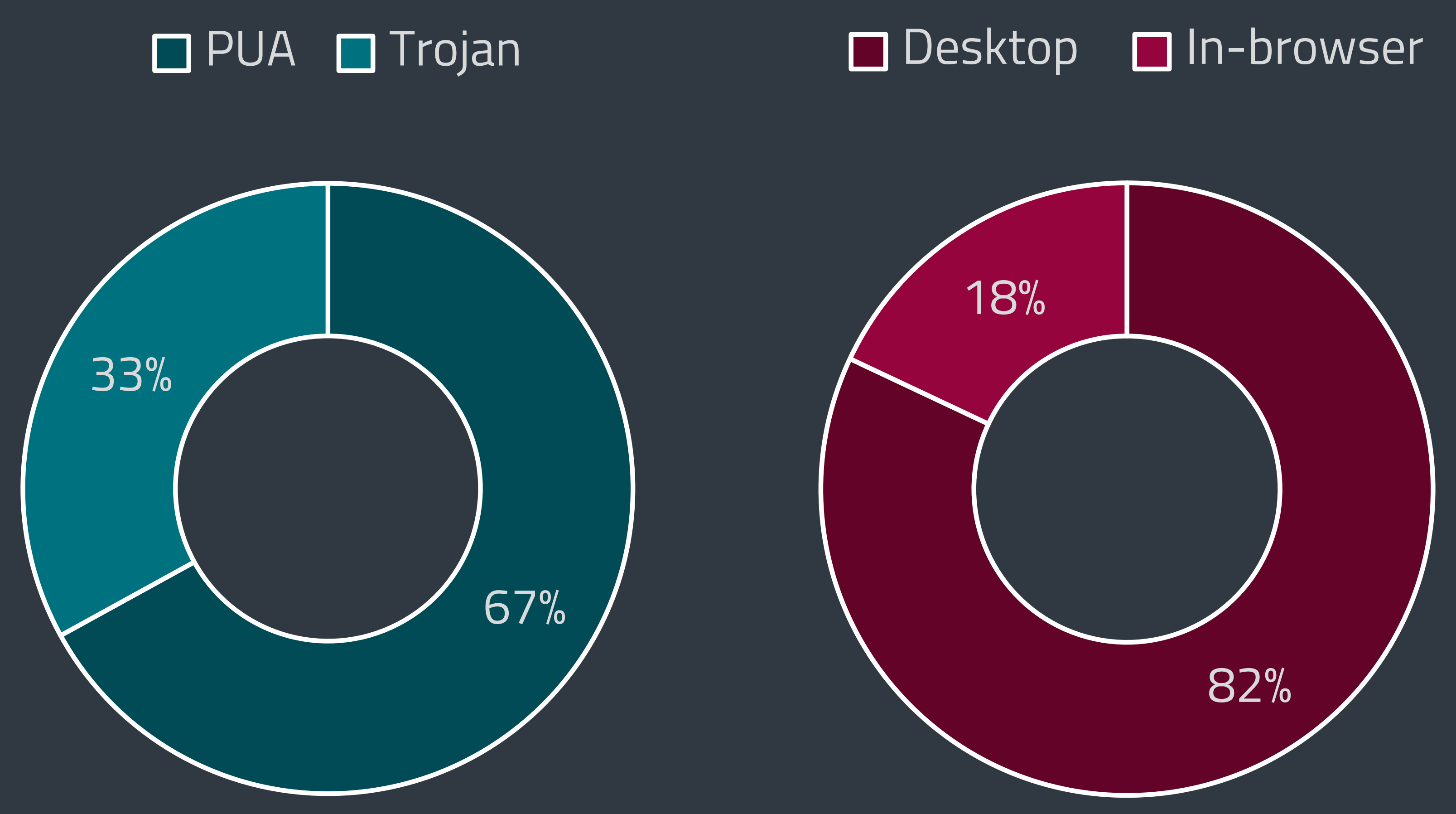
Cryptocurrency threat detection trend in 2022, seven-day moving average



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

	T3 2022	2022
1	webminepool[.]com	webminepool[.]com
2	mainevnap[.]com	mainevnap[.]com
3	monerominer[.]rocks	dl-x[.]com
4	dl-x[.]com	wypracowanie[.]edu[.]pl
5	wypracowanie[.]edu[.]pl	slovolam[.]sk
6	mituus[.]com	monerominer[.]rocks
7	slovolam[.]sk	mituus[.]com
8	cdnx.de2wa[.]com	carrierecalciatori[.]it
9	consit[.]ru	arafifblues[.]com
10	nursing-theory[.]org	cdnx.de2wa[.]com

Top 10 most visited cryptojacking domains in T3 2022 and 2022 overall



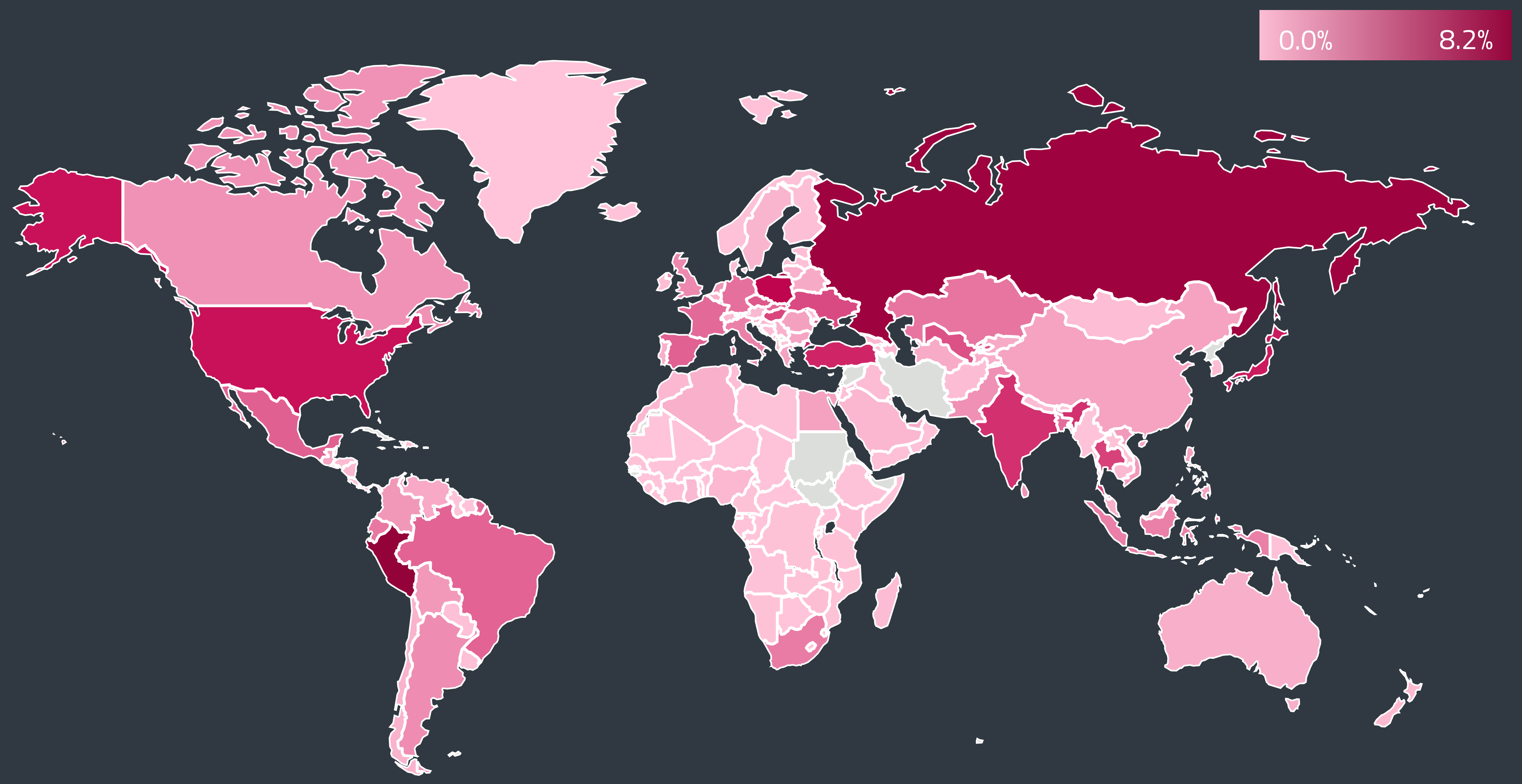
PUA:Trojan and desktop:in-browser ratio of cryptominer detections in T3 2022

The other two ranks in the top three also stayed the same, occupied by the Win/CoinMiner trojan with 13.3%, closely followed by the JS/CoinMiner PUA with 13%. These three families claimed the top three in the yearly statistics as well, the only change being the JS/CoinMiner PUA just barely beating the Win/CoinMiner trojan to second place.

Showing minimal changes when compared to T2 2022, the PUA:Trojan ratio in T3 2022 was 67% to 33%, and the Desktop:In-browser ratio, i.e., the proportion of cryptominers distributed as executables to those lurking in web browsers, was 82% to 18%. The number of cryptojacking domains in T3 also remained mostly unchanged in relation to T2, decreasing by only 4%.

The top-visited cryptojacking domain in both T3 and the whole of 2022 was `webminepool[.]com`, which promises visitors a way to earn money from their websites by putting in JavaScript mining code. It is basically another version of Coinhive, a service known for its rampant abuse in cryptojacking operations, which shut down back in 2019. Another such domain that appeared in both lists is `monerominer[.]rocks`, which was third in T3 and sixth in 2022.

It seems that the T2 surge in Cryptostealer detections was the exception that proves the rule; indeed that past 50% increase was swiftly undone by an almost equal 49% decrease in T3. This decrease also affected the culprit behind the rarely seen growth in this subcategory, PowerShell/PSW.CoinStealer. Despite dropping by 42.3% in T3, it managed to replace the Win/Spy.Agent trojan's cryptocurrency theft-focused variants as the most detected cryptostealer with 31.5%. According to ESET telemetry data, PowerShell/PSW.CoinStealer was mostly seen in Peru, India, and Bangladesh. In each of those countries, it made for more than half of their total cryptostealer detections for T3. As for the overall



Global distribution of Cryptocurrency threat detections in T3 2022

2022 top cryptostealer statistics, the PowerShell/PSW.CoinStealer trojan was in second place (20.2% of cryptostealers), even though it only appeared in our telemetry at the end of T1.

Second place in T3 was once again claimed by Win/PSW.Delf (24.5%), which had an overall stable number of detections when compared to T2. It was third in the overall 2022 chart with 19.4%. The Win/PSW.Delf trojan, specifically its OSF variant, was also responsible for the T3 cryptostealer detection peak from October 5.

The Win/Spy.Agent trojan—or more precisely, the several cryptostealing variants of this malware family that is otherwise much more prevalent among spyware detections – dropped by 63% and ended the year in third place, accounting for 22.2% of cryptostealers. Interestingly, even with the significant drop in numbers, this trojan detection experienced an upward trend (numerically) in T3, with its numbers picking up in the back half of the period. We registered most of its detections during the time of this surge in Peru, Mexico, and Bolivia. Despite the 63% decrease in T3, Win/Spy.Agent still managed to stay in the number one spot of the 2022 top list with 31.7%.

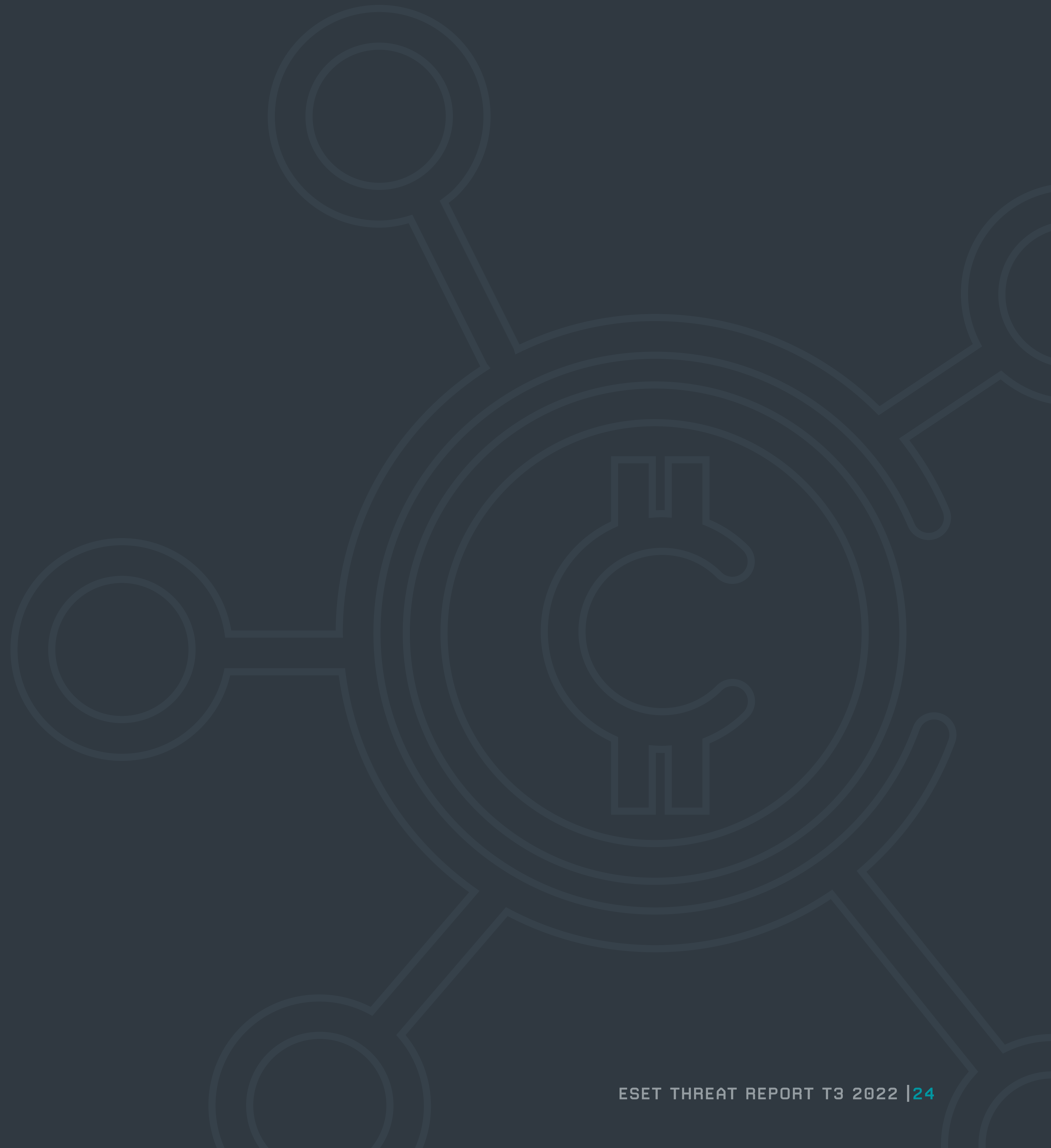
Peru was the country that registered the most cryptocurrency threats in T3 2022 (8.2%), followed by Russia (7.2%), and Poland (4.6%). As for the yearly statistics, Russia was first with 8.5%, Peru second with 7.5%, and the United States third with 4.5%.

TRENDS & OUTLOOK

It is very likely that the decline of cryptominers will continue into 2023. Cryptocurrency mining is no longer very interesting for cybercriminals; it has lost its profitability, even when taking over a large number of computers. Going after Ethereum is now completely out due to it adopting the proof-of-stake system.

The security of web browsers, such as malicious script blocking and plugin vetting, has been improving, which has in turn caused a decrease in in-browser cryptominers and cryptostealers. On the other hand, cryptocurrency-related scams and phishing have been going through a renaissance and will most probably continue to grow in 2023.

Igor Kabina, ESET Senior Detection Engineer



WEB THREATS

Cryptocurrency-themed phishing lures were on the rise; overall web threats continued their decline.

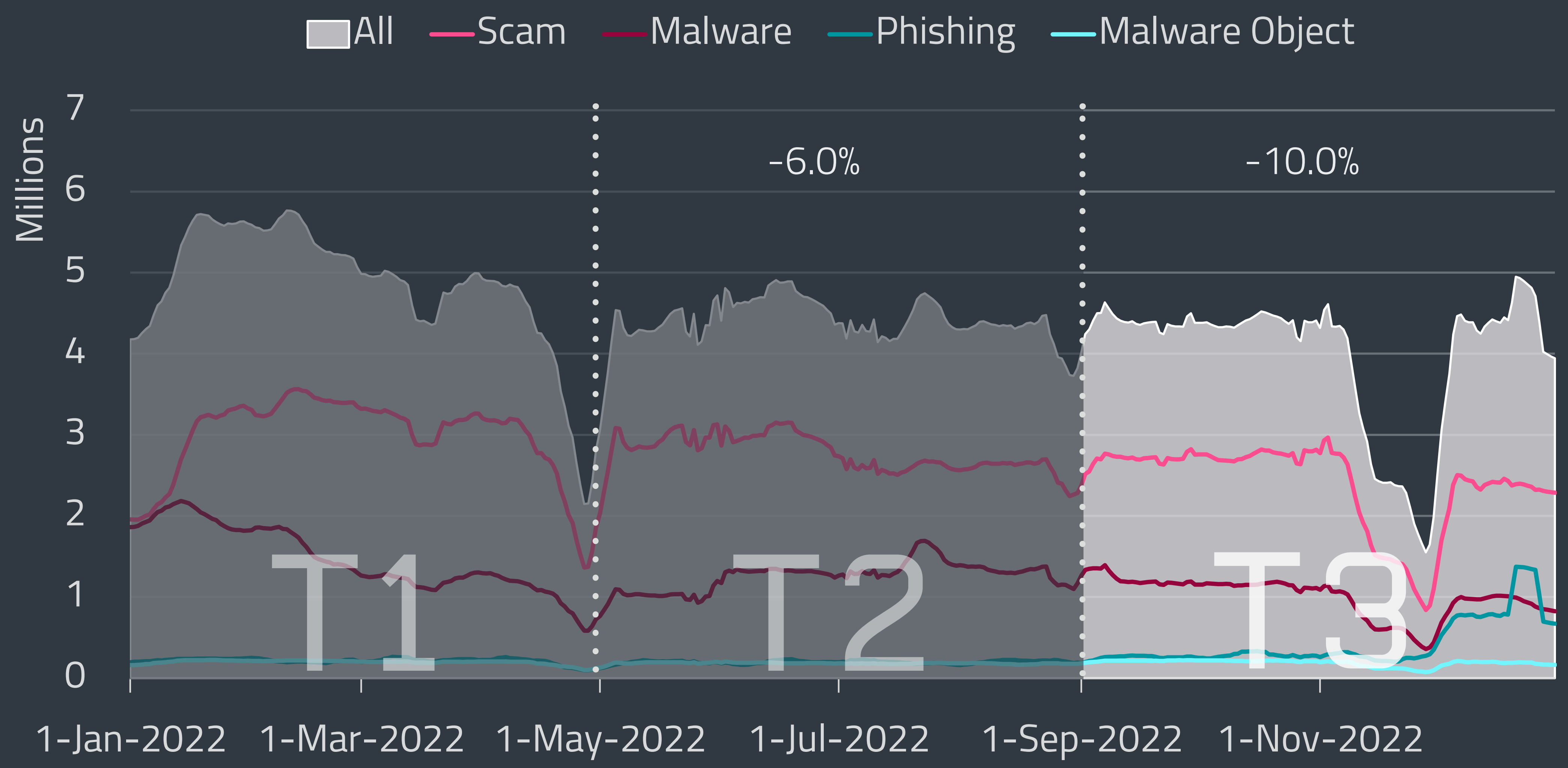
Continuing a trend that started at the beginning of the year, web threats ended 2022 in decline. In T3, the number of all blocked web threats went down by 10%, while the number of unique blocked URLs suffered a smaller, 5.9%, decrease. On the other hand, when comparing the statistics from 2021 to those of 2022, it was the unique URL blocks that fell more sharply – they diminished by 25.7% compared to all blocks, which suffered a 10.6% decrease.

The web threats trend chart shows an overall decreased amount of blocks in November in all subcategories apart from Phishing, which was the only subcategory to end T3 above where it was at the start. This category was also responsible for a spike visible in the overall web threat trend chart on November 21, when the number of phishing URL blocks exceeded three million. Altogether, ESET products blocked more than double the number of phishing websites in T3 2022 than in T2 – more specifically, these blocks went up by 114.6%.

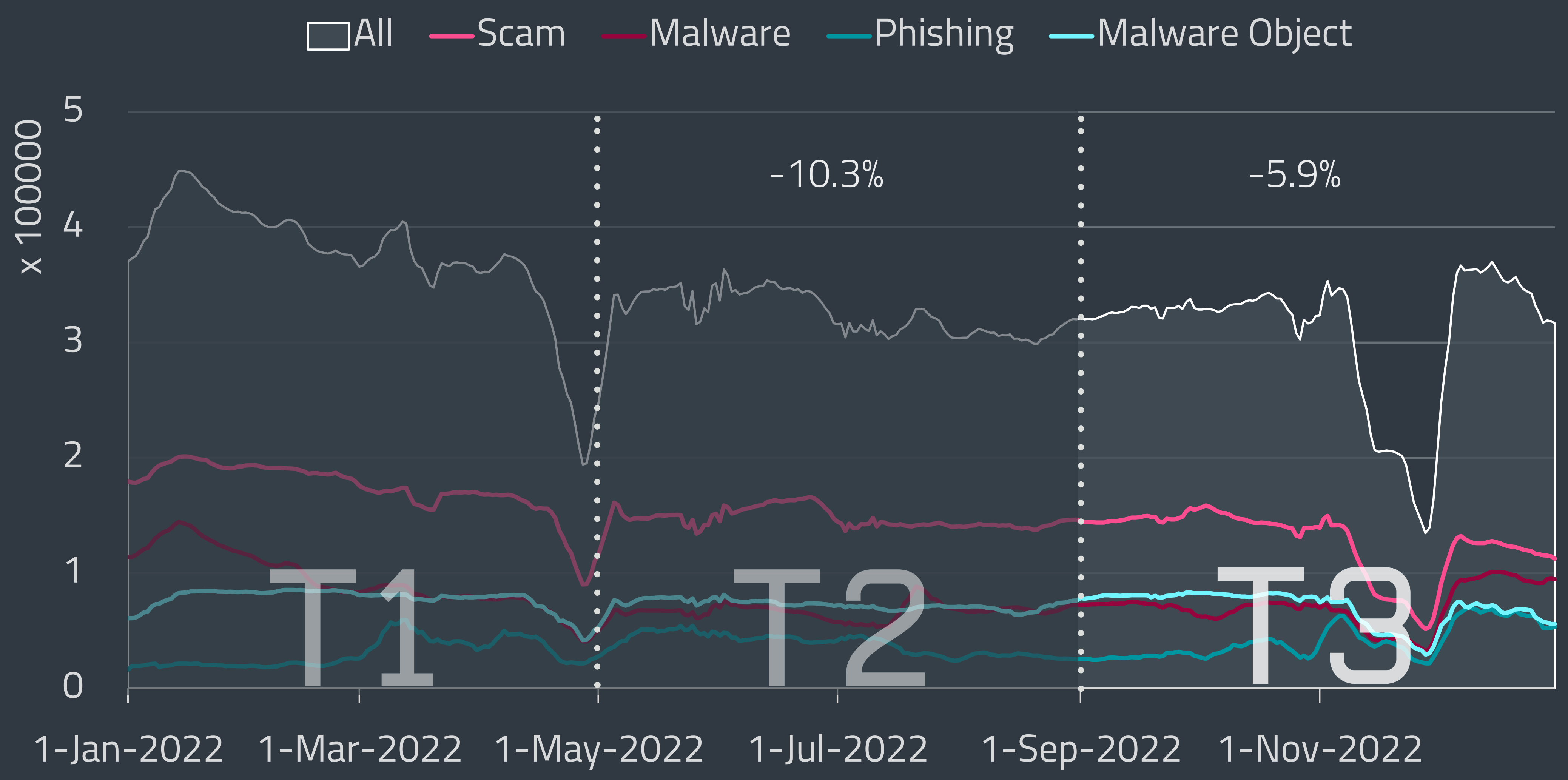
Even if we did not see a steep increase in the blocks of unique phishing URLs in T3 (just under 8%), yearly statistics reveal that our products blocked 80% more unique phishing websites in 2022 than in 2021, a total of over 13 million. At the same time, the number of total phishing website blocks in 2022 remained more or less equal to that of 2021.

	Malware	Scam	Phishing
1	aj2396[.]online	s.sarafan[.]fun	pogothere[.]xyz
2	d1ywb8dvwodsnl.cloudfront[.]net	survey-smiles[.]com	123w0w[.]com*
3	creepingbrings[.]com	alleviatepracticableaddicted[.]com	sjsmartcontent[.]org
4	inrhyhorntor[.]com	v.vfghe[.]com	prombid[.]com
5	webanalyser[.]org	grunoaph[.]net	furiousfar[.]com
6	jecromaha[.]info	tracking.eu.jod23jgo32[.]com	propu[.]sh
7	lephaus[.].net	mybetterck[.]com	mrproddisup[.]com
8	perljs[.]com	newrrb[.]bid	watchvideoplayer[.]com
9	wzhmg.shxusong[.]com	thenovosti[.]com	foreign-movies.baby-supernode[.]xyz
10	i.hhrspb7[.]top	serch07[.]biz	reklama.klimatyzacja[.]pl

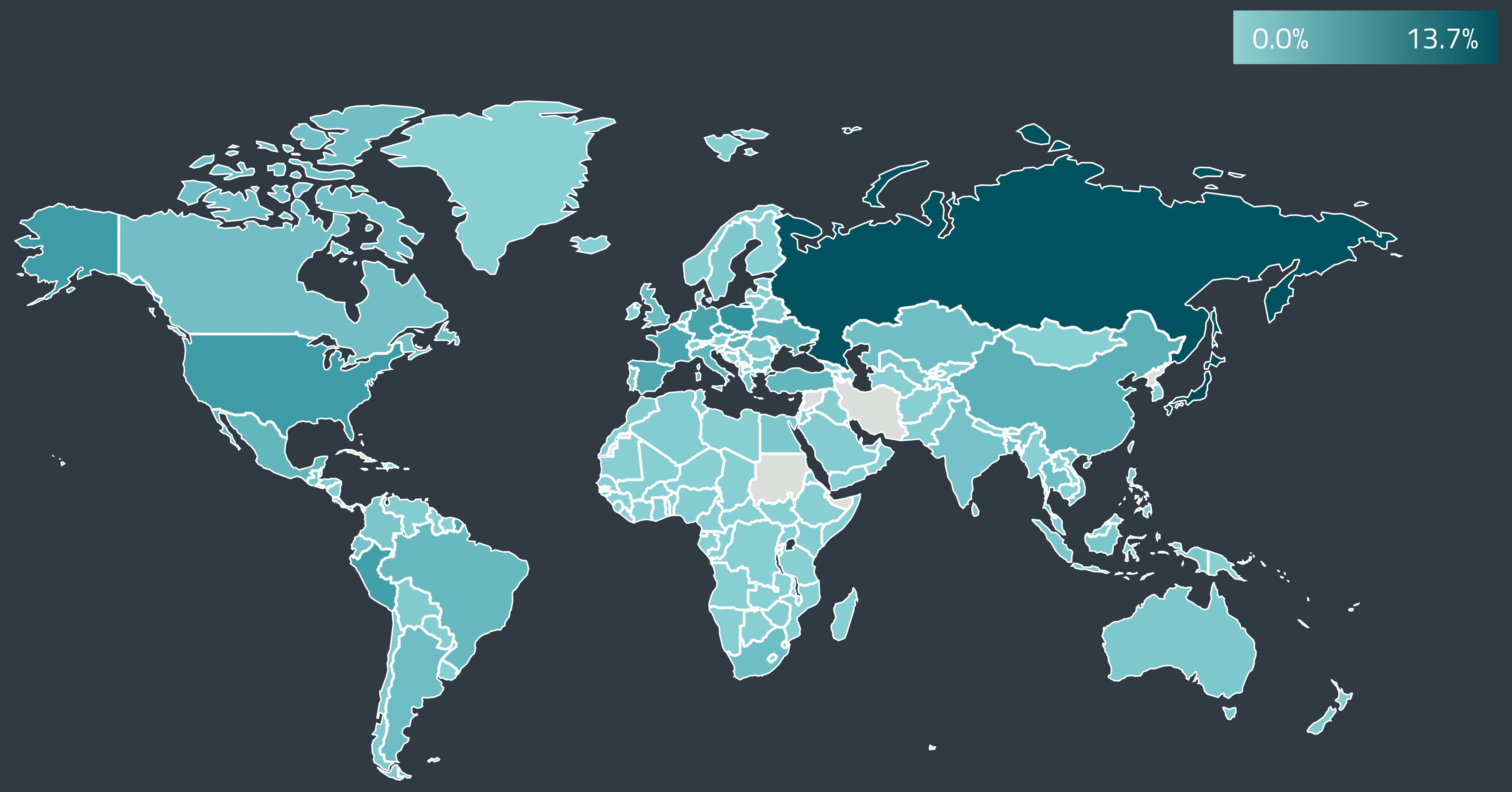
Top 10 blocked Malware, Scam and Phishing domains in T3 2022; domains first detected in this period are marked with *



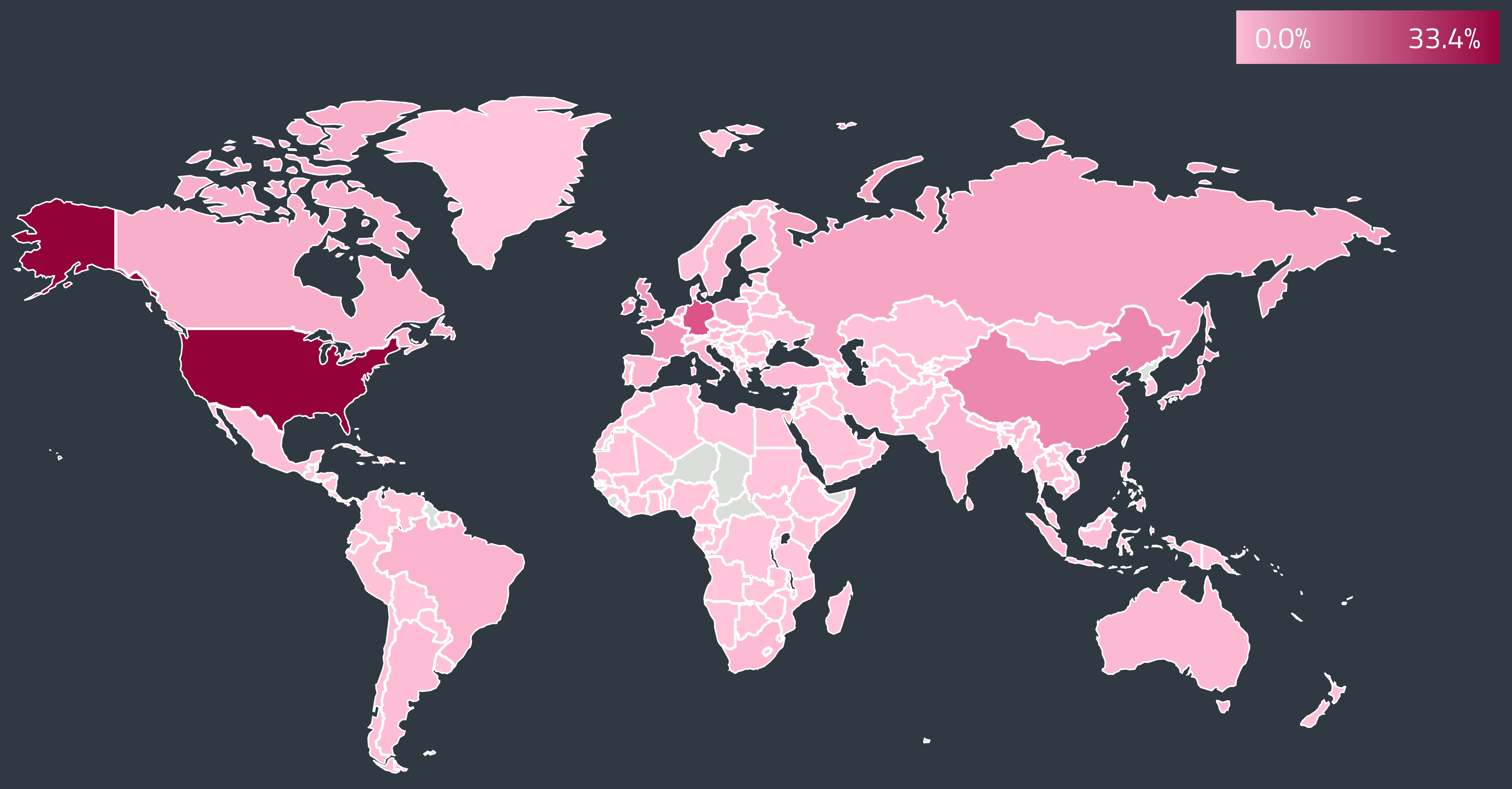
Web threat block trend in 2022, seven-day moving average



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



Global distribution of Web threat blocks in T3 2022



Global distribution of blocked domain hosting in T3 2022

As was the case throughout 2022, ESET registered the biggest decline in blocks in the Malware subcategory. This time, its overall number decreased by 21.7%, going from 1.2 million daily blocks on average in T2 to just under 1 million in T3. Year-on-year, it dropped by 30%. Although the number of unique malicious URLs in T3 show a slight increase of 5.5%, we saw 35.9% fewer of them in 2022 than the year before.

During T3 2022, ESET products encountered legitimate websites hosting malware (categorized as Malware object) at a relatively similar rate as seen in T2: the number of all blocks was basically unchanged, and unique blocks declined only slightly by 5%. Yearly, though, there is a definite decrease in both all and unique blocks, which went down by 29.5% and 25.2%, respectively.

The blocking of scam websites in T3 was down by 14.4% for all such websites and by 15% for unique scam URLs. The overall number of these website blocks did not change very much when compared to 2021, but the unique blocks decreased by 29.4%.

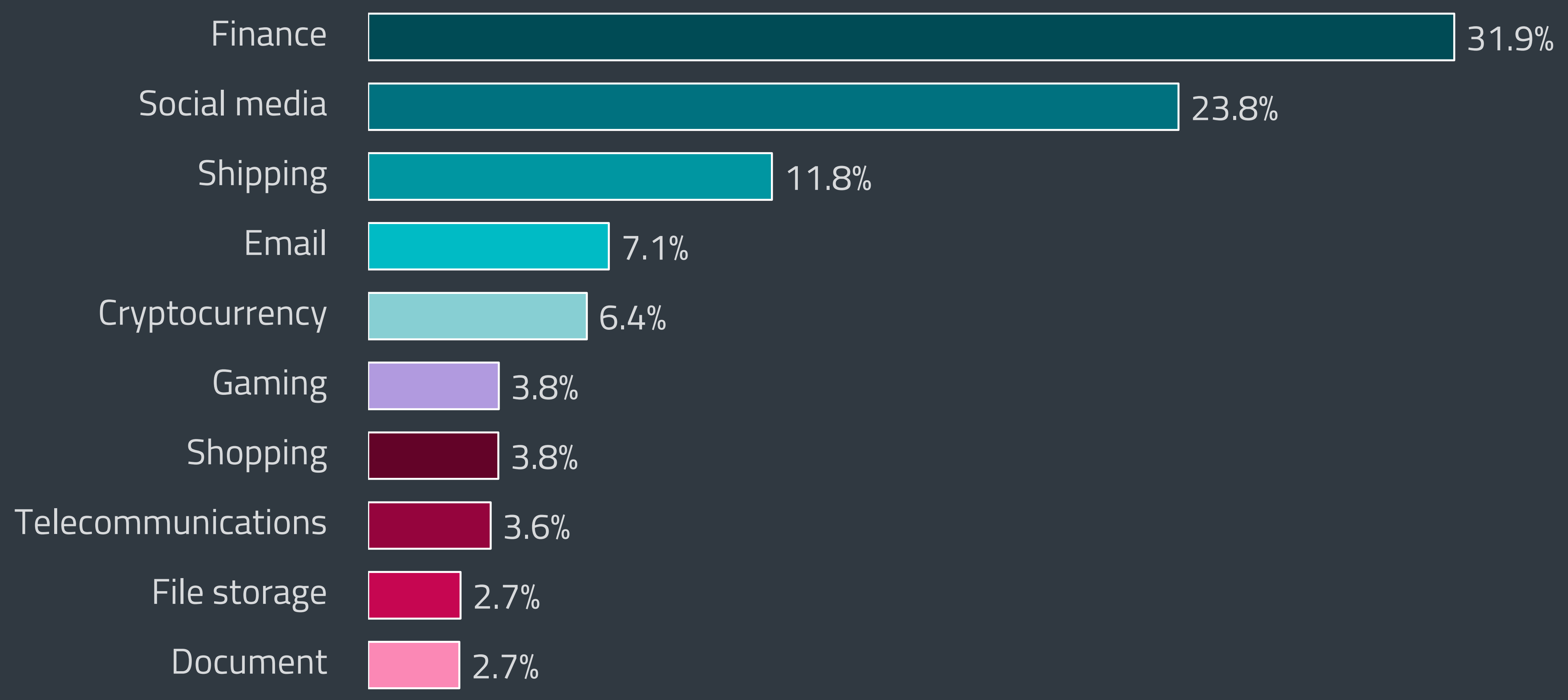
Malware, scam, and phishing domains that our products blocked the most frequently can be seen in the table on the previous page.

GeoIP tracking again shows that the US hosted the largest number of harmful domains in T3 2022, accounting for 33.4% of them. Hosting in other countries was much less popular: Germany, which was the second choice for web-based threats, was far behind the US with 10%. German numbers were in turn twice those of China, the third in the list, which was home to 5% of phishing, malware, and scam websites.

Looking at the countries that these threats targeted the most, we see that the unfortunate first place belongs to Japan, which faced 13.7% of all web threat attack attempts. Russia was not far behind with 12%, and the third-most targeted country according to our data was Poland with 4.4%.

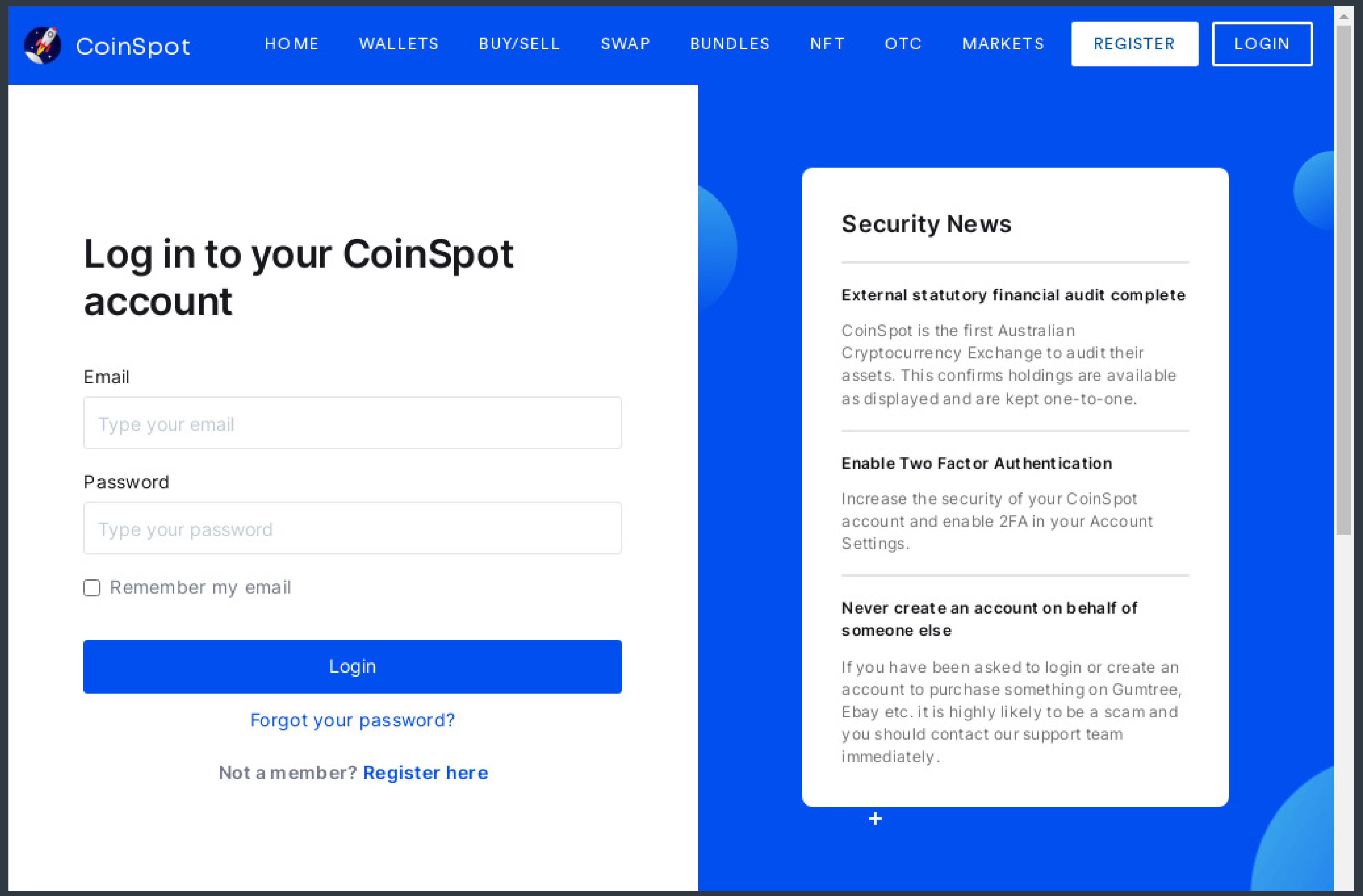
The categories of phishing websites that were the most prevalent according to ESET phishing feeds did not change much compared to T2. Finance, followed by social media and shipping, remained at the top of the most-impersonated list, each with about the same percentage of phishing URLs as in the previous period. Social media-related phishing websites were dominated by Facebook look-alikes, while the company to be the most spoofed in the finance sector was Bancolombia. As for shipping, DHL replaced USPS in T3 as the number one impersonated service.

More substantial changes in the top phishing categories based on unique URL counts happened in the slightly lower ranks. Cryptocurrency-themed phishing websites moved up a place to the fifth position, their numbers having increased by 62%. This is in line with the rising popularity of cryptocurrency-themed scams and phishing mentioned in the *Cryptocurrency threats* section.



Top 10 phishing website categories in T3 2022 by number of unique URLs[1]

In this category, ESET products blocked, among others, websites pretending to be the Australian cryptocurrency exchange CoinSpot, which were asking for user credentials. There were also several websites whose domains contained the word "tesla" while advertising fraudulent bitcoin giveaways and prominently displaying a photo of Tesla CEO Elon Musk. Examples of such websites include reytesla[.]com, teslaevents[.]net, and tesla-crypto[.]top.



Log in to your CoinSpot account

Email

Type your email

Password

Type your password

□ Remember my email

Login

Forgot your password?

Not a member? Register here

Security News

External statutory financial audit complete

CoinSpot is the first Australian Cryptocurrency Exchange to audit their assets. This confirms holdings are available as displayed and are kept one-to-one.

Enable Two Factor Authentication

Increase the security of your CoinSpot account and enable 2FA in your Account Settings.

Never create an account on behalf of someone else

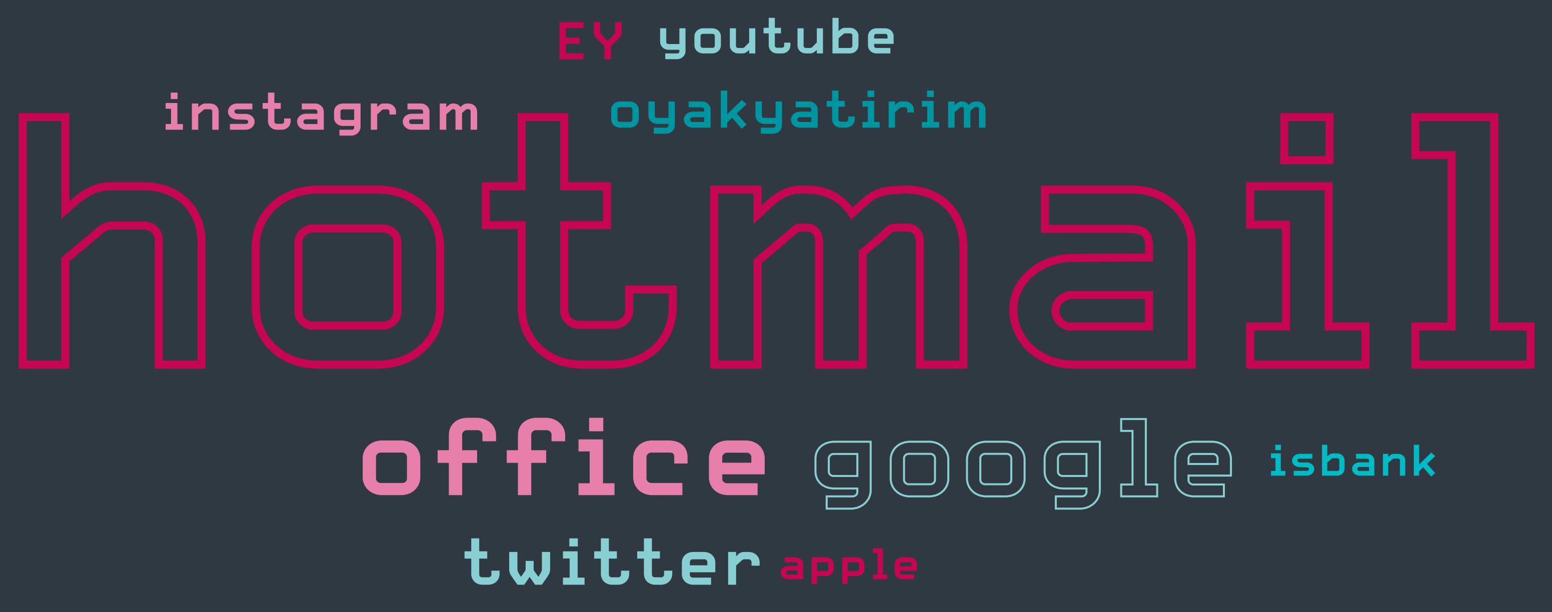
If you have been asked to login or create an account to purchase something on Gumtree, Ebay etc. it is highly likely to be a scam and you should contact our support team immediately.

Phishing website impersonating CoinSpot

Unsurprisingly, the Shopping category also increased quite considerably when compared to T2. It went from ninth to seventh place and shot up by 84%, as cybercrooks targeted people buying gifts for the year-end holidays.

Current events, such the World Cup 2022 in Qatar, continued to be abused as phishing lures. As ESET *warned* [55] in an article on the various scams that had been popping up even before the event started, it is always prudent to be wary of offers that sound too good to be true, and it especially pays to be vigilant during major occasions that attract a lot of attention. Phishing websites that we saw related to the World Cup included one that impersonated the official website of the championship and claimed to be selling tickets to the matches, as well as websites promising savings and free data plans, presumably as a special offer due to the event.

Homoglyph attack blocks were up by 58% when compared to T2 2022. However, the overall number of homoglyph domains in 2022, as opposed to 2021, was down by 52%. Domains impersonating Hotmail were the most numerous both in T3 and in 2022 as a whole. Even though first place in the top impersonated domain list remained unchanged, there were still two newcomers in T3: the first is a copycat of a Turkish finance company named Oyak Yatirim at oyakyatırım.com[.]tr, where both i's were switched for the dotless-i character, ı; the second domain impersonates another Turkish company in the finance sector, this time Türkiye İş Bankası, again, by replacing the i character with a dotless-i, in the address ısbank[.]com.



Top 10 brands and domain names targeted with homoglyph attacks in T3 2022

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

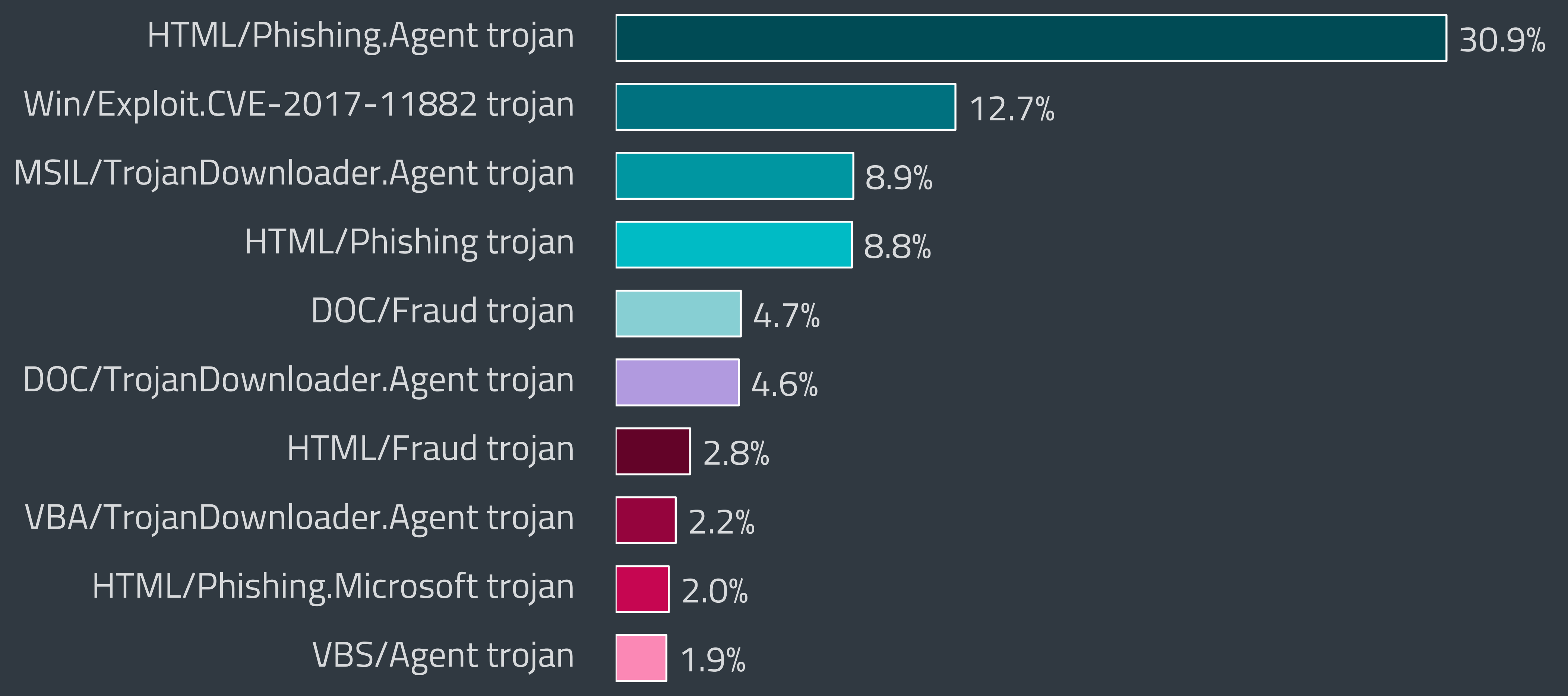
EMAIL THREATS

Email threats dropped by 17% in T3 but grew substantially in the yearly perspective.

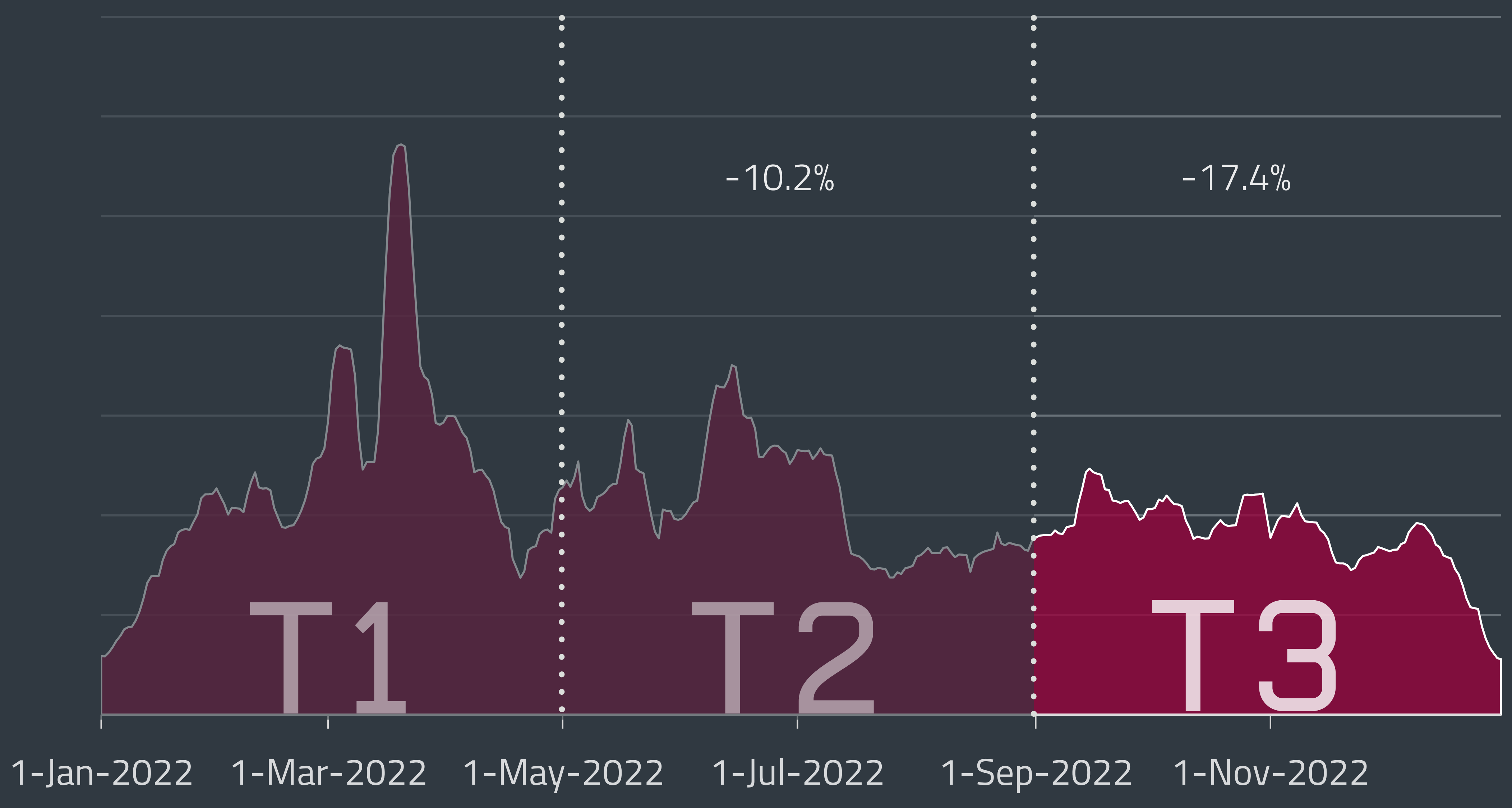
T3 2022 brought further deceleration in the Email threats department, with the whole category going down by 17%, following a 10% drop in T2. However, the yearly perspective shows that despite these negative figures, Email threats remain a significant danger growing year-over-year by almost 30%.

From the geographical view, most of the email threats delivered in T3 2022 landed in Japanese (12%), Spanish (8%), and Turkish (7%) inboxes. These three countries also dominated the yearly statistics, although the share of the attacks they had to withstand in those 12 months was much higher, with Japan at 46%, Turkey at 22% and Spain at 21%.

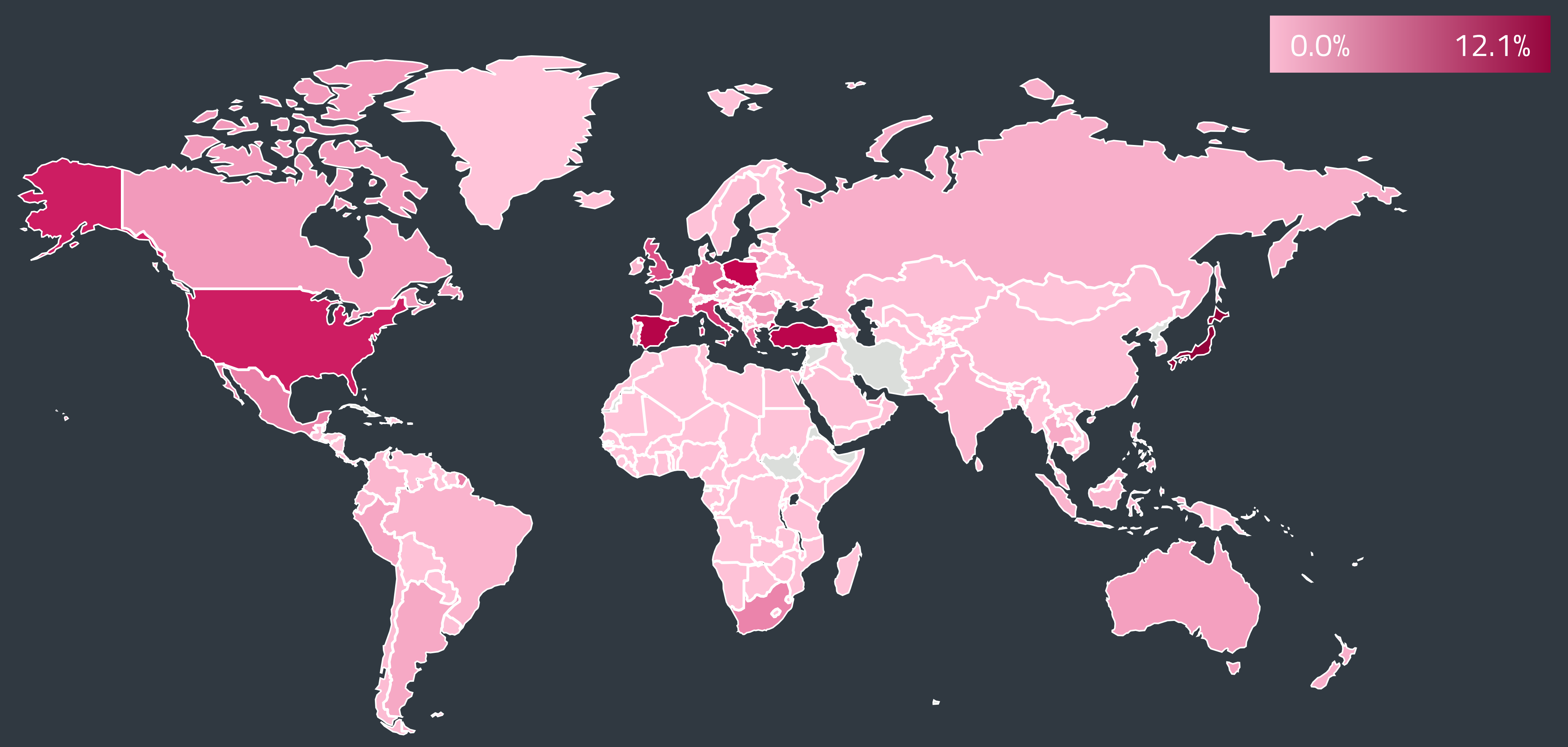
The top email threat of T3 2022, HTML/Phishing.Agent, increased its lead by 10 percentage points, accounting for 31% of all detections. Its most prevalent variant, HTML/Phishing.Agent.AUW, represents a malicious HTML attachment displaying a fake prompt of the local IT department, asking the recipients to provide or change their passwords. To lure the victims, the subject line of the message read "IT HelpDesk: Password expired", which was also the most frequent subject seen in malicious emails in T3.



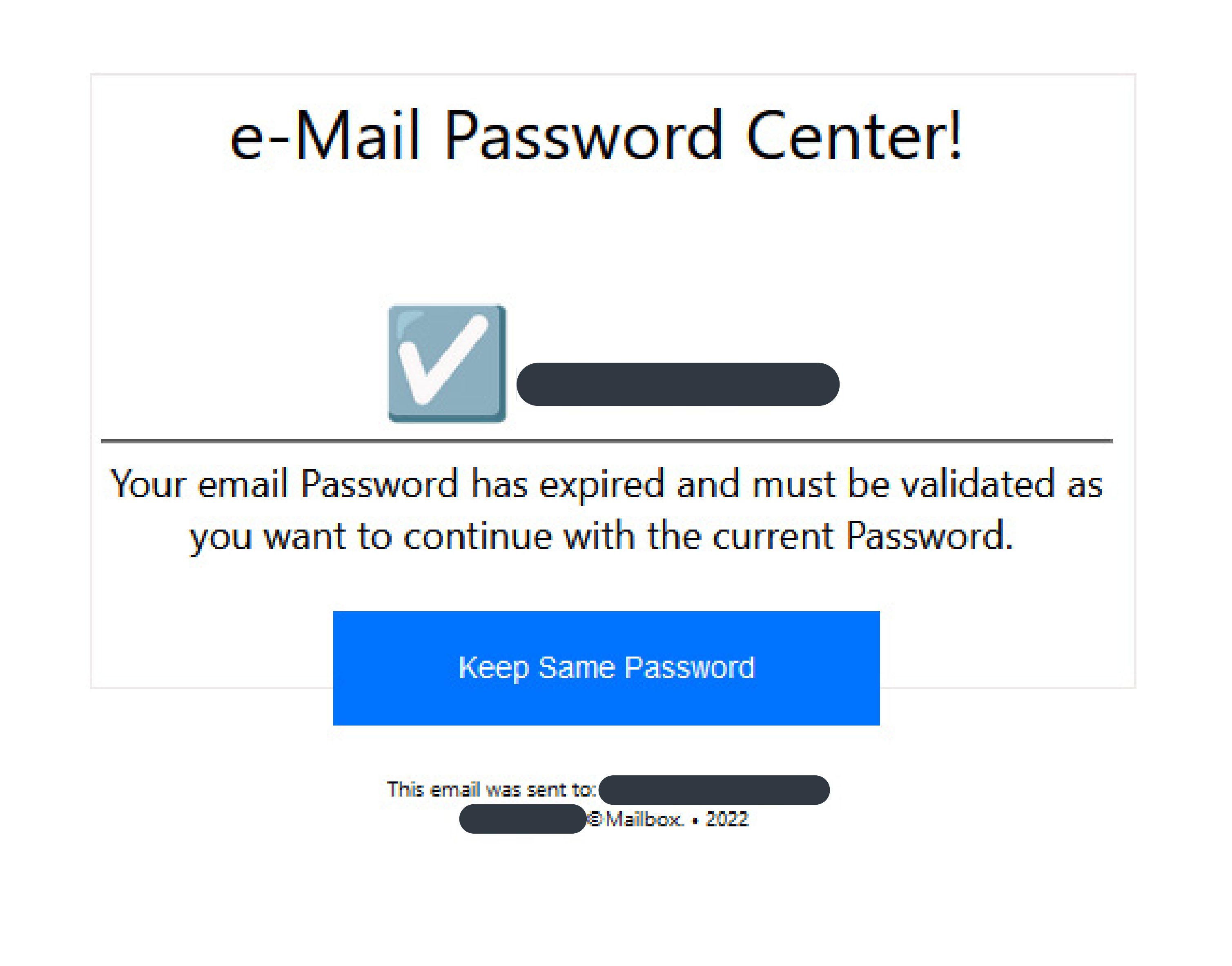
Top 10 threats detected in emails in T3 2022



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



Global distribution of Email threat detections in T3 2022



e-Mail Password Center!

☑ [redacted]

Your email Password has expired and must be validated as you want to continue with the current Password.

This email was sent to: [redacted]

[redacted]©Mailbox. • 2022

A fake IT department prompt requesting a password change, detected as HTML/Phishing.Agent.AUW

The share of the second most frequent detection, Win/Exploit.CVE-11882, shrunk from 17% to 13% in T3 2022. The decrease was seen globally, possibly caused by a takedown of malicious infrastructure or the operators abandoning the activity.

Looking at the most frequent variants of this threat, the C and F variants led the pack throughout 2022. The geographic distribution of these variants in the last 12 months was densest in Turkey, Poland, and Spain (10%, 9%, and 8%).

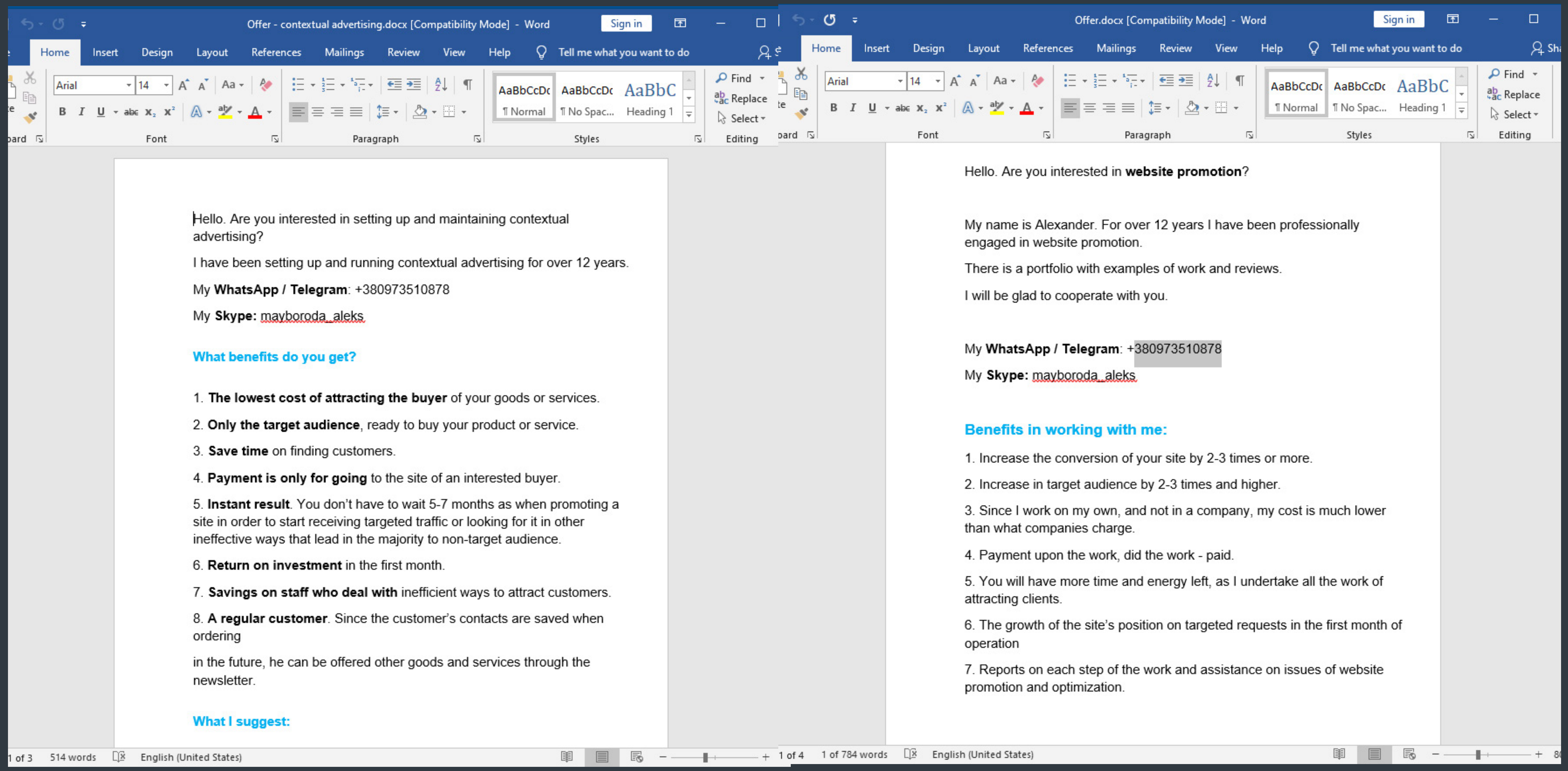
MSIL/TrojanDownloader.Agent – the third most prevalent threat in T3 2022 – grew its share slightly, with most of its activity documented in Turkey, Japan, and Spain. Typically, these are malicious messages that deliver a compromised attachment, which downloads an encrypted DLL injector posing as a JPG or BMP file. If executed, the final payload is delivered, most often Agent Tesla, Fareit, or the MSIL/Agent.CFQ trojan.

The Emotet botnet, which had a notable influence on the whole category in the first half of the year, ran only a small-scale campaign in T3 and thus did not cause an uptick in the detection trend. The inactivity of this botnet was reflected in the decline of weaponized Office files (DOC/TrojanDownloader.Agent), which sunk from 17% in T2 to 5% in T3 2022.

From the brand-specific phishing threats, HTML/Phishing.Microsoft was the only one that made it into the top 10. With 2%, it took the ninth position. While HTML/Phishing.Outlook was on its way up in T2 2022, its numbers crashed in the last four months of 2022, sending it down to twelfth place with just 1.3%. The following brand-specific threats – WeTransfer, Adobe, and DHL – all had detections below 1%.

The topics that malspammers gravitated most to were fake payment information, followed by bogus shipment and bank messages. T3 also saw a further decline in COVID-19 lures. Without the pandemic restrictions and lockdowns, travel replaced it as an increasingly popular malspam decoy.

The leading attachment names reported by ESET telemetry in T3 2022 were `Offer.docx` and `Offer - contextual advertising.docx`. Both are long-running scams detected as DOC/Fraud.ATU and both try to lure the victim to fake advertising services. They also seem to come from the same author, as they provided identical WhatsApp, Telegram, and Skype contact details.



Hello. Are you interested in setting up and maintaining contextual advertising?

I have been setting up and running contextual advertising for over 12 years.

My **WhatsApp / Telegram**: +380973510878

My **Skype:** mayboroda_aleks

What benefits do you get?

1. **The lowest cost of attracting the buyer** of your goods or services.
2. **Only the target audience**, ready to buy your product or service.
3. **Save time** on finding customers.
4. **Payment is only for going** to the site of an interested buyer.
5. **Instant result**. You don't have to wait 5-7 months as when promoting a site in order to start receiving targeted traffic or looking for it in other ineffective ways that lead in the majority to non-target audience.
6. **Return on investment** in the first month.
7. **Savings on staff who deal with** inefficient ways to attract customers.
8. **A regular customer**. Since the customer's contacts are saved when ordering

in the future, he can be offered other goods and services through the newsletter.

What I suggest:

Hello. Are you interested in **website promotion**?

My name is Alexander. For over 12 years I have been professionally engaged in website promotion.

There is a portfolio with examples of work and reviews.

I will be glad to cooperate with you.

My **WhatsApp / Telegram**: +380973510878

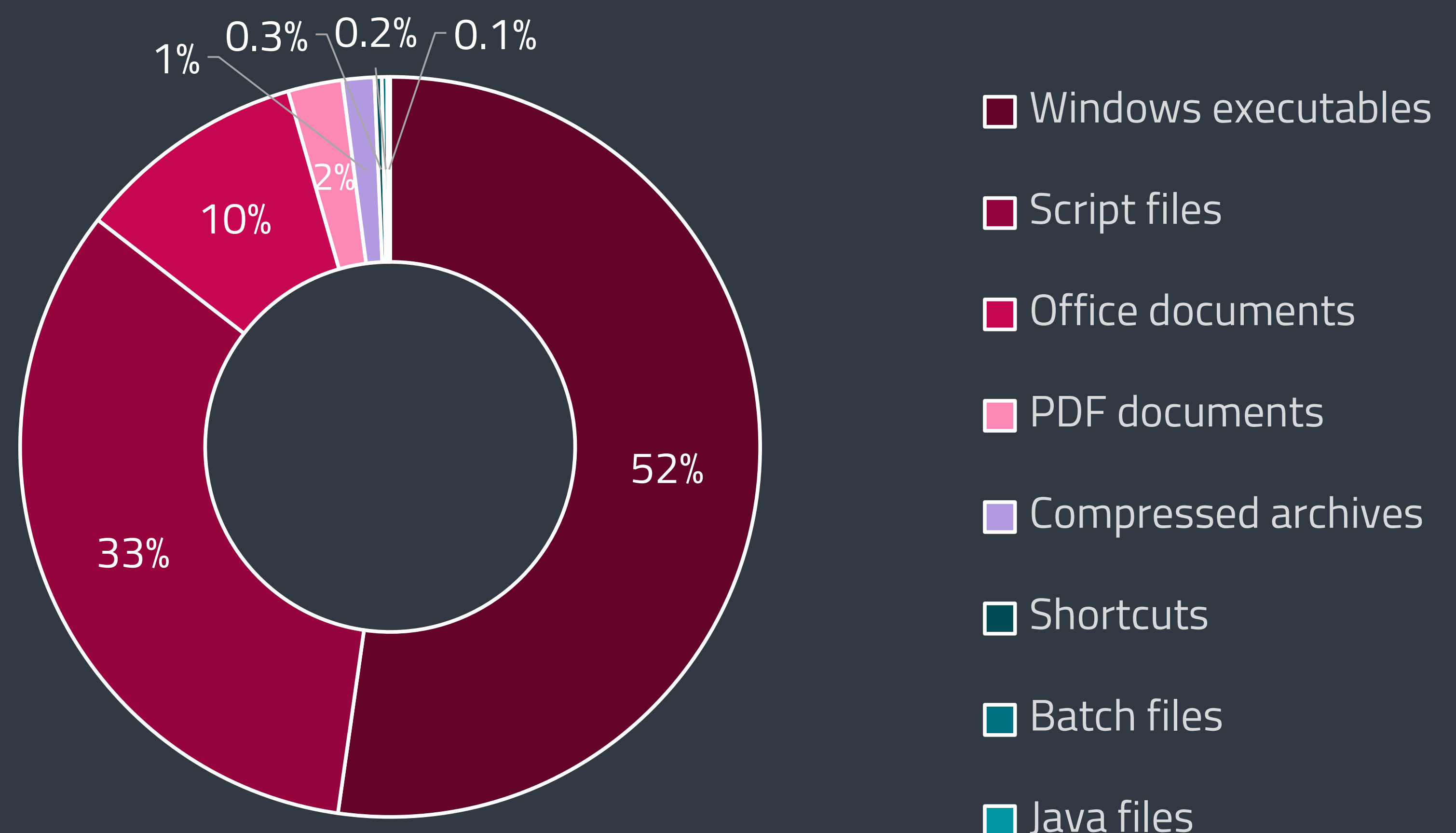
My **Skype:** mayboroda_aleks

Benefits in working with me:

1. Increase the conversion of your site by 2-3 times or more.
2. Increase in target audience by 2-3 times and higher.
3. Since I work on my own, and not in a company, my cost is much lower than what companies charge.
4. Payment upon the work, did the work - paid.
5. You will have more time and energy left, as I undertake all the work of attracting clients.
6. The growth of the site's position on targeted requests in the first month of operation
7. Reports on each step of the work and assistance on issues of website promotion and optimization.

Advertising scams that seem to have the same author, since they provide identical contact details

Windows executables remained the most prevalent malicious attachment type in T3 2022, increasing their lead by 5 percentage points to 52%. The second-placed script files went up by twice as much, namely 10 percentage points, and were seen in 33% of detected email threats. Due to Emotet's low activity (see *Downloaders*), Office files headed in the opposite direction, dropping from 19% to 10%.

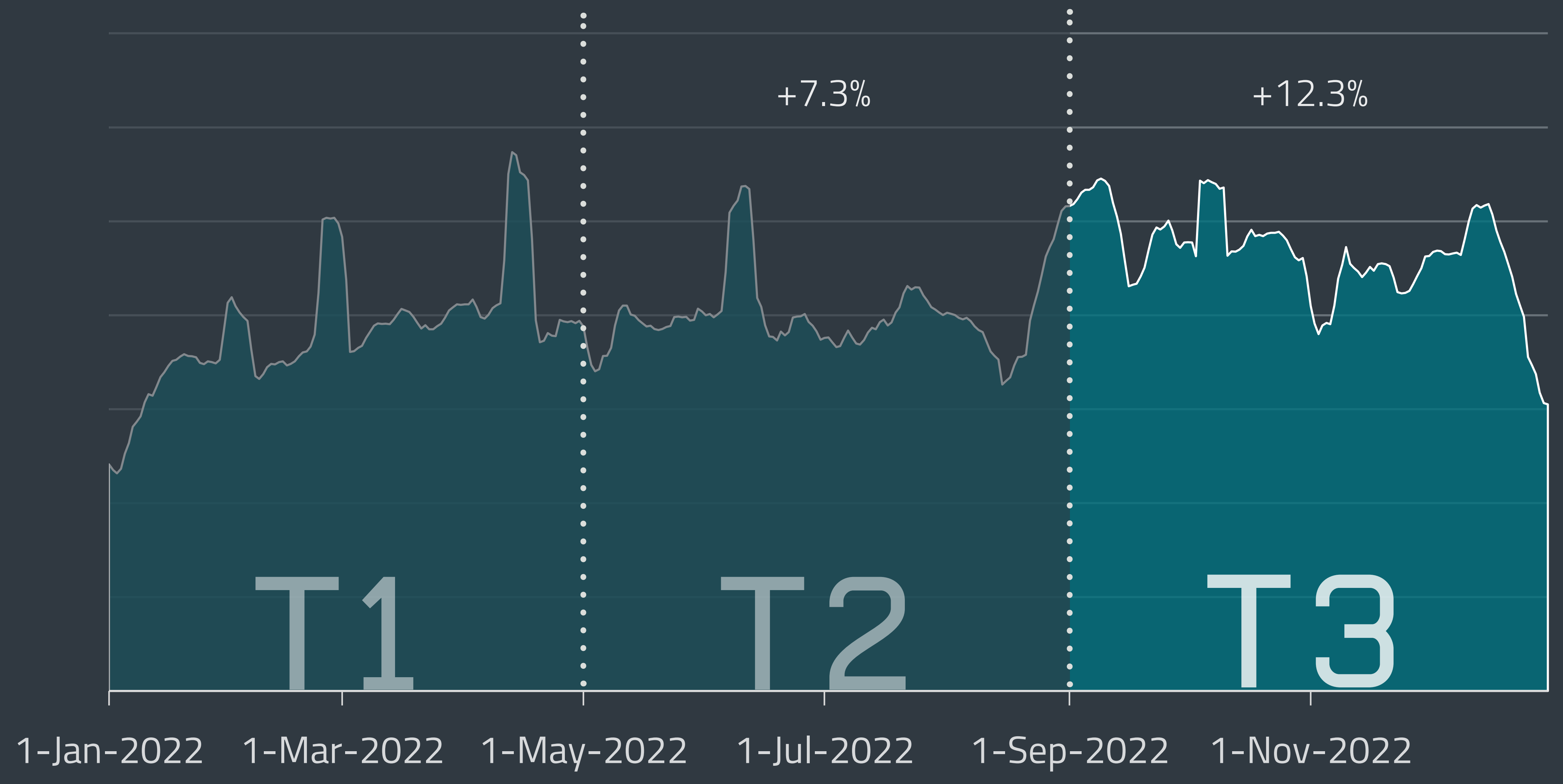


Top malicious email attachment types[2] in T3 2022

Spam increased by 12% in T3 2022, shifting into a higher gear, when compared to the 6% and 7% growths in T1 and T2. The volume of unsolicited emails rose to new heights at the end of August and kept pace almost until the end of 2022, probably due to this season of the year being associated with intense online shopping and frequent sale offers. The upward trajectory also translated into the year-over-year difference, which reached 14.5%.

With 19%, the United States retained its lead as the biggest originator of spam, followed by China with 16% and Japan with 11%. Looking at the T3 2022 share of spam in all emails sent, China remained in the lead with 77%. In a distant second Russia reached 33%, followed by Singapore, where the ratio improved from 41% in T2 to 26% in T3 2022.

Note that ESET's visibility into spam is limited due to email traffic commonly being filtered at other levels, including at the internet email service provider, before reaching ESET-protected endpoints.



Spam detection trend in 2022, seven-day moving average

TRENDS & OUTLOOK

Email is expected to remain one of the top distribution vectors for malware as long as this approach yields results. As confirmed by our data, it still does, and it will probably continue to over the long term.

The main lures used to spread threats via email will also remain largely the same, with the majority posing as generic purchase orders, shipment notifications, and bank payments. These will occasionally be augmented by trending topics from world news and social media that could be attractive to broad audiences, such as the COVID-19 pandemic, the war in Ukraine or the World Cup 2022 in Qatar.

Jiří Kropáč, ESET Director of Threat Detection

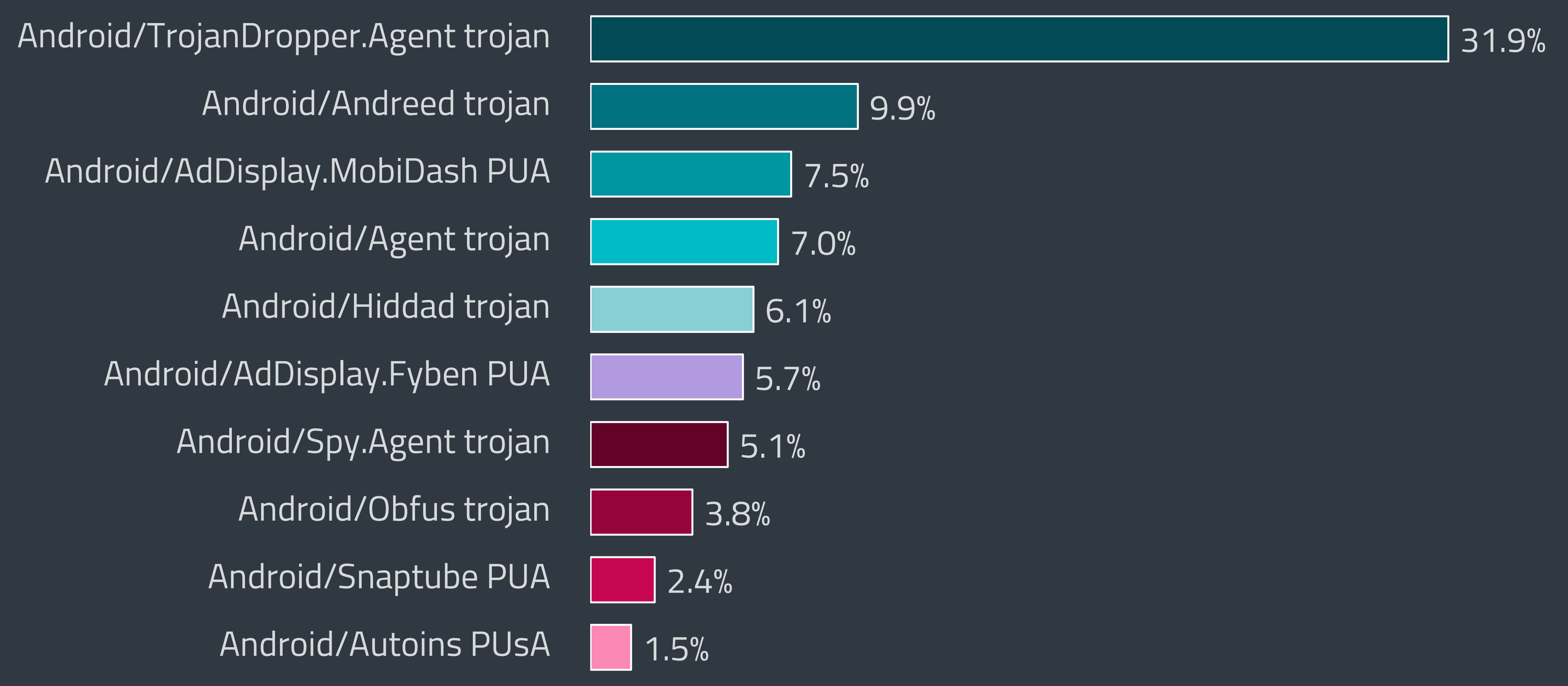
[2] The statistic is based on a selection of well-known extensions.

ANDROID

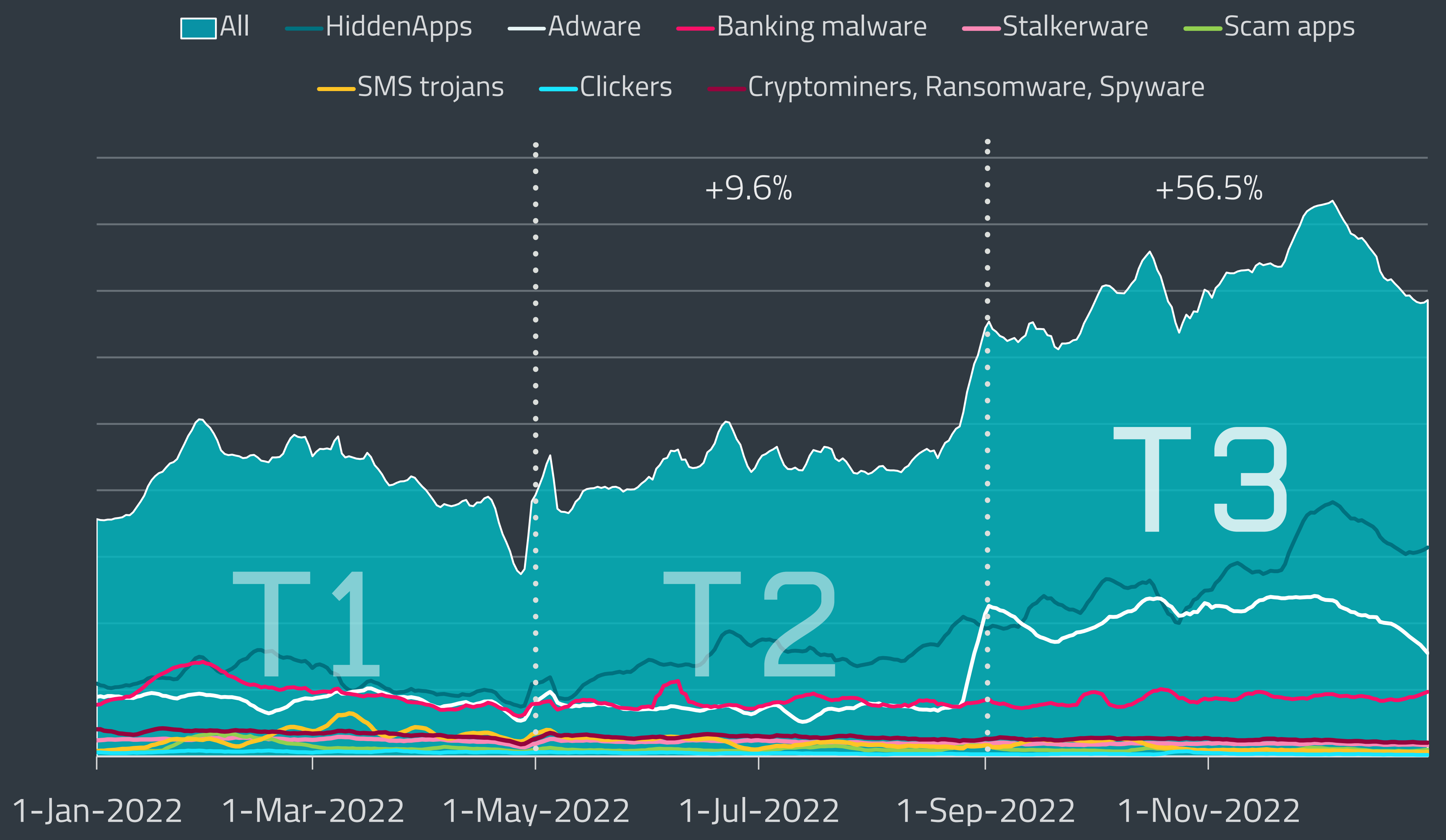
Android detections rose by more than 50% in T3 2022. Nearly 70% of all detections were attempts at making money from various forms of advertisement.

Overall detections of Android threats rose noticeably in T3, by 56.5%, with Adware and HiddenApps being responsible for the biggest share of this growth. Even though toward the end of December its trend chart showed a decrease, Adware grew significantly (by 163.2%) in T3. In the top 10 Android detections, this category is represented by AdDisplay.MobiDash PUA, AdDisplay.Fyben PUA, and Snaptube PUA.

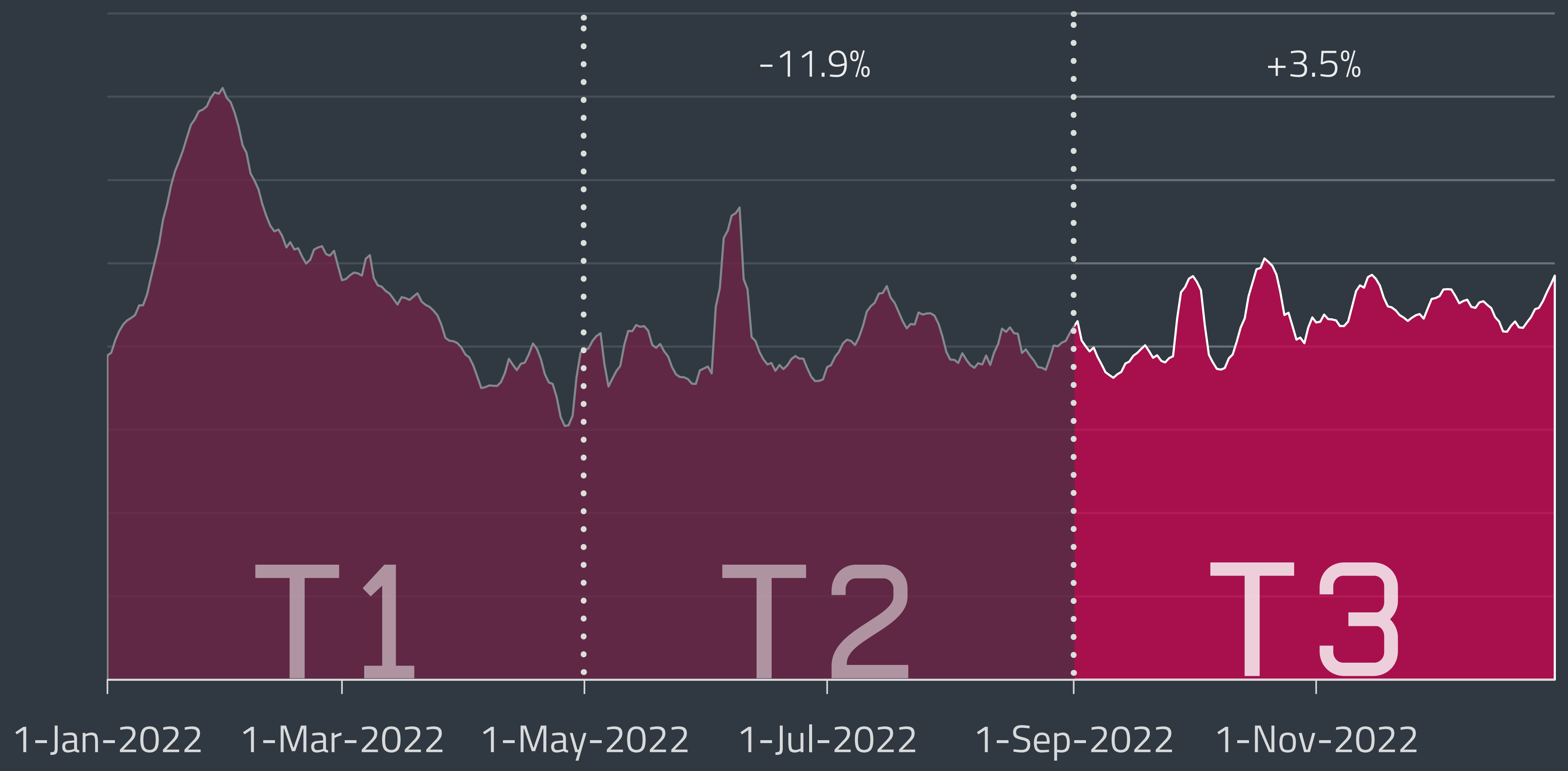
All of these detections are mostly present at third-party stores, packed together with legitimate apps, which is why they are flagged as Potentially Unwanted Applications (PUAs) – the user wants a specific app but is not warned that the cost for it will be paid by watching ads. Behind the growth of Adware is specifically Fyben; compared with T2 it grew by more than 1100% in T3! This detection is packed mostly with mobile games and T3 covers a period of time when developers release new or updated versions of their games to ride on Christmas sales, which could be the reason why this detection grew so much. ESET telemetry saw most Fyben detections in Ukraine, Mexico, Brazil, Russia, and Turkey.



Top 10 Android detections in T3 2022 (% of Android detections)



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



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

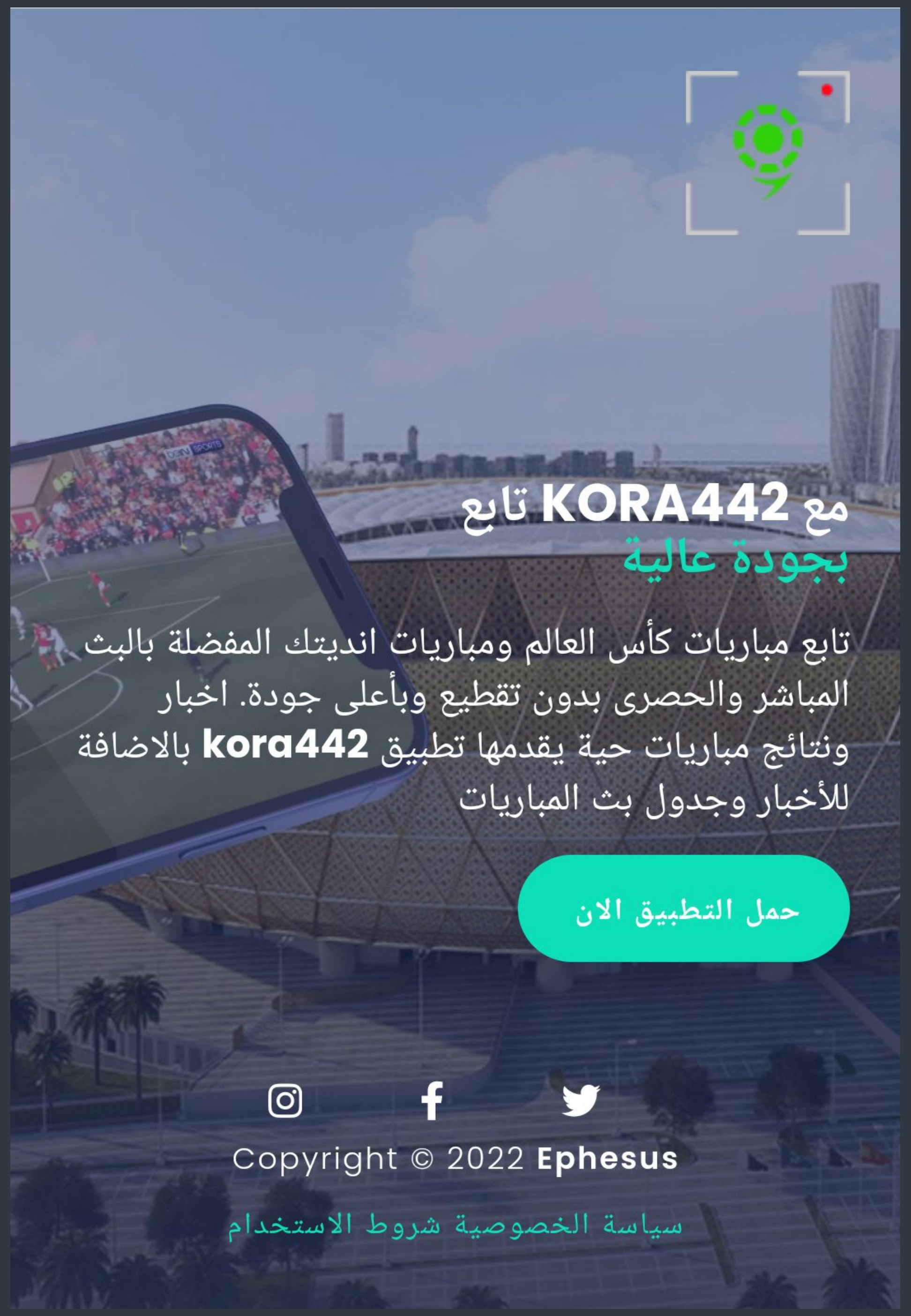
Developers of some mobile games might not make them available in these countries, so people living in them look for these games on unofficial stores or websites, where they are readily available.

Detections of HiddenApps also rose considerably in T3, by 82.9%. This type of Android threat represents deceptive apps that hide their own icons, then stealthily display ads, and in the hands of a less experienced user can be difficult to uninstall. In the top 10, this category is represented by Android/Hiddad in fifth place, which like Fyben is related to gaming apps.

Another category that is turning a profit for cybercrooks, via online ads, is Clickers. They are not as intrusive as HiddenApps; they open ads and click on them only in the background, cashing in money from the advertisers without any consumers actually watching them. Victims of Clickers, therefore, see no visible signs that they installed something on their devices that they shouldn't have, but Clickers can affect a device's performance and internet usage. In some cases, Clickers also show standard pop-up ads. This category saw a 20.9% drop in detection numbers in T3. However, if we count together the detections of all categories living off ads, their share of all Android detections is 69.2%.

Clickers are also usually packed with useful legitimate apps and placed in various digital stores, including major, official ones. For instance, in October 2022 *McAfee* [56] found 16 apps packed with Clicker malware on the Google Play store. The apps had over 20 million cumulative downloads and promised functionalities such as a task manager, Instagram profile downloader, currency converter, and various South Korea-related services such as the bus timetable for the city of Busan. ESET telemetry shows that most detections of these Clickers were found in Japan; our products detect all these apps as variants of Android/Clicker.OW.

Compared to the rest of the year when this category was reaching triple-digit percentage growth, Spyware detection numbers rose only slightly in T3, by 14.9%. In the top 10, this category is represented by Android/Spy.Agent trojan in seventh place. Towards the end of November, with FIFA World Cup 2022 matches starting in Qatar, *ESET researchers found* [57] an ongoing Android RAT campaign that uses the World Cup as a lure. It spreads via a Facebook page linking to a website distributing the RAT, which ESET products detect as Android/Spy.Agent.BOC. The downloaded RAT offered World Cup news and live broadcasts and has extensive malicious capabilities such as exfiltrating SMS messages, call logs, contact lists, photos, clipboard contents, and files with particular extensions; recording phone calls; taking pictures; and more.



مع KORA442 تابع
بجودة عالية

تابع مباريات كأس العالم ومباريات انديتك المفضلة بالبث المباشر والحصرى بدون تقطيع وبأعلى جودة. اخبار ونتائج مباريات حية يقدمها تطبيق kora442 بالاضافة للأخبار وجدول بث المباريات

Website distributing an Android RAT that uses the World Cup as a lure

TRENDS & OUTLOOK

At the beginning of 2022, we thought that the rest of the year would see the Android threat scene dominated by malware allowing cybercriminals to cash in cryptocurrencies – cryptominers, ransomware, and banking malware. However, the drastic changes within cryptocurrency markets showed us that cybercrooks can change their ways very fast and adapt to new environments.

The prevalence of malware and PUAs that make money from ads might be perceived as something positive if other types of threats had diminished prevalence. But that is not the case. Spyware has also increased its presence thanks to easy-to-access, off-the-shelf Android spyware kits available on various online forums and used by amateur attackers. We will also see what a new AI chatbot, called ChatGPT, does with the whole Android threat landscape in 2023. Malware writers have already started to use it to develop new tools, but so far we aren't aware of anything made for Android.

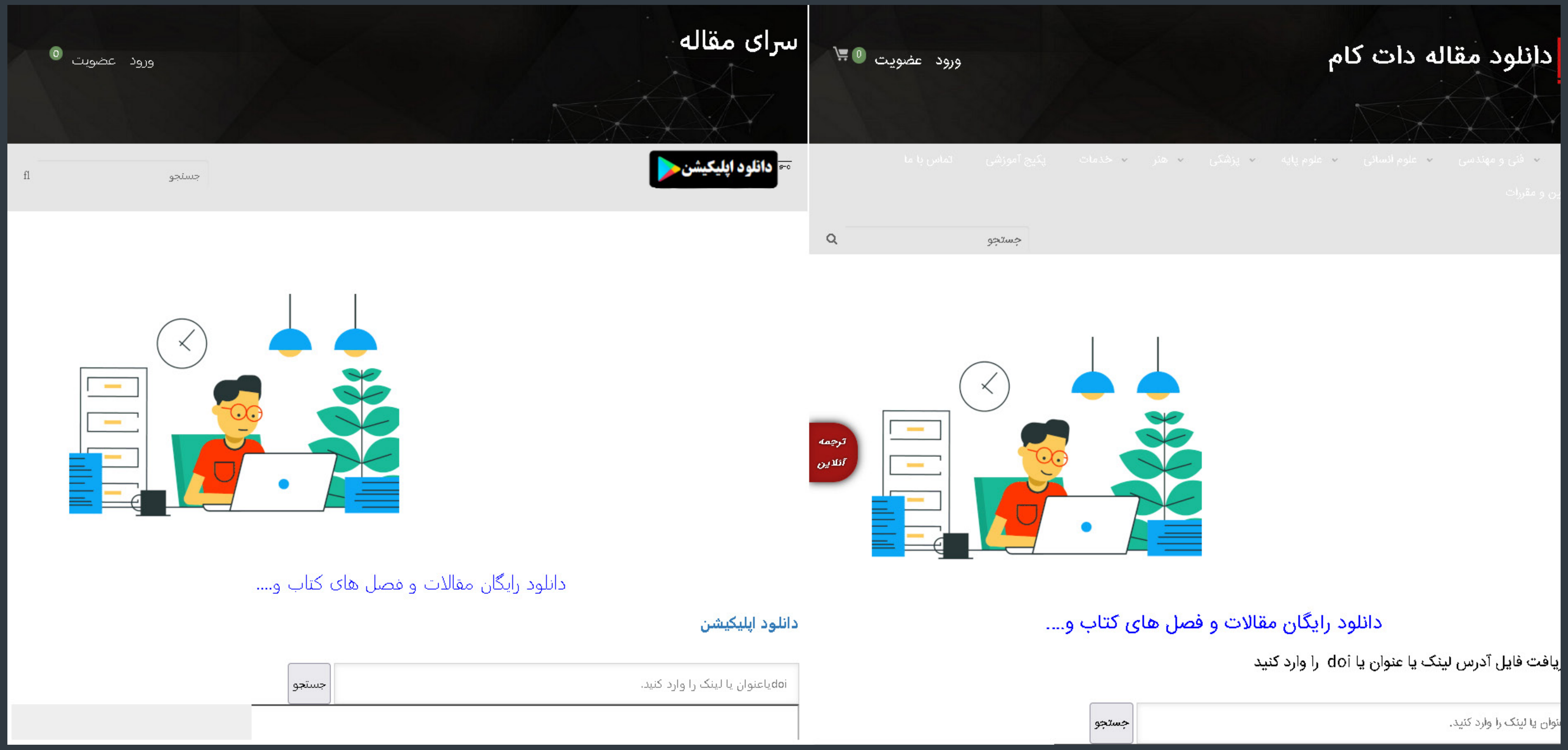
What's more, cybermercenary and APT groups add to this pot by continuing to develop highly targeted spyware to gather information from high-profile targets or vulnerable groups of citizens. This shows that the attackers have fully realized that they can treat smartphones as standard computers and monetize the hell out of them and spy on their owners for geopolitical reasons.

Lukáš Štefanko, ESET Senior Malware Researcher

ESET researchers also discovered an Android campaign conducted by the hack-for-hire group *Bahamut* [12]. The campaign had been active for several months since January 2022, with malicious apps distributed through a fake SecureVPN website. The trojanized versions of legitimate VPN apps exfiltrated contacts, SMS messages, device location, recorded phone calls, and more from affected devices. They also spied on chats exchanged through messaging apps including Signal, Viber, WhatsApp, Telegram, and Facebook Messenger, via keylogging. ESET products detect this threat as Android/Spy.Bahamut.M.

Another Android backdoor that can exfiltrate communications from popular chat and social media apps is detected by ESET products as Android/StrongPity.A. ESET researchers identified a campaign conducted by the *StrongPity APT group* [58] that has distributed the backdoor through a website impersonating Shagle – a random-video-chat service that provides encrypted communications between strangers. The backdoor is presented as the Shagle app, but in fact it's a trojanized and fully functional version of the legitimate Telegram app.

ESET researchers also identified a new version of Android malware named *FurBall* [11] used by the APT-C-50 group. FurBall is part of the group's Domestic Kitten campaign, which conducts mobile surveillance operations against Iranian citizens. Since June 2021, this FurBall variant was distributed as a translation app via a copycat of an Iranian website that provides translated articles, journals, and books. To stay under the radar, the malware (which ESET products detect as Android/Spy.Agent.BWS) has limited functionality – it only accesses contacts, perhaps to follow their collection with spear-phishing via text messages.



دانلود رایگان مقالات و فصل های کتاب و....

دانلود اپلیکیشن

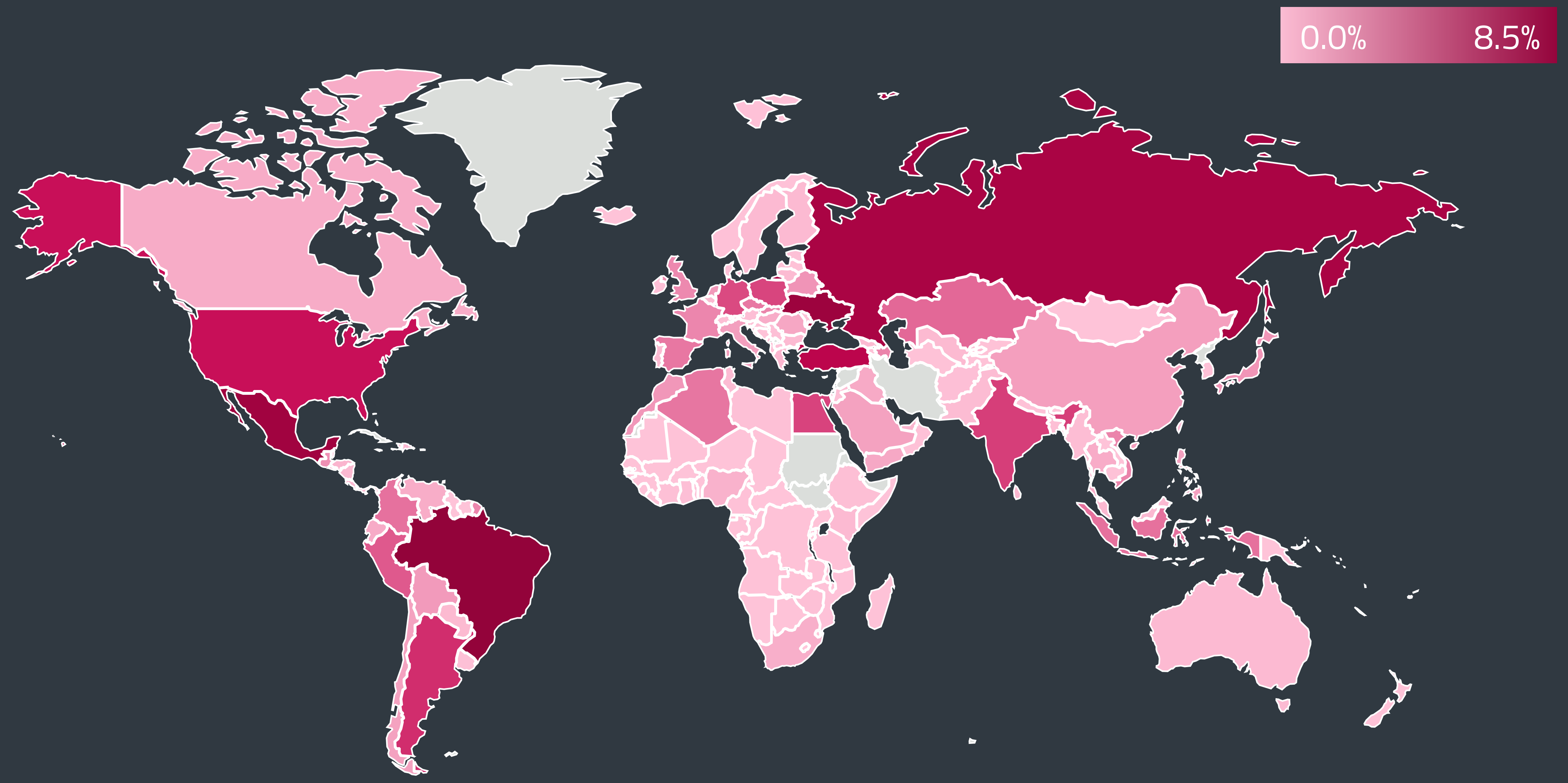
doiیاعنوان یا لینک را وارد کنید.

دانلود رایگان مقالات و فصل های کتاب و....

یافت فایل آدرس لینک یا عنوان یا doi را وارد کنید

نوان یا لینک را وارد کنید.

Fake website (left) vs. the legitimate one (right)



Global distribution of Android detections in T3 2022

Another category that saw a minor increase in its detections is Android Banking malware, by 3.5%. Behind most of its detections are well-known Android banking malware families such as Cerberus and Hydra. *Xenomorph* [59] is, unfortunately, also still infesting Android devices and even appearing on Google Play. *Zscaler* [60] found the banking trojan embedded in a lifestyle app. *Fox IT* [61] found the Sharkbot banking malware on Google Play masquerading as mobile security and cleaner apps, and *BitDefender* [62] detected the same malware family on Google Play posing as file managers.

All other Android categories experienced lower detection numbers in T3: SMS Trojans declined by 34.2%, Ransomware by 15.5%, Stalkerware by 13.6%, ScamApps by 13.1%, and Cryptominers by 7.1%.

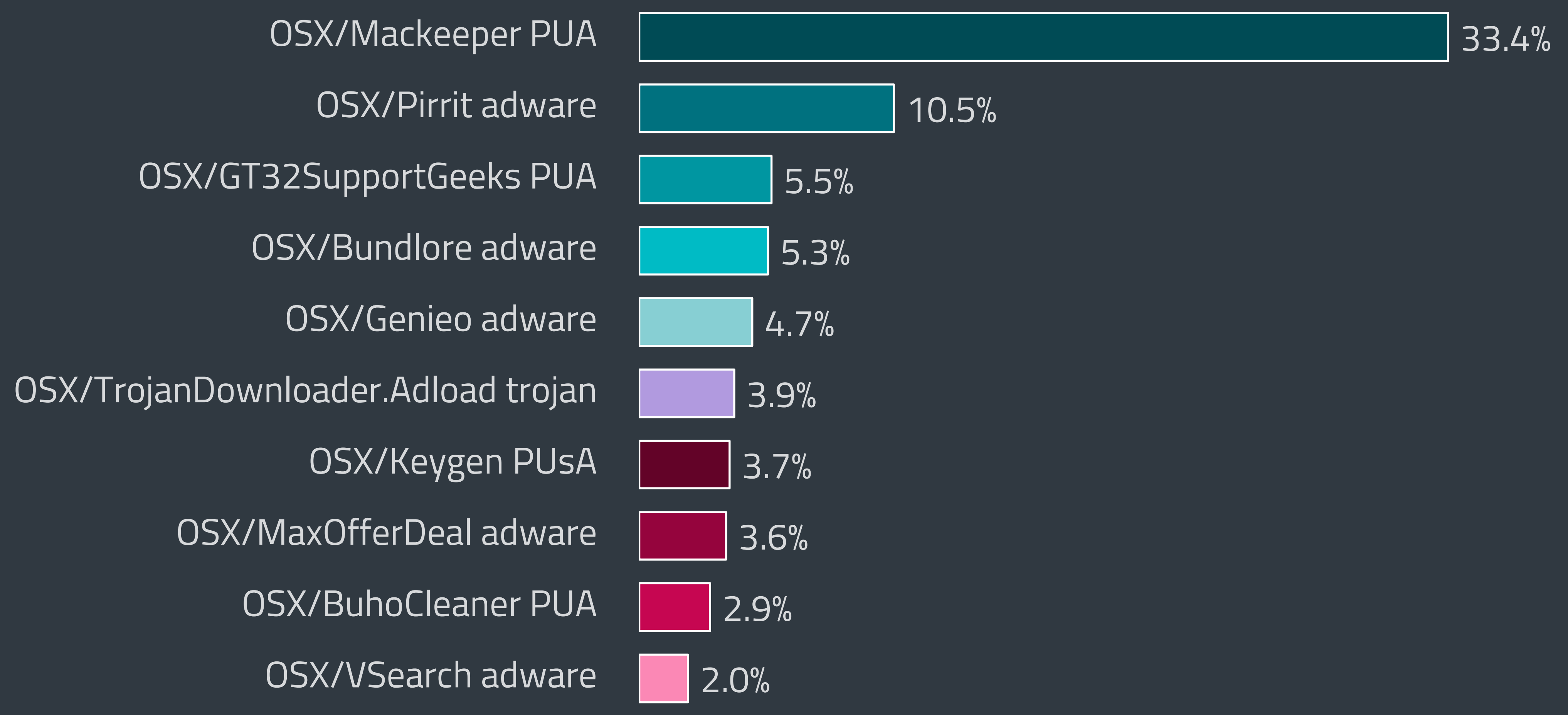
Countries where ESET telemetry detected the most Android threats in T3 were Brazil (8.5%), Ukraine (7.6%), Mexico (7.3%), Russia (6.6%), Turkey (5%), and the United States (4%). However, if we look at the whole year 2022, most Android detections were found in Ukraine (9.3%) and Russia (9.2%).

macOS AND iOS

macOS detections continued to decline slightly in T3 2022, with Potentially Unwanted Applications accounting for more than half of them.

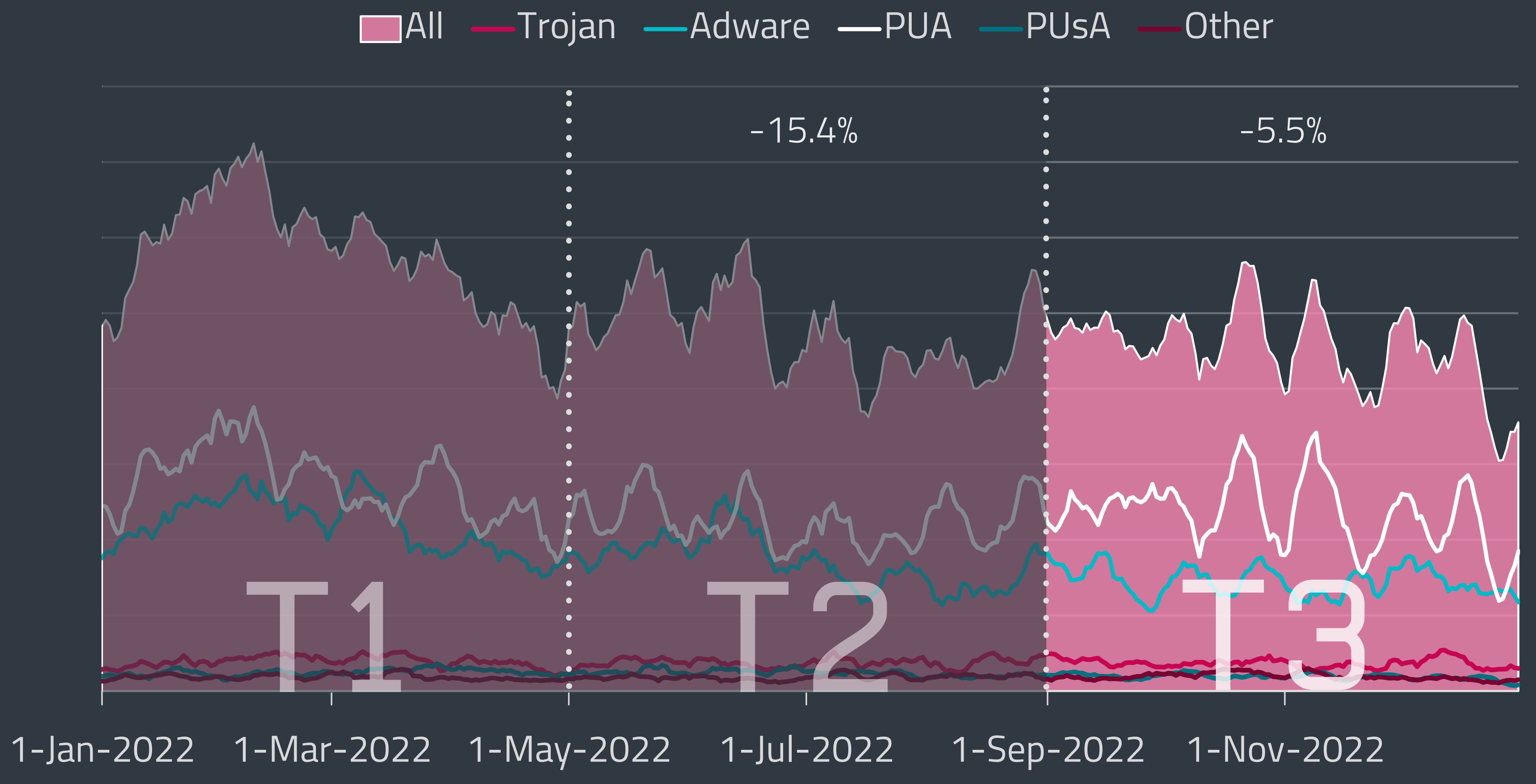
In T3 2022, ESET telemetry saw a decline in nearly all types of macOS detections, by 5.5% compared with T2. The only exception is presented by Potentially Unwanted Applications (PUAs); their detection numbers grew slightly by 3.3% and continued to be the most widespread type of macOS detection. In T3 2022, PUAs accounted for 52% of all macOS detections and were represented in the top 10 by OSX/Mackeeper, OSX/GT32SupportGeeks, and a newcomer in the top 10, OSX/BuhoCleaner.

PUAs in general are not malware. Users install them voluntarily because they promise useful functionality, such as cleaning macOS devices. However, they might perform actions that negatively impact macOS performance and can increase the possibility of being infested with actual malware because they have extensive permissions and access to macOS processes and files. In some cases, they can employ shady marketing practices, and their end-user license agreements can be hard to find. Cybersecurity vendors usually provide their customers with the choice of whether they want this type of software to be flagged, or not.



Top 10 macOS detections in T3 2022

Even though the macOS detection trend graph shows the biggest drop in the detection numbers of PUAs and all macOS detections towards the end of December 2022, we are confident that it is only a momentary decline. The drop presents an annual phenomenon we attribute to the specific time of the year during which people around the world, including malware operators, celebrate various religious and cultural festivities and simply use their computers less often.



macOS detection trend in 2022, seven-day moving average

The second most prevalent category of macOS detections, Adware, experienced a decrease of 15.4%. This category is represented in the top 10 macOS threat list by OSX/Pirrit, OSX/Bundlore, OSX/Genieo, OSX/MaxOfferDeal, and VSearch. These threats display intrusive ads, bundle adware with legitimate apps, and intercept internet searches. Potentially Unsafe Applications (PUsAs) saw the largest decrease in detections in T3, by 20.6%, and Trojans decreased slightly by 3.4%.

ESET telemetry registered the most macOS detections in T3 2022 in the United States (20.7%), Japan (11.7%), France (7.7%), Germany (5.6), and the United Kingdom (4%). In all of these countries, the number of macOS detections decreased compared to T2 2022, with the exception of Germany, where detections rose by 21%.

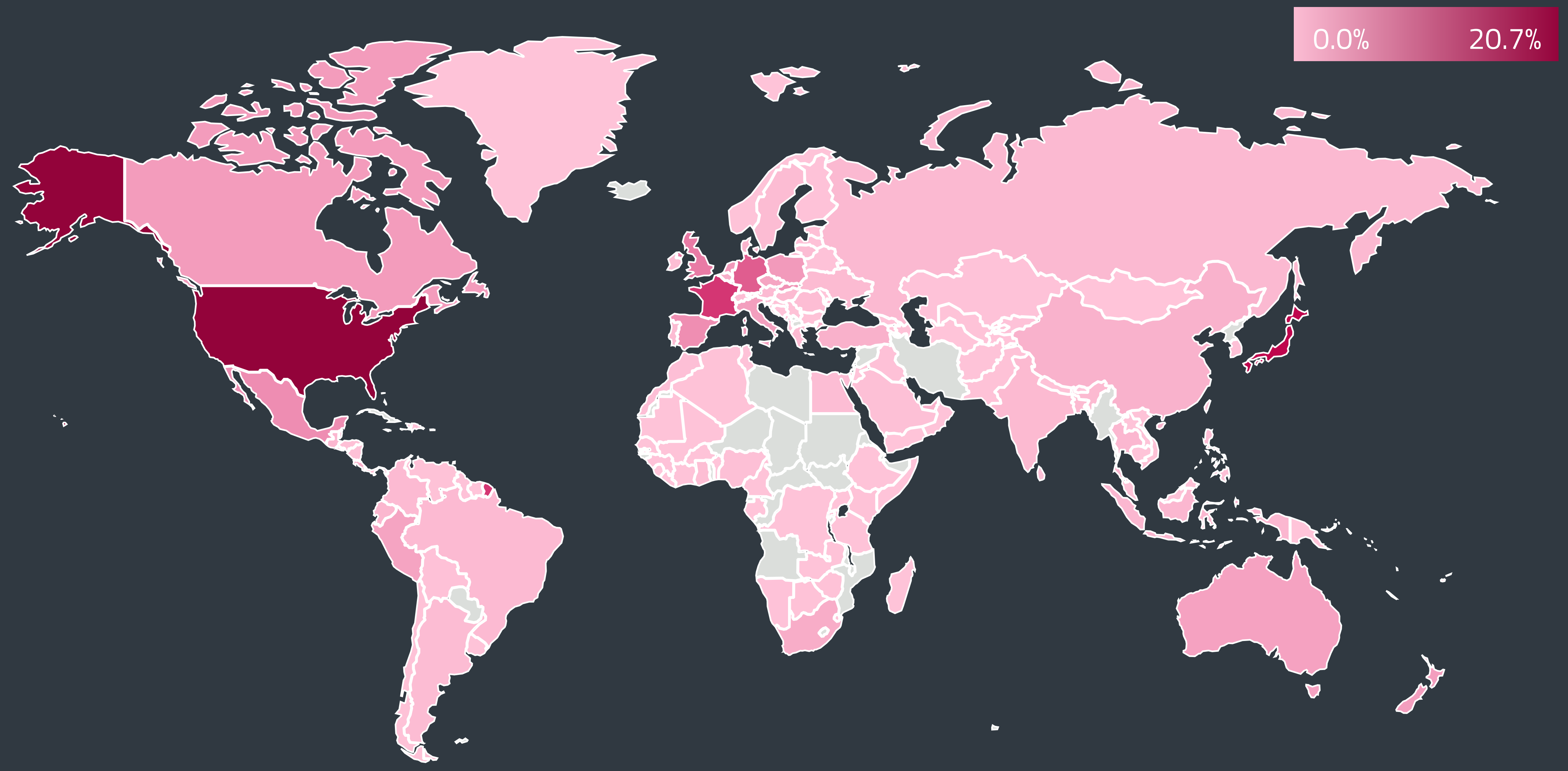
Even though the overall macOS threat detection numbers are decreasing, ESET researchers have previously shown that various groups continue to develop new threats to the users of this platform or deploy cross-platform malware. Researchers at *Talos* [63] discovered a new attack framework named Alchimist capable of deploying cross-platform malware named Insekt, which has remote administration capabilities. *ReversingLabs* [64] discovered a new supply-chain attack using a malicious module that poses as a software development kit from the cybersecurity company SentinelOne. The module is unrelated to SentinelOne but abuses its name to lure victims. The goal of SentinelSneak, as the researchers named it, is to exfiltrate sensitive developer-related files.

On VirusTotal, *Trend Micro* [65] discovered keychain-stealing malware, named KeySteal, which is embedded in a trojanized version of an open-source application. Keychain is a macOS app that stores passwords and account information. Trend Micro researchers have not seen KeySteal in the wild and while ESET products detect it as a variant of OSX/Spy.GogoKChain.A, ESET telemetry also has zero hits on this threat, which could mean KeySteal has been used in a narrowly targeted campaign.

Besides malware and similar threats, vulnerabilities and bugs also present a cause for concern for macOS users. A *bug in macOS Ventura 13.0* [66] obstructs security products from the access they need to do their scans, and it is therefore advised to upgrade to a later Ventura version. On devices running macOS 13.0, ESET products show *a warning* [67] that the system is not fully protected.

This bug is not the only reason why users should update their systems as soon as they can. As was revealed in a Virus Bulletin presentation by *Intego* [68], and later confirmed in an *Apple document* [69], the company doesn't always patch the same bug in older versions of its software. For example, if a vulnerability is actively exploited and Apple patches it on versions 13.X, it might not be addressed in previous versions, such as 12.X.

In a way, Apple is sending mixed messages. After a tug of war *with US agencies* [70], the company has finally decided to expand end-to-end encryption protections in its iCloud service providing added protection to pictures, notes, and most importantly iCloud backups. The feature called Advanced Data Protection for iCloud has to be *enabled by the user* [71] and is available on iPhones with iOS 16.2, iPads with iPadOS 16.2, Macs with macOS 13.1, and other Apple devices, providing those with another reason to upgrade their operating systems if they want to benefit from better protection.



Global distribution of macOS detections in T3 2022

IoT SECURITY

The Mozi botnet has one foot in the grave; ZHtrap dropped dead. Mirai-based botnets grew in size but became less active.

In T3 2022, the ZHtrap botnet suddenly closed shop. ESET telemetry shows that in the last four months, the number of new bots and attacks went down by 97%, and almost half of its payload servers disappeared. Despite no takedown being reported, its detections fell from tens of thousands in T1 and T2 2022 to almost zero in T3 2022, causing ZHtrap to effectively vanish from our radar.

That swift end contrasts with the almost glacial decline of the Mozi botnet, once a prime threat for IoT devices. After its creators were *arrested* [72] by Chinese authorities in 2021, Mozi ran on autopilot, spreading to hundreds of thousands of new devices throughout the year.

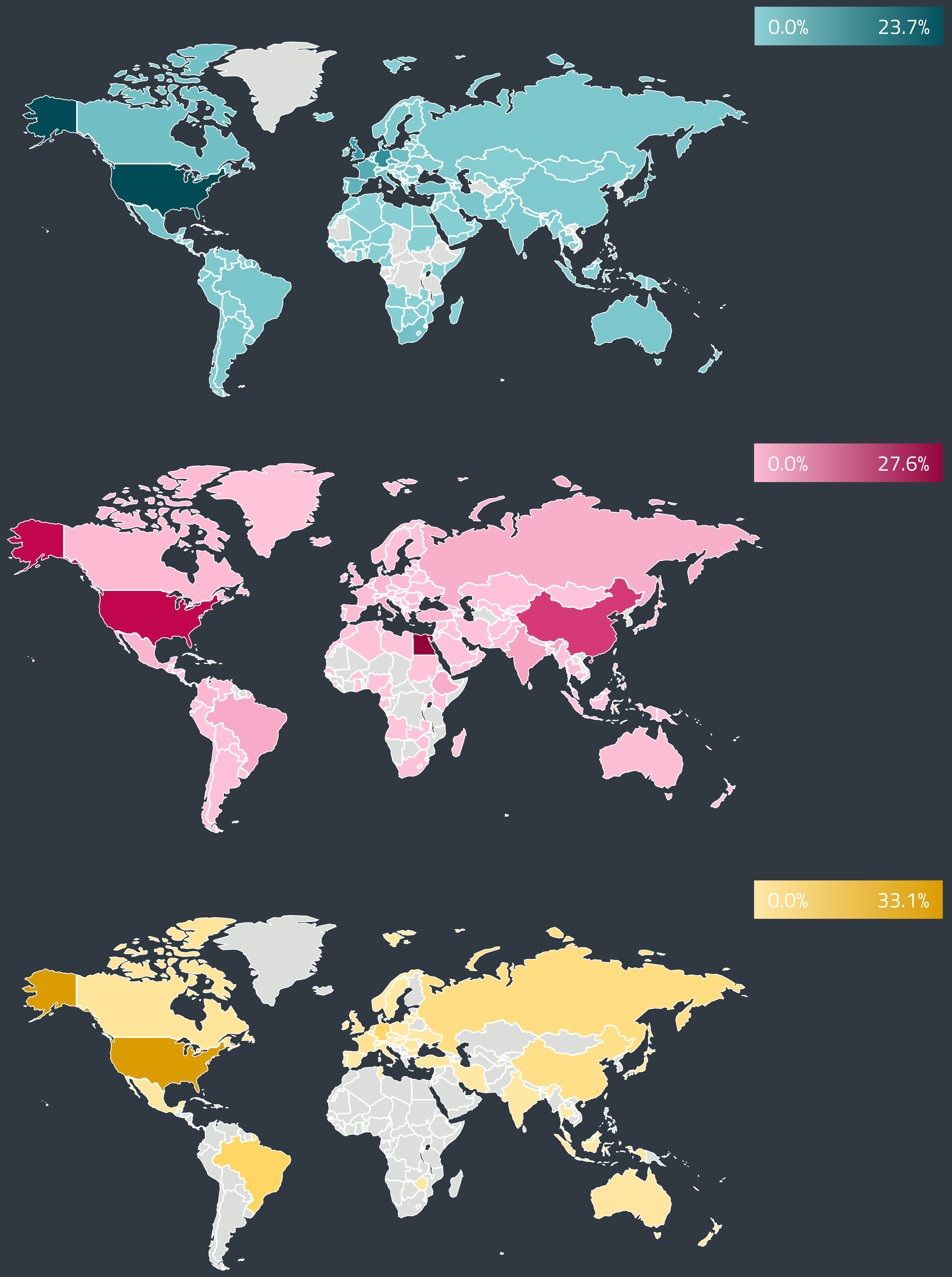
While that remains true, it started losing pace in T2 2022 when it infested "only" 383,000 new devices compared to 498,000 in T1 2022, slowing down by 23%. Between T2 and T3 2022, this trend continued, and Mozi spread to only 289,000 new devices, decelerating by another 25%. If this trend persists, Mozi might bite the dust by the end of 2023.

But for now, the zombie botnet still looks hungry, yet without its operators, there is no one to point it at "fresh brains". That's probably why it bites new victims almost exclusively in China and India, where 45% and 42% of the new bots were detected. Of its 2.8 million attacks in T3 2022, 30% were aimed at the United States, 6.5% at Germany, and 6% at the UK – almost identical to T2 2022.

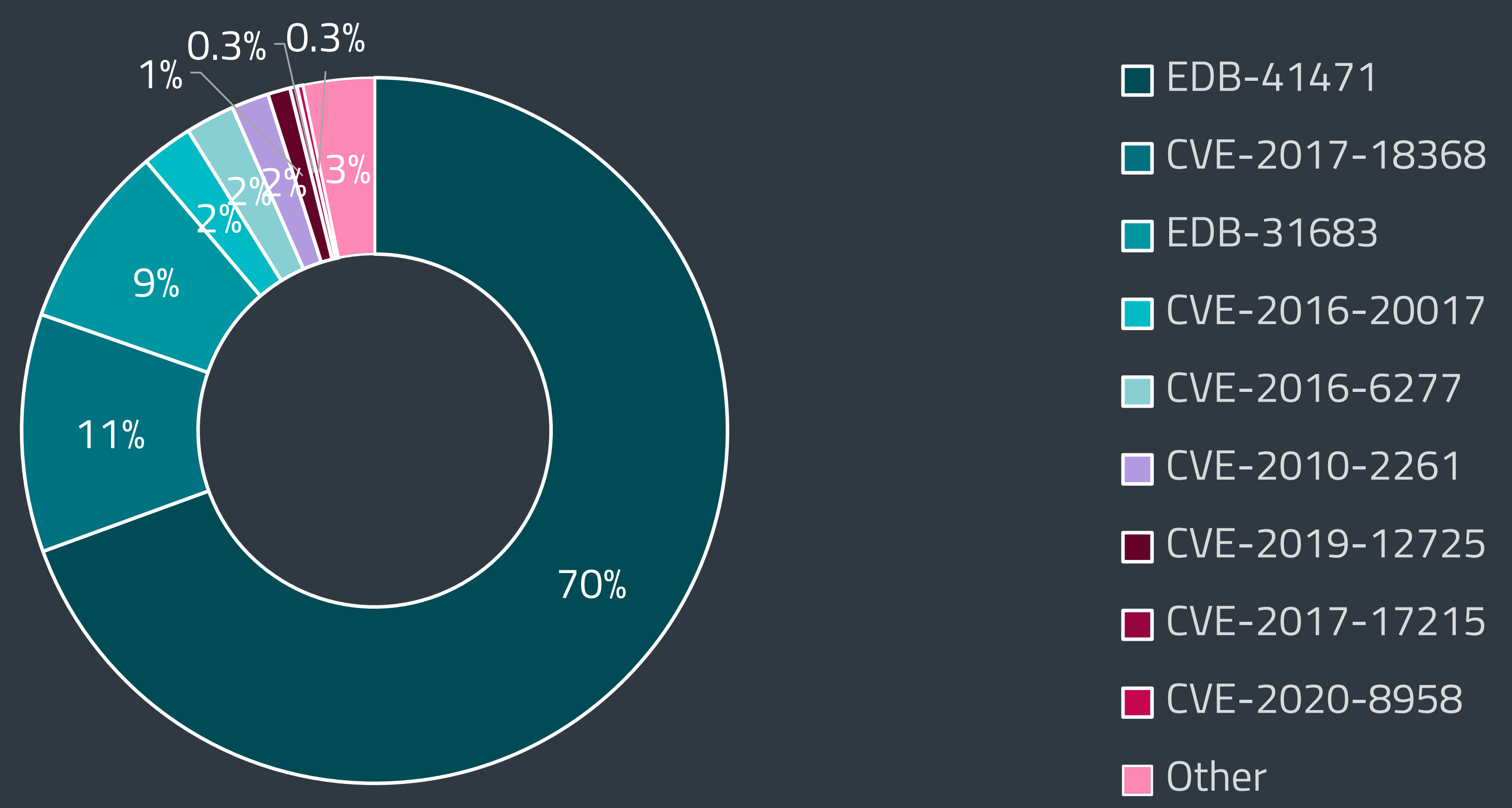
Unfortunately, not all IoT botnets drop dead or are on their way to the grave, a case in point being the group of Mirai-based botnets. Their creators use spin-offs of years-old Mirai malware to build new networks of compromised devices that can be used or rented for nefarious purposes. In ESET telemetry, Gafgyt, BotenaGo, Dofloo, Tsunami, and recently, Zero, are included in this group.

The number of devices turned into bots by these Mirai-based botnets grew in T3 2022 by 11% to almost 200,000. They found the most fertile ground in Egypt (63%), the US (7%), and China (4%). Looking for targets, these networks of enslaved IoT devices aimed at 83,000 IP addresses – a 20% drop between T2 and T3 2022 – primarily in Germany (15%), the US (11%), and Japan (6%).

Egyptian Mirai bots were also at the helm regarding the number of attacks, being responsible for 28% of the 11 million detections. The devices in the United States were the second most active with 15%, followed by South Korean ones with 13%. The largest portion of the attack waves hit the shores of the US (24%), Germany (8%), and the United Kingdom (7%). The good news is that the 11 million detections meant that Mirai-based botnets were 6% less active than in T2 2022.



Global distribution of Mirai-based attacks, bots and payload servers (top to bottom) in T3 2022



Vulnerabilities most exploited by Mirai-based botnets in T3 2022

A third of the 800 payload servers used in the campaigns of Mirai-based botnets were observed in the United States, 8% in Brazil, and another 8% in Germany. What's noteworthy about this is that Brazil became the second most used server base in T3 2022, although it didn't even make it to the top 10 in T2 2022. Contrasting with that was the Netherlands, which in T2 2022 hosted 11% of the servers for Mirai-based botnets, but only had 7% of them in T3 2022, descending from second to fourth place.

With 69%, the 2017 *EDB-41471* [73] bug in MVPower DVR devices remained the number one flaw exploited by Mirai-based botnets for their further spread. The second most exploited vulnerability was a 2017 command injection in ZyXEL routers (*CVE-2017-18368* [74]) used in 11% of the detected cases, followed by the 2014 vulnerability *EDB-31683* [75] in Linksys E-series routers seen in 8% of incidents.

The end of the year brought also several car hacks, impacting *Hyundai, Genesis* [76], *Nissan, Infinity* [77], and *Tesla Model Y* [78] cars – all of which were vulnerable to attacks that could lock and unlock their doors, start their engines, or take control over their features such as the horn and headlights.

A *mass arrest* [79] of 31 suspects in a bust against a car-stealing gang across Europe showed that these types of attacks are not theoretical anymore and criminals are already deploying them in the wild. The dismantled criminal ring exploited vulnerable keyless entry and start systems to get into cars and drive them away.

As IoT security has been lacking for years, several developed economies are looking at regulatory mechanisms to address the most common shortcomings. In T3 2022, the US White House hosted private and governmental partners in a meeting that aimed to *develop* [80] a voluntary label program to help Americans better understand the security of their smart devices. One step ahead of that is Germany and Singapore's *agreement* [81] to recognize each other's already existing IoT security labels.

Let's hope that the increased transparency and government-set standards will end the era of insecure and unfixable devices, which are the main fodder for the IoT botnets described in the first part of this chapter.

TRENDS & OUTLOOK

Looking back at the data from 2022, our prediction that the Mozi botnet is on its way out was correct. With no new developments around its creators or the private keys they held, no new exploits added, and no significant increase in activity observed, it is almost certain that this botnet is running out of steam. The question remains, "Who will replace it as the leader in the IoT space?", since currently, we do not see any likely successor.

However, one threat area that might produce such a successor is that of Mirai-based botnets. These malicious networks are actively managed by their operators, who frequently update the long list of misused old vulnerabilities with new exploits that can further help them expand their size. That is also why we expect Mirai-based botnets to remain the primary threat for 2023 in the IoT space.

In the coming year, we'll also keep an eye on industrial IoT, as our honeypots suggest these devices are becoming increasingly popular targets among cybercriminals, who use them for reflected and other DDoS attacks.

Milan Fránik, ESET Malware Researcher

EXPLOITS

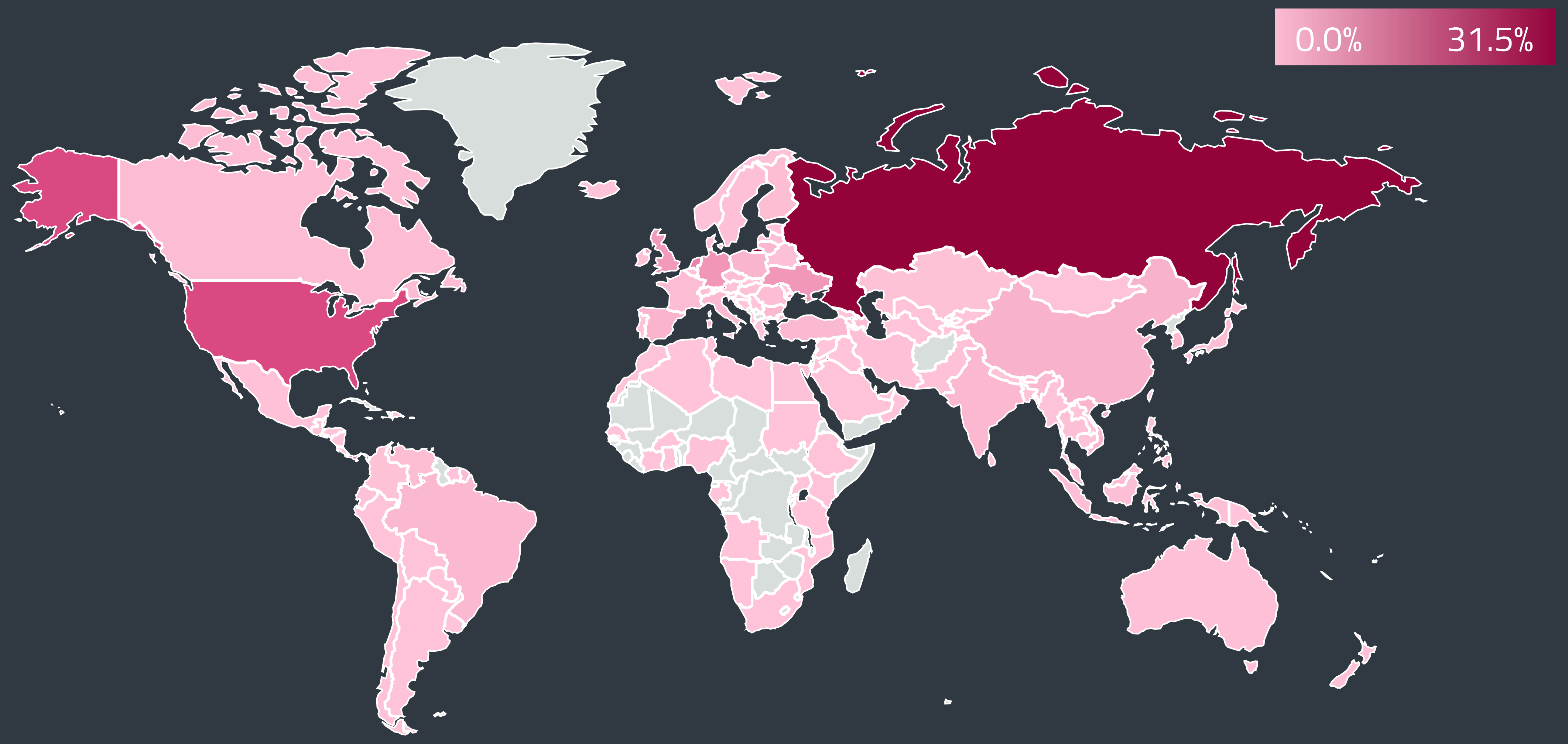
While RDP password guesses remained down, SQL attacks picked up the pace. Log4J vulnerability detection and exploitation attempts continued to grow.

In 2021, brute-force attacks against public-facing RDP were one of the most booming areas of cybercriminal activity with no signs of change ahead, yet it only took the first 10 days of 2022 for it to go into a nosedive.

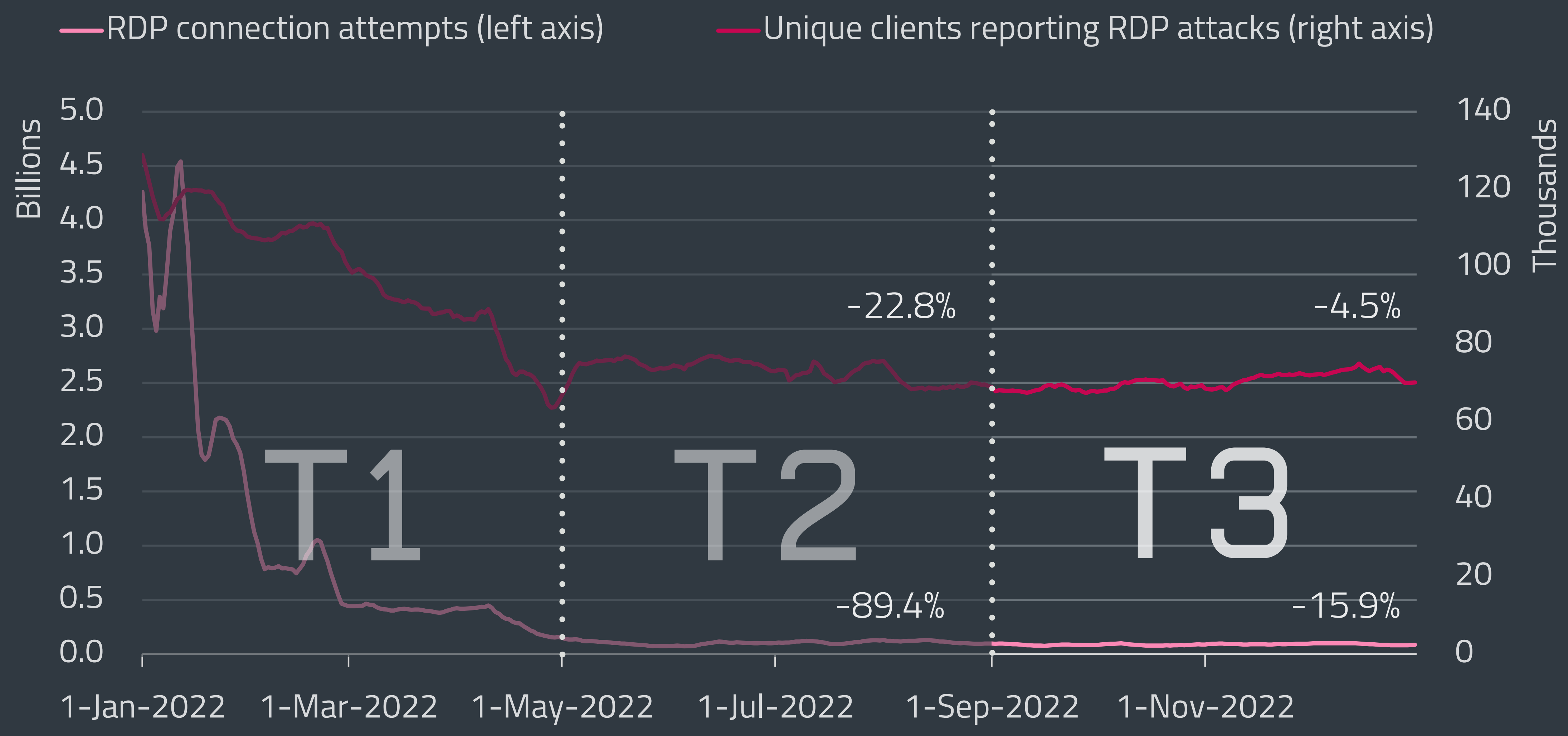
That rapid decline continued until May 2022 when the RDP figures mostly stabilized, but even between T2 and T3 2022 the figures showed a drop of 16%. The average daily number of blocked password guesses went from over 1 billion in T1 to 105 million in T2 and 89 million in T3.

Statistically speaking, the number of password guesses has dropped year over year by 49% going from 288 billion in 2021 to less than 146 billion in 2022. However, if the first ten detection-heavy days were subtracted, the drop would be even more dramatic, reaching as much as 63%.

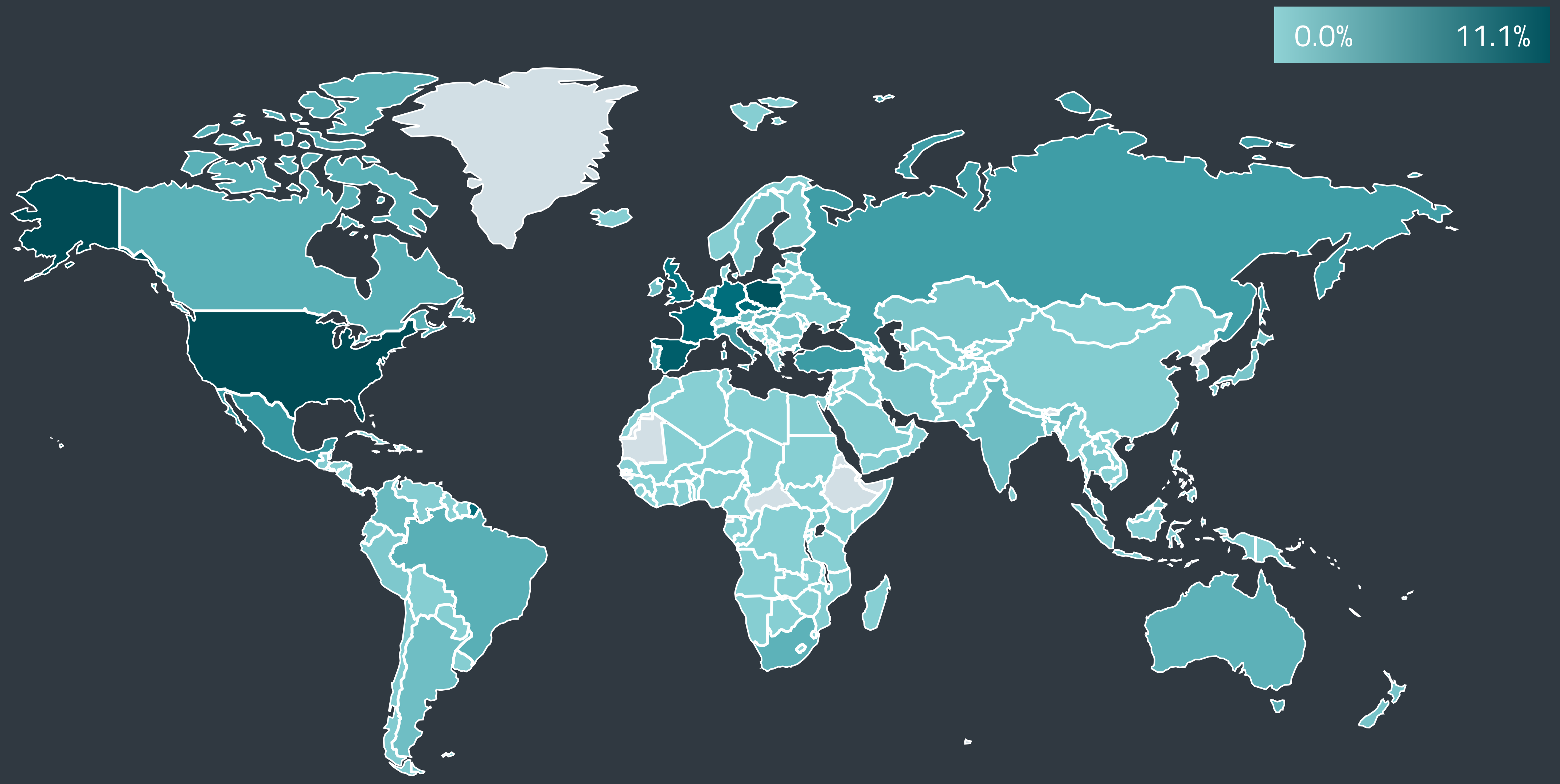
As for factors that might have contributed to this major trend change, we stand by our hypotheses from previous editions of this report: the declining amount of remote work, improved setup and countermeasures by company IT departments, Russia's aggression against Ukraine, and a new brute-force blocking feature built into Windows 11.



Global distribution of RDP password guessing attack attempt sources in T3 2022



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



Global distribution of RDP password guessing attack attempt targets in T3 2022

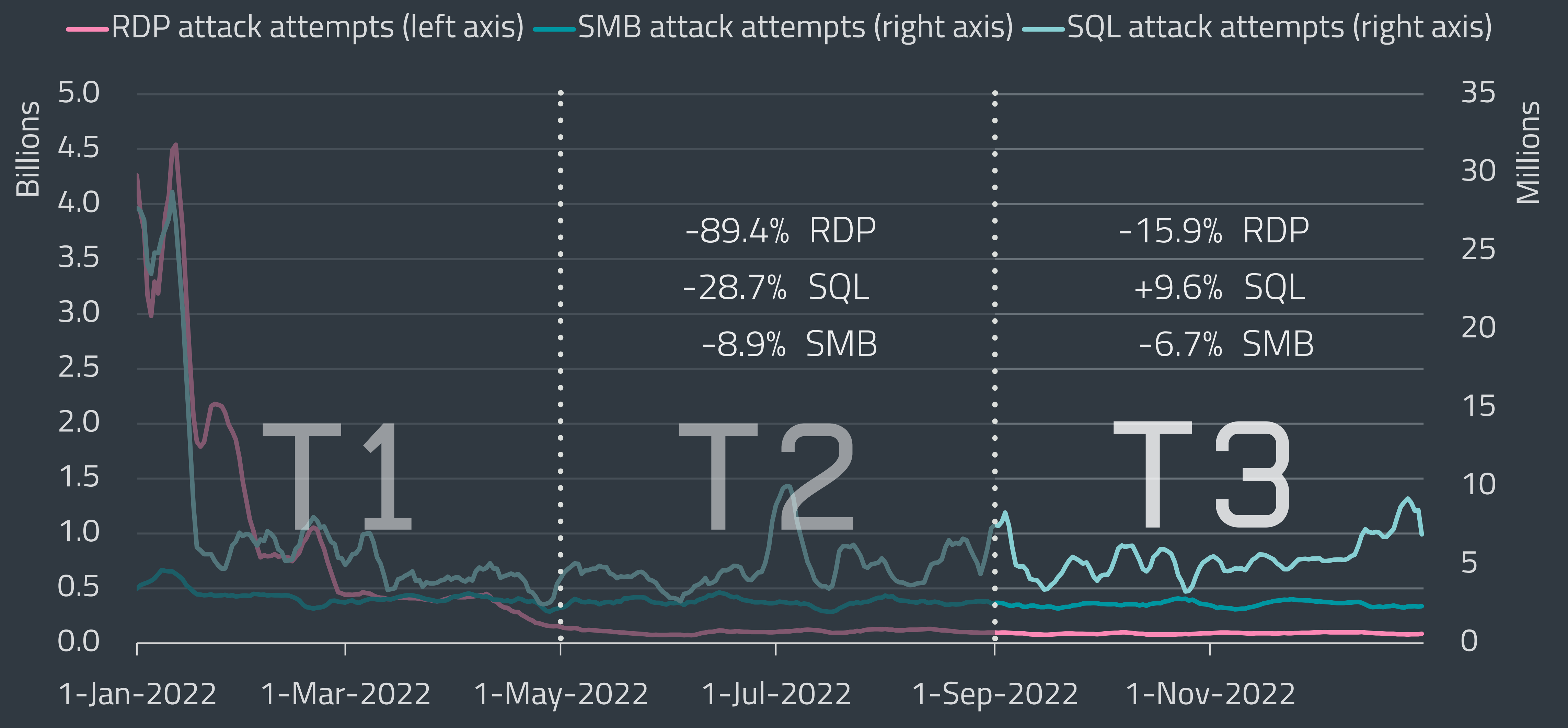
Looking at the daily average of unique clients reporting at least one blocked attack against RDP, T3 2022 brought the lowest figure of 70,000, a 4% decline from 73,000 in T2 2022 and a 31% drop from 102,000 in T1 2022.

From the geographical point of view, most of the attacks in 2022 – as many as 55% – originated from Russian IP addresses. The second most potent source was Germany, with 14%, followed by the US, with 6%. On the receiving end of these connections were mostly French, Spanish, and German IPs, with 14%, 13%, and 7%, respectively.

If focused only on T3 2022, Russian IPs remained the leading attackers but only with 32%, followed by the US with 10%, and IPs in an unknown region with 7%. As for the most prominent targets of T3 2022, the US led the pack with 11%, followed by Poland with 10%, then Spain with 8%. We need to stress that the use of VPNs, server rentals, and proxy services might influence the geographical data mentioned above.

At first, it looked like the number of blocked password guesses against exposed SQL and SMB services would follow RDP, as all three collapsed almost simultaneously in January.

However, SMB stabilized after the initial drop and continued steadily for the rest of 2022. The number of attacks went from 356 million (T1 2022) to 324 million (T2 2022) to 302 million (T3 2022) – accounting for drops of 9% and 7%. Despite that, the overall figures for 2022 added up to 983 million, which puts them at the same levels seen in 2021. Countries that faced the biggest portion of SMB attacks were Mexico, France, and the United States.



Trends of RDP, SMB and SQL attack attempts in 2022, seven-day moving average

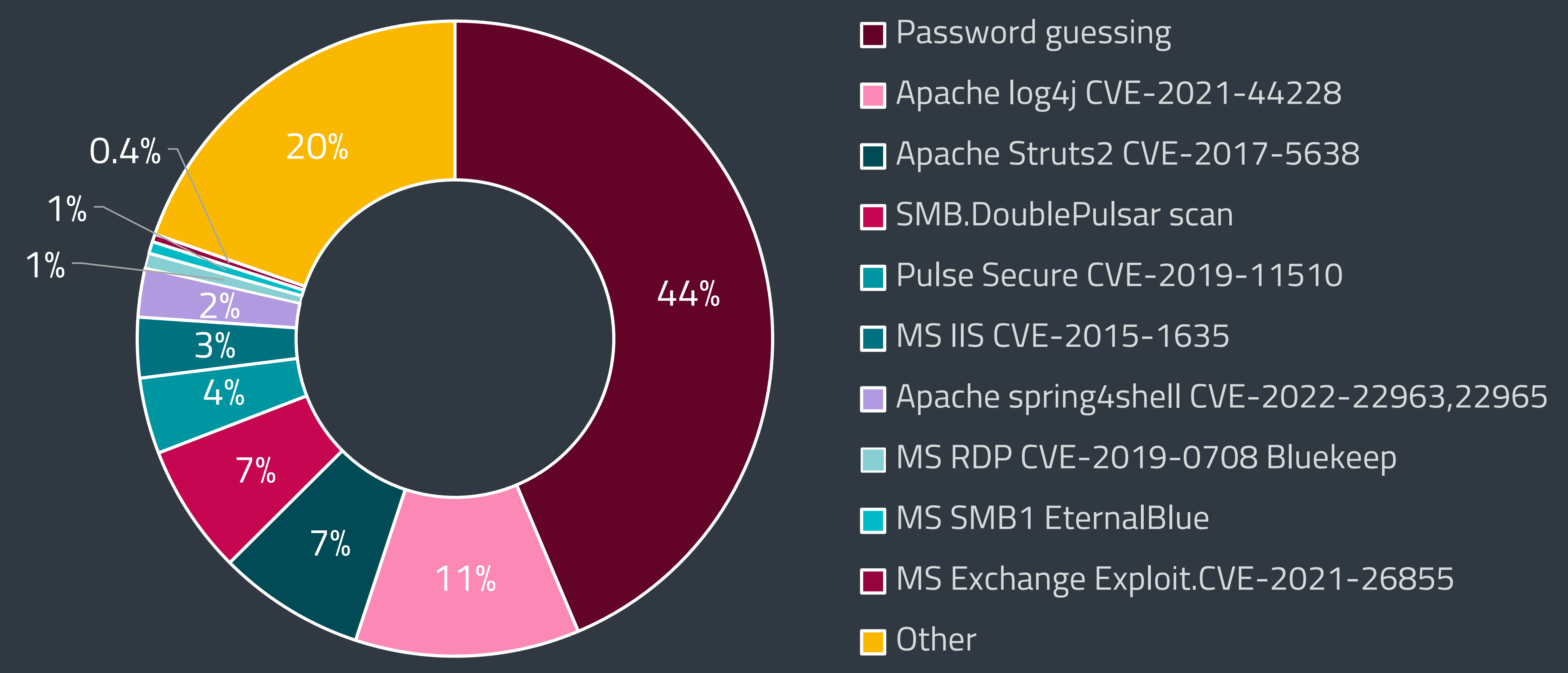
The number of detected attacks aimed at public-facing SQL services also found new ground in January, yet the figures started growing again, exhibiting notable upticks throughout the year. The absolute counts of SQL attacks went from 872 million in T1 2022 to 620 million in T2 2022 – a decline of 29% – but increased to 671 million in T3 2022, meaning a 10% growth.

Looking at the year-over-year context, the number of attacks against SQL saw a 42% dive, with absolute numbers going down from 3.7 billion to 2.1 billion. Geographically, most SQL password guesses in 2022 were directed at services in Turkey, Malaysia, and the US.

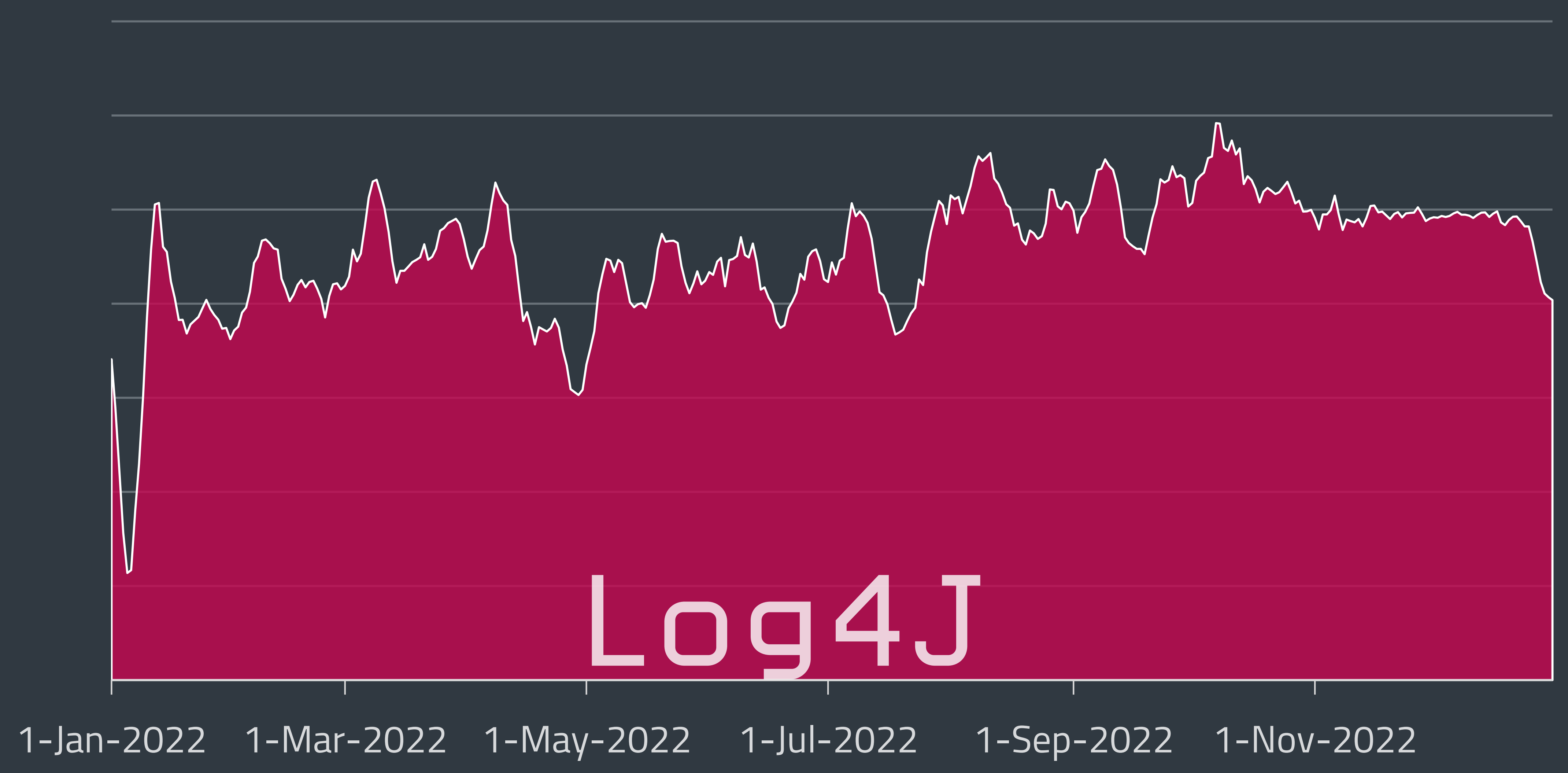
The leading exploited network attack vectors remained largely unchanged compared to T2 2022. Password guessing was still the most favored intrusion avenue, growing its share in the last four months by 3 percentage points from 41% to 44%.

Albeit losing 2 percentage points of its share, the *Log4J vulnerability* [82] still landed second in the external intrusion vector ranking. Despite patches being available for the flaw since December 2021, the absolute number of attacks against it grew by 9% between T2 and T3 2022. Almost 40% of the Log4J exploitation attempts were blocked in the US, 8% in the UK, and 6% in the Netherlands.

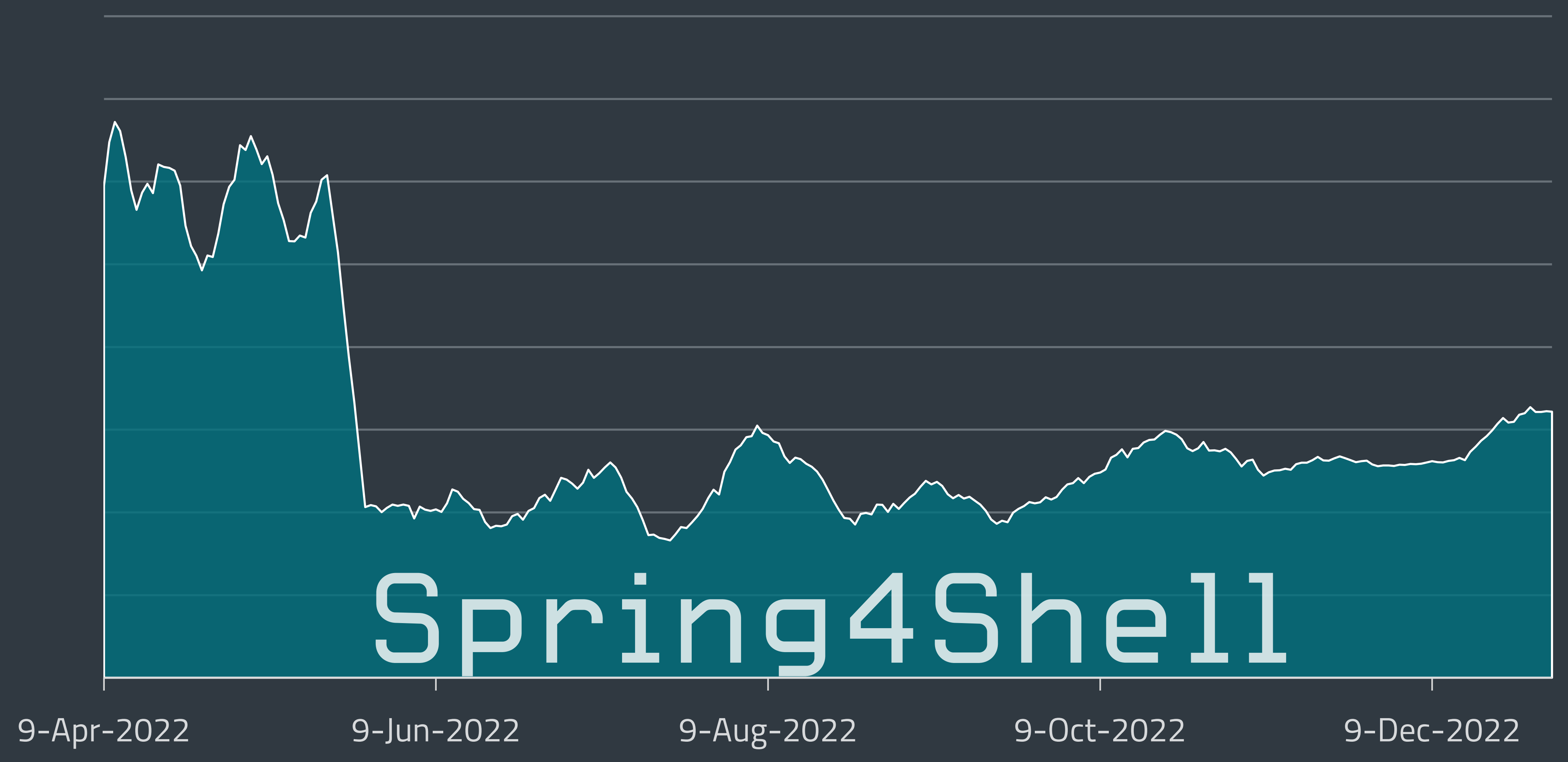
The last four months also brought further reports of the flaw being abused by cybercriminals and sophisticated threat actors such as the *Lazarus APT group* [83] aiming at energy companies in Canada, the US, and Japan, and *Iranian threat actors* [84] targeting the US government. With a quarter of new Log4J library downloads *reportedly* [85] being of vulnerable instances, the “popularity” of this endemic flaw is likely to increase further.



External network intrusion vectors reported by unique clients in T3 2022



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



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

On a more positive note, *Spring4Shell* [86] attacks have not recovered since the notable drop in May 2022. At the point of its publication in April, this 9.8 CVSS vulnerability was seen as a potential follower of Log4Shell, but the last four months of 2022 showed a decline of 8% and a drop to seventh place among the most exploited intrusion vectors. If the trend continues, Spring4Shell's time in the limelight is likely over.

TRENDS & OUTLOOK

Even though RDP password guesses dropped significantly at the beginning of the year, this area of cyberattacks is far from dead. If we omit the first three months, the average number of attack attempts every day still reaches 100 million, which is not a small number.

Looking to 2023, with the growing market share of Windows 11 and Windows Server 2022, which both come with built-in account lockout policy, the success rate for attacks against Microsoft services will decrease. And let's not forget that Microsoft also added protection to older-but-still-supported operating systems, but left the decision to turn it on to the administrators. Based on that, we expect the number of password guesses to go down in the months and years to come.

Ladislav Janko, ESET Senior Malware Researcher

ESET RESEARCH CONTRIBUTIONS

Latest engagements and achievements of ESET Research experts

UPCOMING PRESENTATIONS

RSA Conference 2023

We (could have) cracked open the network for under $100 [87]

Exploiting a vulnerability or conducting a spearphishing attack to capture network login credentials is hard work. Why bother when you can purchase them online? During this presentation, ESET specialized security researcher Cameron Camp and ESET chief security evangelist Tony Anscombe will provide new ESET research that suggests a widespread problem with corporate network management practices that has not been previously recognized – not only in small companies but large multinationals. More information to come closer to RSA.

Botconf 2023

Asylum Ambuscade: Crimeware or cyberespionage? [88]

Asylum Ambuscade is a threat group that came under research scrutiny after it targeted European government personnel in late February 2022, just after the beginning of the Russia-Ukraine war. Dozens of different threat actors have been caught by the security community attacking Ukrainian institutions and their allies, so what makes Asylum Ambuscade different from the others? The presentation by ESET senior malware researcher Matthieu Faou will show how the group engaged in crimeware-related activities and, at the beginning of the war, also started to conduct cyberespionage. Asylum Ambuscade has been spying on European diplomats to steal information related to the war, while also compromising bank customers and cryptocurrency traders worldwide. Unlike other groups in the region, Asylum Ambuscade goes after high-value espionage targets using a custom crimeware-like toolkit. The presentation will describe the group's compromise chain, victimology, TTPs, and why a crimeware group could be engaged in espionage activities.

Life on a crooked RedLine: Analyzing the infamous infostealer's backend [85]

RedLine Stealer is widely known information-stealing malware that operates on a malware-as-a-service (MaaS) model. It is sold via forums and on Telegram, where affiliates can buy a control panel that generates stealer samples, functions as a C&C server, and manages stolen information. During one of our investigations, we uncovered the modules that form the third layer of the MaaS infrastructure, namely the backend server for the control panels themselves. The backend server has never been publicly documented. This presentation by ESET malware researcher Alexandre Côté Cyr will cover the prevalence and features of RedLine, common methods of compromise, and the stealer logs market. The main focus of the presentation will be on the technical analysis of the backend server software, written in C#, including the `LoadBalancer` and `DbController` modules, concluding with a demo of the control panel and backend in a virtual network.

DELIVERED PRESENTATIONS

AVAR 2022

Lazarus declares war on Windows system monitoring [89]

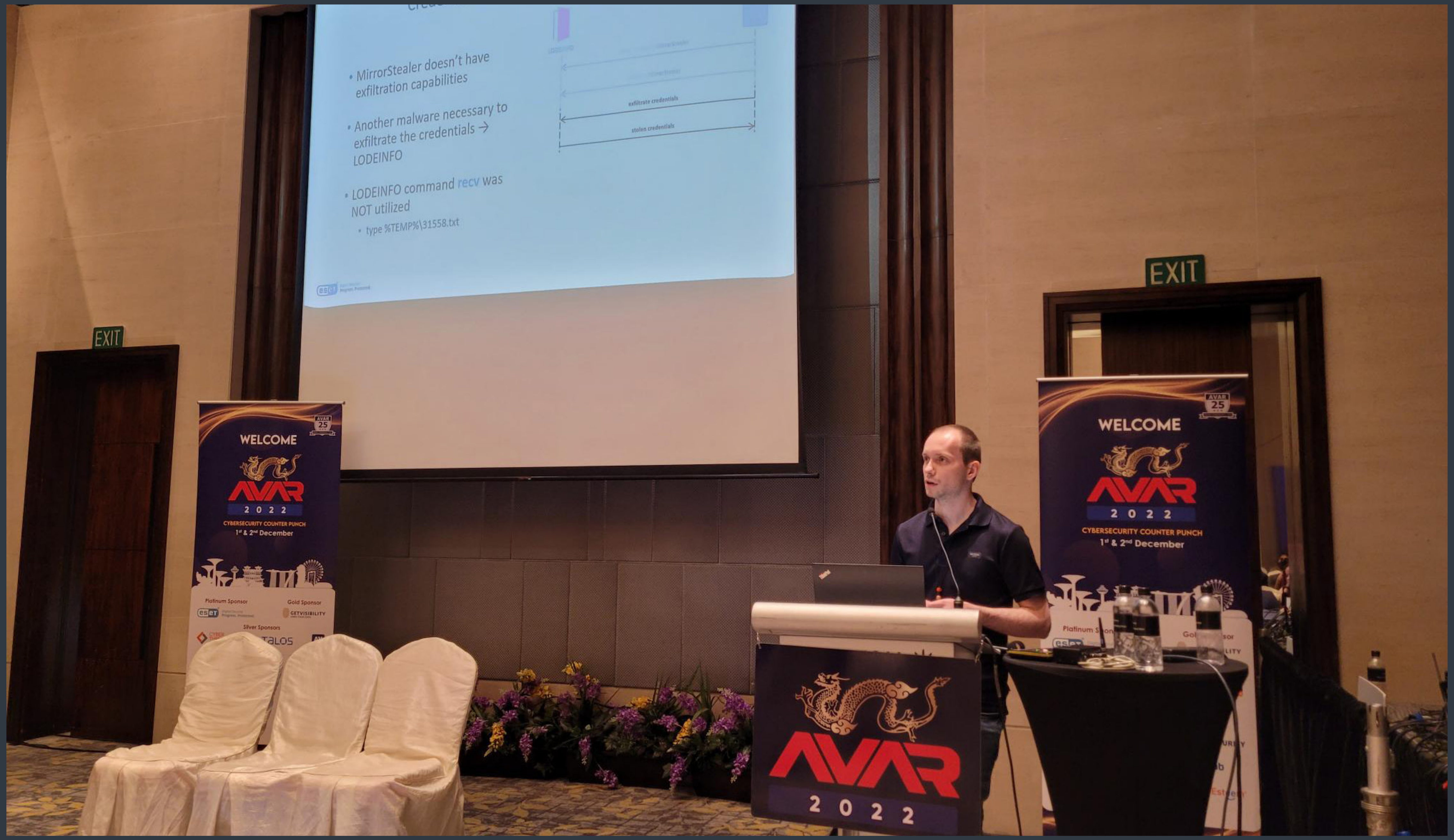
Since late 2021, Lazarus group malware authors have been improving new malware that is able to turn off as many Windows monitoring features as possible, effectively blinding most monitoring tools, security solutions, and event logging. In their presentation, ESET malware researcher Peter Kálnai and ESET malware analyst Matěj Havránek focused on a recent version of this malicious module, discovered in Q2 2022 and that contained the then newly added blinding features. They demonstrated 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 hopefully provided the impetus to reevaluate their implementations and to increase their solutions' self-protection.

Who's swimming in South Korean waters? Meet ScarCruft's Dolphin [90]

ScarCruft, also known as APT37 or 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 explained in his presentation, ESET Research discovered a second, more sophisticated backdoor called Dolphin that was deployed via BLUELIGHT on selected compromised machines. In his talk, Jurčacko presented a technical description of the Dolphin backdoor and its capabilities, provided useful information for threat hunters looking to track ScarCruft activity, and showed the evolution of multiple Dolphin versions that ESET researchers observed after their initial discovery.

Behind the MirrorFace mask: LODEINFO malware interfering with Japanese elections [7]

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 accessed 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 introduced the audience to the MirrorFace APT group, a threat actor exclusively targeting Japanese entities with the LODEINFO malware, and provided a detailed description of this campaign against Japanese political entities. During his analysis, Breitenbacher unearthed MirrorFace tactics and procedures that hadn't been published in detail before. The presentation also included a description of the evolution of the LODEINFO malware over the past few years.


MirrorStealer doesn't have exfiltration capabilities
Another malware necessary to exfiltrate the credentials → LODEINFO
LODEINFO command recv was NOT utilized
type %TEMP%\31558.txt
exfiltrate credentials
stolen credentials
EXIT
WELCOME
AVAR 2022
CYBERSECURITY COUNTER PUNCH
1st & 2nd December
EXIT
WELCOME
AVAR 2022
AVAR 2022

MAIMLA: Make artificial intelligence machine learning again [91]

Although machine learning has been transforming the cybersecurity industry for decades, many people only start paying attention when buzzwords such as "artificial intelligence" enter the conversation. With the arrival of "next-gen" security vendors, the technology itself was buried under layers of "silver bullet" marketing, obscuring its true contribution to threat detection. Filip Mazán, ESET senior machine learning engineer, tried to cut through the noise, and showcased in his presentation how ESET has been deploying machine learning since the 1990s and how it has become a key component of our multilayered architecture. As a reality check, Mazán demonstrated how natural language processing methods can help mitigate one of the admin's worst nightmares – a destructive ransomware attack. He also explained how adversaries use genetic and automation algorithms to create new variants of their malicious products. In the final section of this talk, the attendees were told about potential threats that might, in the foreseeable future, leverage machine learning technology.

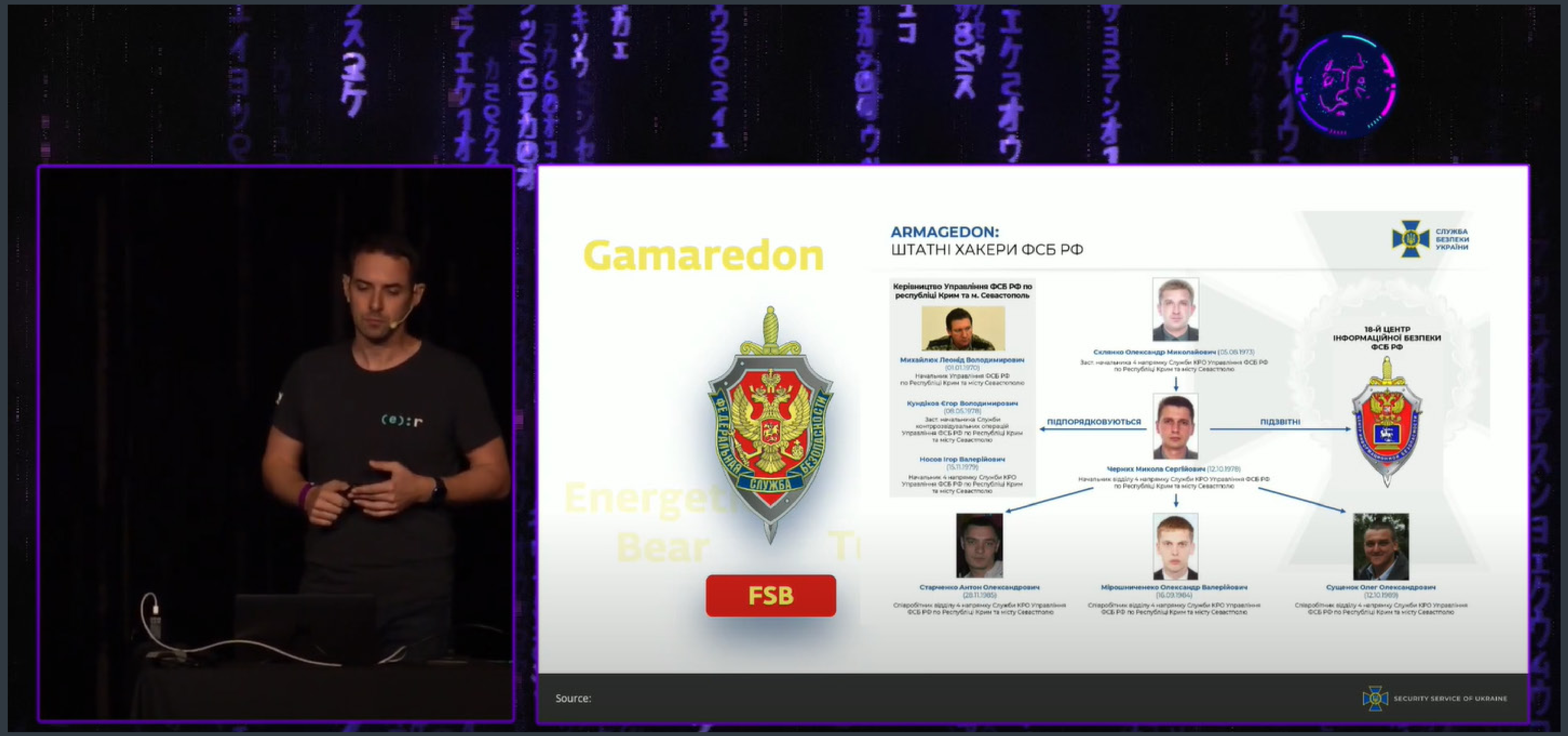
SparklingElf, recent supplies to SparklingGoblin's Linux malware arsenal, new ties to APT41 [92]

ESET researchers Thibaut Passilly and Vladislav Hrčka presented 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 explained the connections between StageClient and Specter, introduced the SparklingGoblin APT group to the audience, and described the code similarities between StageClient and SideWalk. They also described 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 [93]

For the past eight years, Ukraine has been the target of enormous cyber-aggression by numerous APT groups. ESET principal malware researcher Robert Lipovsky walked the attendees of his talk through the most notable attacks, including those against the country's power grid, with a special focus on a prominent 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 outlined how the attack unfolded, why it was unsuccessful, and used reverse-engineered code to show how the code has evolved since the first version. The presentation also focused 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, a destructive wiper deployed in May. It also disclosed how the attackers have been trolling ESET.



MITRE ATT&CK EVALUATIONS

In April 2023, ESET will be participating in the next round of MITRE Engenuity ATT&CK® evaluations, which will focus on tactics, techniques, and procedures (TTPs) applied by the Turla APT group. This Russia-aligned cyberespionage group has been active for more than 12 years; the group executes highly targeted campaigns aimed at exfiltrating sensitive information from Linux and Windows infrastructure. It has compromised many governments, especially diplomatic entities, all around the world, operating a large malware arsenal that ESET Research *has documented* [94] *over* [95] *the* [96] *last* [97] few *years* [98]. The group is known for its targeted intrusions and innovative stealth techniques. After establishing a foothold and conducting victim enumeration, Turla persists with a minimal footprint through in-memory or kernel implants. Besides *our published research* [99], we also have made *several contributions* [100] to the MITRE ATT&CK Enterprise Matrix related to this threat actor.

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 will be publicly available and collaboratively produced with participants. However, the evaluation will not provide any competitive analysis, no ranking of products, nor "a winner". Instead, the evaluation will show how each vendor approaches threat detection through the language and structure of the MITRE ATT&CK knowledge base and provide tools to allow the community to assess which cybersecurity products best fit their individual needs.

OTHER CONTRIBUTIONS

ESET researchers *discovered* [101] three vulnerabilities in the UEFI firmware of several Lenovo notebooks, affecting various Yoga, IdeaPad, and ThinkBook devices. All of these vulnerabilities were reported to the manufacturer; affected devices with active development support have been fixed. Lenovo provided a list of affected devices and firmware update instructions in a *security advisory* [102] and ESET Research highly recommends updating to the latest firmware version.

The vulnerabilities allow disabling UEFI Secure Boot or restoring factory default Secure Boot databases, including the forbidden signature database (dbx) simply from an operating system. While disabling UEFI Secure Boot allows direct execution of unsigned UEFI apps, restoring factory default dbx enables the use of known vulnerable bootloaders to bypass Secure Boot, while keeping it enabled. As in our previous discovery mentioned in *ESET Threat Report T2 2022* [103] (CVE-2021-3971, CVE-2021-3972), the vulnerabilities weren't caused by flaws in the code. The affected drivers were meant to be used only during the manufacturing process but were mistakenly included in the production version.

The reported vulnerabilities can be exploited by simply creating special NVRAM variables:

CVE-2022-3430 [104]

This vulnerability is found in the DXE driver `WmiSetupUnderOsDxe`, which checks for the `L05WSBD` NVRAM variable and performs an action based on its value. To disable UEFI Secure Boot, the attacker would set the value of `L05SecureBootData.Action` to `2`.

CVE-2022-3431 [105]

In this case, the value of the variable is irrelevant. The DXE driver `BootOrderDxe` simply disables UEFI Secure Boot if NVRAM variables `BootOrderSecureBootDisable` or `BootOrderDualBootMode` exist.

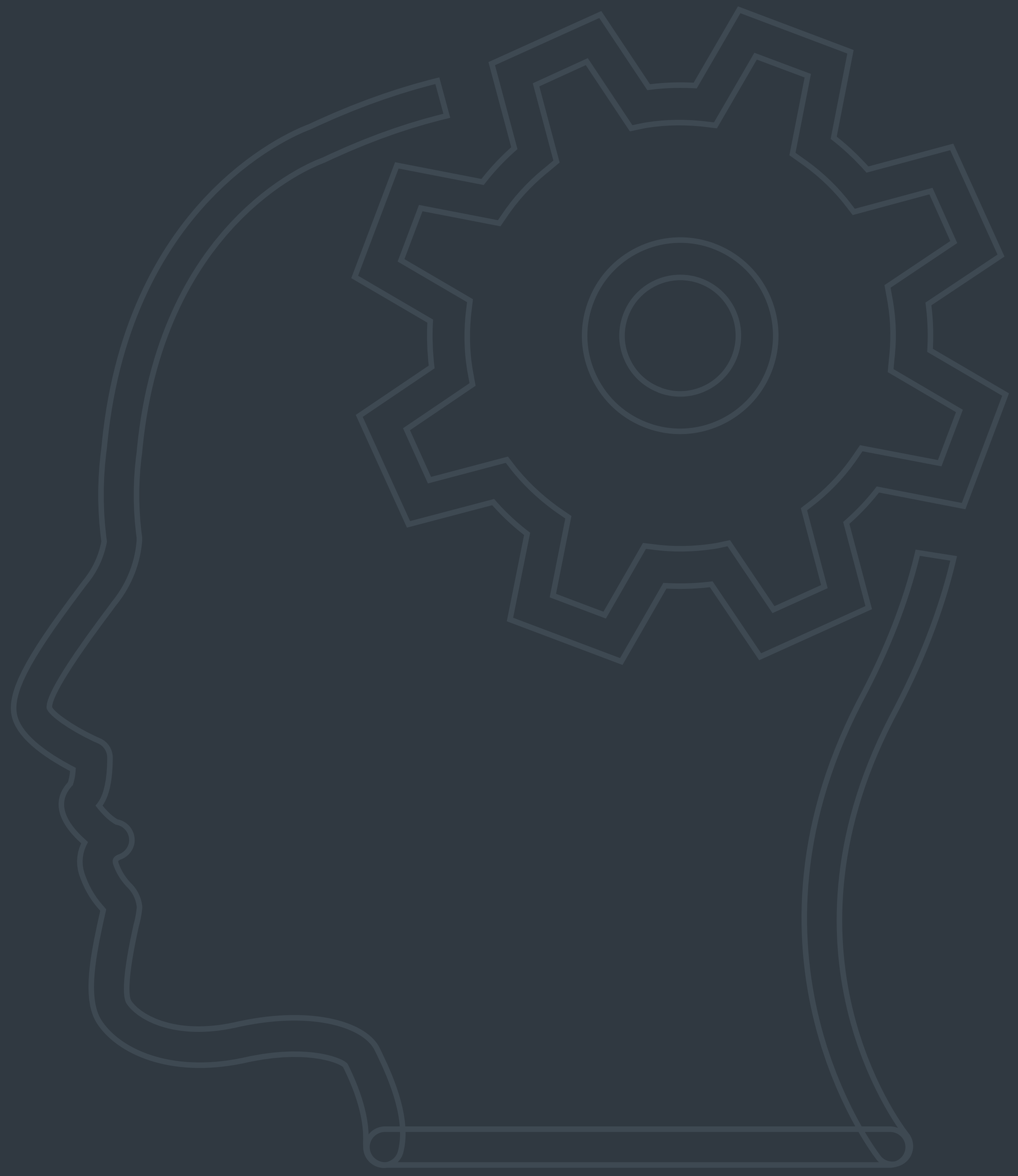
CVE-2022-3432 [106]

This vulnerability relates to the `BdsDxe` DXE driver. This driver retrieves the value of the `L05SecBootSmm` NVRAM variable, and if the value is `0`, it disables UEFI Secure Boot. If the value is `1`, it enables Secure Boot and restores factory keys/databases.

In addition to the Lenovo vulnerabilities, ESET researchers discovered another similar vulnerability in Acer laptops. As in the Lenovo case, it allows deactivating UEFI Secure Boot by creating an NVRAM variable directly from the operating system. A list of affected Acer models is available on the *Acer website* [107], and according to the company, the update will be distributed as a critical Windows update; alternatively, an updated BIOS version is also *available for download* [108].

CVE-2022-4020 [109]

This vulnerability is found in the DXE driver `HQSwSmiDxe`, which checks for the `BootOrderSecureBootDisable` NVRAM variable. If the variable exists, the driver disables Secure Boot.



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
Dominik Breitenbacher
Igor Kabina
Jakub Kaloč
Jakub Souček
Ján Šugarek
Jean-Ian Boutin
Jiří Kropáč
Ladislav Janko
Lukáš Štefanko
Marc-Étienne M.Léveillé
Martin Červeň
Martin Lackovič
Michal Malík
Milan Fránik
Miroslav Legéň
Patrik Sučanský
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* [110], *potentially unsafe applications* [111] and *adware* [112], 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 from other sources. However, absolute values or orders of magnitude are provided where deemed beneficial.

REFERENCES

[1] https://en.wikipedia.org/wiki/2022_Japanese_House_of_Councillors_election

[2] https://www.macnica.co.jp/business/security/manufacturers/files/mpressioncss_ta_report_2019_4_en.pdf

[3] https://blogs.jpcert.or.jp/en/2020/02/malware-lodeinfo-targeting-japan.html

[4] https://www.rimarts.co.jp/becky.htm

[5] https://en.wikipedia.org/wiki/Ichitaro_(word_processor)

[6] https://docs.microsoft.com/en-us/security-updates/SecurityAdvisories/2014/2915720

[7] https://aavar.org/cybersecurity-conference/index.php/behind-the-mirrorface-mask-lodeinfo-malware-interfering-with-japanese-elections/

[8] https://www.welivesecurity.com/2022/12/14/unmasking-mirrorface-operation-liberalface-targeting-japanese-political-entities/

[9] https://www.welivesecurity.com/2022/09/06/worok-big-picture/

[10] https://www.welivesecurity.com/2022/09/14/you-never-walk-alone-sidewalk-backdoor-linux-variant/

[11] https://www.welivesecurity.com/2022/10/20/domestic-kitten-campaign-spying-iranian-citizens-furball-malware/

[12] https://www.welivesecurity.com/2022/11/23/bahamut-cybermercenary-group-targets-android-users-fake-vpn-apps/

[13] https://www.volexity.com/blog/2021/08/17/north-korean-apt-inkysquid-infects-victims-using-browser-exploits/

[14] https://securelist.com/apt-trends-report-q2-2021/103517/

[15] https://www.welivesecurity.com/2022/11/30/whos-swimming-south-korean-waters-meet-scarcrufts-dolphin/

[16] https://www.welivesecurity.com/2022/09/30/amazon-themed-campaigns-lazarus-netherlands-belgium/

[17] https://www.microsoft.com/en-us/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/

[18] https://www.welivesecurity.com/2022/10/11/polonium-targets-israel-creepy-malware/

[19] https://www.welivesecurity.com/2022/11/28/ransomboggs-new-ransomware-ukraine/

[20] https://twitter.com/ESETresearch/status/1596181925663760386

[21] https://www.welivesecurity.com/2022/12/07/fantasy-new-agrius-wiper-supply-chain-attack/

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

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

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

[25] https://www.bleepingcomputer.com/news/security/2k-games-says-hacked-help-desk-targeted-players-with-malware/

[26] https://www.bleepingcomputer.com/news/security/new-malware-bundle-self-spreads-through-youtube-gaming-videos/

[27] https://www.bleepingcomputer.com/news/security/new-azov-data-wiper-tries-to-frame-researchers-and-bleepingcomputer/

[28] https://cert.gov.ua/article/2724253

[29] https://thehackernews.com/2022/12/russian-courts-targeted-by-new-crywiper.html

[30] https://twitter.com/malwrhunterteam/status/1498678603613155343

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

[32] https://attack.mitre.org/versions/v12/techniques/T1484/001/

[33] https://www.welivesecurity.com/wp-content/uploads/2023/01/eset_apt_activity_report_t32022.pdf#page=11

[34] https://thehackernews.com/2022/09/europol-and-bitdefender-release-free.html

[35] https://www.bitdefender.com/blog/labs/ranhassan-ransomware-decryptor-now-available/

[36] https://krebsonsecurity.com/2022/11/researchers-quietly-cracked-zeppelin-ransomware-keys/

[37] https://www.politie.nl/nieuws/2022/oktober/14/09-nederlandse-gedupeerde-geholpen-in-unieke-ransomware-actie.html

[38] https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya

[39] https://storage.courtlistener.com/recap/gov.uscourts.njd.504081/gov.uscourts.njd.504081.1.0.pdf

[40] https://thehackernews.com/2022/10/canadian-netwalker-ransomware-affiliate.html

[41] https://www.cisa.gov/uscert/ncas/alerts/aa22-335a

[42] https://www.cisa.gov/uscert/ncas/alerts/aa22-321a

[43] https://www.fincen.gov/sites/default/files/2022-11/Financial%20Trend%20Analysis_Ransomware%20FTA%202_508%20FINAL.pdf

[44] https://www.uptycs.com/blog/another-ransomware-for-linux-likely-in-development

[45] https://www.pcmag.com/news/is-the-monti-ransomware-contis-successor-or-doppelganger

[46] https://asec.ahnlab.com/en/42037/

[47] https://www.darkreading.com/remote-workforce/rash-new-ransomware-variants-in-the-wild

[48] https://www.bleepingcomputer.com/news/security/ransomware-gangs-switching-to-new-intermittent-encryption-tactic/

[49] https://riskybiznews.substack.com/p/risky-biz-news-internal-chats-for

[50] https://thehackernews.com/2022/10/oldgremlin-ransomware-targeted-over.html

[51] https://twitter.com/ESETresearch/status/1580242729509875712

[52] https://thehackernews.com/2022/09/emotet-botnet-started-distributing.html

[53] https://www.group-ib.com/media-center/press-releases/massive-crypto-attack/

[54] https://www.ic3.gov/Media/Y2022/PSA221003

[55] https://www.welivesecurity.com/2022/11/11/fifa-world-cup-2022-scams-fake-lotteries-ticket-fraud/

[56] https://www.mcafee.com/blogs/other-blogs/mcafee-labs/new-malicious-clicker-found-in-apps-installed-by-20m-users/

[57] https://twitter.com/ESETresearch/status/1596222232384401408

[58] https://www.welivesecurity.com/2023/01/10/strongpity-espionage-campaign-targeting-android-users/

[59] https://www.welivesecurity.com/videos/xenomorph-what-know-android-banking-trojan/

[60] https://www.zscaler.com/blogs/security-research/rise-banking-trojan-dropper-google-play-0

[61] https://blog.fox-it.com/2022/09/02/sharkbot-is-back-in-google-play/

[62] https://www.bitdefender.com/blog/labs/android-sharkbot-droppers-on-google-play-underlines-platforms-security-needs/

[63] https://blog.talosintelligence.com/alchimist-offensive-framework/

[64] https://www.reversinglabs.com/blog/sentinelsneak-malicious-pypi-module-poses-as-security-sdk

[65] https://www.trendmicro.com/en_us/research/22/k/pilfered-keys-free-app-infected-by-malware-steals-keychain-data.html

[66] https://www.wired.com/story/apple-macos-ventura-bug-security-tools/

[67] https://support.eset.com/en/kb8339-upgrade-your-eset-product-for-macos-for-macos-13-ventura-support

[68] https://www.virusbulletin.com/conference/vb2022/abstracts/inconvenient-truth-about-apple-security-updates/

[69] https://arstechnica.com/gadgets/2022/10/apple-clarifies-security-update-policy-only-the-latest-oses-are-fully-patched/

[70] https://www.reuters.com/article/us-apple-fbi-icloud-exclusive-idUSKBN1ZK1CT

[71] https://support.apple.com/en-us/HT212520

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

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

[74] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-18368

[75] https://www.exploit-db.com/exploits/31683

[76] https://twitter.com/samwcyo/status/1597695281881296897

[77] https://twitter.com/_specters_/status/1597984481511903234

[78] https://www.theverge.com/2022/9/12/23348765/tesla-model-y-unlock-drive-car-thief-nfc-relay-attack

[79] https://www.europol.europa.eu/media-press/newsroom/news/31-arrested-for-stealing-cars-hacking-keyless-tech

[80] https://www.mondaq.com/unitedstates/security/1245816/white-house-aims-for-spring-2023-rollout-of-internet-of-things-labeling-program

[81] https://www.zdnet.com/article/singapore-germany-to-mutually-recognise-iot-cybersecurity-labels/

[82] https://nvd.nist.gov/vuln/detail/CVE-2021-44228

[83] https://therecord.media/cisco-log4j-vulnerability-used-to-attack-energy-companies-in-canada-us-and-japan/

[84] https://thehackernews.com/2022/11/iranian-hackers-compromised-us-federal.html

[85] https://www.sonatype.com/state-of-the-software-supply-chain/open-source-supply-demand-security

[86] https://nvd.nist.gov/vuln/detail/cve-2022-22965

[87] https://www.rsaconference.com/usa

[88] https://www.botconf.eu/botconf-2023/botconf-2023-list-of-workshops-and-talks/

[89] https://aavar.org/cybersecurity-conference/index.php/lazarus-declares-war-on-windows-system-monitoring/

[90] https://aavar.org/cybersecurity-conference/index.php/whos-swimming-in-south-korean-waters-meet-scarcrufts-dolphin/

[91] https://aavar.org/cybersecurity-conference/index.php/maimla-make-artificial-intelligence-machine-learning-again/

[92] https://aavar.org/cybersecurity-conference/index.php/sparklingelf-recent-supplies-to-sparklinggoblins-linux-malware-arsenal-new-ties-to-apt41/

[93] https://www.youtube.com/watch?v=uejnkHaNxOA

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

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

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

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

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

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

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

[101] https://twitter.com/ESETresearch/status/1590279782318878720

[102] https://support.lenovo.com/us/en/product_security/LEN-94952

[103] https://www.welivesecurity.com/wp-content/uploads/2022/10/eset_threat_report_t22022.pdf

[104] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3430

[105] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3431

[106] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3432

[107] https://community.acer.com/en/kb/articles/15520-security-vulnerability-regarding-vulnerability-that-may-allow-changes-to-secure-boot-settings

[108] https://www.acer.com/us-en/support?search=Aspire%20A315-22&filter=global_download&suggest=A315-22;0

[109] https://cve.mitre.org/cgi-bin/cvename.cgi?name=2022-4020

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

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

[112] 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.

WeLiveSecurity.com
@ESETresearch
ESET GitHub

Digital Security
Progress. Protected.