Digital Security
Progress. Protected.

Threat Report

H1 2023

December 2022 – May 2023

(eset):research

Contents

Executive summary

Android

Predatory lending practices find new ground on Android

Instead of quick financial assistance, victims of malicious loan apps are met with death threats and digital usury practices.

Cryptocurrency threats

The many faces of cryptocurrency threats

Cryptocurrency threat detections were falling in H1 2023 despite bitcoin's comeback, but we shouldn't celebrate just yet.

Emotet | Downloaders | Attack vectors

Emotet campaigns shrink as operators struggle to find a new attack vector

A once notorious botnet family tries to stay afloat with three seemingly low-impact campaigns in H1 2023.

Attack vectors

Malicious OneNote files: The short-lived limelight of a new intrusion vector

Several high-profile malware families have been testing OneNote as a spreading mechanism.

Email threats | Web threats | Scams | Phishing

Email threats see a sextortion scam comeback

The past half year saw a rise in sextortion scams and phishing.

Exploits | Attack vectors | SQL attacks

Microsoft SQL Server: An increasingly attractive target for brute-force attacks

MSSQL password guessing attacks take a nasty upturn; Log4Shell exploitation attempts continue their endemic growth.

Infostealers | Malware-as-a-Service

RedLine Stealer: Malware as a business

A look at the infamous RedLine infostealer, which recently faced disruption by ESET Research.

macOS | Supply-chain attacks

macOS affected by the first case of two linked supply-chain attacks

One of the spikes observed in macOS detections reveals the first case of interconnected supply-chain attacks, compromising a significant number of macOS devices.

Ransomware

Same code, different ransomware? Leaks kick-start myriad of new variants

Leaks allow more criminals to try their luck with ransomware yet make preexisting detections increasingly effective against emerging malware.

Foreword

Welcome to the H1 2023 issue of the ESET Threat Report!

We are pleased to present the latest issue of ESET Threat Report, which brings changes aimed at making its contents more engaging and accessible. One notable modification is our new approach to data presentation: rather than detailing all data changes within each detection category, our intention is to provide more in-depth analyses of selected, notable developments. For those seeking a comprehensive overview of the telemetry data related to each category, we have included the full set of charts and figures in a dedicated Threat Telemetry section.

Another notable update is the change in publication frequency, transitioning from triannual to a semiannual release schedule. In this issue, we focus on the highlights of H1 2023, covering the period from December 2022 through May 2023. When comparing this period to H2 2022, we refer to the timeframe from June 2022 to November 2022.

In H1 2023, we observed trends highlighting cybercriminals' remarkable adaptability and relentless pursuit of new avenues to achieve their nefarious goals – be it through exploiting vulnerabilities, gaining unauthorized access, compromising sensitive information, or defrauding individuals. One of the reasons for shifts in attack patterns is stricter security policies introduced by Microsoft, particularly on opening macro-enabled files. In a new attempt to bypass these measures, attackers substituted macros with weaponized OneNote files in H1 2023, leveraging the capability of embedding other files directly into OneNote. In response, Microsoft readjusted, prompting cybercriminals to continue exploring alternative intrusion vectors, with intensifying brute-force attacks against Microsoft SQL servers possibly being one of the tested approaches.

Our telemetry data also suggests that operators of the once-notorious Emotet botnet have struggled to adapt to the shrinking attack surface, possibly indicating that a different group acquired the botnet. In the ransomware arena, actors increasingly reused previously leaked source code to build new ransomware variants. While this allows amateurs to engage in ransomware activities, it also enables defenders like us to cover a broader range of variants, including newly emerging ones, with a more generic set of rules and detections.

Although cryptocurrency threats have been steadily declining in our telemetry – not even to be resurrected by the recent increase in bitcoin's value – cryptocurrency-related cybercriminal activities continue to persist, with cryptomining and cryptostealing capabilities increasingly incorporated into more versatile malware strains. This evolution follows a pattern observed in the past, when malware such as keyloggers was initially identified as a separate threat, but eventually became a common capability of many malware families.

Looking at other threats focused on financial gain, we observed a comeback of so-called sextortion scam emails, exploiting people's fears related to their online activities, and an alarming growth of deceptive Android loan apps masquerading as legitimate personal loan services, taking advantage of vulnerable individuals with urgent financial needs.

I wish you an insightful read.

Roman Kováč
ESET Chief Research Officer

Threat Landscape Trends

Android

Predatory lending practices find new ground on Android

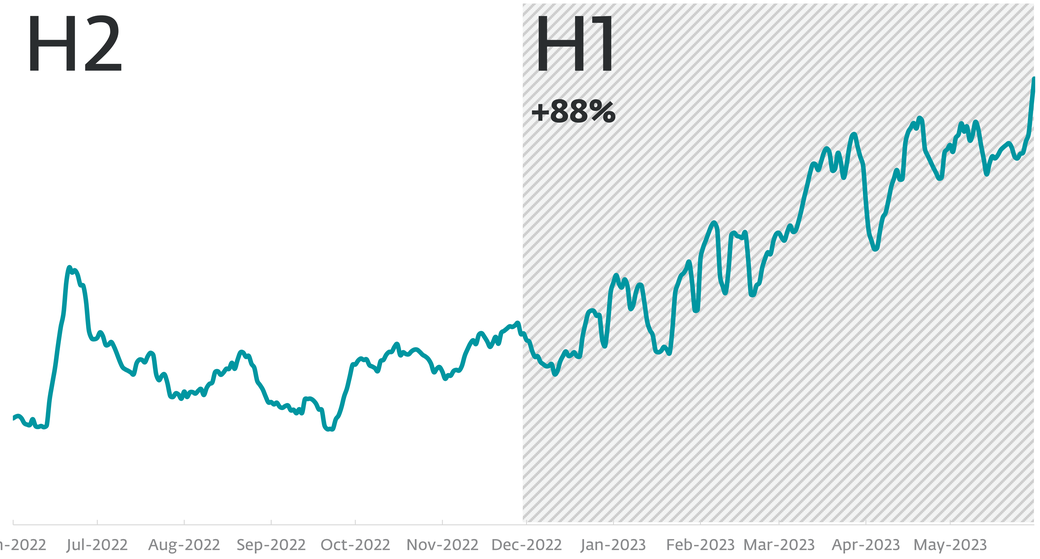
Instead of quick financial assistance, victims of malicious loan apps are met with death threats and digital usury practices.

In H1 2023, ESET telemetry identified an alarming growth of deceptive Android loan apps, which masquerade as legitimate personal loan services, promising users quick and easy access to funds. However, these services are designed to defraud users and gain their personal and financial information. ESET products therefore recognize these apps using the detection name SpyLoan, which directly refers to their spyware functionality combined with loan claims.

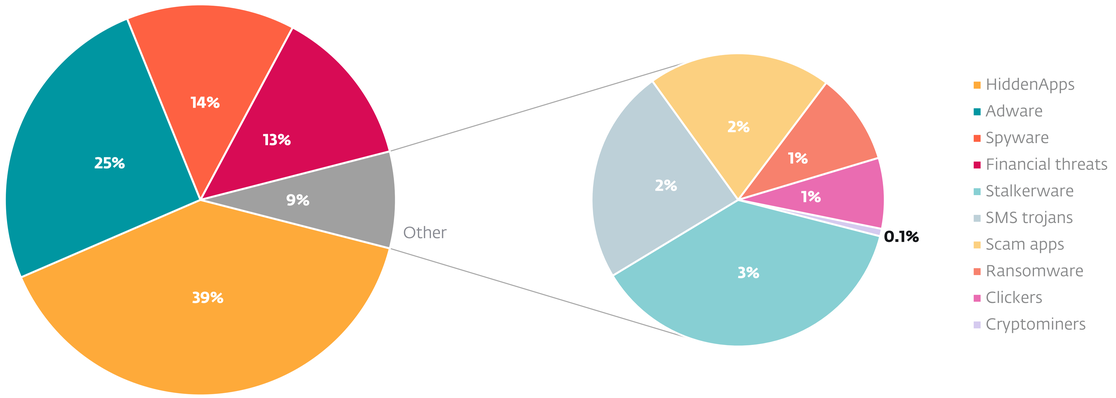
These fraudulent apps are marketed through social media and SMS messages offering personal loans, but the apps themselves are available to download from dedicated scam websites, third-party app stores, and Google Play, as they are not only able to mislead users but also bypass Google Play policies. As a Google App Defense Alliance partner, ESET shared its findings with Google and communication about these applications remains in progress.

Compared to H2 2022, detections of all SpyLoan apps grew by nearly 90% in H1 2023, leading to the overall growth of the Android Spyware category by 19%.

Spyware is by far not the most prevalent threat on Android; this platform has been swarmed by detections that turn a profit for cybercrooks via online ads – Adware, HiddenApps, and Clickers. In ESET Threat Report T3 2022, we explained that behind the pre-Christmas growth of Adware and HiddenApps were free mobile games packed with adware, and the availability of development tools and resources for Android that make it easier for Adware and HiddenApps developers to create and distribute their wares. In H1, which in our case also encompasses



SpyLoan detection trend in H2 2022 and H1 2023, seven-day moving average



Android detection categories in H1 2023

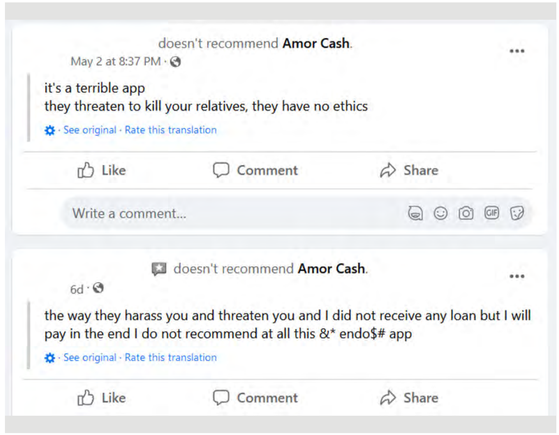
December 2022, the rise of HiddenApps (+42%) and Adware (+19.5%) detections was still mainly connected to gaming apps that serve ads to their users. If we count together the detections of all categories living off ads, their share of all Android detections is 68.4%.

Even though other Android detections visibly declined in H1 2023 – SMS trojans by 62.5%, Ransomware by 50%, and Cryptominers by 16% – the prevalence of Adware and HiddenApps is so significant that overall Android detections increased by 20.2%.

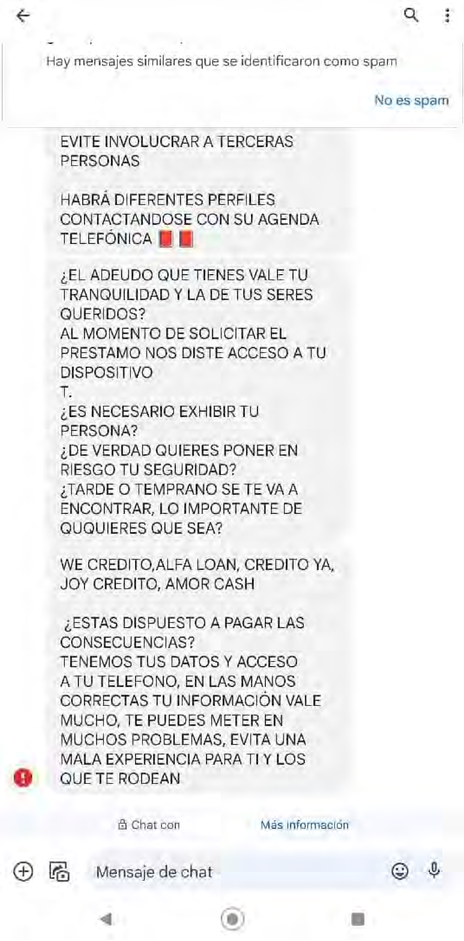
The only type of detection that held its numbers steady was Financial threats, which encompass Banking malware and Cryptostealers – which grew by 4.5%, even though their trend across the current reporting period is generally downward.

While SpyLoan apps also represent a form of financial threat, they differ from banking malware in that they present a form of modern-day digital usury, which refers to the charging of excessive interest rates on loans, taking advantage of vulnerable individuals with urgent financial needs, or borrowers who have limited access to mainstream financial institutions.

Once installed, these apps request permissions to access a list of accounts, call logs, calendar events, device information, installed app lists, local Wi-Fi network information, information about files on the device (such as Exif metadata without actually sending the photographs themselves), contact lists, location data, and SMS messages. Interestingly, according to the reviews, it doesn't matter whether a person applies for or even receives a loan: the app's enforcers start to harass and blackmail their victims into payment, sometimes mentioning death threats, as was documented by their victims. The users of SpyLoan apps also mention that the interest rates are very high, and loan tenure is extremely short – sometimes as short as five or seven days.



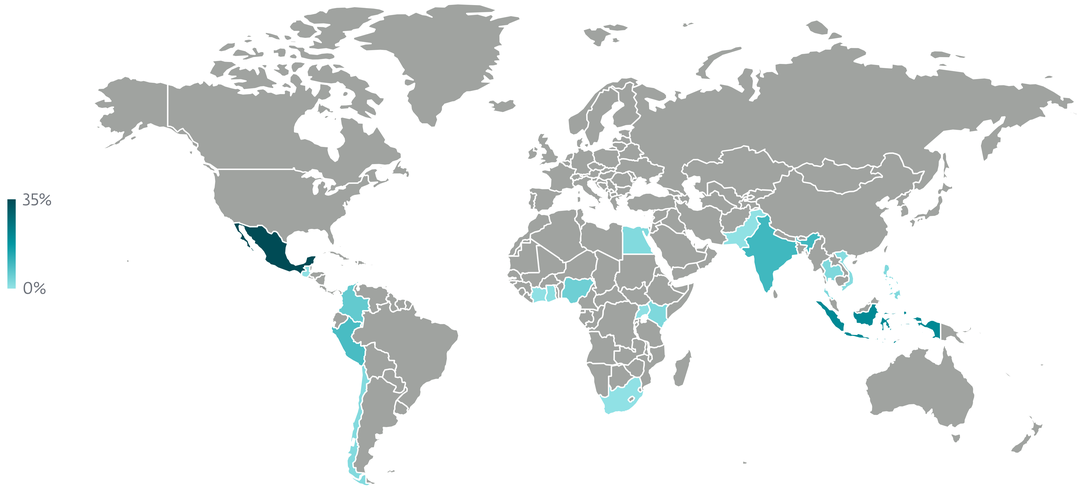
Users of SpyLoan apps claiming to be harassed and threatened



Machine-translated threatening messages posted by one of the reviewers: Is the debt you have worth your peace of mind and that of your loved ones?... Do you really want to put your safety at risk?... Are you willing to pay the consequences? You can get into a lot of problems, avoid a bad experience for yourself and those around you.

According to ESET telemetry, the enforcers of these apps operate mainly in Mexico, Indonesia, Hong Kong, Thailand, India, Pakistan, Colombia, Peru, the Philippines, Egypt, Kenya, Nigeria, and Singapore. We believe that any detections outside of these countries are related to phones that have, for various reasons, access to a phone number registered in one of these countries.

The deceptive communication deployed by SpyLoan apps is so layered and complex that we will describe it in an upcoming blogpost on WeLiveSecurity.com. In general, SpyLoan apps use wording and design elements that closely resemble legitimate loan apps, and this intentional similarity makes it difficult to determine the authenticity of an app, especially when financial and legal terms are involved.



Geographic distribution of SpyLoan detections seen by ESET telemetry in H1 2023

EXPERT COMMENT

Despite the challenges posed by these fraudulent loan apps, there are effective steps users can employ to safeguard themselves. These include sticking to official app sources, reading negative app reviews – as positive ones may be coerced from previous victims – and using a reputable security app. Individuals who have fallen victim to SpyLoan apps should report the incident to local law enforcement or relevant legal authorities, contact consumer protection agencies, *and* notify the governing institution for private loans (often the national bank or its equivalent). If the deceptive loan app was obtained through Google Play, individuals can seek assistance from Google Play Support to report the app and request the removal of their associated personal data. However, it is important to note that the data may have already been extracted to the attacker's command and control server.

Lukáš Štefanko, ESET Senior Malware Researcher

Cryptocurrency threats

The many faces of cryptocurrency threats

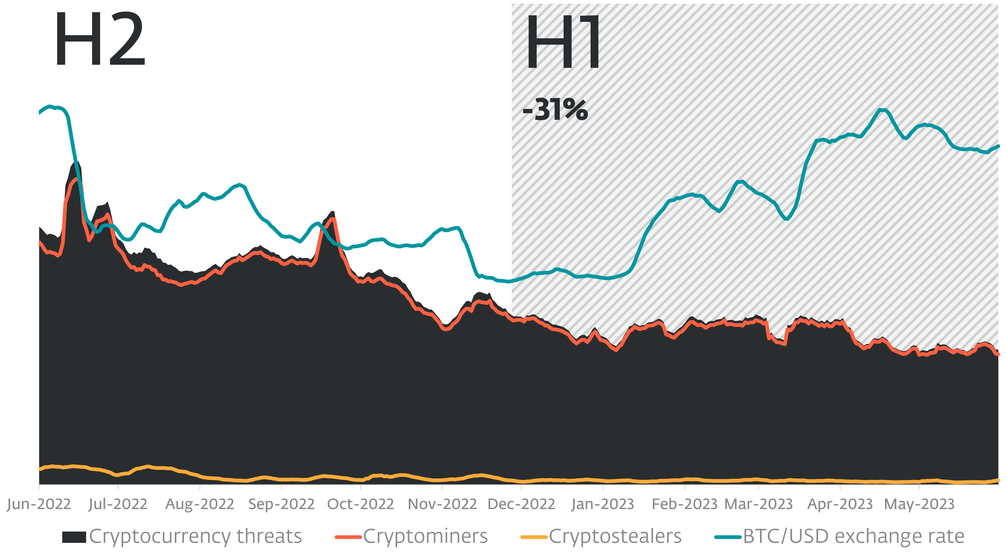
Cryptocurrency threat detections were falling in H1 2023 despite bitcoin's comeback, but we shouldn't celebrate just yet.

Ever since ESET started tracking cryptocurrency threats, their trend roughly corresponded to bitcoin exchange rates. Whether bitcoin rose or fell, it seemed to be a given that cryptocurrency threats[1] would follow suit – until H1 2023, when the trends diverged.

In H1 2023, bitcoin was experiencing a partial resurgence in popularity. After a prolonged decline and the rate staying beneath USD 20,000 per BTC for the most part of November and December of 2022, the cryptocurrency climbed up to the USD 30,000 mark in the middle of April, and hovered around there until the end of the period. Even though that's far from its previous heights, bitcoin is not in freefall anymore. Its recent growth could be a reaction to several bank closures (SVB, Signature Bank, Silvergate), with people forgoing the traditional banking system in favor of decentralized currencies. Still, after the wave of bankruptcies and cryptocurrency hedge fund collapses, culminating in the failure of FTX, it remains to be seen whether bitcoin's growth lasts.

Conversely, the cryptocurrency threats trend saw no growth in H1 2023. Detections in this category continued to steadily decrease, amounting to an overall 31% decline between periods. This raises questions – where has all the cryptomalware gone? Are cybercriminals simply done with cryptomining and cryptostealing, or is there something more going on?

On the one hand, ESET telemetry has indeed registered a decline in new cryptocurrency threat detections in the past few months. There have also been a number of successful law enforcement operations targeting cryptocurrency-related crime recently. Fear of retaliation might play a part in why threat actors could be reconsidering their crypto-focused operations, leading to a lower number of detections. The ever-fluctuating exchange rates of cryptocoins probably act as a further deterrent. On the other hand, looking only at threats that solely focus on cryptocurrency might not be enough anymore when talking about this part of the threat landscape. Over the years, malicious



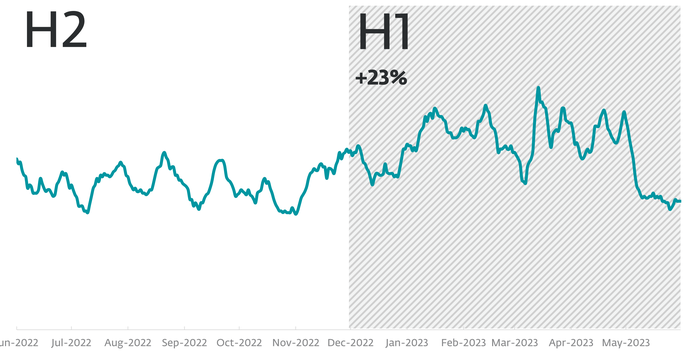
Cryptocurrency threat detection trend and bitcoin/USD exchange rate in H2 2022 and H1 2023, seven-day moving average

[1] *Cryptomining and cryptostealing malware*

activity surrounding cryptocurrencies has diversified considerably. Since threat actors presumably want to maximize their profits, it would make sense for them to abandon threats focused purely on cryptocurrencies in favor of malware with broader capabilities. As such, cryptostealing and/or cryptomining components have now also become part of other malware.

Among the most well-known infostealers, **RedLine Stealer**, Agent Tesla, and Racoon Stealer all have cryptostealing capabilities, while for example the Fareit trojan is able to mine cryptocurrency on a compromised machine. These are all big malware families with the combined detections counting in the hundreds of thousands – even if cryptocurrency is not their main focus, they have a wide reach.

Other threats have also jumped on the cryptomalware bandwagon: as a feature, cryptostealing is now integrated into so many ClipBanker families (i.e., threats that steal or manipulate the data in the clipboard) that they cannot be cleanly separated from cryptocurrency threats anymore. These threats grew by 23% in H1 2023.



ClipBanker detection trend in H2 2022 and H1 2023, seven-day moving average

The situation is very similar over in Android threats, where we reclassified the banking subcategory as Financial threats due to the prevalence of cryptostealing features. Compared to the ClipBanker families, the trend of Android financial threats has been stable over H2 2022 and H1 2023.

For an example of just how insidious cryptocurrency threats preying on Android users can be, ESET researchers **found** dozens of clippers in the form of trojanized WhatsApp and Telegram apps that can switch cryptocurrency wallet addresses that victims send in chat messages to addresses belonging to the attacker. Often, the victim has no chance of knowing the wallet address has been switched, as the changed address is visible only to the recipient of the message.

Another way of spreading cryptomalware is via botnets. One such botnet is Amadey, a popular downloader sold on underground forums whose source code has been leaked online. Among other capabilities, the malware can steal cryptowallet information. This botnet experienced significant growth in H1 2023; its numbers skyrocketed by almost 370% between periods. Danabot, another botnet tracked by ESET, was seen pushing both executables with crypotostealers, and later also LaplasBanker, which can replace cryptowallet addresses.

EXPERT COMMENT

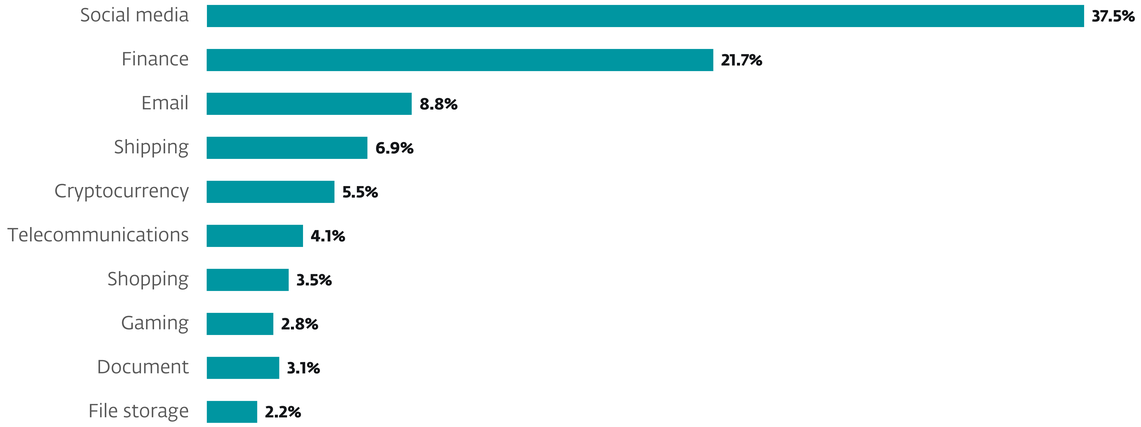
It appears that the decline of the cryptocurrency threat landscape, which even bitcoin's current return to form could not reverse, will continue. However, the greed of cybercriminals means that as long as there are cryptocurrencies, there will also be threats going after them, at least in some shape or another. Even though over time there might be less and less crimeware in this category, features targeting cryptocurrency are becoming part of other malware. Those multipurpose threats, alongside various scams and phishing efforts, serve as a reminder to always stay vigilant.

Igor Kabina, ESET Senior Detection Engineer

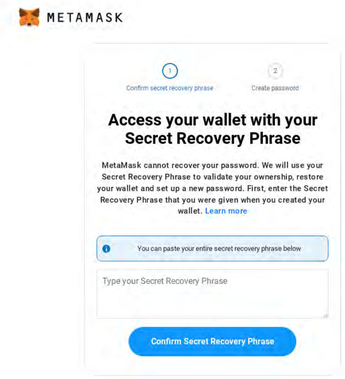
While cryptocurrency crimeware has become more and more widespread over time, the activity of cybercriminals has coalesced around various cryptoscams and phishing. A prime example is the notorious **"pig butchering"** scheme, with many such scams still going strong in H1 2023. In these schemes, criminals first use social engineering methods to gain their victims' trust, build a close relationship with them, and then convince them to put increasing amounts of money into fake cryptocurrency ventures, such as copycat investment apps. Once the targets have no more money to give, the scammers steal the funds and disappear. These schemes seem to be immensely profitable: recently, the US Department of Justice **seized** over USD 112 million in funds from various operations running pig butchering scams.

Similar to other malware, phishing services can also be turned into a product, with threat actors offering phishing-as-a-service (PhaaS) to interested parties. Recently, a PhaaS operation focusing on cryptocurrency scams has been **identified** by Scam Sniffer. The operation is run by a scam vendor called Inferno Drainer; it had made close to USD 6 million in stolen cryptocurrency at the time of reporting, having created hundreds of phishing websites impersonating well-known crypto-brands such as MetaMask and OpenSea. The operators offer an administration panel to manage the phishing campaigns, as well as the option to build phishing websites for the prospective buyers in exchange for a 30% slice of the proceeds.

According to ESET phishing feeds, cryptocurrency-themed phishing lures ranked fifth in H1 2023. Searching through the feeds, we saw numerous instances of cryptocurrency exchange platform impersonators, fraudulent play-to-earn games, and cryptocurrency-giveaway scams.



Top 10 phishing website categories in H1 2023 by number of unique URLs



Examples of cryptocurrency-themed phishing and scam websites seen in ESET phishing feeds

Emotet Downloaders Attack vectors

Emotet campaigns shrink as operators struggle to find a new attack vector

A once notorious botnet family tries to stay afloat with three seemingly low-impact campaigns in H1 2023.

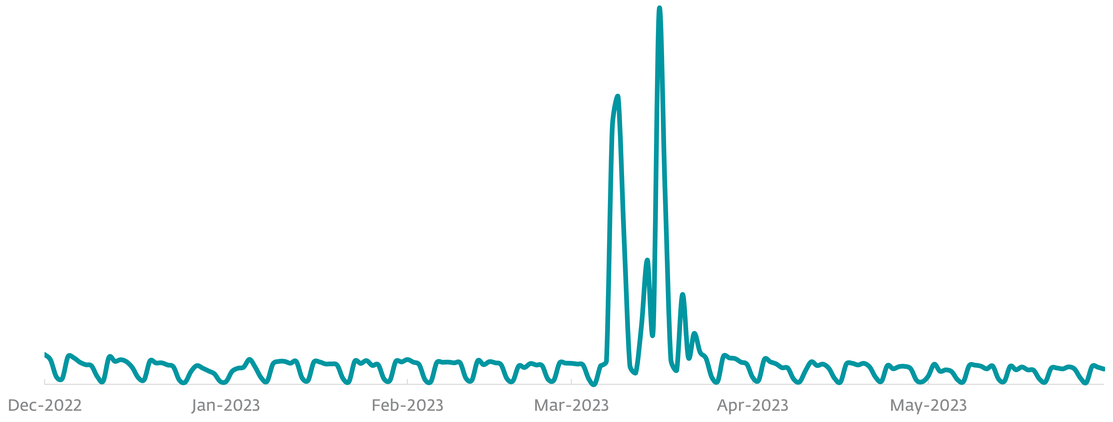
Ever since Visual Basic for Applications (VBA) macros from the internet have been disabled in Office documents, Emotet operators have been scrambling to find an alternative attack vector that would prove similarly effective. In H1 2023, they ran three distinctive malspam campaigns, each testing a slightly different intrusion avenue and social engineering technique. However, the shrinking size of the attacks and constant changes in the approach may suggest dissatisfaction with the outcomes.

After a typical several-month-long hiatus, the Emotet botnet became active again. Around March 8, 2023, it started distributing Word documents with embedded malicious VBA macros, masquerading as invoices. To avoid detection and prolong the sample processing, the operators artificially inflated the size of the files to over 500 MB – a well-known technique previously used by crimeware and APT groups.

Two notable things about this wave of malspam: First the operators didn't use reply-chain attacks, a technique that would make the malicious emails look more legitimate by injecting them into a preexisting conversation of the victim.

Second, it seems an odd choice to use VBA macros, which Microsoft disabled by default in documents coming from the internet. This means most of the victims simply couldn't run the embedded malicious code. Even if they jumped through all the hoops necessary to activate the macro, a reliable multilayered security solution would still detect and block either the download of Emotet's binary or its subsequent activity.

In their second campaign between March 13 and March 18, attackers seemingly acknowledged these flaws, and apart from using the reply-chain approach, they also switched from VBA macros to OneNote files (`.one`)



2023 Emotet campaigns as seen in ESET telemetry.

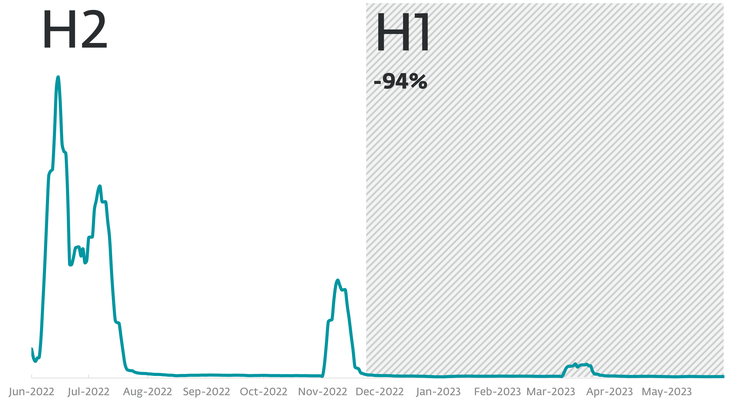
with embedded VBS scripts. If victims opened these files, they were greeted by what looked like a protected **OneNote page**, asking them to click a View button to see the content. Behind this graphic element was a hidden VBS script, set to download and execute the Emotet DLL.

Despite a OneNote warning that this action might lead to malicious content, people tend to click at similar prompts by habit and thus can potentially allow the attackers to compromise their devices.

According to ESET telemetry, March 20 saw the launch of the last of these campaigns, taking advantage of the end of the tax year in the United States. The malicious emails sent by the botnet pretended to come from the US Internal Revenue Service (IRS) tax office and carried the attached ZIP file named `W-9 form`.

Similar to the first 2023 wave, the ZIP file contained an artificially inflated Word document using the same name as the ZIP requiring the user to enable an embedded VBA macro. Again, this has probably hit a dead end with the default macro-disabling policy in place. Using a country-specific tax-related theme also limited the potential impact of the campaign exclusively to the USA. However, ESET systems also detected a less prevalent use of embedded VBScript, indicating that another campaign using the OneNote approach was underway at the same time.

Overall, the 2023 Emotet campaigns accounted only for tens of thousands of detections, a drop of almost 95% compared to the multimillion detection rates in H2 2022. The most frequently used attack vectors were weaponized Office files – typically Word documents and Excel spreadsheets – accounting for 58% of the detected attacks, followed by VBA macros in 29% of cases and 10% using embedded VBS scripts. Most of the attacks detected by ESET systems were aimed at Japan (31%), Italy (11%), and Mexico (5.5%),



Latest Emotet campaigns compared to its previous activity in H2 2022.

although these numbers may be biased by the strong ESET user base in these regions.

It remains unclear why Emotet operators relied so heavily on the disabled-by-default VBA macros and why some campaigns didn't use the reply-chain attacks, which would have helped improve their reach. Emotet has been known for its effectiveness in the past, and these flaws might further support rumors from H2 2022 that a different – probably less-skilled – threat group has bought the botnet and its infrastructure.

EMOTET OVERVIEW

First sighted as a banking trojan in June 2014, Emotet has since changed into a crime-as-a-service platform, selling access to compromised systems to other criminal groups. Thus, once Emotet is running on a computer, it typically downloads and executes other strains of malware.

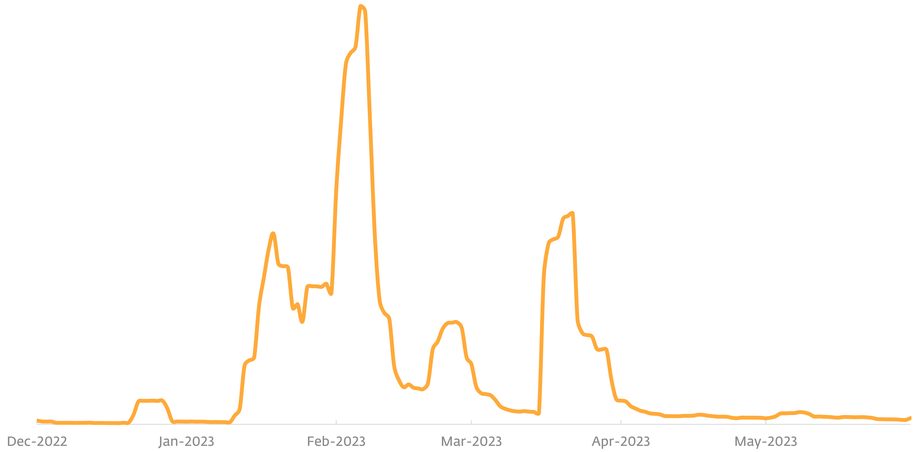
Emotet has a modular program design, with a main module distributed through spam emails, historically containing malicious Microsoft Word documents. Emotet then uses additional modules to spread further, brute-force network share usernames and passwords, turn compromised systems into proxies, steal email addresses and messages from the compromised systems, and perform other malicious actions.

Microsoft's move to **throw out the "Enable Content" button** came at a time for Emotet when, after recovering from **takedown efforts from 2021**, it had been **churning out spam campaigns** in March and April 2022. Taking note of the change, Emotet's developers have shifted to experimenting with different techniques to replace their dependence on macros as the initial stage of their malware delivery platform.

Attack vectors

Malicious OneNote files: The short-lived limelight of a new intrusion vector

Several high-profile malware families have been testing OneNote as a spreading mechanism.



Detection trend of weaponized OneNote files seen in ESET telemetry in H1 2023

Hiding an attached malicious file or a script behind what looks like a clickable button in a OneNote file (.one) might sound too simple to be a viable attack vector. However, ESET telemetry shows it was used by a broad range of cybercriminals in H1 2023, with attackers distributing weaponized Microsoft OneNote files in order to spread additional malware.

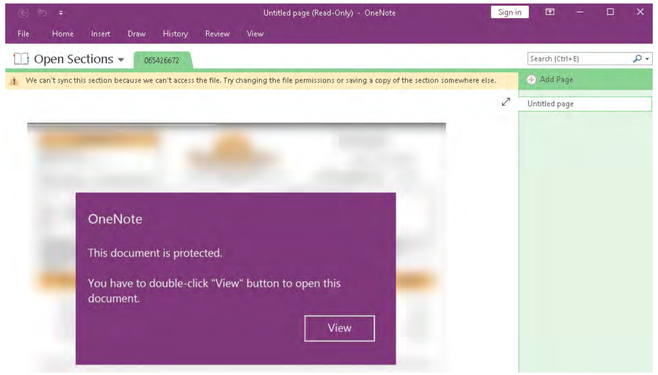
When first detected in December 2022, OneNote files as attack vectors only accounted for a couple of hundred detections. Compared to that, the number of attacks utilizing this approach from January to May 2023 grew dramatically, increasing to a total of almost 90,000 detections. Looking at the trend chart, February and March were the busiest months, with OneNote becoming a part of the intrusion chain of a long list of malware families, including **Emotet**, **RedLine Stealer**, Qbot, Formbook, AsyncRAT, XWorm, Quasar, IcedID, and even **BlackBasta ransomware**.

Why did cybercriminals suddenly adopt this new vector? It was only after several of their previous go-to attack avenues turned into dead ends. First, Microsoft disabled VBA macros in Office files that come from the internet, closing a loophole abused for years. Attackers then tried to **shift to ISO and password-protected**

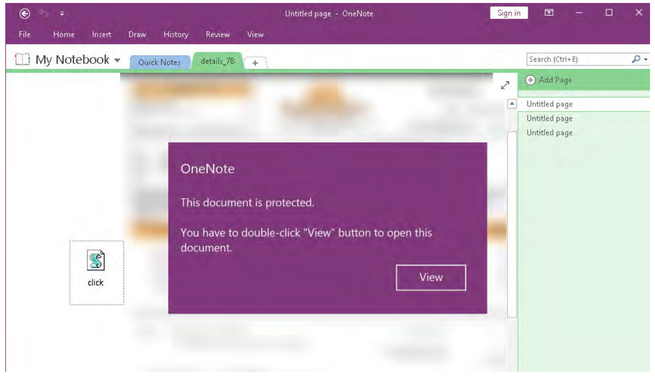
EXPERT COMMENT

If the scenario of VBA macros repeats itself, OneNote files will become significantly less attractive for mass spread campaigns, and cybercriminals will again start looking for new ways to compromise the devices of their victims. However, the limited rollout that excluded the web version, Windows 10, macOS, and mobile platforms from the stricter settings may still leave an interesting attack surface for some cybercriminals who will decide to keep weaponized .one files in their arsenal.

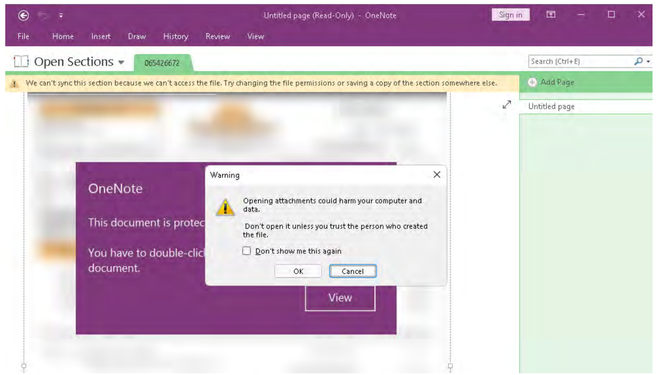
Dušan Lacika, Senior Detection Engineer



A "protected" OneNote notebook, requesting the victim to double-click a View button



A malicious VBScript hidden underneath the notification redirecting to the attacker's server



OneNote warning informing the user of the risks associated with running the embeded content

[ZIP files], which had bugs in their [mark-of-the-web] propagation, yet these were quickly fixed, reigniting the hunt for new vectors once again.

What made OneNote files so attractive to the attackers was that while serving as a digital notebook, the app also allows users to embed other files directly into the documents and open them with a simple double-click. While this functionality is commonly used to drag-and-drop spreadsheets and/or other documents to amend written notes, malicious actors found it useful when embedding their malicious code, such as VBScripts and HTA files.

To mask their nefarious intentions, attackers created the illusion of protected content in the background, prompting the victim to double-click a View button to access it. Behind the button prompt was a malicious script or a file that accessed a remote site online and downloaded a bundle of further malware and a decoy document displayed to the victim.

As this new vector emerged, administrators could mitigate OneNote threats by disabling a selected group of or all embedded attachments in `.one` files.

Also, OneNote by default displayed a pop-up warning that informed of the potentially malicious nature of the embedded content. Unfortunately, documented by the years of abuse of the "Enable macros" banner in Office documents and by the cookie notices on websites, most users don't pay attention to such warnings and proceed anyway.

To tighten OneNote security, Microsoft decided to disable [120 file extensions] if embedded in a OneNote file, effective since April 2022. The displayed notification had also been updated, informing users that their "administrator has blocked their ability to open this file type in OneNote". Admins have the option to reenable these extensions via Office policies, if they have a specific use case in their environment. However, it is important to note that at the time of writing, this change only affects the OneNote for Microsoft 365 and OneNote in retail versions, but does not apply to the Android, iOS, Win 10, and web versions of OneNote.

RECOMMENDATIONS

- Using the latest version of the Windows operating system ensures that the attachments with 120 potentially risky extensions in `.one` files are disabled by default.
- If there is no use case in the organization, set mail servers to block email messages with attached `.one` files.
- Administrators running OneNote versions that are excluded from the stricter rule setting must install the Microsoft Office group policy templates and use these to disable embedded attachments and specific extensions in OneNote documents. Based on the previous attacks, the suggested file extensions to block are `.js`, `.exe`, `.com`, `.cmd`, `.scr`, `.ps1`, `.vbs`, and `.lnk`.
- A reliable multilayered security solution can detect and block malicious activity stemming from `.one` files.

Email threats Web threats Scams Phishing

Email threats see a sextortion scam comeback

The past half year saw a rise in sextortion scams and phishing.

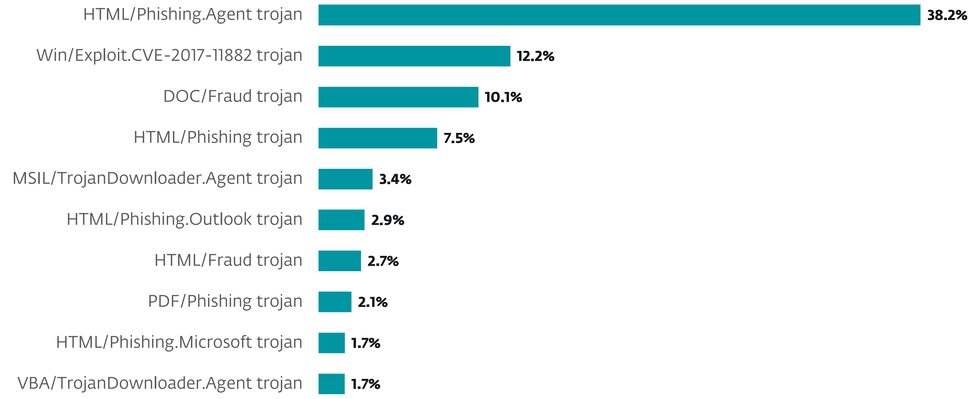
Among email threats, the most remarkable growth rate observed in H1 2023 was the 201% leap in DOC/Fraud detections, primarily affecting Japan, Spain, and France. This family covers mainly Microsoft Word documents with various types of fraudulent content, distributed via email attachments. Due to an increase in sextortion scams, detections returned to levels not seen since 2021.

In a **sextortion scam**, fraudsters send an email claiming to have installed malware on the recipient's computer that enables them to gather data of a sexual nature – such a claim should be confidently ignored as an empty threat.

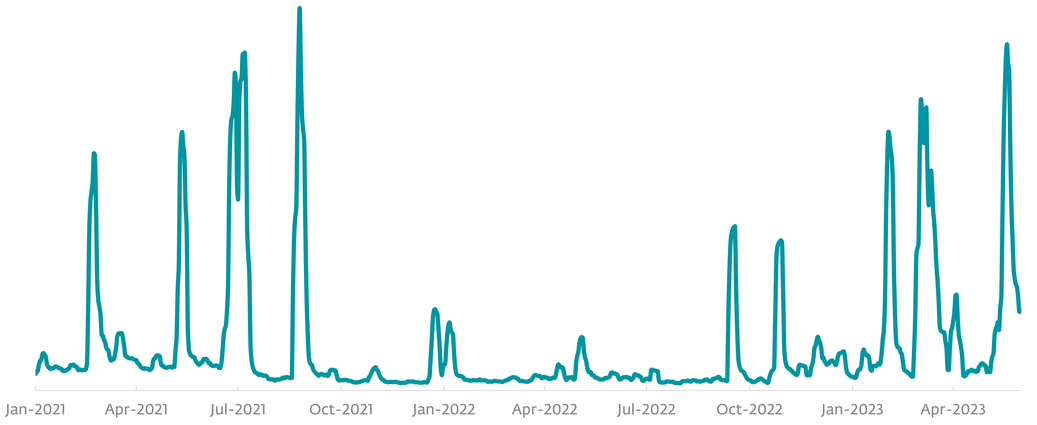
The top variant of this family in H1 2023 was DOC/Fraud.AAW, which we observed demanding USD 1550 worth of Bitcoin in return for not divulging the sexual content the attacker claimed to have recorded via the victim's camera. Subsequent top variants were ATT and ADJ, which are similar scams claiming to have stolen data including sexual content.

At the time of writing, one Bitcoin address observed among these extortion demands successfully garnered over **0.08 Bitcoin**, currently worth over USD 2,000, and was then emptied. Another remained **utterly empty**.

Even with sometimes no financial gain in sight, the family ranked third among all email threats detected by our email scanners.



Top 10 email threats detected in H1 2023



DOC/Fraud detection trend from January 2021 to May 2023

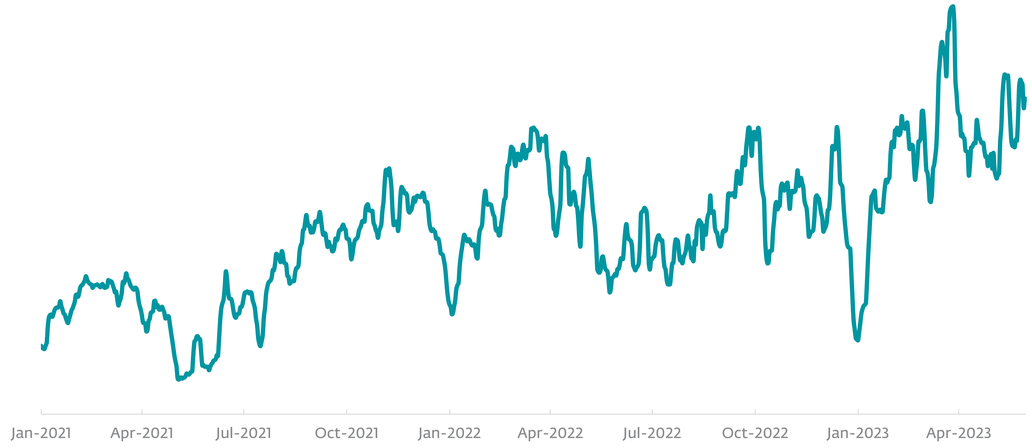
Holding steady as the top email threat in H1 2023, HTML/Phishing.Agent accounted for 38% of detections. This detection name refers to malicious HTML documents sent as email attachments. Opening such an attachment in a web browser opens a phishing site that typically poses as a banking, payment, or social networking provider. Most detections in the current reporting period were in Japan, the United States, and the United Kingdom.

While the current top variants of this family all decreased, on March 22, 2023, the family reached a new peak that has not been seen as far back as 2021.

This peak was driven by two variants: DTS, which first appeared that day, and BRZ.

HTML/Phishing.Agent.DTS is a weak attempt at phishing for Microsoft Outlook credentials using an email without body text and an attachment called `RemittanceAdvice.html`. Opening this HTML file in a browser displays an Outlook login form lacking styling.

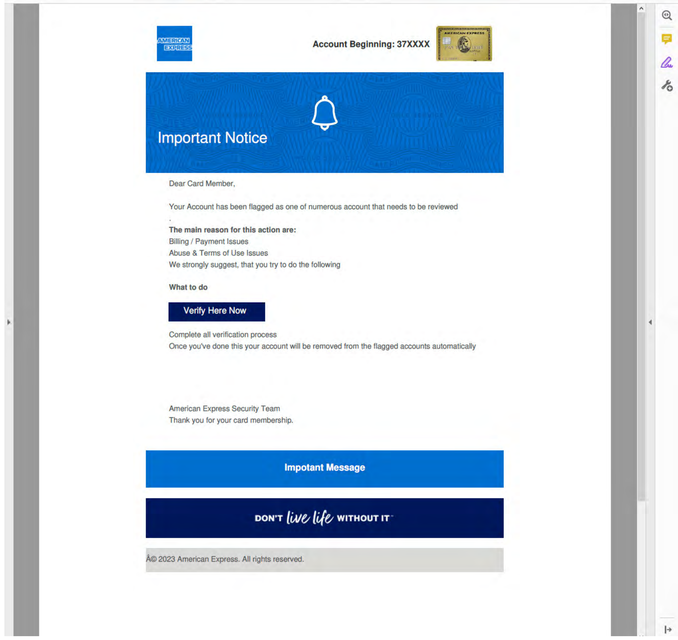
HTML/Phishing.Agent.BRZ is a Microsoft 365 phishing threat we observed spreading as an email attachment called `DepositRemittance.html`. Opening this attachment in a browser displays an Office 365 login page with the username prefilled.



HTML/Phishing.Agent detection trend from January 2021 to May 2023

Homing in on brand-specific phishing threats, HTML/Phishing.Outlook returned to the top 10 email threats list, taking the sixth position after a 30% increase over the previous half year. The most prevalent variant was AQ, which we saw spreading as an email attachment called `Remittance_230323.htm`. Opening this attachment in a browser prefills the username (the same as the email recipient) and exfiltrates any credentials provided by the victim via a legitimate but compromised website (advertising travel in Greece).

Tracked as PDF/Phishing, the abuse of PDF attachments for phishing also grew substantially, by 88%, placing it eighth in the top 10 email threats list. A top variant in H1 2023 consisted of a link in a PDF document that navigates to a login page in Italian asking for account details. Another top variant was a PDF document posing as a notice from American Express with a Verify Here Now button that leads to a phishing website.



Phishing threats also contributed to the growth of web threats. In H1 2023, the number of blocked web threats increased by 31% compared to the previous half year. This increase was partly due to the 125% jump in phishing blocks, although scam blocks were the main growth contributor.

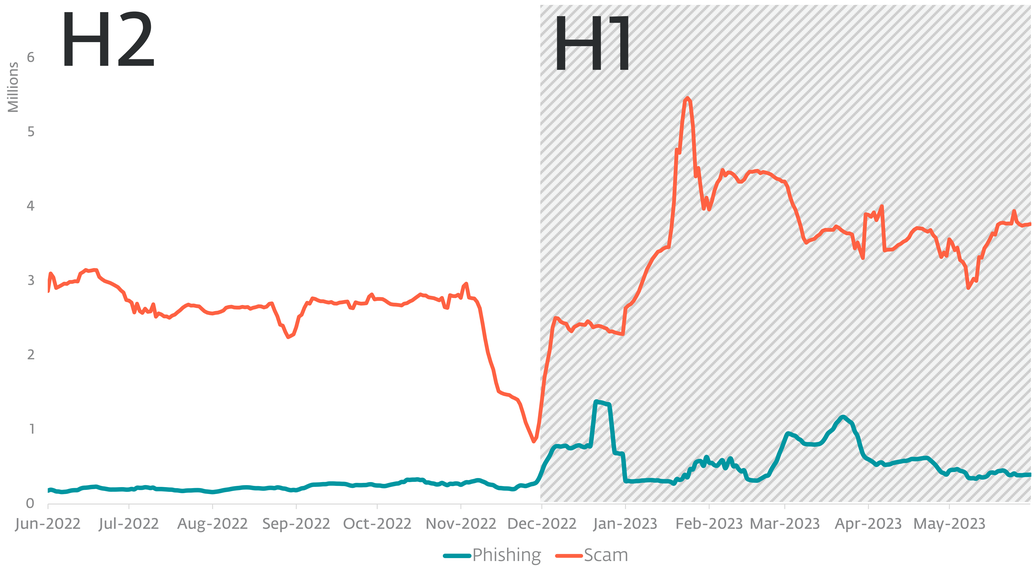
Interestingly, several spikes in our web threat data for H1 2023 revealed a common theme: threat actors are placing malicious domains into redirect chains used by advertisements on legitimate websites. Web pages at such domains sometimes act legitimately, but at other times turn malicious, aggressively pushing scams, malvertising, phishing, and other suspicious content to website visitors.

Racking up over 57 million blocks, one example of a malicious domain is `pogothere[.]xyz`, which was still alive at the time of publication. This domain can be found in ad redirect chains on shady sites offering cracked software or game hacks.

Another example is `123w0w[.]com`, which was found leading to a landing page masquerading as a YouTube video player that requests the download of a plugin to play the video.

Yet another case is `viixikup[.]com`. Usually, this domain redirects to a potentially unwanted or harmful site that harasses visitors with aggressive advertising or scam products. One last specimen is `asxcnx[.]com`, a domain that was seen redirecting to **tech support scam sites** and pages abusing Netflix branding to phish for payment card details.

A landing page for `asxcnx[.]com` that impersonates Netflix in German



Phishing and scam block trends in H1 2023, seven-day moving average

Exploits Attack vectors SQL attacks

Microsoft SQL Server: An increasingly attractive target for brute-force attacks

MSSQL password guessing attacks take a nasty upturn; Log4Shell exploitation attempts continue their endemic growth.

Microsoft SQL (MSSQL) Server has gained renewed interest among cybercriminals as an initial access vector. ESET telemetry data shows a rising trend in blocked password guessing attempts against MSSQL from 940 million in H2 2022 to 1.7 billion in H1 2023. This growth is set against a backdrop of a decline in password guessing attacks against other popular services, such as Remote Desktop Protocol (RDP), from 17.9 billion to 15.8 billion, and Server Message Block (SMB) protocol, from 469 million to 399 million.

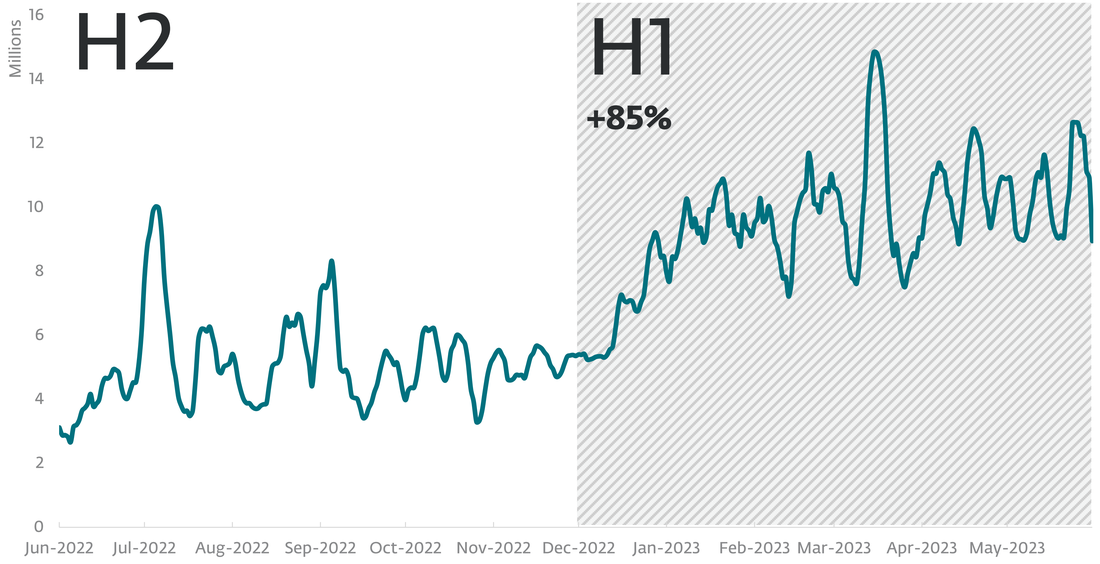
In H1 2023, as usual, the most popular network intrusion method tried by external actors was password guessing, followed by Log4Shell exploitation.

Compared to H2 2022, the list of top external network attack vectors remains unchanged. However, the growing trend of MSSQL attacks in the password guessing category deserves a closer look.

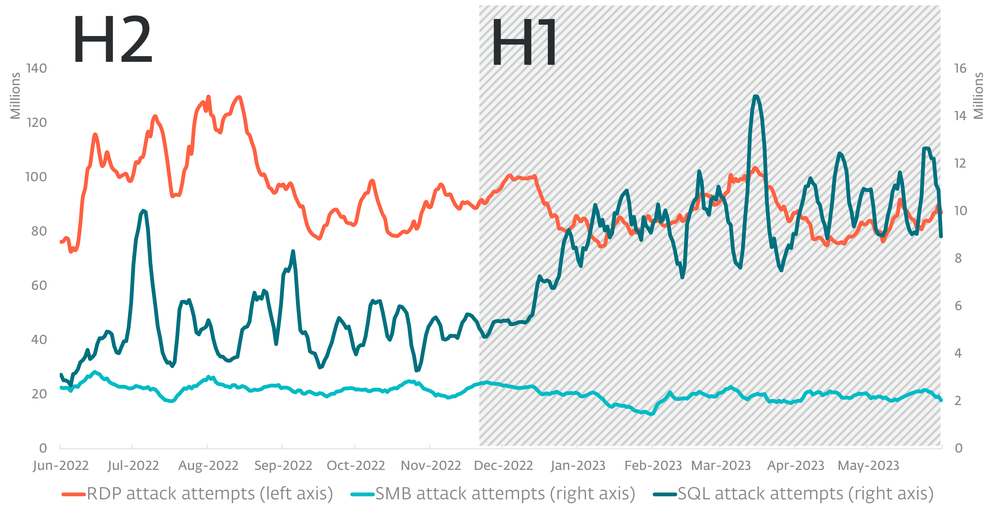
MSSQL brute-force attacks

MSSQL is a relational database management system popular in corporate environments. If this server is made accessible via the internet, it listens by default for TCP connections on port 1433, thus making this port a prime target for brute-force attacks. Obviously, legitimate database users should authenticate before being allowed to access any data. While we hope that strong and unique passwords are being used to deter intruders, the persistent efforts of cybercriminals to find exposed MSSQL services that are poorly secured are sometimes rewarded.

On April 17, 2023, AhnLab researchers **reported** spotting Trigona ransomware (detected by ESET security products as Win32/Filecoder.OLC) on an MSSQL server that could easily be accessed by guessing



Detection trend of MSSQL attack attempts, seven-day moving average



Trends of RDP, SMB, and SQL password guessing attempts, seven-day moving average

valid credentials.

Our data shows that the absolute count of MSSQL attacks increased by 84% between the past two half-year periods.

Considering that Microsoft has been tightening up the security policies around **opening macro-enabled files** and, starting in 2023, files with one of a multitude of **dangerous file extensions used by OneNote**, cybercriminals may be looking at MSSQL and other intrusion vectors more closely.

Geographically, most MSSQL brute-force attacks in H1 2023 were directed at services in Turkey, the USA, and Poland. It should be kept in mind that any geographical data based on IP addresses is probably affected by the use of VPNs, rented servers, and proxy services.

Despite the rise of SQL attacks, it should be noted that RDP brute-force attacks consistently take the lion's share of password guessing attempts, accounting for an average of 87 million attacks per day in our telemetry data. However, the RDP attack trendline continued the decline seen since 2022. The SMB attack trendline followed suit.

EXPERT COMMENT

With the rise of brute-force attacks against MSSQL, database admins should be reminded of the security benefits of **Windows Authentication mode** over mixed mode when setting up the database engine. In Windows Authentication mode, SQL Server Authentication is disabled, compelling database users to connect through their Windows user account, which can be protected with an **account lockout policy** that effectively stops brute-force attacks from progressing.

If you can't avoid using mixed mode, make sure passwords are strong and put the database behind a firewall or VPN, if possible.

Ladislav Janko, ESET Senior Detection Engineer

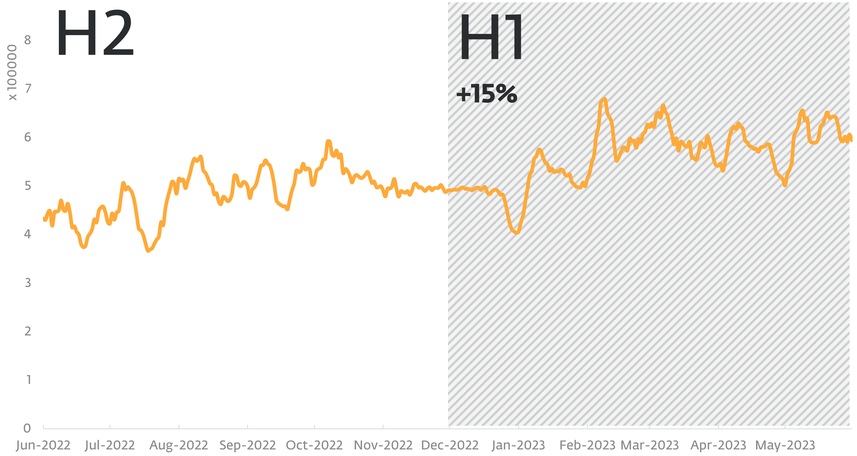
Log4Shell

The **Log4Shell vulnerability** continues to land second in the external intrusion vector ranking. Patches have been available for the flaw since December 2021, yet the graph of exploitation attempts shows a rise of 16% in H1 2023.

While many countries experienced a growth in attacks compared to H2 2022, Poland stands out with an explosion of growth, seeing over triple the average number of daily attacks since mid-September.

Two days after Log4Shell exploitation attempts peaked on February 7, 2023, CISA **warned** that North Korea-aligned ransomware operators had been targeting healthcare systems in South Korea and the USA. One of the techniques used to gain access to victims' networks was the exploitation of Log4Shell. AhnLab researchers **reported** that Lazarus, a North Korea-aligned group, was also exploiting this vulnerability. North Korea seems to be a hotbed of Log4Shell exploiters.

Due to the continued and frequent exploitation attempts of Log4Shell, on May 1, 2023, CISA **added** CVE-2021-45046, discovered after the incomplete fix of CVE-2021-44228, to its Known Exploited Vulnerabilities Catalog. Our data on Log4Shell exploitation attempts does not distinguish between these CVEs. Since it is not possible to inspect encrypted network traffic for additional exploitation attempts, anyone still using



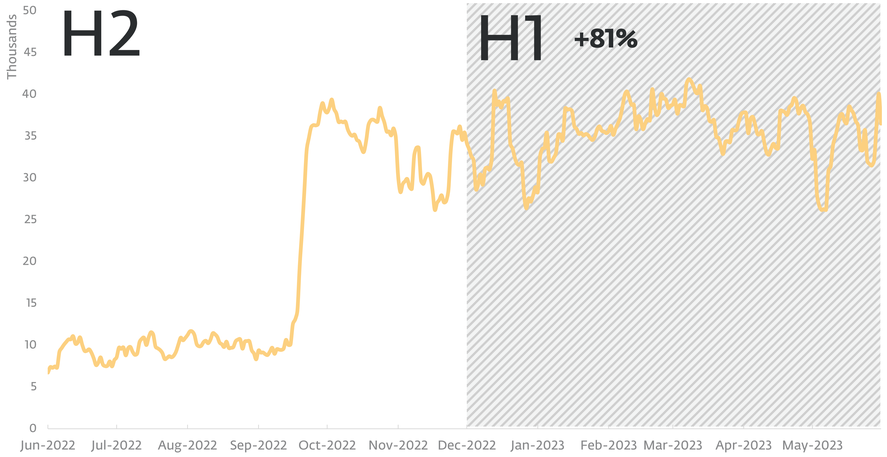
Detection trend of Log4Shell exploitation attempts, seven-day moving average

a vulnerable version of the Log4j library is urged to update rather than hope that attackers attempt to exploit the vulnerability via plaintext.

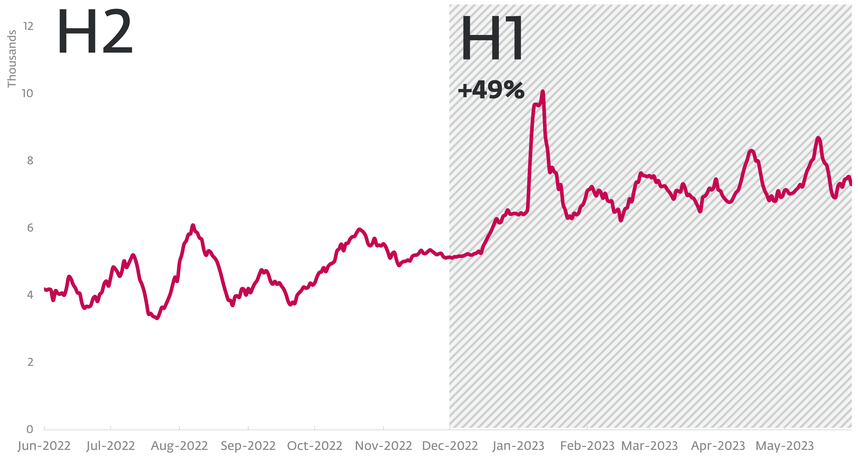
Spring4Shell

Although **Spring4Shell** attacks have not returned to their pre-May-2022 levels, a steady rise has been observed in H1 2023, a 50% increase compared to the previous half year. The spike observed on January 6, 2023 was mainly due to increased detections in the USA, the UK, and China.

Who might be carrying Spring4Shell exploits in their toolkit? In December 2022, Fortinet researchers **published** an analysis of a new botnet called Zerobot. While a Log4Shell exploit is not present within the list of 31 exploits in Zerobot's arsenal, a Spring4Shell exploit is featured.



Detection trend of Log4Shell exploitation attempts in Poland, seven-day moving average



Detection trend of Spring4Shell exploitation attempts, seven-day moving average

Infostealers Malware-as-a-Service

RedLine Stealer: Malware as a business

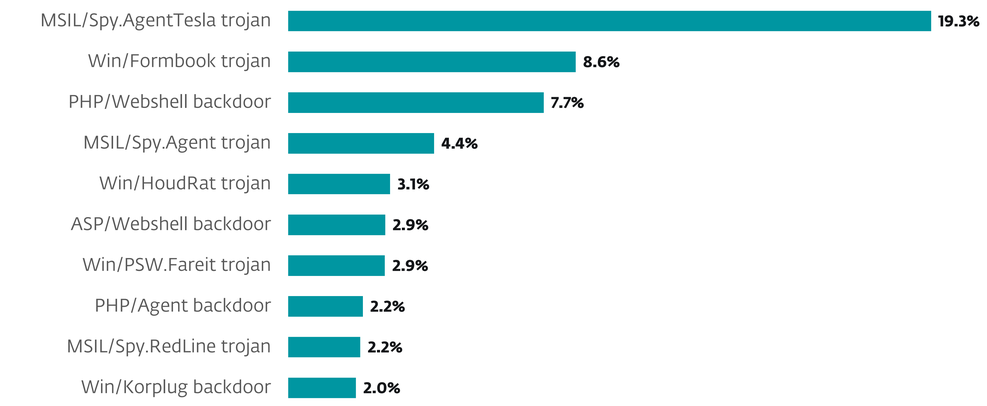
A look at the infamous RedLine infostealer, which recently faced disruption by ESET Research.

RedLine Stealer has been gaining notoriety ever since its discovery in 2020 by **Proofpoint**. Detected by ESET products as MSIL/Spy.RedLine, this infostealer-for-hire, readily available on underground forums, usually makes the news every couple of weeks . In April 2023, the news was positive for once: while investigating the malware with Flare Systems, ESET researchers managed to temporarily disrupt part of RedLine Stealer's operations.

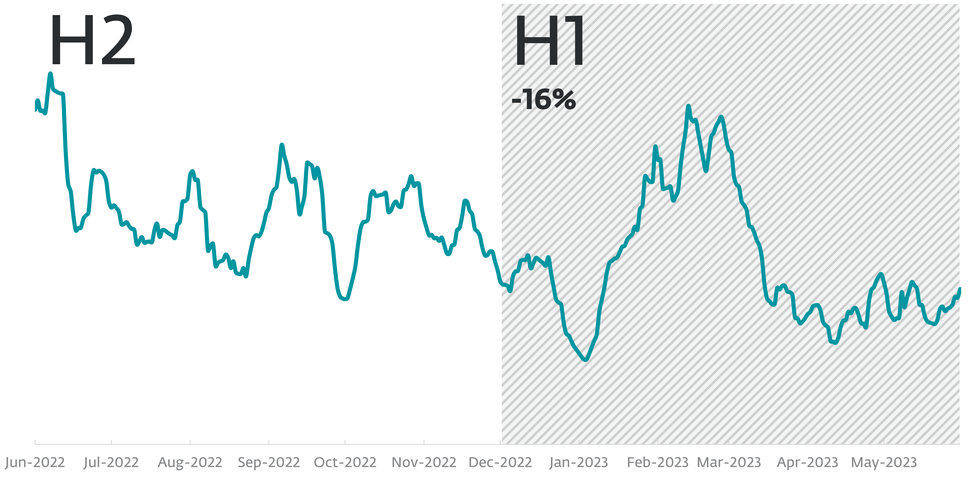
Many threat actors realized long ago that malware can be made into a sustainable (albeit extremely illegal) business. Thus malware-as-a-service, or MaaS, came into existence: threat actors decided to turn their malware into products that can be offered for a fee and produce a steady source of income. A quick look at ESET telemetry data readily demonstrates the prevalence of MaaS among cybercriminals – in H1 2023, there were three MaaS families in our infostealer top-ten statistics: MSIL/Spy.AgentTesla, Win/Formbook, and MSIL/Spy.Redline. The three families together made for more than half of the top ten infostealer detections, with their numbers counting in the hundreds of thousands.

In general, MaaS is a premade malware solution that can be leased by cybercriminals. In exchange for their payments, the clients often gain access to not only the malware itself, but also to botnets and customer service provided by the MaaS creators. This approach brings malware access to criminals who would not ordinarily be able to code a sophisticated solution themselves, thereby contributing to the proliferation of malicious campaigns.

Lately, one particular MaaS variant has risen in prominence – RedLine Stealer. After its discovery in 2020, it soon became one of the most prevalent



Top 10 infostealer families in H1 2023 (% of Infostealer detections)



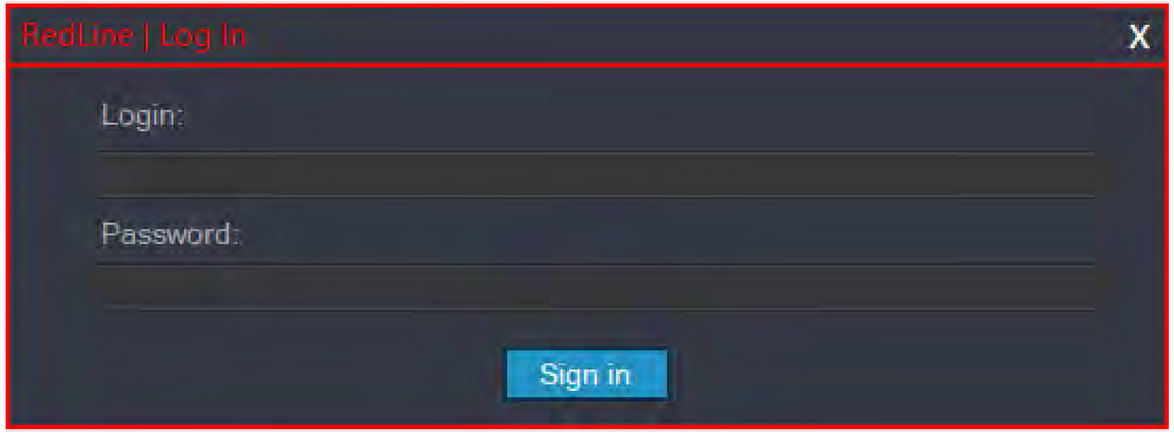
RedLine Stealer detection trend in H2 2022 and H1 2023, seven-day moving average

infostealer families in our telemetry. MSIL/Spy.RedLine first made the list of top ten infostealer detections in H2 2022 and managed to stay there in H1 2023 despite a decrease in total detection numbers, placing ninth.

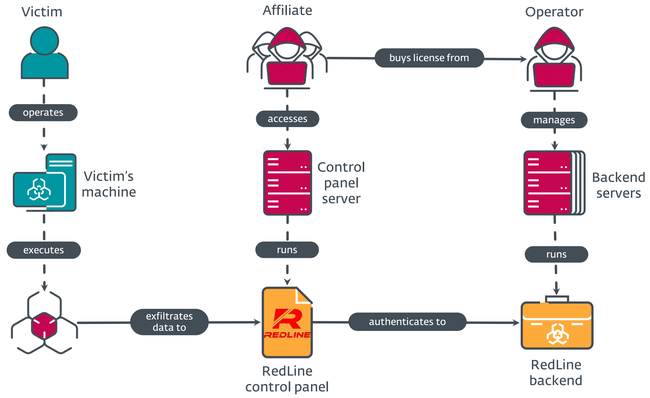
This piece of malware can be bought on underground forums or Telegram channels. In exchange for a relatively low monthly subscription fee (reported as USD 150 per month), it can be used to steal a wide range of information. From passwords, to cryptocurrency wallet information, to saved data from Steam and Discord, RedLine operators aim to satisfy all their customers' nefarious needs.

RedLine's paying clients, referred to as "affiliates", get access to the malware's control panel, which is then used to manage their campaigns. These control panels have a full graphical interface, making deploying the malware to victims easier. To work properly, the panels communicate with the spyware's backend, which is controlled by the actual RedLine operators.

Since the affiliates get a ready-made solution, they can quite easily integrate it into larger malicious operations. As such, the malware has been used in several notable campaigns. In H1 2023 alone, it took advantage of the AI boom by posing as free downloads of ChatGPT and Google Bard. These were being spread via malicious ads on hijacked Facebook business pages. CronUp discovered that in another series of attacks leveraging advertising, RedLine was distributed via Google Ads alongside Ursnif, and potentially Cobalt Strike and ransomware. As uncovered by Avast, this infostealer was also used in a highly targeted phishing campaign that abused Adobe Acrobat Sign: select recipients were sent emails with attachments masquerading as the signing service; however, the attachments actually contained links that eventually led to ZIP files containing RedLine.



RedLine panel login prompt



RedLine operation overview

As detailed by Flare Systems in a joint presentation with ESET at Botconf 2023, RedLine Stealer distribution methods vary as much as its campaigns. In addition to the already mentioned Google Ads and spearphishing, this spyware has also been spread through links, ads or comments in YouTube videos, and through public stealer log samples. The malware infiltrates the victim's

STEALER LOGS

Stealer logs are large collections of data stolen by infostealers that are usually hosted in the cloud. These logs contain mainly user credentials, but other types of sensitive information can be found there as well, such as cookies, document scans, and bank account payment details. These logs are sold and distributed on underground forums and marketplaces.

system disguised as, among other things, Windows 11 upgrades, cracks for video games or other software, mobile app clones, and popular applications such as Visual Studio.

In April, ESET researchers **revealed** on Twitter that they had, during a joint investigation with researchers at Flare Systems, discovered several GitHub repositories used as RedLine control panel dead-drop resolvers. In total, ESET found four such repositories, which were then all taken down with GitHub's help:

`github[.]com/lermontovainessa/Hub`

`github[.]com/arkadi20233/hub`

`github[.]com/ivan123iii78/hub`

`github[.]com/MTDSup/updateResolver`

The control panels used information stored in the dead-drop resolvers to access RedLine's backend servers. Since there were no fallback channels, the removal of the repositories broke the authentication of the RedLine control panels that were in use at the time. Even if our action did not affect the MaaS backend, it still worked as a temporary disruption, because it forced the operators to distribute new versions of the panels.

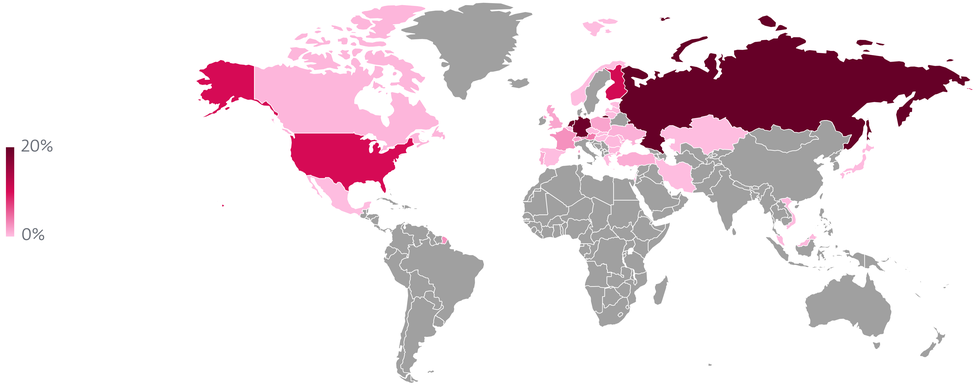
Apart from the GitHub repositories, our researchers also found code-signing certificates that were used to sign RedLine control panels. The certificates were assigned to RAIL AND CIVILS LTD and AMERT, LLC, and were revoked after we reported them.

Based on parsing our telemetry data for the months of December 2022 through March 2023, our researchers have determined that RedLine control panels are hosted mainly in Russia, Germany, and the Netherlands. Each of the three countries hosted close to 20% of the total number of RedLine C&Cs. ESET also found a significant number of the spyware's control panels at IP addresses located in the USA and Finland, with both countries hosting around 10%.

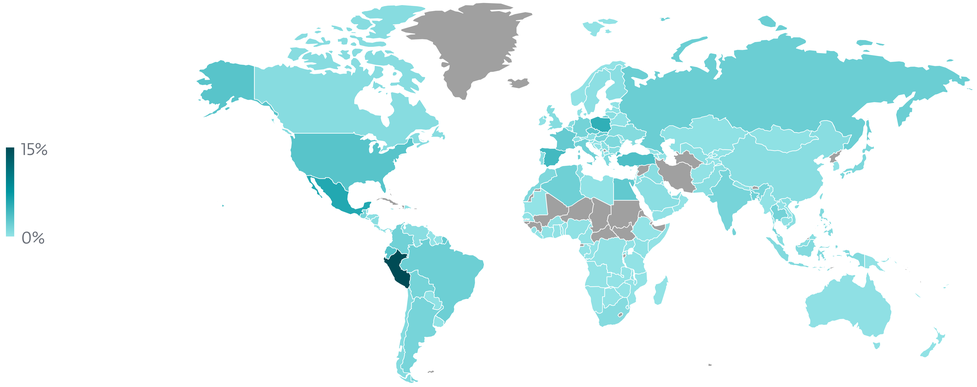
As opposed to hosting control panels, the countries that had to endure the most RedLine attack attempts over the same time period were mainly Peru (15%), Mexico (6%), and Poland (5%).

While ESET researchers managed to inconvenience RedLine's operators by removing the repositories with the dead-drop resolvers, we can nevertheless be sure that we haven't heard the last from this notorious infostealer. Even if RedLine were to suddenly disappear, many actors would be eager to take its place.

Case in point: there seems to be a RedLine competitor currently trying to establish itself. In 2022, malware named META was announced on cybercrime forums, claiming to be a better alternative to RedLine. It remains to be seen whether malicious actors decide to switch to the new malware, but the latest statistics point towards that being a way off yet.



Geographic distribution of RedLine Stealer panels in December 2022–March 2023



Geographic distribution of RedLine Stealer detections seen by ESET telemetry in December 2022–March 2023

macOS Supply-chain attacks

macOS affected by the first case of two linked supply-chain attacks

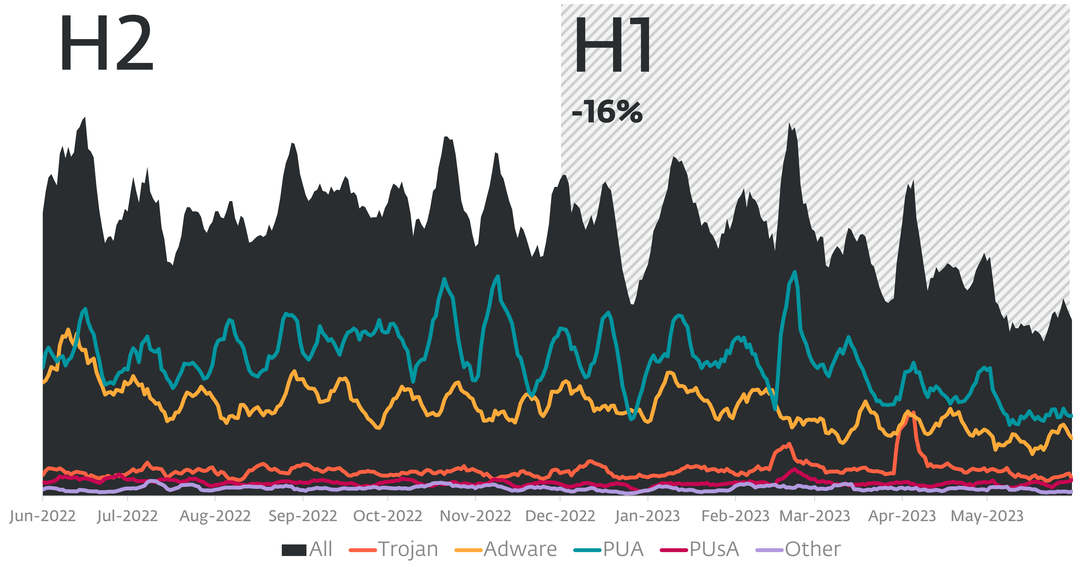
One of the spikes observed in macOS detections reveals the first case of interconnected supply-chain attacks, compromising a significant number of macOS devices.

Supply-chain attacks – which involve threat actors adding malicious code to software, which is then distributed to unsuspecting users via legitimate means – have become a significant concern in the world of cybersecurity. In March 2023, the Windows and macOS platforms were affected by the culmination of the first recorded case of two interconnected supply-chain attacks, when initially the infamous Lazarus group tainted the X_TRADER software, which later enabled a second Lazarus intrusion, with the group compromising 3CX phone system apps and their customers.

The macOS ecosystem, due to its nature and smaller market share, is generally exposed to fewer malware attacks than Windows. According to ESET telemetry, overall macOS detections have been slowly decreasing for some time and most of the detections seen on this platform are of Potentially Unwanted Applications (PUAs); in H1 2023, PUAs accounted for 49.3% of all macOS detections. In fact, one of the spikes visible in the ESET telemetry for mid March occurred when PUA detection was extended to include additional applications.

It is therefore unusual to see a supply-chain attack leaving a visible mark in macOS detection trends, but it was the case at the turn of March and April. This attack is also among the reasons why trojan detections grew by 16.8% in H1 2023 and accounted for 11.2% of all macOS detections, according to ESET telemetry.

In late March, it was discovered that both the Windows and macOS applications developed by 3CX contained malicious code. 3CX offers a phone system that utilizes voice over Internet Protocol (VoIP) to make and receive

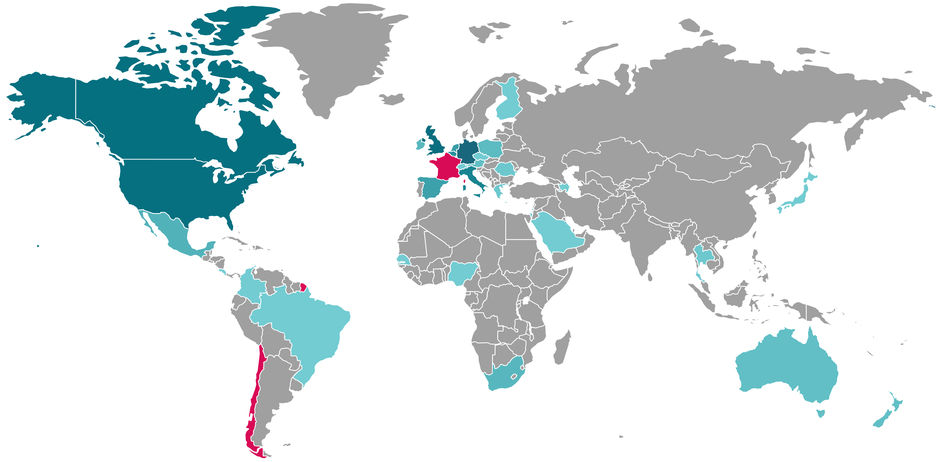


macOS detection trend in H1 2023, seven-day moving average

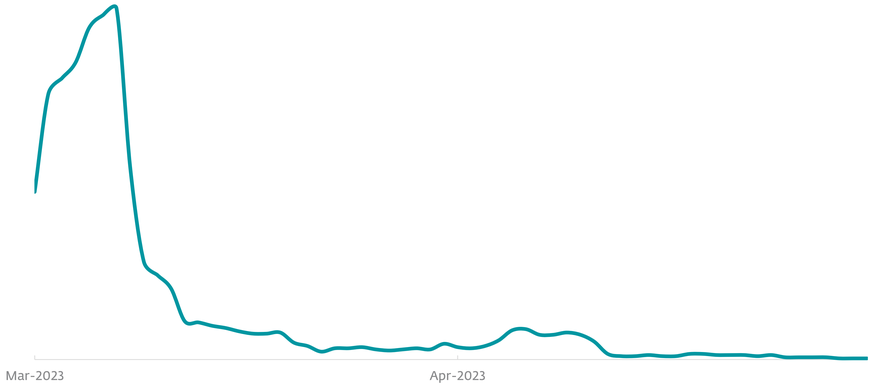
phone calls instead of traditional phone lines, and can be accessed via 3CX's apps. The malicious code added to these applications enabled the attackers to take control of any computer that had these compromised apps installed. It was quickly determined that 3CX was not responsible for adding the harmful code to its apps; rather, its software build chain was compromised, leading to the supply-chain attack.

The details surrounding the affected systems running macOS were extensively covered in a **Twitter** thread and a **blogpost** by Patrick Wardle. Analysis of the trojanized 3CX macOS application, recognized by ESET as OSX/NukeSped.P, revealed it had been digitally signed in late January; we did not, however, detect the presence of the malicious application in our telemetry until February 14, 2023. Later on, the spike appearing towards the end of March shows that ESET telemetry started to record a marked increase in detections of the compromised 3CX app for macOS, primarily in Germany, the United Kingdom, France, the United States, and Canada.

This supply-chain attack was orchestrated by external threat actors with the goal of distributing additional malware to specific 3CX customers. ESET Research, along with other security researchers, strongly believes that the attack was conducted by Lazarus, a well-known and sophisticated North Korea-aligned group.



Heatmap of ESET detections of the compromised 3CX app for macOS; detections of the second-stage malware served by Lazarus are marked in red



Detections of OSX/NukeSped.P, seven-day moving average

The additional malware served by Lazarus to selected 3CX customers using their trojanized macOS application was observed in ESET telemetry only in a small number of cases, in France and Chile; ESET products detect this as OSX/NukeSped.Q. Although indications of the macOS second-stage payload were present in ESET's telemetry as early as February, our researchers did not possess the sample or metadata that would have signaled its malicious nature. **It appears** that the second-stage malware for both Windows and macOS specifically targeted cryptocurrency companies.

On the same day ESET researchers published their findings attributing the attack to Lazarus, 3CX and the company responsible for the incident response of this compromise **disclosed** that the 3CX supply-chain attack was enabled by another supply-chain attack. This occurrence marks the first recorded instance of two interconnected supply-chain attacks, with one attack facilitating the other. The preceding attack targeted Trading Technologies, specifically its decommissioned X_TRADER software version r7.17.90p608, which was installed by a 3CX employee on a personal machine. Trading Technologies currently offers a range of products and services for electronic

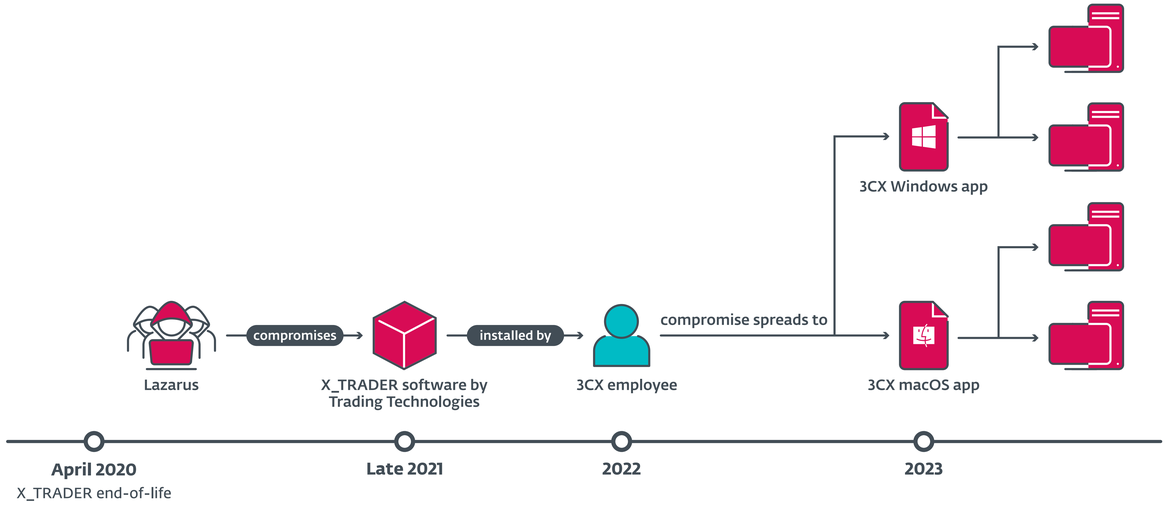
THE LAZARUS GROUP

Lazarus has been active since at least 2009 and has been responsible for significant incidents such as the **Sony Pictures Entertainment hack**, multimillion-dollar **cyberheists in 2016**, the **WannaCryptor** (aka WannaCry) outbreak in 2017, and a history of disruptive attacks targeting **South Korean infrastructure**. ESET Research's discovery of a new **Lazarus Linux payload** further solidified the connection between this threat actor and the 3CX compromise.

trading of various investment categories, including trading of cryptocurrencies.

X_TRADER provided advanced trading capabilities and tools for financial institutions and professional traders. Even though Trading Technologies stopped all support of this software in April 2020 and announced its retirement date as far back as **September 2018**, the 3CX employee installed its tainted version on an undisclosed day in 2022. ESET telemetry detected two instances of the malicious X_TRADER installer in 2022 – one in August in the United Kingdom and another one in December in the United States.

The series of high-profile supply-chain attacks, ranging from **WIZVERA VeraPort** (where Lazarus was also involved), to **NotPetya** and **SolarWinds**, to the recent 3CX/Trading Technologies incident, underscores that in recent years, the threat landscape has expanded beyond traditional targets such as individual computers and networks. It reveals the growing complexity of software development and distribution and the fact that organizations are increasingly reliant on third-party software and hardware providers. These factors have created opportunities for malicious actors to exploit trusted relationships and evade traditional defense mechanisms, as these attacks can be highly effective and difficult to detect. The 3CX supply-chain attack especially indicates that no platform is safe from this attack vector.



Simplified diagram of linked supply-chain attacks

Ransomware

Same code, different ransomware? Leaks kick-start myriad of new variants

Leaks allow more criminals to try their luck with ransomware yet make preexisting detections increasingly effective against emerging malware.

Recently, several notorious ransomware families such as Babuk, Conti, and LockBit 3.0 have published or seen their source code leak into the public domain. This fueled the launch of a myriad of new malware variants and families, with significant code overlaps. While this makes it increasingly simple for amateurs to start ransomware of their own, it may also help the defenders – despite muddying the waters on the scene.

The source code for Babuk, aka Babyk, is a prime example of this phenomenon. Since the group made its **code public domain** in September 2021, it has become a prominent go-to basis for new ransomware strains. What makes it attractive for cybercriminals is its ability to attack Linux and VMWare ESXi systems. Notable emerging families using Babuk as their base included RAgroup, Nokoyawa, Buhti, and Rorschach.

Another example of code that was recently published – **allegedly by a disgruntled insider** – was the "builder" of LockBit 3.0 ransomware. This malware family itself is built upon previously leaked source code, with LockBit 3.0 Black and Green variants being based on Black Matter and Conti, respectively.

Buhti ransomware gang is one of the new players that made use of the published LockBit 3.0 Black when building its Windows-oriented variant. Older code from LockBit 2.0 has also been seen in a mix with Babuk in another emerging ransomware family named Rorschach.

Even ransom notes aren't what they once used to be. While in the past this had been a staple of each threat actor, currently criminals increasingly mimic and inspire each other, blurring the lines even more. While the dropped TXT file might help identify the ransomware strain at play, seeing this ransom demand also means that user data has already been encrypted.

Source-code sharing and similar ransom notes might complicate public tracking of the ransomware, but it also enables defenders to use a more generic or well-known set of detections and rules to identify the threat actor activity. Using these can thus cover a wider range of variants, including newly emerging ones.

Looking into ESET telemetry, ransomware detections between H2 2022 and H1 2023 increased by over 10%. However, this trend is skewed by a large

BABUK RANSOMWARE OVERVIEW

Babuk (or Babyk) ransomware was discovered in 2021 as a further development of Vasa Locker. It made its name by attacking large enterprises, but its most prominent victim was **Washington D.C.'s Metropolitan Police Department**. The gang claimed to have obtained 250 GB of data from the agency and threatened to publish it unless USD 4 million was paid. However, this has significantly increased focus of other law enforcement agents on the gang, which subsequently led to it closing shop and splitting. The source code – including **Windows, NAS and ESXi variants** of the malware – was published in September 2021 and has become one of the go-to bases for new ransomware strains.

number of Win/Filecoder.BlackBasta detections observed on a single day in a single network space in the USA. Omitting that spike, the number of ransomware attacks remained almost identical in both periods.

It is important to note that this detection trend only includes instances where ESET encountered ransomware as the final payload. Attacks detected at an earlier stage – such as a brute-force attack; exploitation of a vulnerability; malspam; or an attack of a dropper, downloader, or infostealer – are not part of the ransomware data set.

NOTABLE NEW PLAYERS

Buhti

This ransomware family has a variant for both Windows and Linux systems, each of them built upon different leaked source code. For Windows, it uses a modified LockBit 3.0 builder and for Linux (and potentially VMWare ESXi) the "open-sourced" Babuk code.

Cactus

Cactus ransomware exploits known vulnerabilities in VPN devices to gain initial access. Subsequently, it extracts the ransomware binary from a password-protected 7-Zip archive, effectively using encryption to evade detection. This is a known technique used already by the WannaCryptor (aka WannaCry) family in 2017.

MalasLocker

An odd new player in the ransomware arena is MalasLocker. Its operators demand that the victim pays the ransom in the form of a donation to an attacker-approved non-profit organization.

MoneyBird

An Iranian-aligned threat actor called Agrius is deploying a new faux ransomware variant called MoneyBird to destroy victims' data. It is a continuation of previously documented wiper campaigns that target Israeli victims.

MortalKombat

Operators behind this malware family conduct brute-force attacks against exposed remote desktop accesses on port 3389 and deploy as a bundle with a clipper called Laplas.

RAgroup

RAgroup ransomware is based on the leaked Babuk source code, and targets mostly businesses in South Korea and the United States. It uses intermittent encryption, encrypting only part of the targeted file and thus speeding up the process (see White Phoenix, in the next column). The operators of RAgroup also attempt to sell the stolen data via their leak site.

Rorschach

Rorschach is one of the fastest encryptors on the ransomware market today, with a high level of customization and similarities with Babuk, Lockbit 2.0, Yanlouwang, and DarkSide.

Trigona

Trigona ransomware uses brute-force attacks against **exposed Microsoft SQL servers** to gain access and subsequently to install ransomware to encrypt victims' data.

ARRESTED/CLOSED SHOP/KEYS RELEASED:

DECRYPTED: Hive ransomware

One of the most active ransomware gangs, known as Hive, had its systems infiltrated, and later disrupted, by law enforcement agents. The action was spearheaded by German, Dutch, and US authorities, with support from Europol and 13 countries. Hive's servers and dark-web leak site were seized. According to the involved agencies, the takedown saved approximately USD 130 million in ransom and produced decryption keys for past victims. No arrests were made.

DECRYPTOR: White Phoenix

Encrypting data takes time and is loud enough to attract defenders' attention. To avoid that scenario, ransomware gangs recently started using intermittent encryption, encrypting only parts of the targeted data. A new decryptor called White Phoenix is taking advantage of that approach, recovering a limited set of file formats. While imperfect, in some cases, it might be enough to help some victims decrypt key pieces of data and avoid paying the ransom.

DECRYPTOR: MegaCortex ransomware

In H1 2023, a new MegaCortex ransomware decryptor has been released. This standalone tool can automatically find and recover affected data on a vicitm's system. MegaCortex was mostly known for its activities in 2019, but it became inactive in 2020. In October 2021, Europol arrested 12 individuals responsible for 1,800 ransomware attacks, who deployed several ransomware strains, including MegaCortex.

DECRYPTOR: ESXiArgs Ransomware

CISA released a recovery script for the ESXiArgs ransomware. This family

propagates mostly via exploitation of known vulnerabilities in unpatched, out-of-service, or out-of-date VMware ESXi servers. According to CISA, threat actors behind the strain have compromised over 3,800 servers globally, encrypting their configuration files thus rendering the virtual machines unusable.

SENTENCE: **A Russian pled guilty to helping Ryuk**

Denis Dubnikov, a Russian national involved in money laundering for Ryuk ransomware, has been **sentenced** by a US court to no jail time except for the period he already served. On top of that Dubnikov must pay a financial penalty of USD 10,000 and a forfeit USD 2,000. While similar offenses can possibly lead to as much as 20 years in prison, the court decided to release Dubnikov on parole after his recent guilty plea.

SANCTIONS: **Affiliates of TrickBot, Ryuk, Conti**

In February, the USA and the UK issued **historical first joint cyber sanctions** aiming at seven individuals affiliated with attacks of TrickBot malware and Ryuk and Conti ransomware. As a result, any property of the sanctioned persons in the USA and the UK must be blocked and reported to the authorities. The same is true for all dealings between citizens of both countries and the designated individuals.

ARREST: **DoppelPaymer gang**

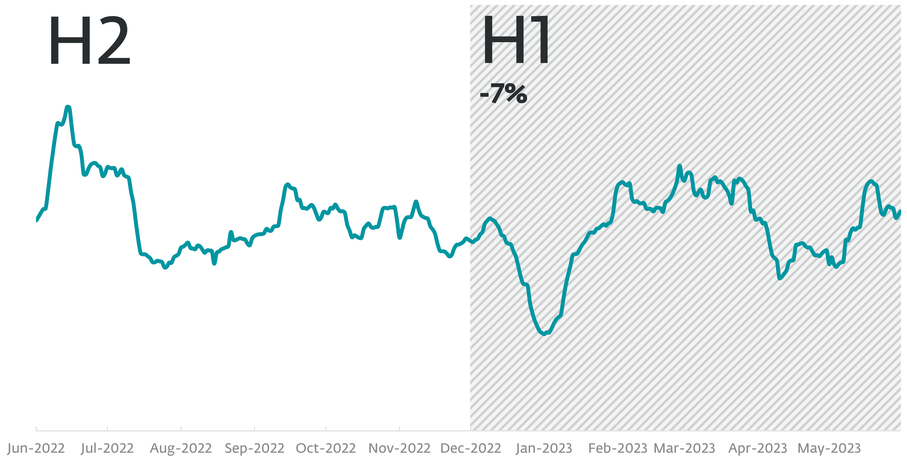
In February, law enforcement agents **raided** three locations in Germany and Ukraine, targeting two individuals suspected of being core members of the DoppelPaymer ransomware gang. Three additional arrest warrants were issued by the German authorities aimed at the "masterminds behind the criminal group". In Germany alone, the DoppelPaymer gang attacked 37 companies including a hospital in Düsseldorf. The US victims of the group are known to have paid at least EUR 40 million between 2019 and 2021.

BOUNTY **LockBit, Babuk, Hive**

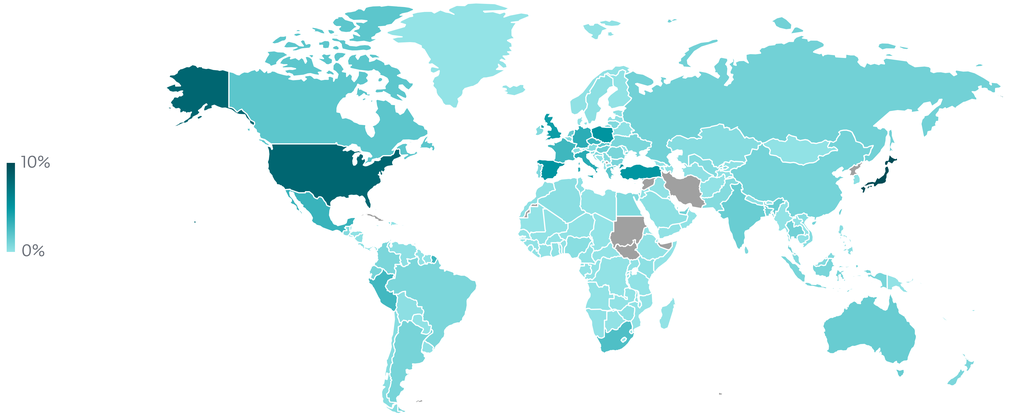
The US authorities have **charged** Mikhail Pavlovich Matveev – a criminal with ties to LockBit, Babuk, and Hive ransomware, and who is believed to be operating from Russia – over cyberattacks against critical infrastructure. A USD 10 million bounty has also been issued for information that would lead to his capture. Overall, victim ransom payments to those three gangs amount to USD 200 million, with ransom demands being twice as high.

Threat Telemetry

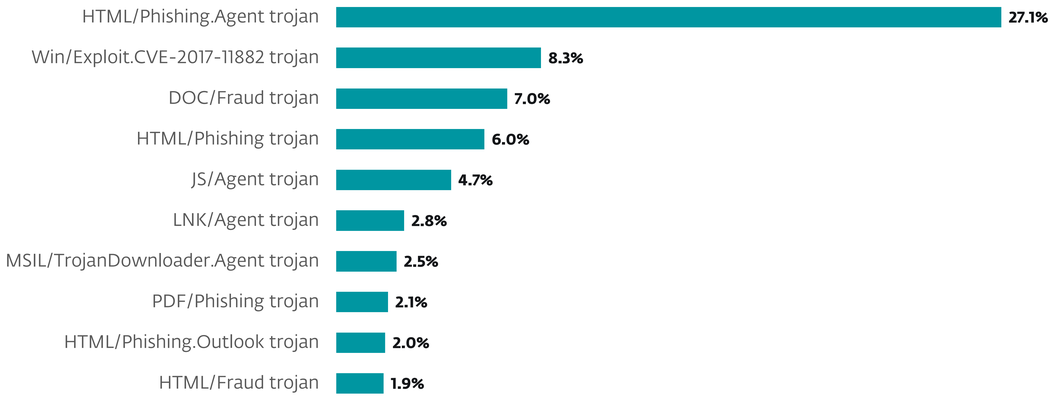
All threats



Overall threat detection trend in H2 2022 and H1 2023, seven-day moving average

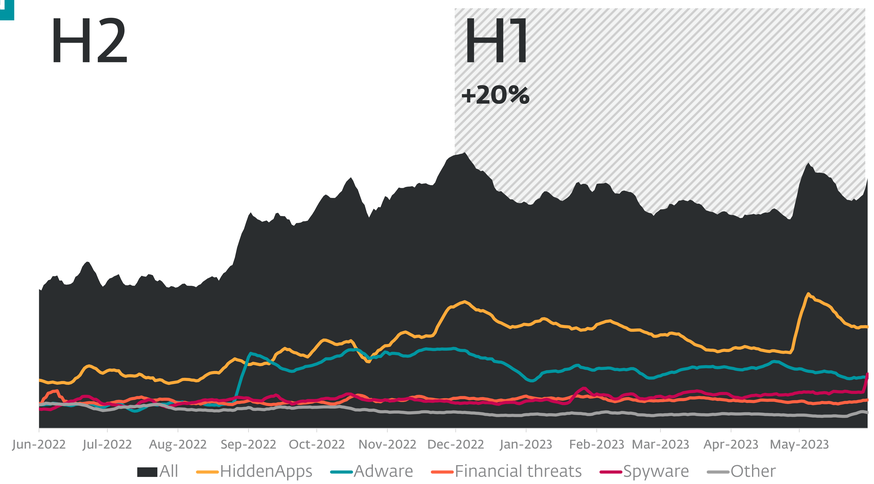


Geographic distribution of malware detections in H1 2023

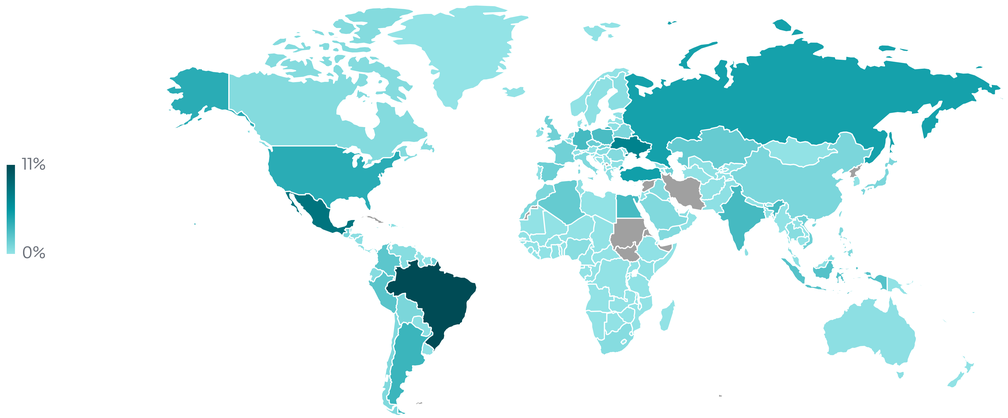


Top 10 malware detections in H1 2023 (% of malware detections)

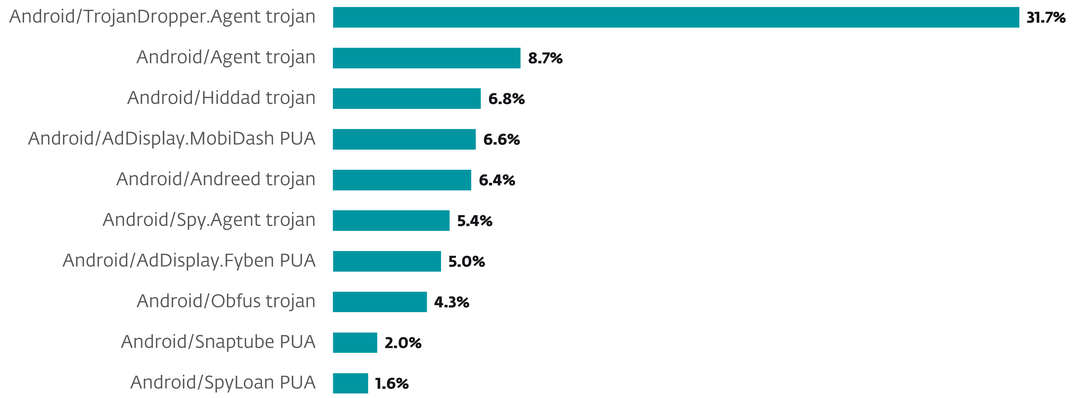
Android



Detection trends of selected Android detection categories in H2 2022 and H1 2023, seven-day moving average (trends of Clickers, Cryptominers, Ransomware, Scam apps, SMS trojans, and Stalkerware are combined in the trendline Other)

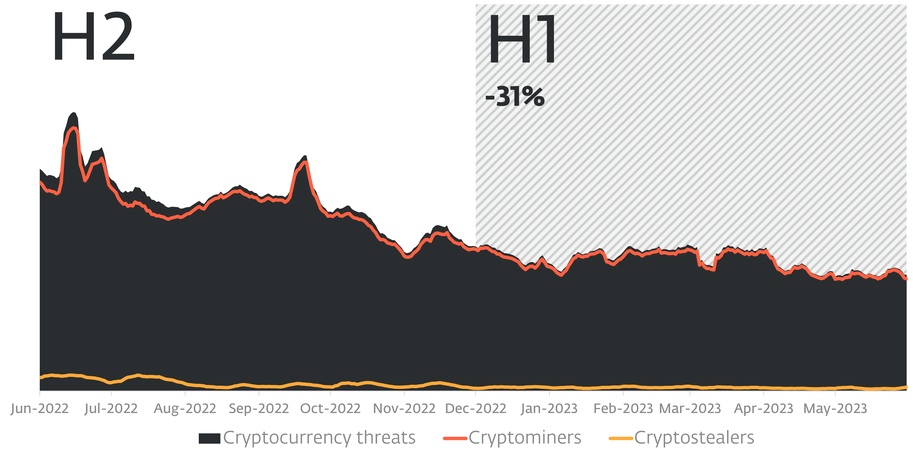


Geographic distribution of Android detections in H1 2023

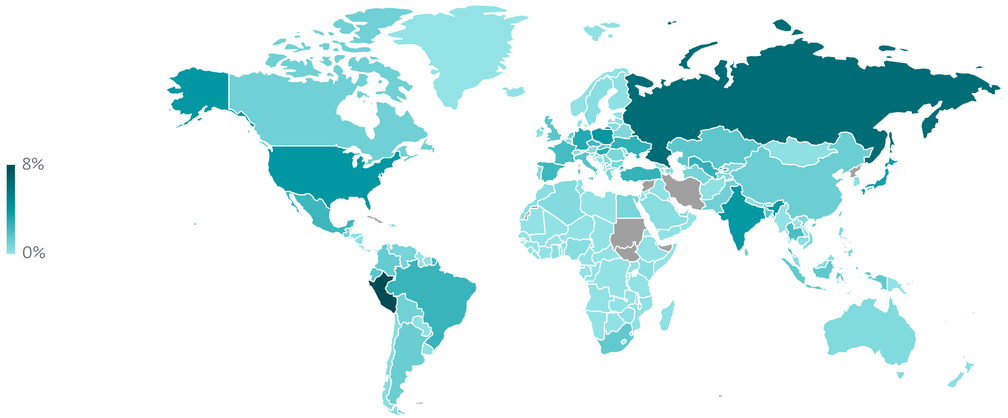


Top 10 Android detections in H1 2023 (% of malware detections)

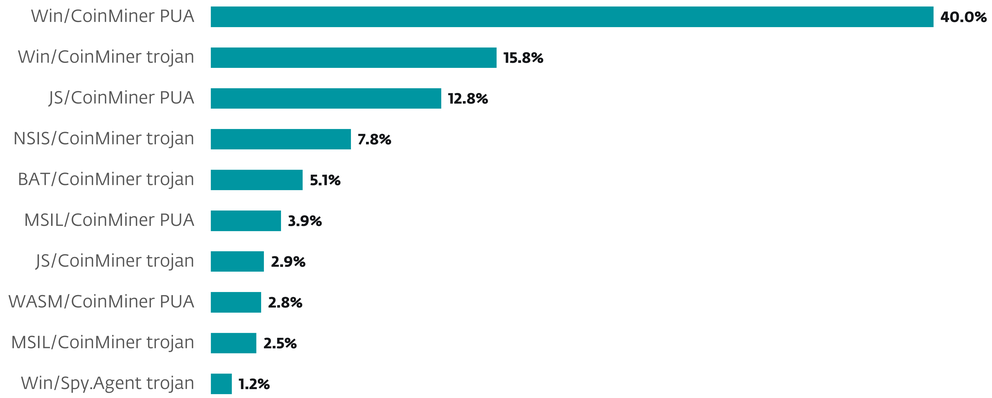
Cryptocurrency threats



Cryptocurrency threat detection trend in H2 2022 and H1 2023, seven-day moving average

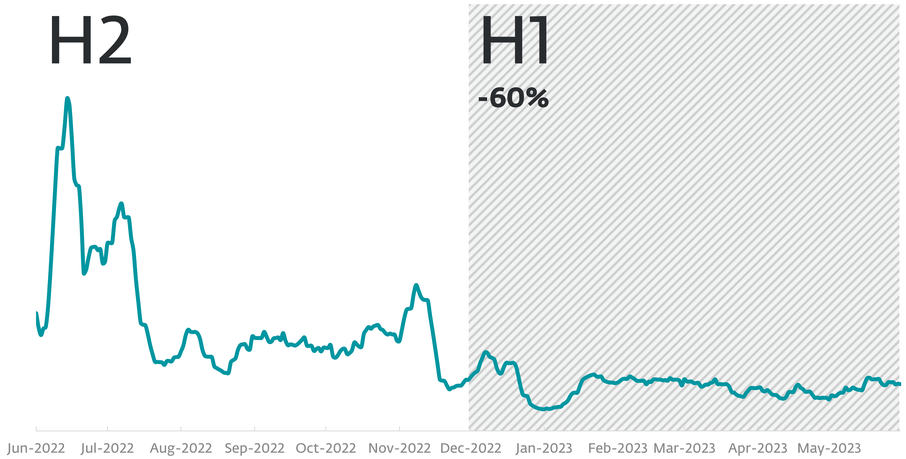


Geographic distribution of Cryptocurency threat detections in H1 2023

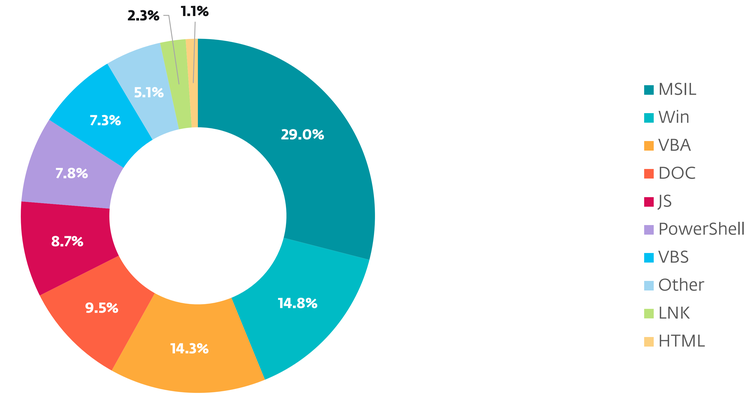


Top 10 Cryptocurrency threat detections in H1 2023 (% of malware detections)

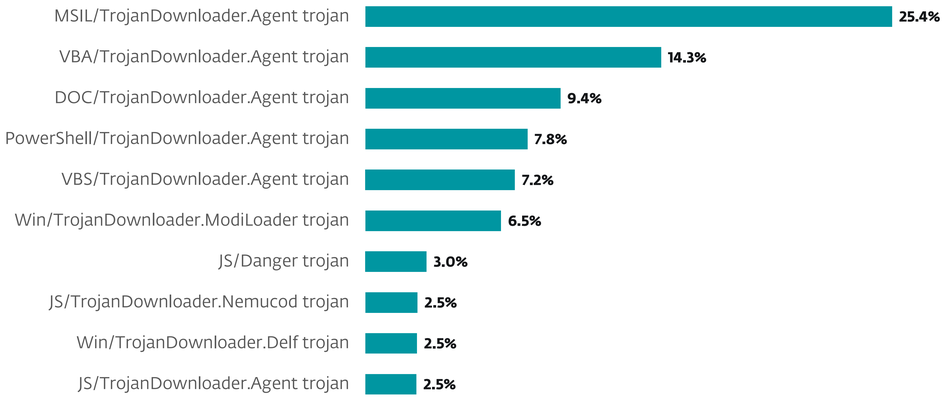
Downloaders



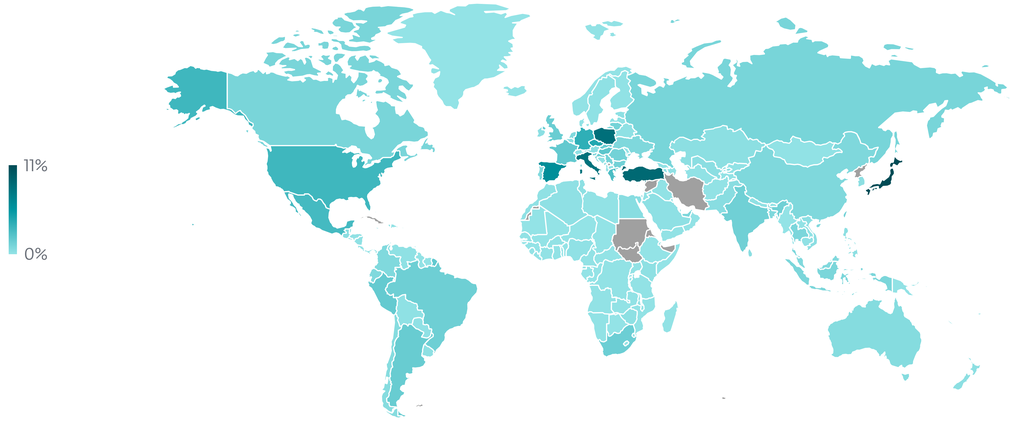
Downloader detection trend in H2 2022 and H1 2023, seven-day moving average



Downloader detections per detection type in H1 2023

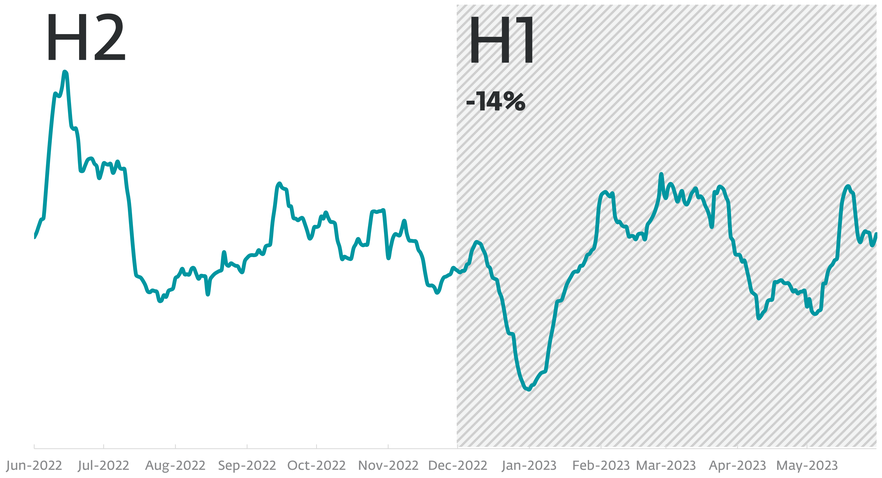


Top 10 Downloader detections in H1 2023 (% of malware detections)

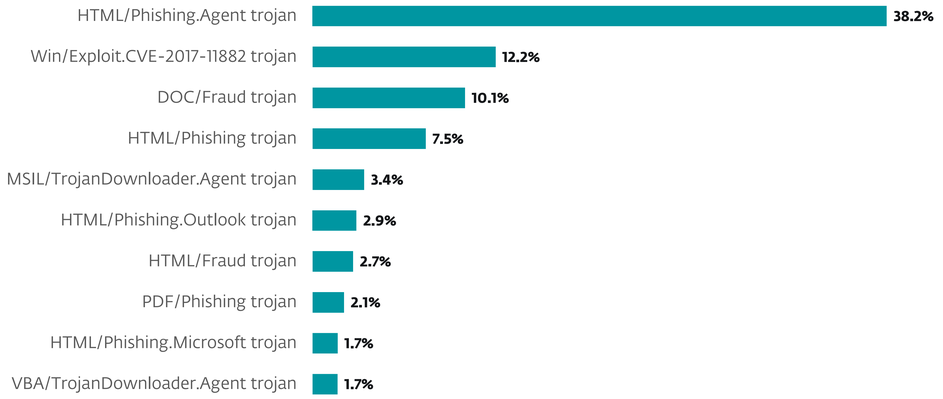


Geographic distribution of Downloader detections in H1 2023

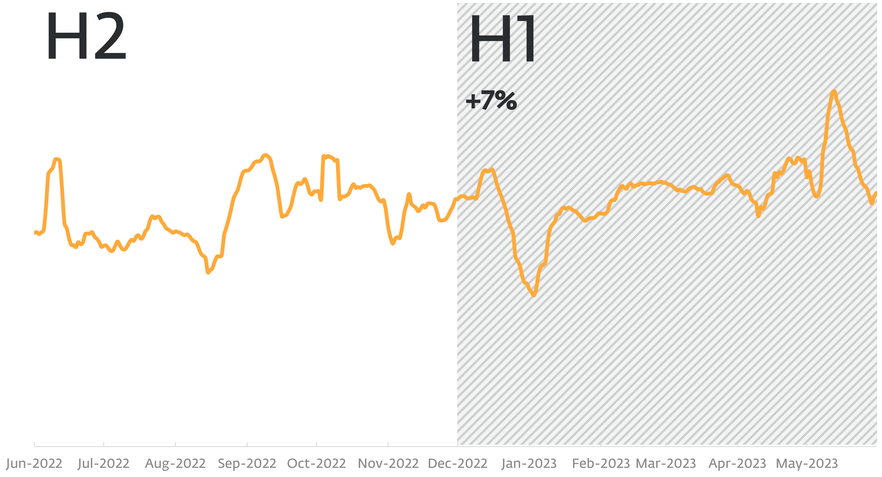
Email threats



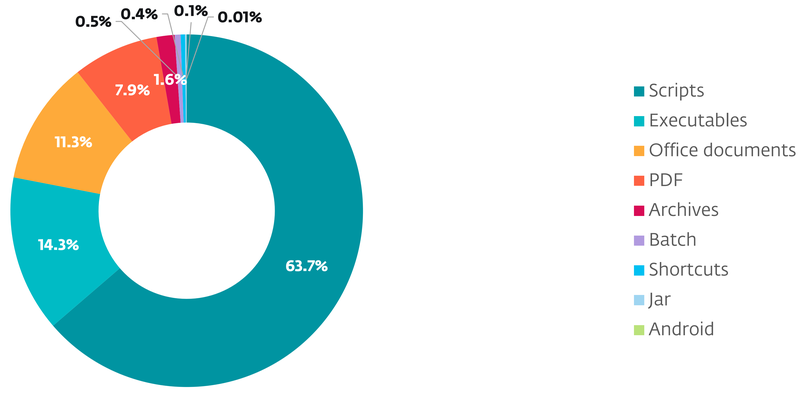
Malicious email detection trend in H2 2022 and H1 2023, seven-day moving average



Top 10 threats detected in emails in H1 2023

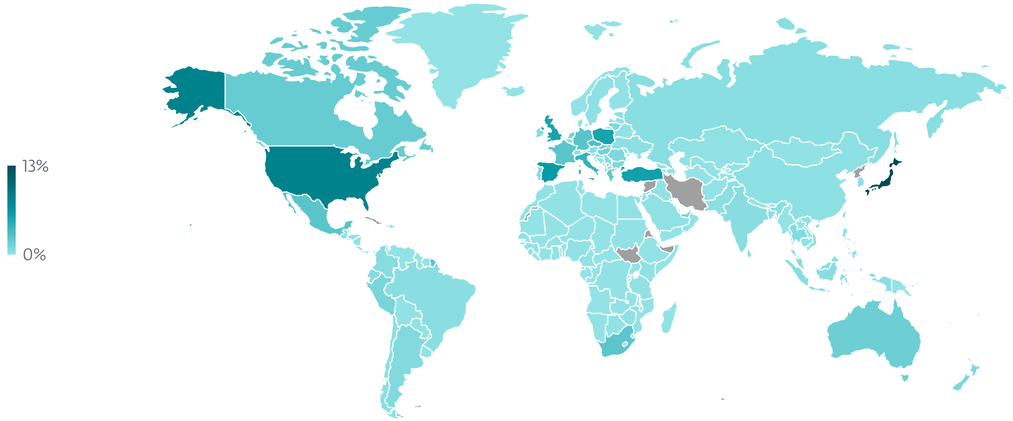


Spam detection trend in H2 2022 and H1 2023, seven-day moving average



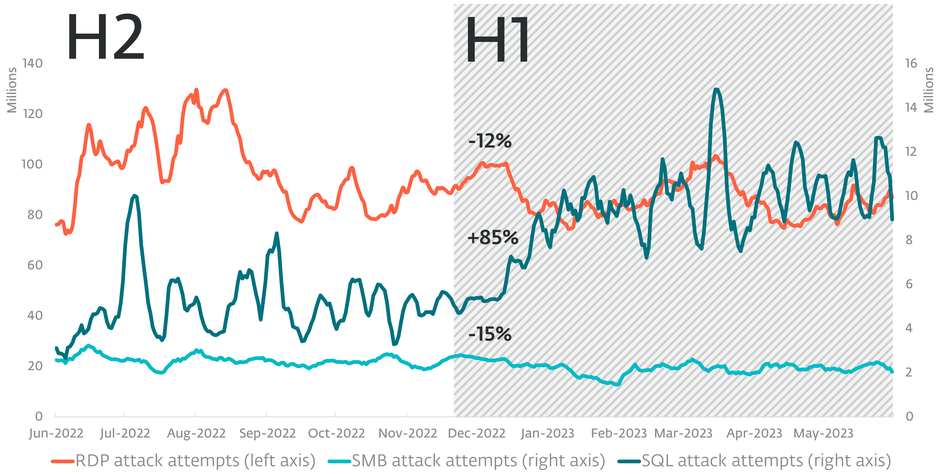
Top malicious email attachment types in H1 2023

Email threats

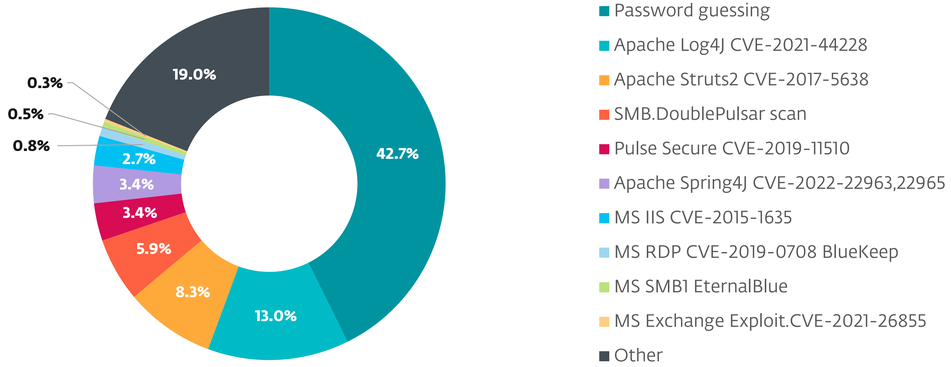


Geographic distribution of Email threat detections in H1 2023

Exploits

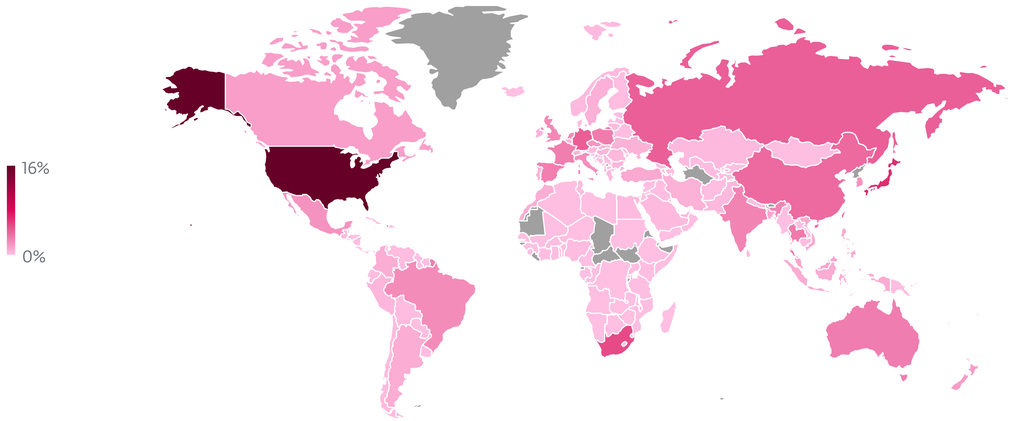


Trends of RDP, SMB and SQL attack attempts in H2 2022 and H1 2023, seven-day moving average

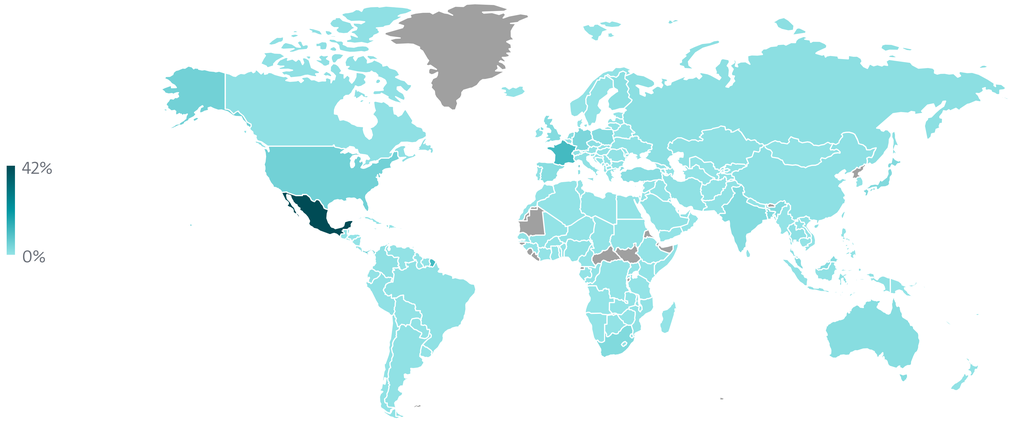


External network intrusion vectors reported by unique clients in H1 2023

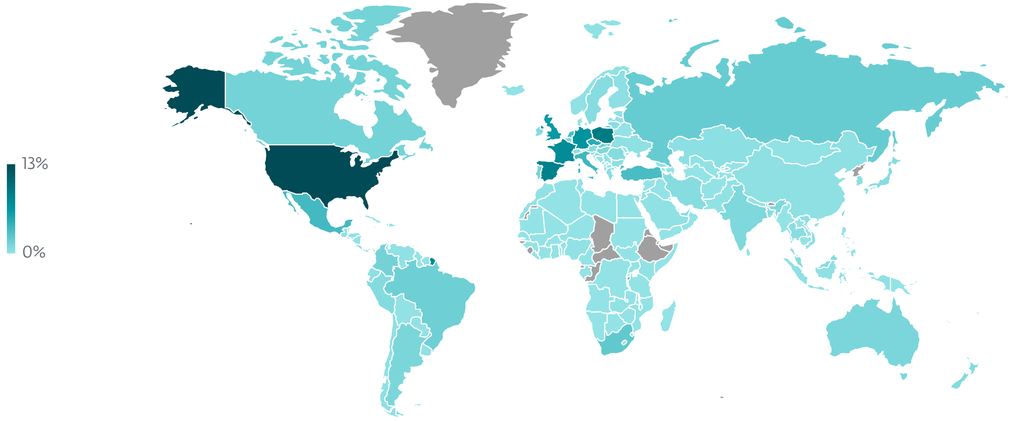
Exploits



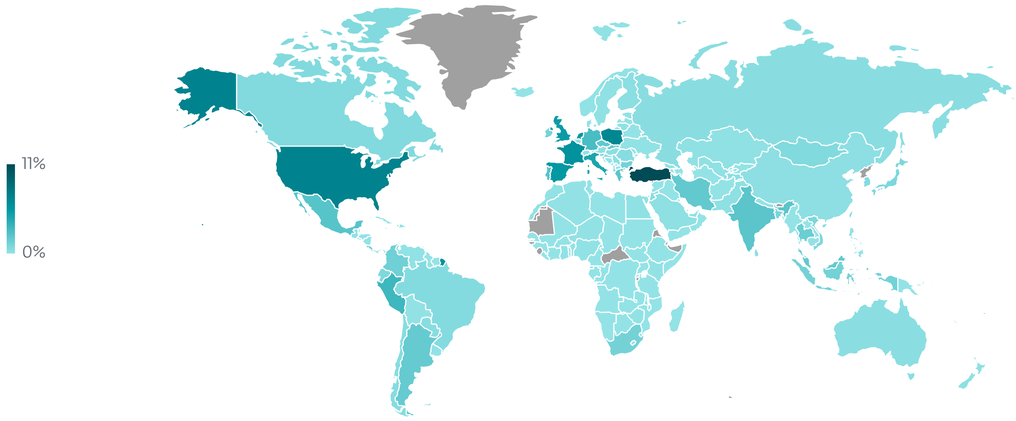
Geographic distribution of RDP password guessing attack attempt sources in H1 2023



Geographic distribution of SMB password guessing attack attempt targets in H1 2023

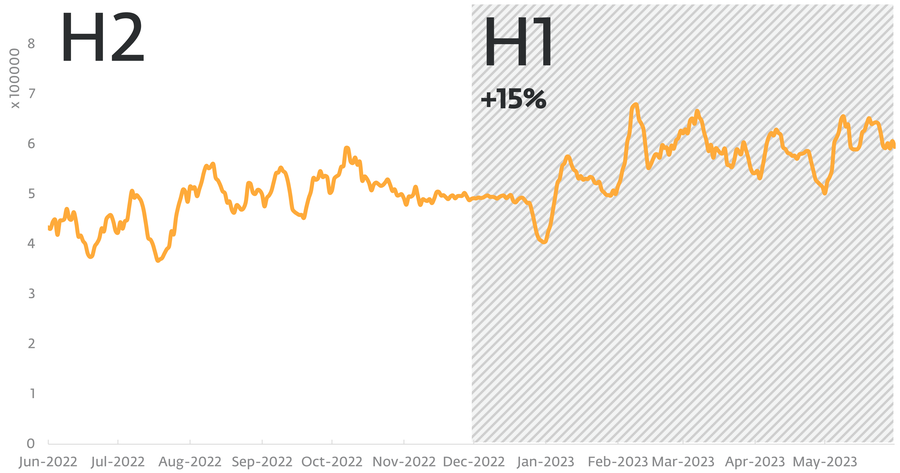


Geographic distribution of RDP password guessing attack attempt targets in H1 2023

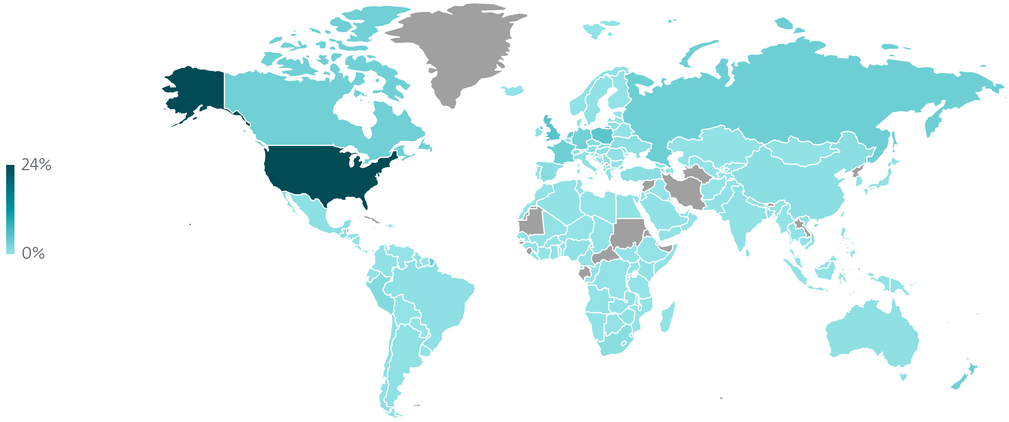


Geographic distribution of SQL password guessing attack attempt targets in H1 2023

Exploits

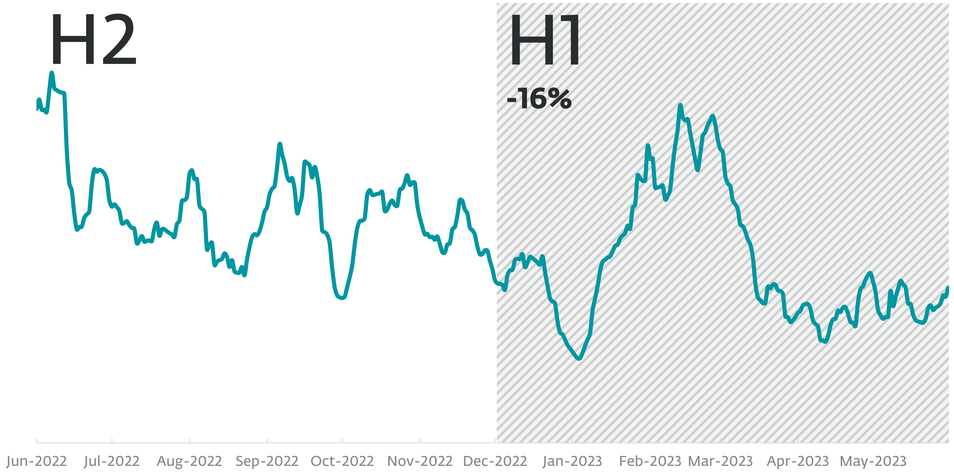


Detection trend of Log4Shell exploitation attempts in H1 2023

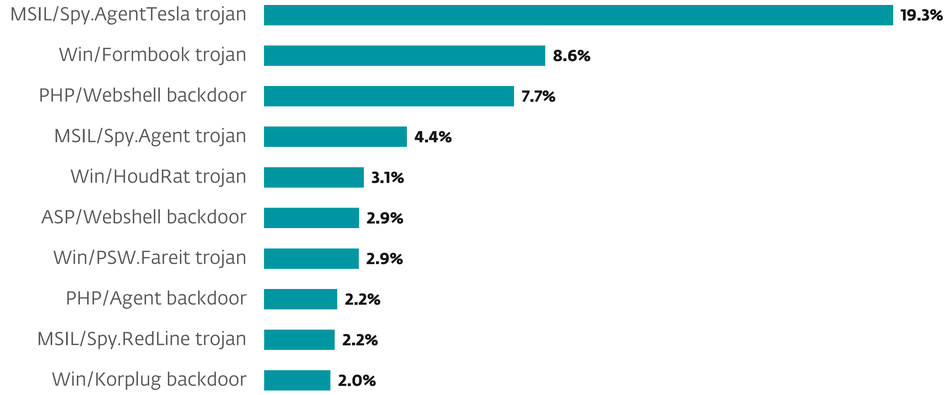


Geographic distribution of Log4Shell exploitation attempts in H1 2023

Infostealers

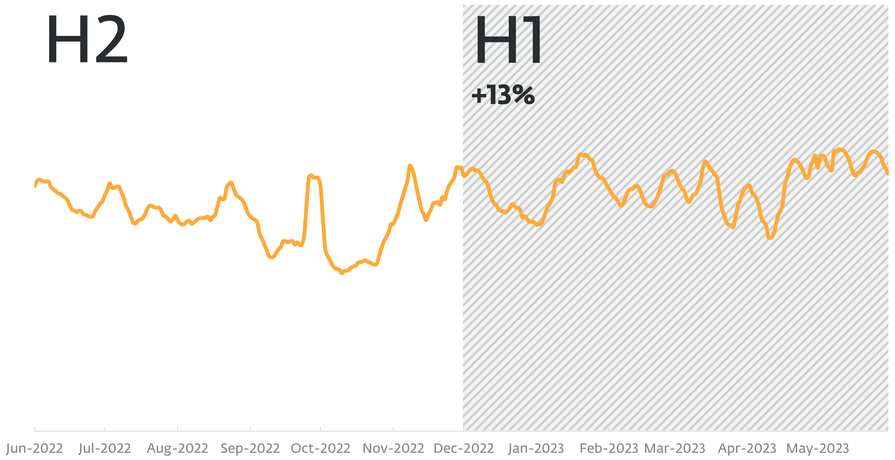


Infostealer detection trend in H2 2022 and H1 2023, seven-day moving average

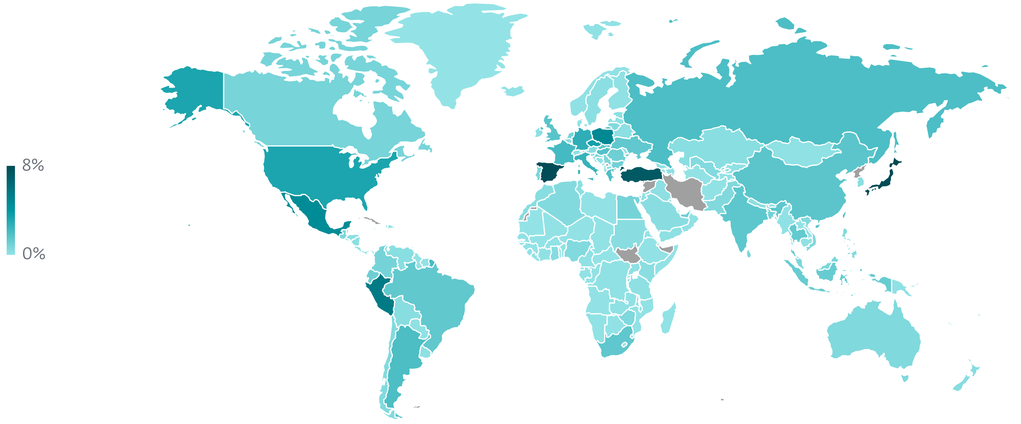


Top 10 Infostealer families in H1 2023 (% of Infostealer detections)

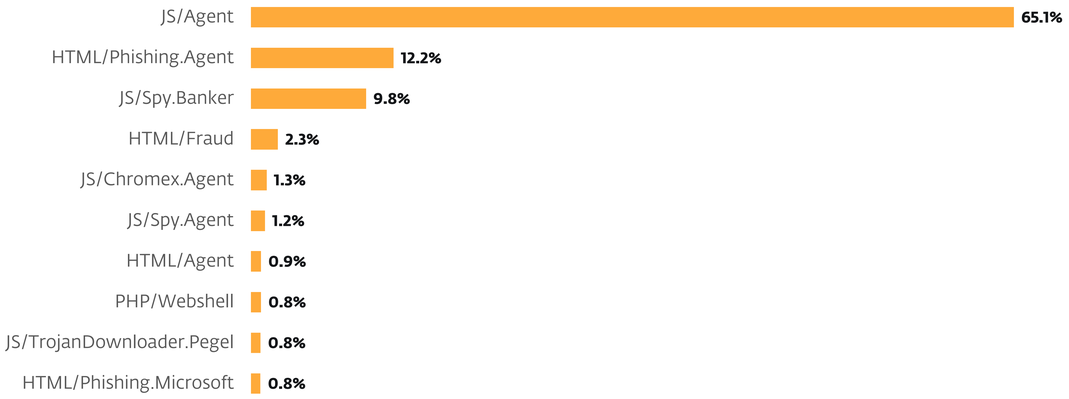
Infostealers



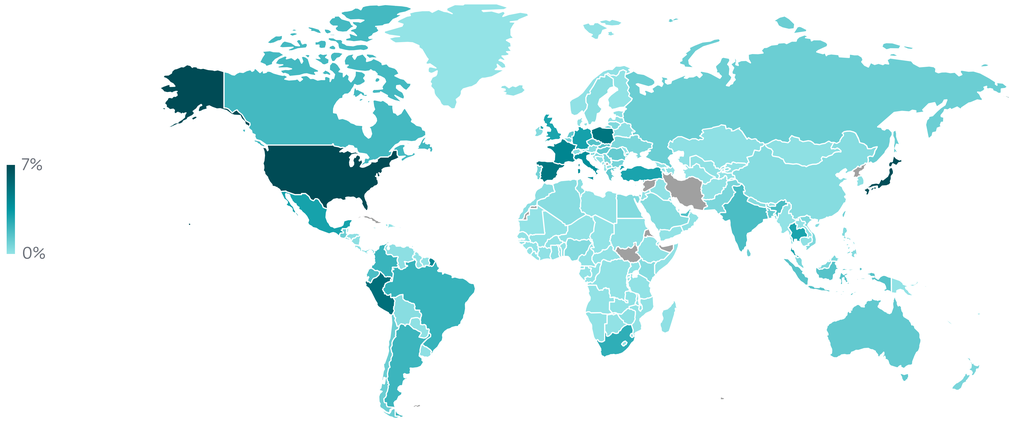
Online infostealer detection trend in H2 2022 and H1 2023, seven-day moving average



Geographic distribution of Infostealer detections in H1 2023

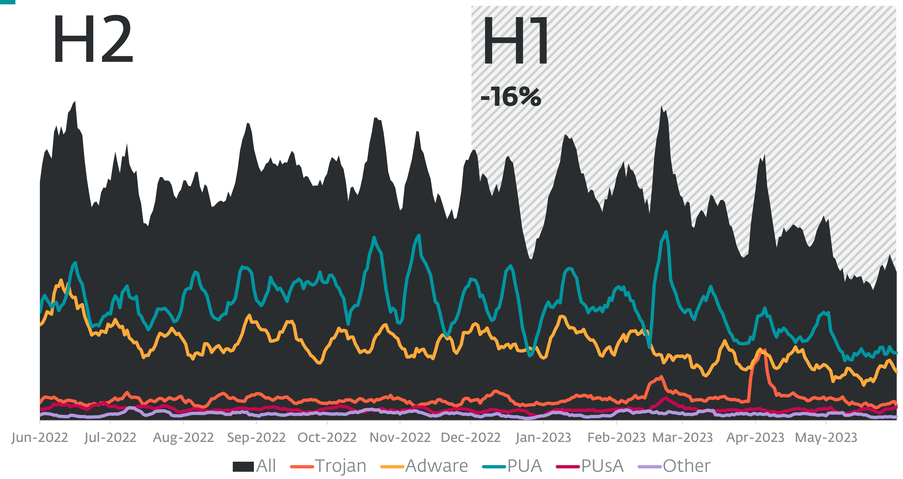


Top 10 Online infostealer detections in H1 2023 (% of malware detections)

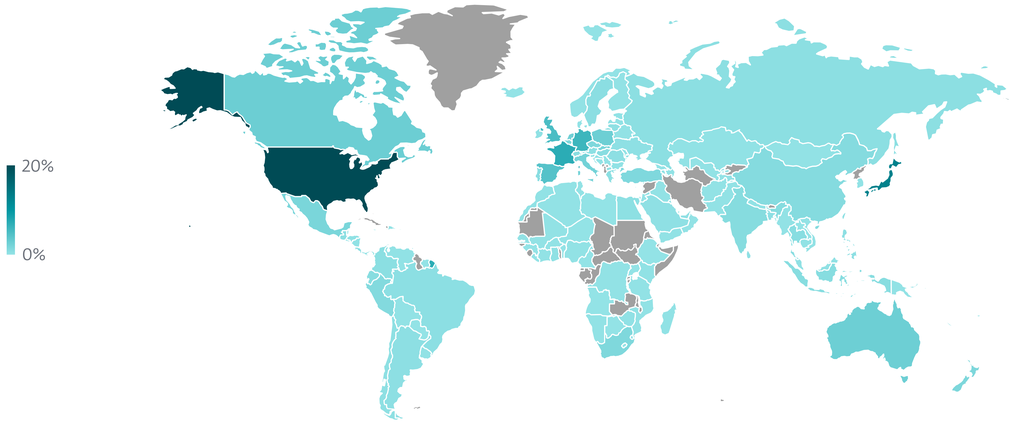


Geographic distribution of Online infostealer detections in H1 2023

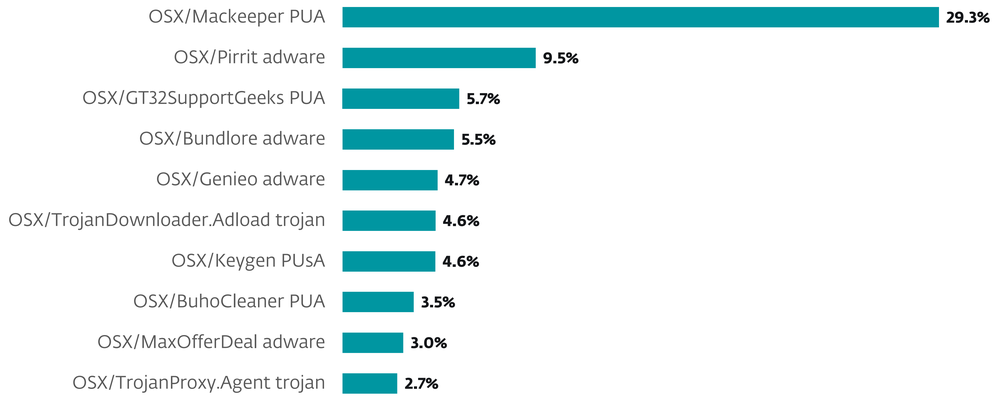
macOS



macOS detection trend in H2 2022 and H1 2023, seven-day moving average

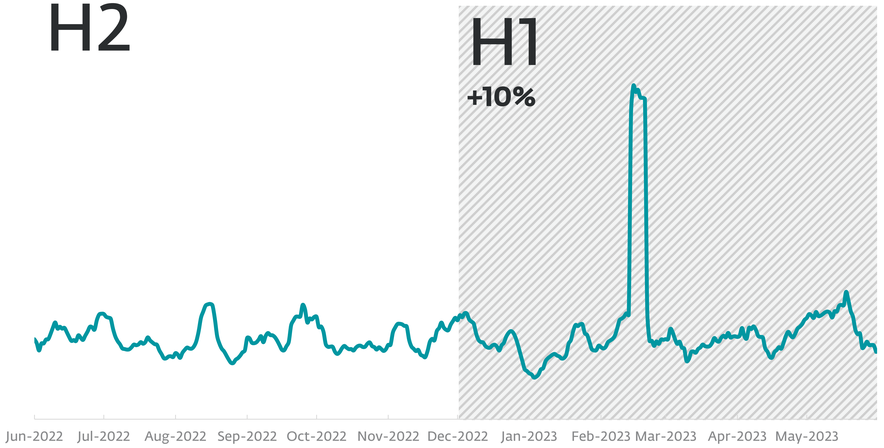


Geographic distribution of macOS detections in H1 2023

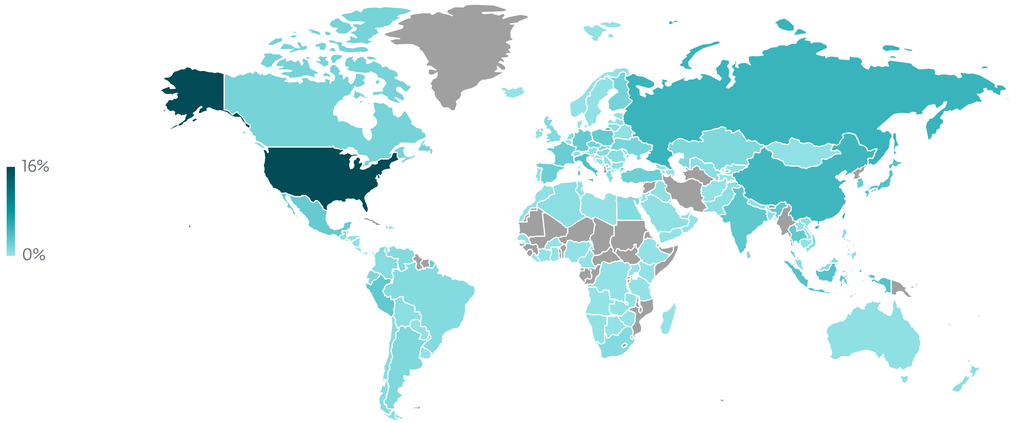


Top 10 macOS detections in H1 2023 (% of macOS detections)

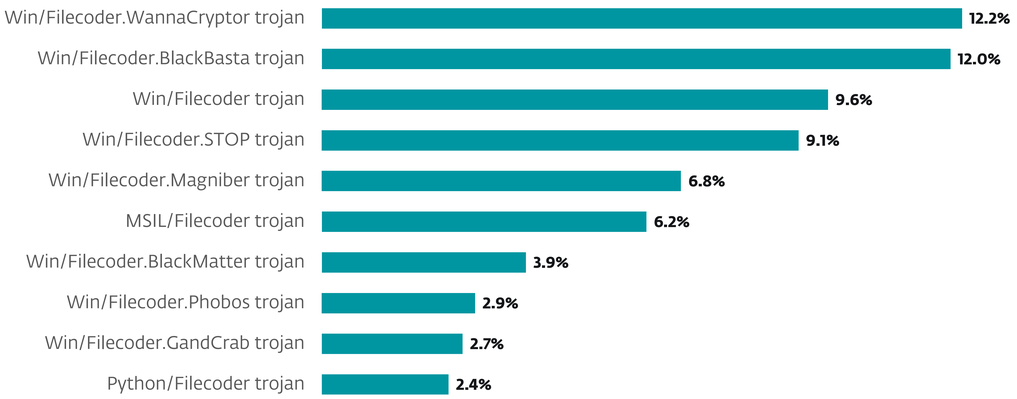
Ransomware



Ransomware detection trend in H2 2022 and H1 2023, seven-day moving average

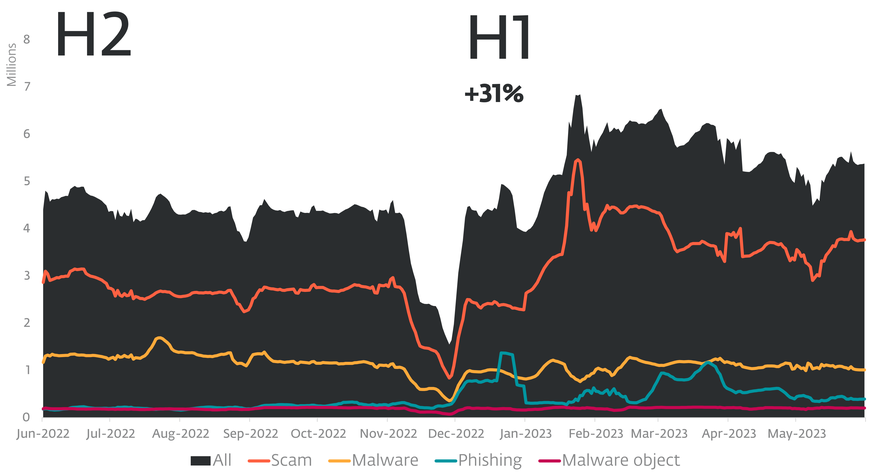


Geographic distribution of Ransomware detections in H1 2023

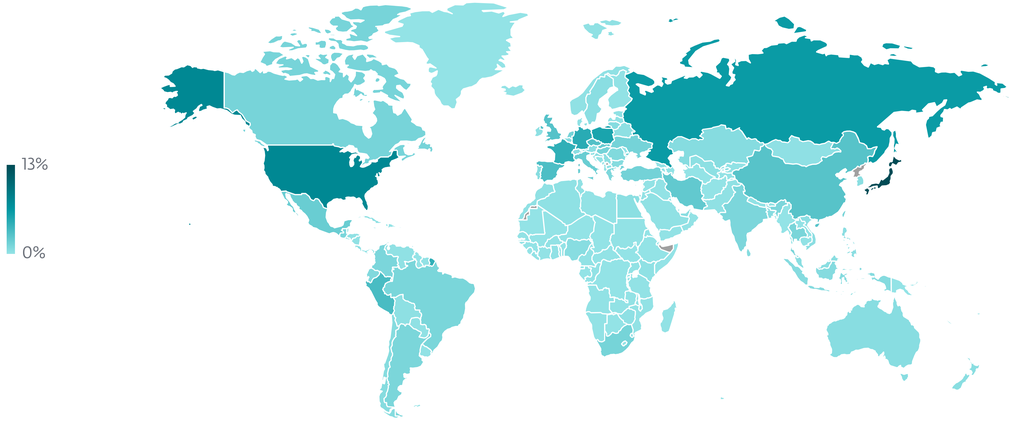


Top 10 Ransomware detections in H1 2023 (% of Ransomware detections)

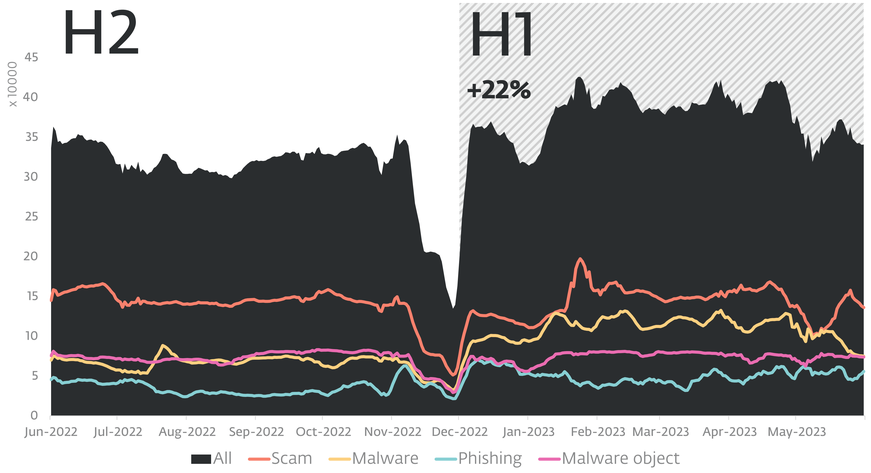
Web threats



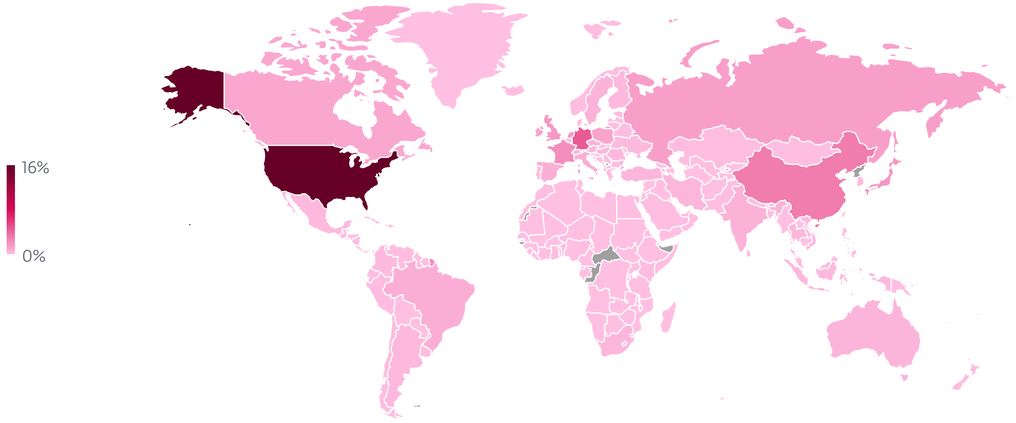
Web threat block trend in H2 2022 and H1 2023, seven-day moving average



Global distribution of Web threat blocks in H1 2023



Unique URL block trend in H2 2022 and H1 2023, seven-day moving average

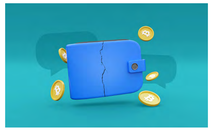


Global distribution of blocked domain hosting in H1 2023

Research publications

Shedding light on AceCryptor and its operation

ESET researchers reveal details about a prevalent cryptor, operating as a cryptor-as-a-service used by tens of malware families



Not-so-private messaging: Trojanized WhatsApp and Telegram apps go after cryptocurrency wallets

ESET researchers analyzed Android and Windows clippers that can tamper with instant messages and use OCR to steal cryptocurrency funds

BlackLotus UEFI bootkit: Myth confirmed

The first in-the-wild UEFI bootkit bypassing UEFI Secure Boot on fully updated UEFI systems is now a reality

Android app breaking bad: From legitimate screen recording to file exfiltration within a year

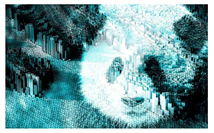
ESET researchers discover AhRat – a new Android RAT based on AhMyth – that exfiltrates files and records audio

The slow Tick-ing time bomb: Tick APT group compromise of a DLP software developer in East Asia

ESET Research uncovered a campaign by APT group Tick against a data-loss prevention company in East Asia and found a previously unreported tool used by the group

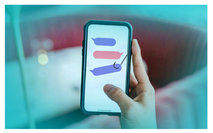
WinorDLL64: A backdoor from the vast Lazarus arsenal?

The targeted region, and overlap in behavior and code, suggest the tool is used by the infamous North Korea-aligned APT group



Evasive Panda APT group delivers malware via updates for popular Chinese software

ESET Research uncovers a campaign by the APT group known as Evasive Panda targeting an international NGO in China with malware delivered through updates of popular Chinese software



Love scam or espionage? Transparent Tribe lures Indian and Pakistani officials

ESET researchers analyze a cyberespionage campaign that distributes CapraRAT backdoors through trojanized and supposedly secure Android messaging apps – but also exfiltrates sensitive information

These aren't the apps you're looking for: fake installers targeting Southeast and East Asia

ESET researchers have identified a campaign using trojanized installers to deliver the FatalRAT malware, distributed via malicious websites linked in ads that appear in Google search results and can receive commands to delete files

Linux malware strengthens links between Lazarus and the 3CX supply-chain attack

Similarities with newly discovered Linux malware used in Operation DreamJob corroborate the theory that the infamous North Korea-aligned group is behind the 3CX supply-chain attack

MQsTTang: Mustang Panda's latest backdoor treads new ground with Qt and MQTT

ESET researchers tease apart MQsTTang, a new backdoor used by Mustang Panda, which communicates via the MQTT protocol

StrongPity espionage campaign targeting Android users

ESET researchers identified an active StrongPity campaign distributing a trojanized version of the Android Telegram app, presented as the Shagle app – a video-chat service that has no app version

ESET APT Activity Report Q4 2022–Q1 2023

Summary of activities of selected advanced persistent threat (APT) groups analyzed by ESET Research from October 2022 to March 2023.

Credits

Team

Peter Stančík, Team Lead
Klára Kobáková, Managing Editor

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

Contributors

Alexandre Côté Cyr
Dušan Lacika
Igor Kabina
Jakub Kaloč
Ján Šugarek
Jiří Kropáč
Juraj Jánošík
Ladislav Janko
Lukáš Štefanko
Marc-Étienne Léveillé
Martin Červeň
Michal Malík
Milan Fránik
Patrik Sučanský
Peter Kálnai
Tomáš Procházka
Vladimír Šimčák
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 , potentially unsafe applications and adware , except where noted in the more detailed, platform-specific sections and in the Cryptocurrency threats section.

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

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

About ESET

For more than 30 years, ESET has been developing industry-leading IT security software and services to deliver comprehensive, multilayered protection against cybersecurity threats for businesses and consumers worldwide. ESET has long pioneered machine learning and cloud technologies that prevent, detect and respond to malware. ESET is a privately owned company that promotes scientific research and development worldwide.

WeLiveSecurity.com

@ESETresearch

ESET GitHub

ESET Threat Reports and APT Activity Reports