Digital Security
Progress. Protected.

Threat Report

H1 2024

December 2023 – May 2024

(eset):research

Contents

Executive summary

Android iOS Financial threats

GoldDigger tunneling from Asia to new territories

New Android and iOS trojan steals facial recognition data from victims in Asia to create deepfake videos for authentication of financial transactions. An older Android sibling also found its way to Latin America and South Africa.

Linux Botnets Infostealers

Ebury lives on, plundering Linux servers

With hundreds of thousands of servers compromised, Ebury operators deploy tools to maximize profits.

AI Web threats Infostealers

Malware posing as generative AI assistants

A quick look behind fake generative AI assistants used as traps set by infostealers.

Web threats

More WordPress plugin vulnerabilities, more malicious scripts

Over 20,000 websites in H1 2024 compromised via injections of malicious JavaScript code.

Infostealers Web threats Gaming

Scripted encounters: Cybercriminals preying on gamers

Infostealers threaten personal data of gaming enthusiasts.

Downloaders

Downloaders switch delivery methods to stage a comeback

After upheaval in 2022, downloader threats are slowly coming back to life.

Ransomware

Look back at LockBit: Life after Operation Cronos?

Post disruption, life for the LockBit ransomware gang shows signs of struggle as more threat actors utilizing the leaked LockBit builder loom large.

Foreword

Welcome to the H1 2024 issue of the ESET Threat Report!

These past six months painted a dynamic landscape of Android Financial threats – malware going after victims' mobile banking funds – be it in the form of "traditional" banking malware or, more recently, cryptostealers.

A curious newcomer on this scene is GoldPickaxe, new mobile malware capable of stealing facial recognition data to create deepfake videos used by the malware's operators to authenticate fraudulent financial transactions. Armed with both Android and iOS versions, this threat has been targeting victims in Southeast Asia through localized malicious apps. As ESET researchers dug into this malware family, they discovered that an older Android sibling of GoldPickaxe, called GoldDiggerPlus, has also tunneled its way to Latin America and South Africa by actively targeting victims in these regions.

Keeping up with the times, infostealing malware can now be found impersonating generative AI tools as well. In H1 2024, Rilide Stealer was spotted misusing the names of generative AI assistants, such as OpenAI's Sora and Google's Gemini, to entice potential victims. In another malicious campaign, the Vidar infostealer was lurking behind a supposed Windows desktop app for AI image generator Midjourney – even though Midjourney's AI model is only accessible via Discord. Since 2023, we have been increasingly seeing cybercriminals abusing the AI theme – a trend that is expected to continue.

Gaming enthusiasts who venture out from official gaming ecosystems could unfortunately discover that infostealer threats have also found a way to spoil their favorite hobby: some cracked video games and cheating tools used in online multiplayer games were recently found to contain infostealer malware such as Lumma Stealer and RedLine Stealer.

RedLine Stealer saw several detection spikes in H1 2024, caused by one-off campaigns in Spain, Japan, and Germany. Although this "Infostealer-as-a-Service" suffered a disruption in 2023 and appears no longer to be under active development, its recent waves were so significant that RedLine Stealer detections in H1 2024 surpassed those from H2 2023 by a third.

Balada Injector, a gang notorious for exploiting WordPress plugin vulnerabilities, continued to run rampant in the first half of 2024, compromising over 20,000 websites and racking up over 400,000 hits in ESET telemetry for the variants used in the gang's recent campaign.

On the ransomware scene, former leading player LockBit was knocked off its pedestal by Operation Chronos, a global disruption conducted by law enforcement in February 2024. Although ESET telemetry recorded two notable LockBit campaigns in H1 2024, these were found to be the result of non-LockBit gangs using the leaked LockBit builder.

The Ebury botnet, previously examined in ESET's 2014 white paper Operation Windigo, remains dangerous even ten years later: recent investigation by ESET researchers uncovered that this threat has compromised nearly 400,000 servers since 2009. Although Ebury's toolkit was already substantial at the time of the original research, these latest findings revealed expanded functionalities of the botnet, focusing mostly on monetization methods such as cryptocurrency and credit card theft.

I wish you an insightful read.

Jiří Kropáč
ESET Director of Threat Detection

Threat landscape trends

Android iOS Financial threats

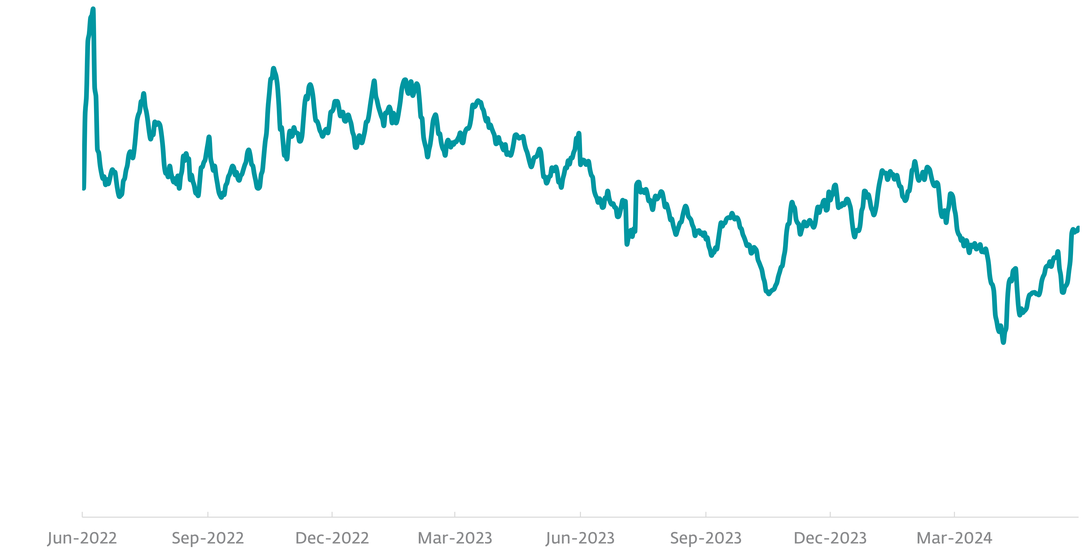
GoldDigger tunneling from Asia to new territories

New Android and iOS trojan steals facial recognition data from victims in Asia to create deepfake videos for authentication of financial transactions. An older Android sibling also found its way to Latin America and South Africa.

During the first half of 2024, ESET telemetry recorded a substantial decrease in the detection of nearly all Android threats we track. Despite fluctuations in many of these categories, often influenced by seasonal events such as Christmas and similar holidays (as discussed in ESET Threat Report T3 2022), Android Financial threats have remained consistently prevalent.

This category witnessed a relatively modest decrease in H1 2024, compared to the previous half year, of 3.8%, demonstrating no significant changes in detection rates over the past two years. However, malware in this category has exhibited ongoing changes in behavior and the methods used to victimize its targets.

In ESET Threat Reports, **Android Financial threats** incorporate both Android banking malware and cryptostealers. This merger reflects the fact that many banking trojans have begun to incorporate functionality for stealing credentials to cryptocurrency wallets and pilfering these funds, leading us to consolidate these threats into a single category.



Android Financial threats detection trend from H2 2022 to H1 2024, seven-day moving average

Adding to this dynamic landscape, Group-IB discovered a malware family stealing facial recognition data, which is then used to create deepfake videos. The creation is facilitated by face-swapping artificial intelligence services and such videos are then used for authentication of financial transactions. The malware, dubbed GoldPickaxe, has both Android and iOS versions and focuses on owners of cryptocurrency wallets and clients of financial services provided in Southeast Asia. ESET discovered that an older Android sibling of GoldPickaxe, called GoldDiggerPlus, has also tunneled its way from this region to Latin America and South Africa.

Facial recognition data has become an important part of the digital authentication process and is therefore of interest to cybercriminals. Certain financial apps, or those used in specific regions, require that users record a brief video of their faces from various angles using the front camera of their mobile device. This is in addition to uploading images of both sides of their personal identification documents. Such videos are used for identity verification purposes. This process, often referred to as biometric authentication or facial recognition, helps financial apps confirm that the person creating the account or conducting the transaction is the same individual who owns the identification documents provided. Ironically, it was intended to add an extra layer of security to prevent identity theft and fraudulent activities.

GoldPickaxe picking both Android and iOS

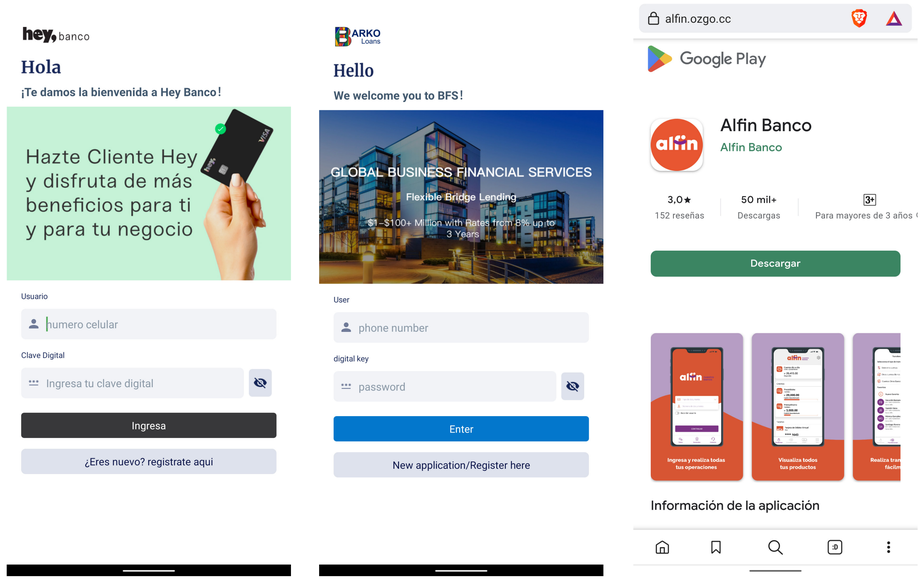
The GoldPickaxe Android version, detected by ESET security solutions as Android/Spy.Banker.CNA, is distributed via websites posing as the official Google Play store. The iOS version, detected by ESET security solutions as iOS/Riskware.Frp.A, was initially distributed through Apple's mobile application testing platform, TestFlight; however, after its removal from that platform, the threat actors adopted a more sophisticated approach. They now use a multistage social engineering scheme to persuade victims to install a Mobile Device Management profile, which allows the threat actors to gain complete control over the victim's iOS device.

Group IB believes the threat actor behind GoldPickaxe is a group it calls GoldFactory – a well-organized Chinese-speaking cybercrime group – which is also behind GoldPickaxe's siblings: GoldDigger and GoldDiggerPlus. GoldPickaxe is in fact based on GoldDigger. While we are unable to confirm some of the findings about GoldFactory, we were able to detect changes in the distribution of some GoldDiggerPlus variants, which are detected by ESET security products as Android/Spy.Banker.CAY and Android/Spy.Banker.CMQ.

GoldDigger has only Android versions and abuses Android accessibility services to extract personal information, steal banking app credentials, intercept SMS messages, and carry out a range of other actions. The latest known version, GoldDiggerPlus, has a unique feature that enables threat actors to make real-time calls to their victims. When a victim taps on the customer service button within the malicious app, the malware attempts to connect with an available member of the gang behind this threat, creating the illusion that the cybercriminals are operating a legitimate customer service center.

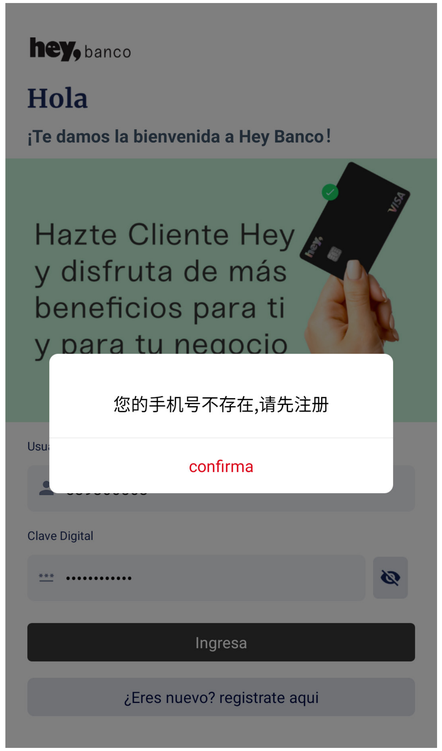
In active pursuit of new victims in Latin America and South Africa

Although GoldDiggerPlus has primarily targeted victims in Southeast Asia, ESET telemetry data shows us that this trojan has been detected also in Latin America and South Africa. Further, we can confirm that the threat actors behind GoldDiggerPlus are actively targeting these regions and that these detections do not merely represent Southeast Asian device owners located in these other countries.

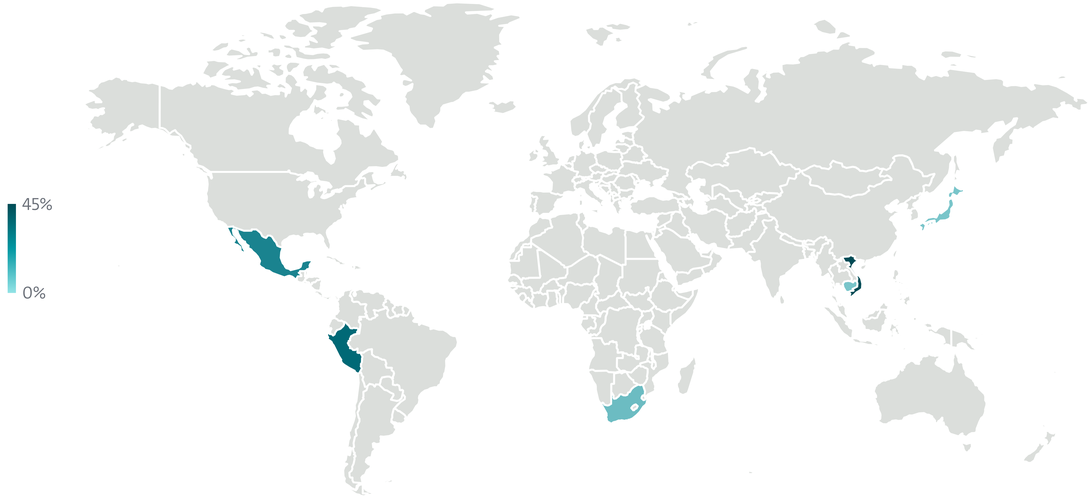


Malicious versions of the Mexican Hey Banco app, South African Barko Financial Services, and Peruvian Alfin Banco as provided via a website impersonating Google Play

The GoldDiggerPlus malware that we analyzed disguises itself as the official apps of Alfin Banco in Peru, Hey Banco in Mexico, and Barko Financial Services in South Africa. The distribution method is identical to that used in Southeast Asia, with the malicious apps being distributed through websites that impersonate the official Google Play store. All these malicious apps are provided in the local language of the targeted region. Interestingly, traces of Chinese can occasionally be detected within the apps, for instance, when users input fake or incorrect data into the malicious version of the Hey Banco app, they are presented with a message in Chinese that translates to "Your mobile phone number does not exist, please register first". Amusingly, the "confirm" button is correctly localized.



Malicious version of the Mexican Hey Banco app prompting the user to register, but it is written in Chinese



Geographic distribution of GoldDiggerPlus detections in H1 2024

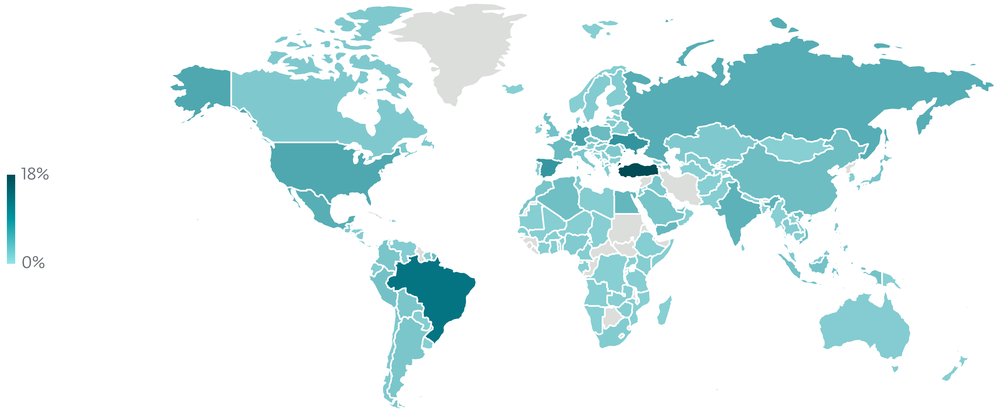
Tactical changes in Financial threats

In recent years, Android Financial threats have significantly evolved in response to enhanced security measures and the changing digital landscape. The tactics employed by the GoldDigger family described above represent only a fraction of the adaptations made by threat actors. Such changes are driven by attackers' pursuit of more sophisticated and less detectable methods of intrusion.

For instance, misusing Android accessibility services allows attackers to trigger and log any event on a device, thereby gaining full control, and the Virtual Network Computing technology facilitates the streaming of the victim's screen in real-time. Attackers have also developed Automated Transfer Systems, which enable the unauthorized transfer or deposit of funds from the victim's account, making the transaction appear less suspicious; they have found ways to bypass software-based two-factor authentication systems like Google Authenticator; and they can bypass the **Restricted Settings** security measure introduced in Android 13.

Whenever a new mobile financial threat surfaces, it frequently exhibits links to Latin America or Southeast Asia. These regions have increasingly become epicenters for cybercriminal activities, particularly involving mobile financial threats. However, in the past two years, Türkiye (formerly known as Turkey) has been the country most impacted by Android financial threats according to ESET telemetry.

The reason for Türkiye's top position, and the prevalence of these threats in Latin America, Southeast Asia, and certain African countries, is straightforward: rapid digital transformation. A significant portion of the population in these regions bypass the stage of owning a PC or laptop and move directly online through the use of smartphones. Many individuals who previously



Geographic distribution of Android Financial threats detections in H1 2024

lacked access to traditional online banking services are now using their smartphones for financial transactions. This swift shift to digital banking has, unfortunately, also sparked a rise in cybercrime. Cybercriminals often target these regions, taking advantage of their vulnerabilities to commit fraud.

The stable detection trend of Android Financial threats occurred against the backdrop of declines in nearly all categories we monitor: HiddenApps (-67%), Spyware (-43%), SMS trojans (-25%), Adware (-23%), Stalkerware (-22%), Ransomware (-18%), and Clickers (-15%). This has led to an overall drop in detections of all Android threats by 41%. Bucking this downward trend was the Scam apps category, which saw an 18% increase.

However, tracking some of the declining Android threats is becoming harder, because they arrive on the device via droppers. These programs are often disguised as legitimate apps and once they are installed on a device, they can deploy a variety of malicious software, usually without the user's knowledge. The main purpose of a dropper is to ensure the persistence of the malware on the device, even if the malicious app it initially installs is detected and removed. In H1, we saw several common droppers installing HiddenApps, but ESET telemetry cannot track them as HiddenApps because these droppers can install different kinds of threats, or even completely change what they install in the future. Nevertheless, droppers also saw a decline during the first half of this year.

NEW COMPROMISE VECTORS FOR IOS DEVICES?

The prevalence of threats on the iOS platform is notably lower compared to other operating systems, but not nonexistent, as illustrated by the iOS version of GoldPickaxe. This lower risk is primarily due to Apple's rigorous app approval process and the closed environment of the iOS ecosystem. It operates on a **sandboxing principle** that isolates each app, preventing them from interfering with each other and even easily accessing each other's data, hence reducing potential malicious activities. This principle also means a security app on an iOS device can't scan the entire device or other apps, only itself, making threat detection more challenging. Typically, potential iOS threats should be identified and mitigated by Apple's built-in security protocols.

Historically, unlike Android, iOS hasn't allowed apps to be downloaded from third-party sources, further reducing the chance of encountering threats. However, a significant shift in this policy is on the horizon – at least for iOS device users in the European Union (EU).

Driven by the European Commission's **Digital Markets Act**, EU-based iOS users will soon be able to download apps from websites and alternative app marketplaces, in addition to the traditional App Store. This change, influenced by **several lawsuits and regulatory scrutiny**, aims to open up Apple's traditionally closed ecosystem to smaller competitors, offering consumers broader choice.

However, this change comes with its own set of challenges. To safeguard users, Apple has implemented a **Notarization process** for all apps regardless of distribution channel, ensuring that they meet baseline platform integrity standards. The new web download program requires developers to meet specific criteria, such as having an app with over one million downloads in the EU. Moreover, companies can offer an app store for iPhones in the EU, so long as it only offers access to one company's apps.

Despite this, potential attackers could still find ways to exploit this system by disguising malicious software as legitimate apps, or compromising less-secure alternative app marketplaces. How soon they will be able to do this is yet to be seen.

ESET advises EU users to be cautious when downloading iOS apps from unfamiliar sources, and to understand that Apple's ability to assist with issues related to apps downloaded from outside the App Store will be limited.

Linux Botnets Infostealers

Ebury lives on, plundering Linux servers

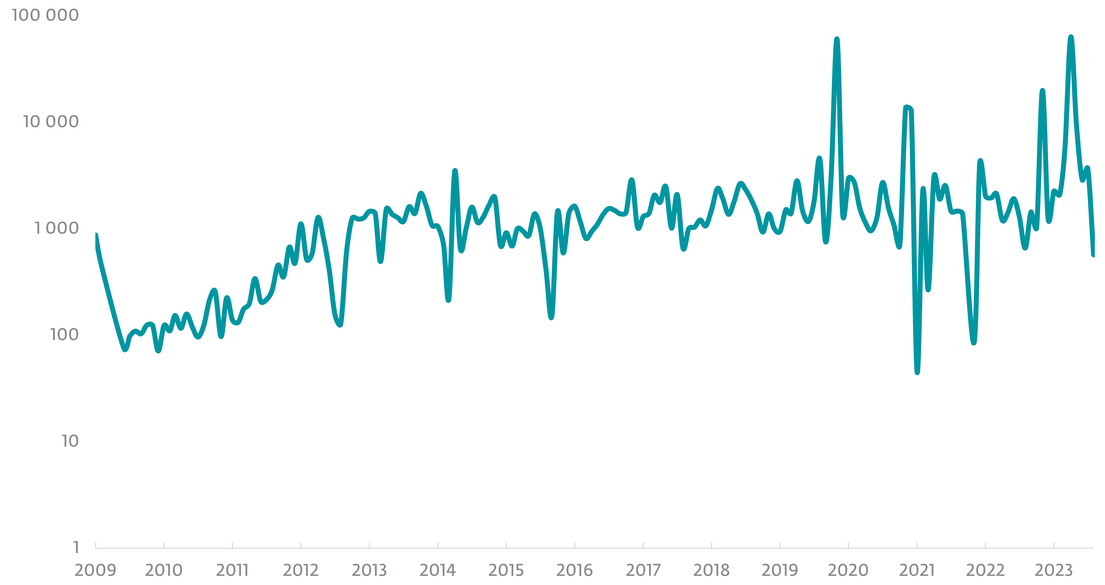
With hundreds of thousands of servers compromised, Ebury operators deploy tools to maximize profits.

Ten years ago, ESET Research released a white paper describing a large-scale campaign nicknamed Operation Windigo, in which malicious actors employed a botnet to compromise thousands of Linux and Unix servers with the Ebury malware family. Despite the arrest and extradition of one perpetrator in 2015, the botnet's activities persist to this day: Ebury's numbers have been rising more-or-less continually since 2009, with regular updates occurring on tens of thousands of servers annually, resulting in nearly 400,000 affected servers overall.

In May 2024, after a long-term and extensive investigation of the botnet in collaboration with law enforcement, ESET Research published a new white paper detailing our updated findings.

Although Ebury's toolkit was already quite substantial at the time of the original research, ESET's customized honeypots, along with law enforcement's help, revealed expanded functionalities of the botnet. These focus mostly on making money from the compromised servers via various means, such as cryptocurrency and credit card theft.

Ebury is an OpenSSH backdoor and credential stealer that forms the core of a cluster of server-side threats, initially used for web redirections, Windows malware delivery, and spamming. The Ebury botnet nowadays also intercepts HTTP POST requests made to the servers to steal financial details from transactional websites.



Ebury deployments per month since 2009, logarithmic Y axis

When going after cryptocurrency funds, Ebury leverages its presence in data centers worldwide to conduct **adversary-in-the-middle** attacks. Once the operators identify a valuable server, they are able to redirect network traffic to a system under their control to capture its SSH credentials and subsequently run scripts to exfiltrate cryptocurrency wallet data from the system.

As for credit card theft, the botnet makes use of network traffic eavesdropping, waiting for the moment victims submit their credit card information to a compromised online store. Once the data is submitted, Ebury can deploy various tools to intercept the information.

In addition to stealing credit card data and cryptocurrency funds, the threat actors behind Ebury developed other means to further support their monetization efforts. These include Apache modules exfiltrating HTTP requests or proxying traffic, Linux kernel modules performing redirections, and modified Netfilter tools injecting firewall rules.

The visibility into perpetrator activities also shed light on how Ebury propagates by stealing credentials and compromising hosting provider infrastructure, deploying malware on all customer-rented servers, sometimes resulting in thousands of servers compromised, hosting millions of domains.

Ebury's decades-long, large-scale operations and its ability to compromise even the most knowledgeable Linux users, such as those running `linux.org`, highlight multiple gaps in the state of Linux security.

Much more technical detail is available in the white paper, as is advice for those wanting to make sure that their systems are safe. The latter is tricky due to the rootkit techniques employed by Ebury malware, but methods for detecting the presence of userland rootkits using various techniques are also provided. Note that to ensure that an Ebury-compromised system is completely free from ongoing compromise, a complete reinstallation is necessary, without reusing any of the keys or credentials from the affected server.

AI Web threats Infostealers

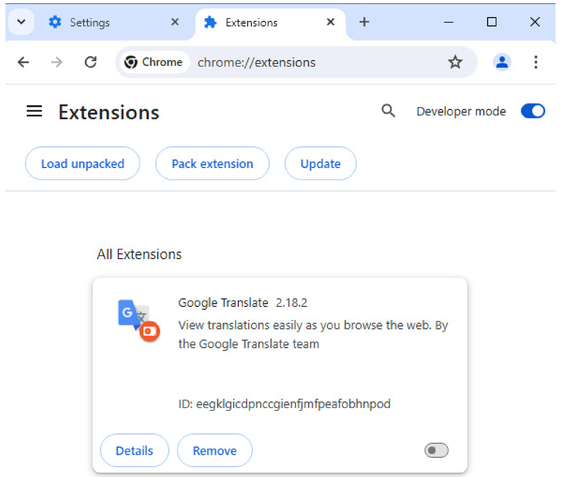
Malware posing as generative AI assistants

A quick look behind fake generative AI assistants used as traps set by infostealers.

ESET telemetry has recorded various attempts to use the names of generative AI assistants to spread malware. Perhaps the most interesting cases we observed in H1 2024 are a malicious Chrome browser extension, known as Rilide Stealer, and a malicious installer claiming to provide a desktop app for AI software but delivering the Vidar infostealer instead.

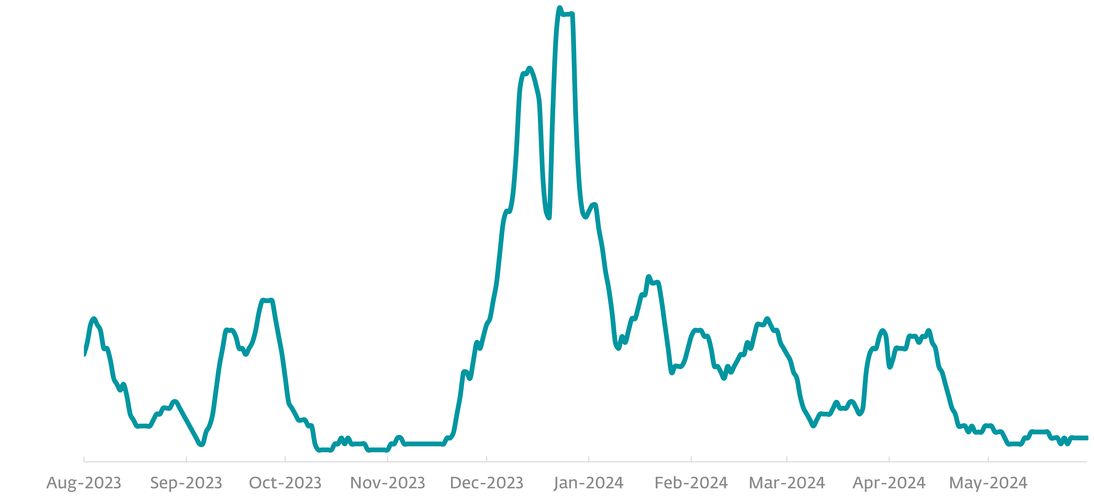
Rilide Stealer

In the case of the malicious browser extension, it is delivered to victims who have been duped into clicking on malicious ads, typically on Facebook, that promise the services of a generative AI model. Although the extension itself masquerades as Google Translate, it offers the official webpage to one of the AI services used as a lure; the lures include OpenAI's Sora and Google's Gemini. Detected as JS/Extenbro.Agent.EK and JS/Extenbro.Agent.EP by ESET security products, this extension is actually an infostealer, known as Rilide Stealer V4, that goes after Facebook credentials.



Rilide Stealer V4 Chrome browser extension, masquerading as Google Translate

Since August 2023, ESET telemetry has recorded over 4,000 attempts to install the malicious extension.



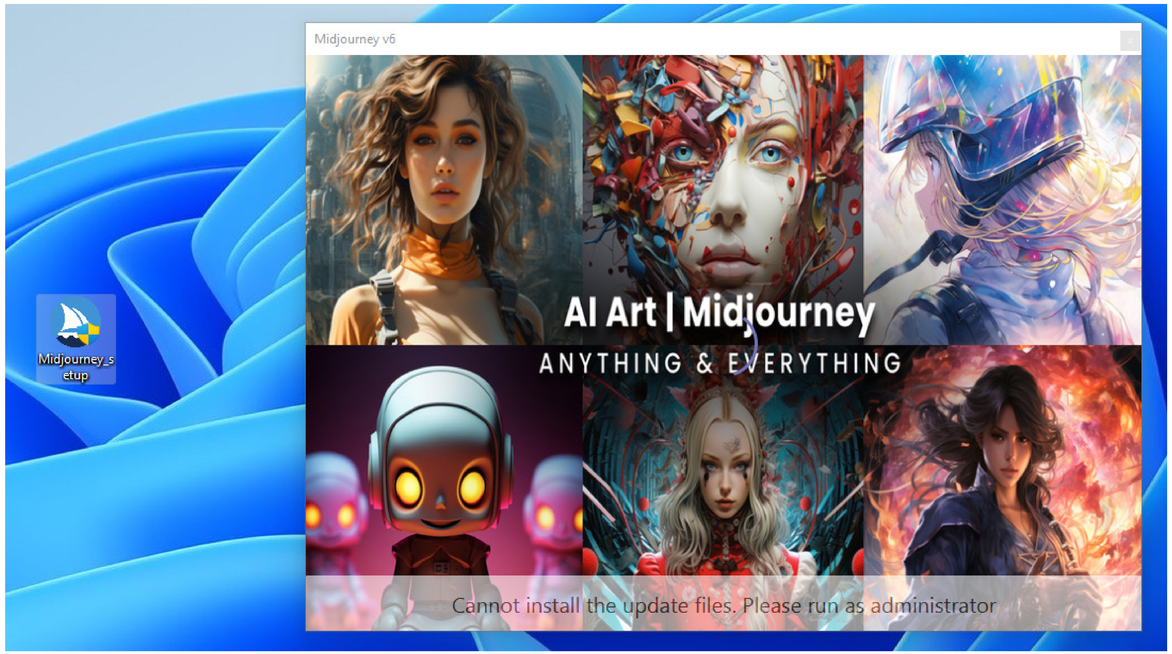
Detection trend of Rilide Stealer V4 browser extension, seven-day moving average

Vidar infostealer

Spread via Facebook ads, Telegram groups, and dark web forums, the malicious installer purports to offer **Midjourney**, an AI image generator, but delivers the Vidar infostealer instead. Upon execution, if the installer detects that a Java runtime environment (JRE) is not installed on the system, an error message about the missing runtime is shown and the official Java download page is opened; Java is required for the installer to run. If the JRE was already installed, then a splash screen advertising Midjourney is shown.

The installer, detected as Java/TrojanDownloader.Agent.NWR, drops several pieces of malware and **AutoIt** version 3, which in turn delivers Vidar. This infostealer can log keystrokes, and pilfer credentials stored by browsers and data from cryptowallets.

However, Midjourney doesn't offer a desktop app; its AI model is accessible as a Discord bot on the **official Midjourney Discord server**, by **directly messaging** the bot in Discord, or by **adding it to a third-party Discord server**. Considering the malware uses the name `Midjourney v6`, it is attempting to pose as the **latest version of the Midjourney model** currently available.



Splash screen shown by Vidar infostealer installer, impersonating Midjourney

EXPERT COMMENT

Although the ongoing development of generative AI models has been accompanied by safeguards to prevent their abuse, this has not prevented cybercrooks from pressing the topic of generative AI into cybercriminal service. Since 2023, we have seen predominantly infostealers abusing this theme and expect that trend to continue. Instead of clicking on untrustworthy links promising access to generative AI models, always navigate to the official websites of the providers. And to stay protected against infostealers, make sure to run reputable security solutions on your devices.

Jiří Kropáč, ESET Director of Threat Detection

Web threats

More WordPress plugin vulnerabilities, more malicious scripts

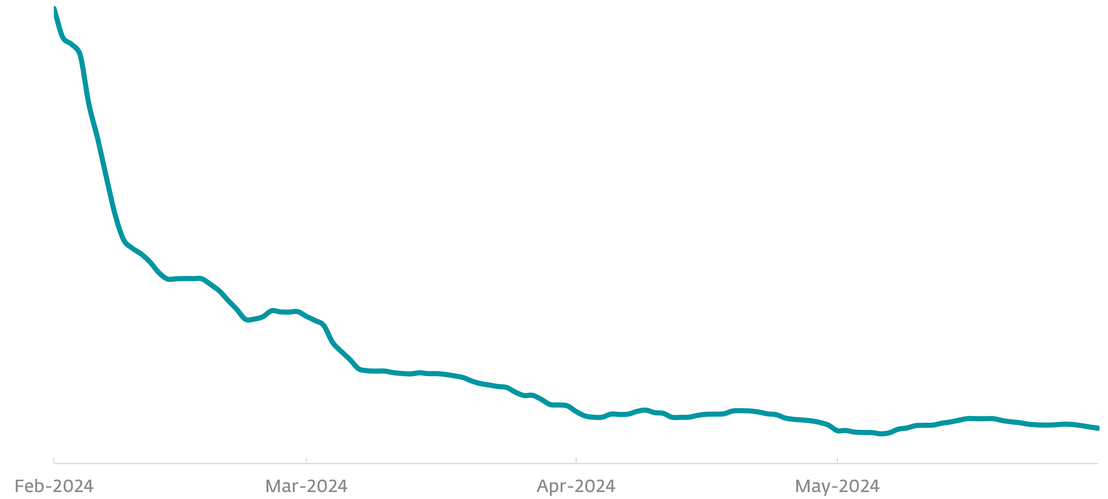
Over 20,000 websites in H1 2024 compromised via injections of malicious JavaScript code.

As noted in our **H2 2023 Threat Report**, exploiting vulnerabilities in WordPress plugins is a favored initial access technique used by the Balada Injector gang. In January 2024, the gang struck again, causing a new wave of malicious JavaScripts from the JS/Agent family to spring to life in ESET telemetry.

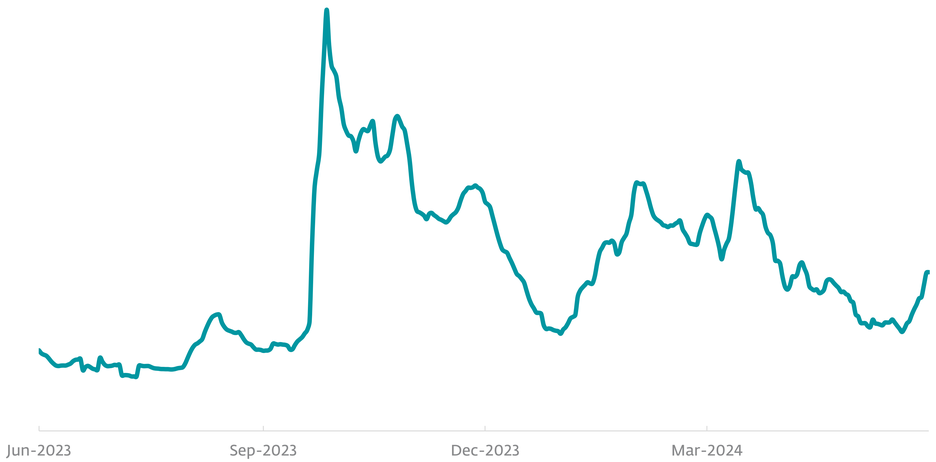
The variants detected are the same as or similar to those described in a **Sucuri** blogpost, released the same month, concerning ongoing attacks against websites running vulnerable versions of the **Popup Builder** WordPress plugin. The malicious scripts are all lightly obfuscated pieces of JavaScript whose main job is to redirect to a malicious server and deliver further malware, ultimately leading to the compromise of web admin accounts and web servers, delivery of backdoors, or targeting of the compromised website's visitors.

Most detections are due to JS/Agent.RJR, a new variant first seen in 2024 with Poland (9%), France (7%), and the US (6%) taking the largest individual shares of these detections; however, .RJR is widely dispersed, including Spain, Italy, and Germany at 5% each and Czechia at 3%. Interestingly, other variants, such as .RKY and .RJZ, have another variant embedded inside – .RKA.

The total number of hits in ESET telemetry for the Balada Injector variants used in this campaign was over 400,000, with the number of affected websites over 20,000. In H1 2024, the .RJR variant took fourth place among all JS/Agent variants, contributing significantly to the ongoing swells seen in the trendline for this family since September 2023.



Balada Injector detection trend in H1 2024, seven-day moving average



JS/Agent detection trend from June 2023 to May 2024, seven-day moving average

EXPERT COMMENT

Since the Balada Injector scripts could lead to the full take over of your web server, make sure to remove them from your website and update any vulnerable plugins to prevent future exploitation. As the Balada Injector threat actors have an uncanny knack for installing multiple persistence mechanisms, don't forget to expunge those too by checking for rogue admin accounts and malicious files on your web server, and to swap out credentials.

Ján Adámek, ESET Senior Detection Engineer

Infostealers Web threats Gaming

Scripted encounters: Cybercriminals preying on gamers

Infostealers threaten personal data of gaming enthusiasts.

Video games have grown into a multi-billion-dollar industry and this success, understandably, attracts cybercrime. Some gaming companies have already been targeted by ransomware gangs: the most recent high-profile **ransomware attack** occurred near the beginning of H1 2024, when the company Insomniac Games, developers best known for their two big-budget Spider-Man games, fell victim to a large-scale data leak after refusing to pay ransom to the notorious Rhysida ransomware group. Sensitive **data,** ranging from developers' personal information to Insomniac Games' roadmap of future game releases, was uploaded to the internet.

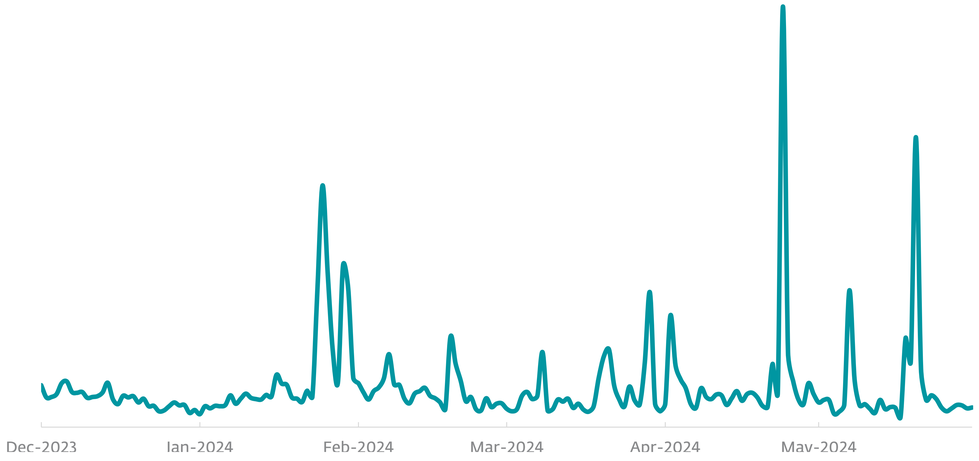
Even so, it is not only large businesses that are at risk; personal information of people who play video games is also an enticing target for cybercrooks, as evidenced by threat actors hiding malware payloads in all sorts of game-related files.

Fans of video games usually come into contact with malware by venturing out from the official ecosystem (storefronts, official video game content repositories) to the uncharted waters of torrent sites and shady Discord servers offering cracked games and cheating tools. These grey areas are exactly where criminals thrive – the possibility of getting a game for free, or of flawlessly executing headshots through walls in multiplayer shooters, constitute perfect bait for unsuspecting gamers. What awaits the victims once hooked, are often infostealers that go after their passwords, credit card data, or cryptowallets.

Infostealers-as-a-Service

Frequently, these attacks are conducted using infostealers distributed as a service; both **RedLine Stealer** and **Lumma Stealer**, described in previous ESET Threat Reports, have been found to be the payloads of files masquerading either as **cheating software** or as **video game cracks**. Looking at our telemetry data, we can confirm that these two threats were still quite active in H1 2024.

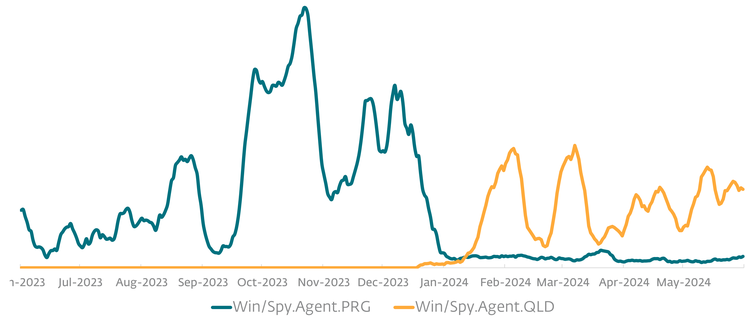
When it comes to RedLine Stealer, it seems this infostealer-for-hire refuses to die even after the **disruption** conducted in 2023. Our data suggests that even though RedLine Stealer is no longer being



RedLine Stealer daily detection trend in H1 2024

updated, it is still in use, though it's mostly relegated to one-off campaigns isolated to one or two countries – in 2024, its three biggest data peaks were registered on January 25 (50% of detections registered in Germany), April 24 (87% in Spain), and May 20 (91% in Japan). However, these peaks were so significant that RedLine Stealer detections in H1 2024 have actually surpassed those from H2 2023, with the increase amounting to 31%.

After Lumma Stealer's meteoric **rise** in H2 2023, detections of this threat, which primarily targets cryptowallets, were going down in H1 2024. Yet, interestingly, there seems to have been a shift in the specific threat variants used by the malware family. In H2 2023, ESET registered Lumma Stealer detections mostly as Win/Spy.Agent.PRG; these have almost entirely quieted in 2024. On the other hand, at the end of 2023, the malware switched to a new variant, specifically to Win/Spy.Agent.QLD. In contrast to the .PRG variant, .QLD was growing in H1 2024.



Win/Spy.Agent.PRG and Win/Spy.Agent.QLD detection trends in H2 2023 and H1 2024, seven-day moving average

Compromised mods

Gamers not inclined to pirate games or use cheats can still come across harmful files when downloading other video game-related assets. As an example, mods, or modifications for a video game made by the game's fanbase, can also be compromised by cybercriminals. While it is best to stick to well-known mod repositories or go through official platforms such as Steam, there have been cases when even those weren't safe.

In June 2023, hackers managed to **compromise** several accounts on Minecraft modding platforms and injected infostealing code into existing projects. More recently, in December 2023, a popular mod for the game Slay the Spire was **breached** to push Epsilon Stealer (which ESET detects as the JS/PSW.Agent trojan, variants .CH and .CI) via the Steam update system. In these cases, the best line of defense is to use up-to-date security software to help catch any potentially malicious files.

VIDEO GAME MODS

Modifications for existing video games, usually made by the fanbase and offered for free. These modifications can add new features, alter the way in-game models look, or even add new gameplay and story content. Some popular video games began as extensive mods; one of the most famous examples is the competitive first-person shooter Counter-Strike, which originated as a mod for Half-Life. While many developer companies embrace mods made by their community, game modding occupies a legal grey area due to copyright laws.

VIDEO GAME CRACKS

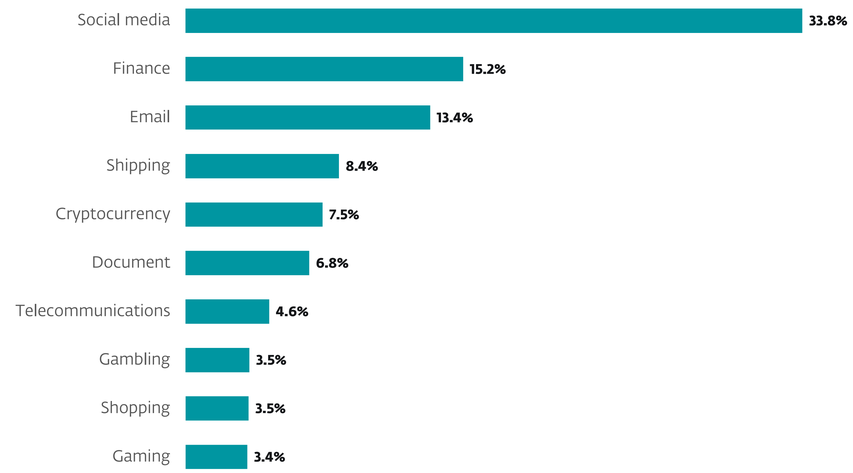
Versions of games with their copy protection removed. This is usually done to bypass anti-piracy measures.

CHEATING TOOLS

Mostly used in online multiplayer games, cheating tools are third-party software enabling players to gain unfair advantages over other players. Examples include aim assistance in first-person shooters (also known as aimbots), and making cheaters able to see through objects (wallhack).

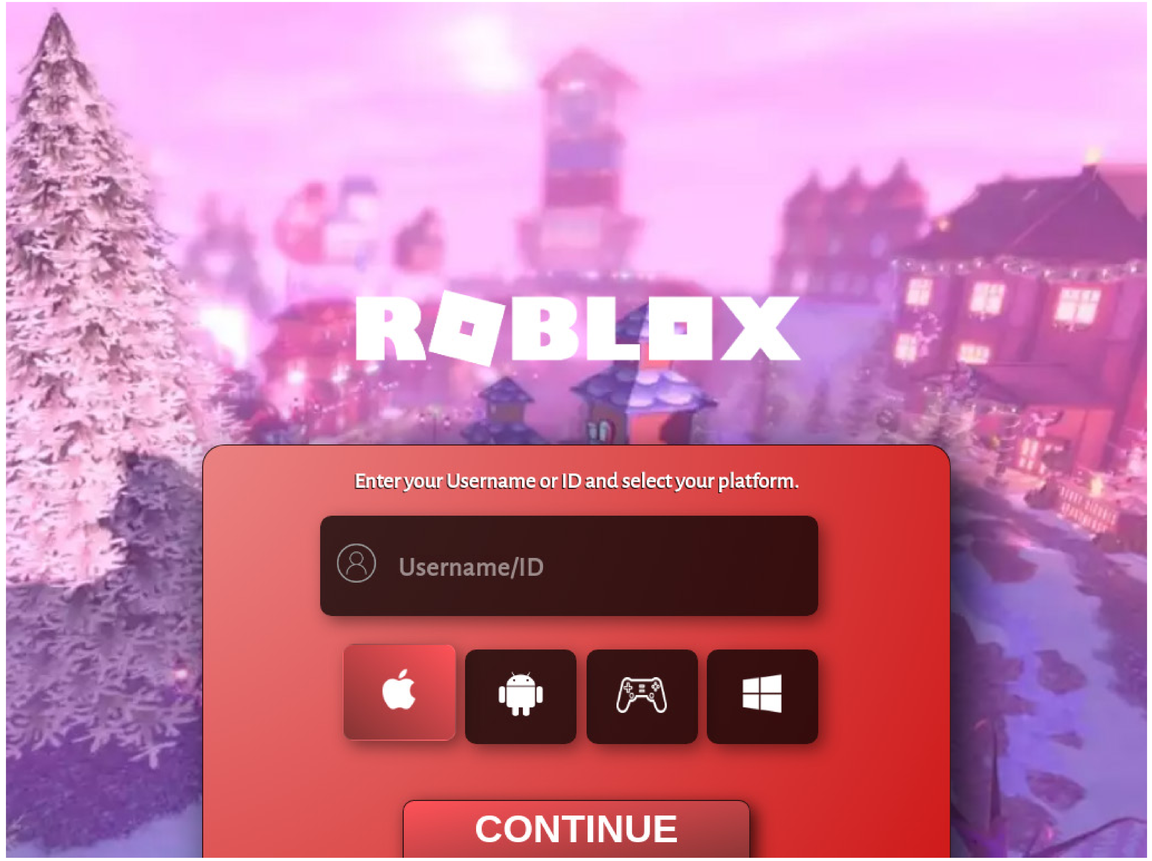
Phishing scams

Apart from being tricked into downloading malicious payloads, gamers can also fall victim to phishing scams. According to ESET phishing feeds, gaming placed tenth in the top phishing website category ranking for H1 2024.



Top 10 phishing website categories in H1 2024

Phishing can get especially dangerous when it targets games with children as the primary audience. Last year, Cisco Talos published a **report** about the many ways Roblox, a sandbox gaming platform very popular with kids, is being abused by cybercriminals. Scams involving phishing were listed first in the list Cisco Talos compiled. Since Roblox contains virtual currency named Robux that can be purchased with real money, it is a highly attractive target for cybercriminals. In our phishing feeds, we saw several instances of fake Roblox login screens or websites claiming to give out Robux to people upon signing in.



Phishing website impersonating Roblox at `robuq[.]com`

Downloaders

Downloaders switch delivery methods to stage a comeback

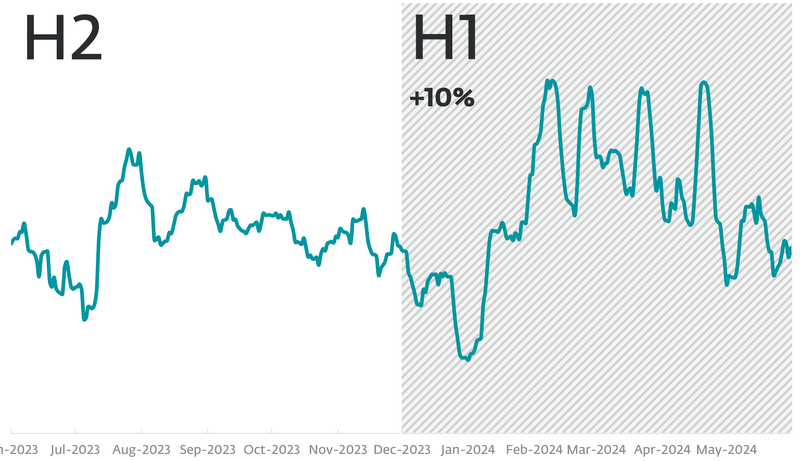
After upheaval in 2022, downloader threats are slowly coming back to life.

With Microsoft's **disabling** of internet macros in 2022, malicious downloaders took a significant hit, especially those using macros. The subsequent demise of **Emotet**, which relied extensively on this attack vector, seemed only to confirm that the golden age of downloaders was gone. This phenomenon was clearly visible in ESET telemetry: between 2022 and 2023, the data shows a 65% drop in downloader numbers. However, starting in the latter half of 2023, these threats slowly began to recoup their losses. In H2 2023, they were already up by 10% when compared to H1 of the same year, and this upward trend continued in H1 2024 as well, with another increase of 10%.

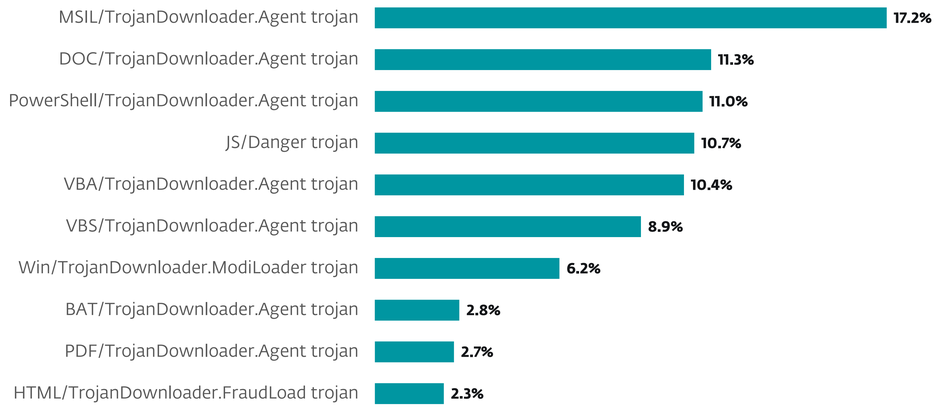
The increase in H1 2024 actually concerns the majority of downloaders we track. Looking at the top 10 downloaders detected in this period, there were only two that did not experience significant growth. Based on ESET telemetry data, this phenomenon started at the end of January and has been continuing ever since, suggesting elevated activity of threat actors in this area.

To stay in the game once automatic macros had been disabled, many cybercriminals decided to change their delivery methods. Which is why, nowadays, the most prevalent downloaders come in the form of spam emails with attachments that contain non-macro malicious scripts. These are executed after the victim clicks on them.

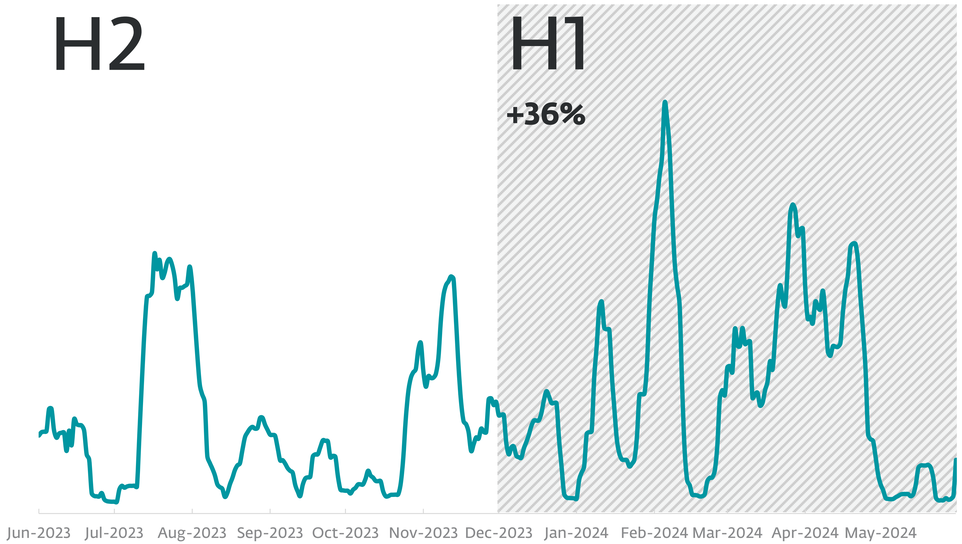
One of the examples of this shift can be seen in the rise in emails with malicious JavaScript attachments, collected in our telemetry under the name JS/Danger trojan. After a sharp detection decrease back in the



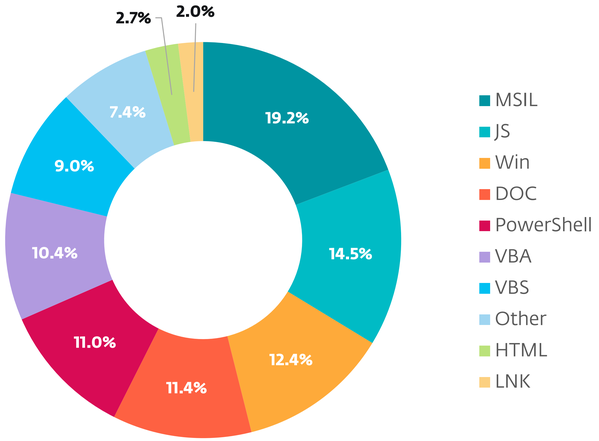
Downloader detection trend in H2 2023 and H1 2024, seven-day moving average



Top 10 Downloader detections in H1 2024 (% of Downloader detections)



JS/Danger trojan detection trend in H2 2023 and H1 2024, seven-day moving average



Downloader detections per detection type in H1 2024

beginning of 2021, this malware family seems to be experiencing a renaissance, most recently seeing a 36% increase in H1 2024. In the same period, JS downloaders also became the second-most prevalent downloader category in ESET telemetry.

The overall growth of downloaders goes hand in hand with rising detection numbers of malware families they deliver. For example, the two biggest detection spikes of VBS/TrojanDownloader.Agent in the US (February 9 and March 8) were caused by variants downloading **Agent Tesla**, a notorious infostealer that was up by 40% in H1 2024.

Interestingly, even the threats that rely on macros saw growth in H1 2024: the VBA/TrojanDownloader.Agent trojan family was up by 24%. We even registered a detection spike caused by VBA/TrojanDownloader.Agent.EGF, on February 22. This variant comes in the form of a Word document macro that runs a short downloader PowerShell script used to download further malware.

EXPERT COMMENT

The reason why the number of macro-reliant downloaders has risen could be merely a coincidence. Threat actors keep circulating these threats hoping that at least a fraction of people might go and manually enable macros in their Microsoft documents. In this way, the criminals' approach is similar to the infamous advance-fee mailing schemes that offer earnings too good to be true – the small number of people who fall for the trick is enough for the scam to be worthwile to the criminals.

Dušan Lacika, Senior Detection Engineer

Ransomware

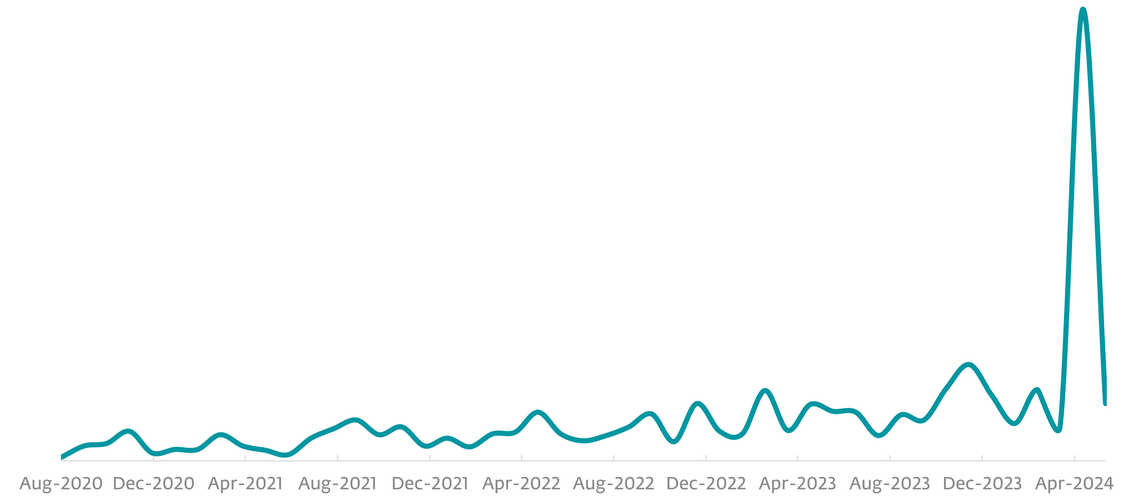
Look back at LockBit: Life after Operation Cronos?

Post disruption, life for the LockBit ransomware gang shows signs of struggle as more threat actors utilizing the leaked LockBit builder loom large.

Originating in 2019 from a ransomware family known as ABCD, LockBit went on to become a powerful player in the ransomware scene, **reportedly** holding the top place for share of ransomware attacks around the world from September 2023 to April 2024. LockBit subsequently lost this mantle as a result of the banning of LockBitSupp – the notorious public face of LockBit – from hack forums such as XSS and Exploit, and even more importantly, **Operation Cronos**, a global disruption coordinated by the UK's National Crime Agency, Europol, and Eurojust in February 2024.

This disruption led to the arrests of two LockBit affiliates in Poland and Ukraine, while French and US judicial authorities issued indictments and international arrest warrants against multiple LockBit co-conspirators. In addition, law enforcement agencies managed to confiscate over 200 cryptowallets, found a list of almost 200 affiliate names, **unmasked** the true identity of LockBitSupp, and developed and released a decryption tool.

ESET telemetry corroborates that the LockBit gang is struggling after its disruption. We have observed two notable LockBit campaigns since the disruption, though both involved samples built with the LockBit builder leaked in September 2022. A telltale sign of non-LockBit groups using this code lies in the ransom



LockBit ransomware daily detection trend since August 2020

Ransomware is typically the final payload at the end of a chain of threats that could be preceded by phishing, exploitation, brute-force attacks, compromised credentials, downloaders, or custom malware. Many would-be ransomware attacks are thus probably never realized because they are caught early in the attack lifecycle. If attackers manage to exploit vulnerabilities or other chinks in an organization's armor and are actually able to deploy ransomware, then reputable security products should detect this late link of the chain.

notes: unlike those dropped by the LockBit group, which refer the victim to a LockBit leak site, the ones dropped by these samples usually provide only an email or **Tox** contact.

One of the campaigns referred to above happened right after the February disruption. Multiple threat actors attempted to deliver LockBit via exploitation of the then **newly publicized** ScreenConnect vulnerabilities **CVE-2024-1708** and **CVE-2024-1709**. Victims were from various verticals, mainly located in Europe and the US.

The other was a malicious email campaign in mid-April 2024 that distributed LockBit ransomware via email attachments. Both the attachment format and name, and the email text, suggest widespread targeting with no special focus on any vertical. According to one **report**, the Phorpiex botnet was responsible for sending these malicious emails.

LockBit is typically a highly targeted threat; however, due to this campaign's far-reaching grasp, it significantly affected ESET telemetry for LockBit, causing a huge spike on April 17, 2024.

EXPERT COMMENT

Contrary to initial skepticism, the effects of Operation Cronos are already evident with LockBit being dethroned as Number One and desperately trying to save its brand by posting old victims on its leak sites.

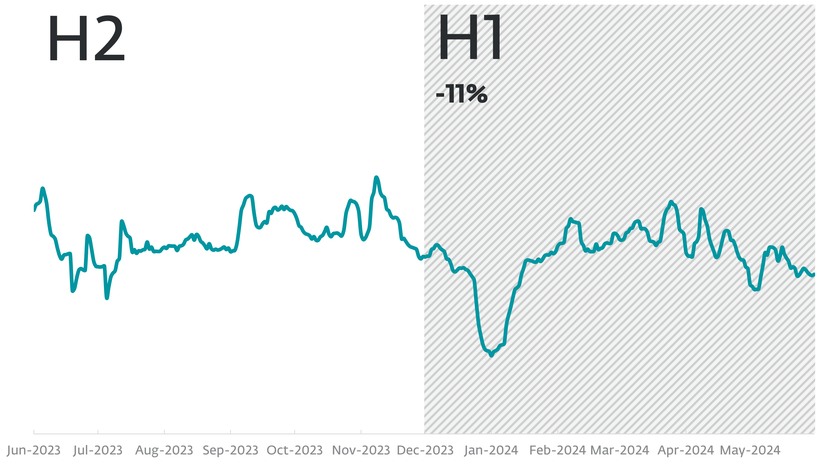
The ransomware landscape has been further shaken up by the **exit scam** pulled by BlackCat after the Change Healthcare incident. Both RansomHub, a gang that first appeared in mid-February, and Play, an older gang active since mid-2022, have been taking advantage of this opportunity to lure in new affiliates and try to climb up the ransomware-as-a-service ladder.

Data posted on leak sites indicates that the number of ransomware attacks in Q1 2024 grew by more than 20% compared to the previous quarter; however, we expect this number to be lower in Q2 2024, mainly as a result of some of the aforementioned gangs being weakened and the landscape descending into chaos. This doesn't mean that ransomware-as-a-service is going away; the second half of 2024 will surely present a clearer picture of which gangs dissatisfied affiliates move to, with ransomware rankings reflecting those shifting alliances.

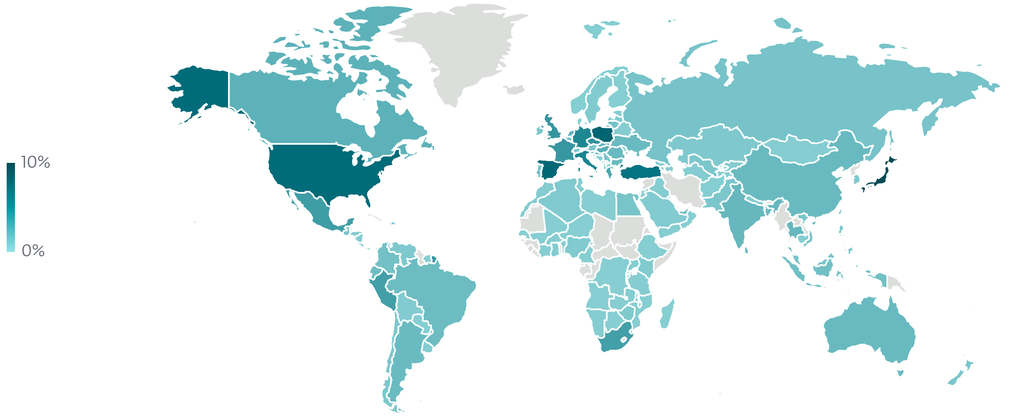
Jakub Souček, ESET Senior Malware Researcher

Threat telemetry

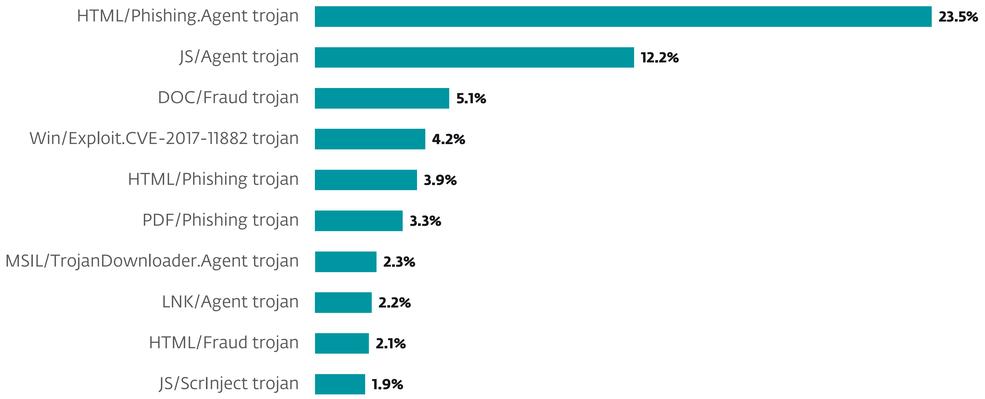
All threats



Overall threat detection trend in H2 2023 and H1 2024, seven-day moving average

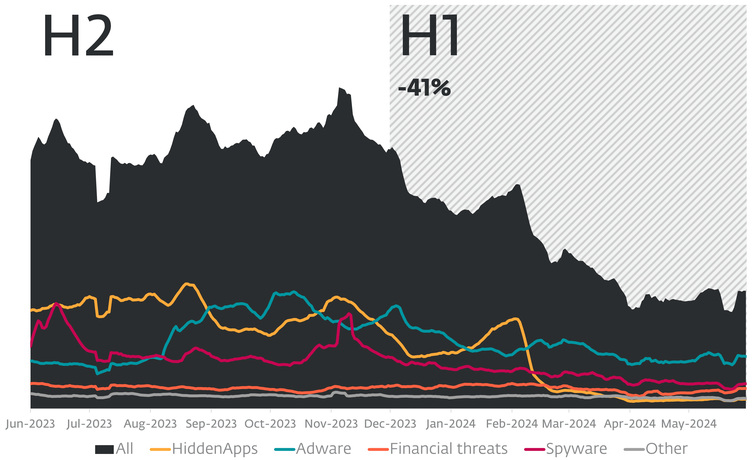


Geographic distribution of malware detections in H1 2024

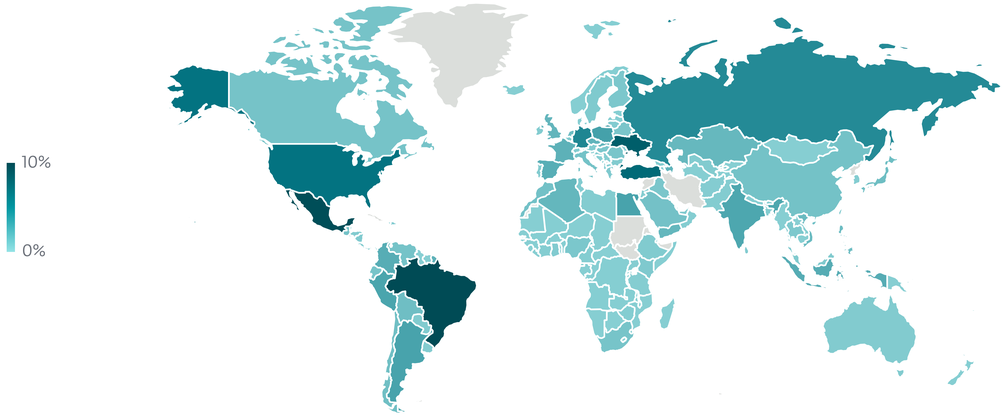


Top 10 malware detections in H1 2024 (% of malware detections)

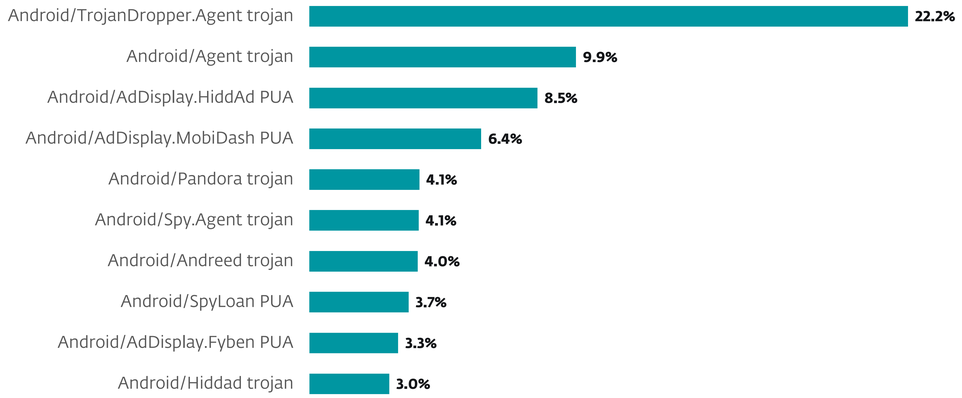
Android



Detection trends of selected Android detection categories in H2 2023 and H1 2024, seven-day moving average (trends of Clickers, Cryptominers, Ransomware, Scam apps, SMS trojans, and Stalkerware are combined in the trendline Other)

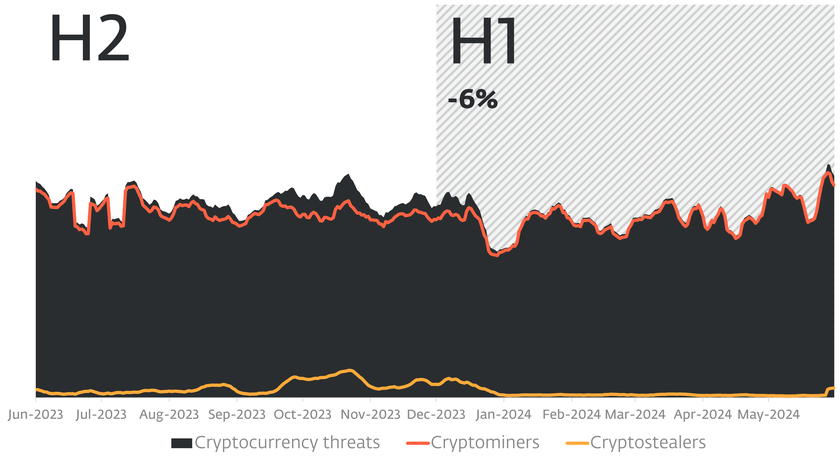


Geographic distribution of Android detections in H1 2024

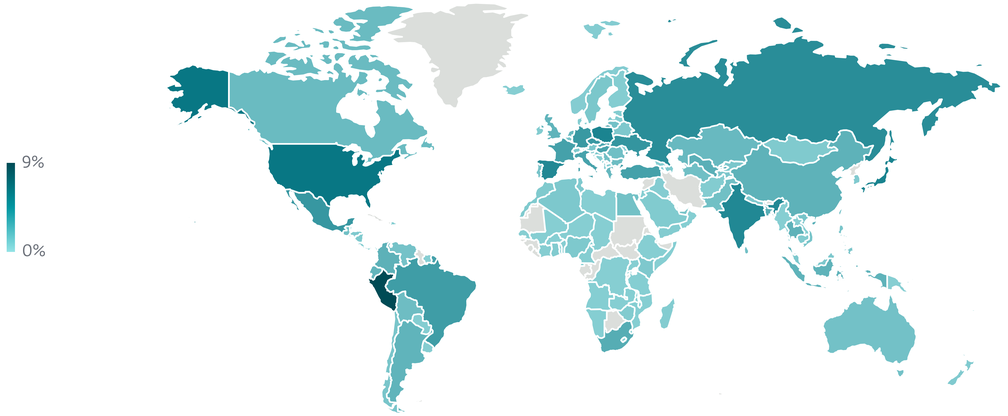


Top 10 Android detections in H1 2024 (% of Android detections)

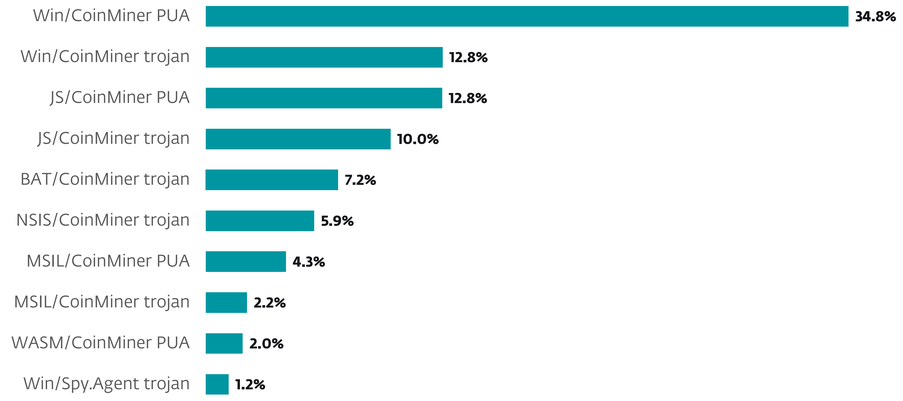
Cryptocurrency threats



Cryptocurrency threat detection trend in H2 2023 and H1 2024, seven-day moving average

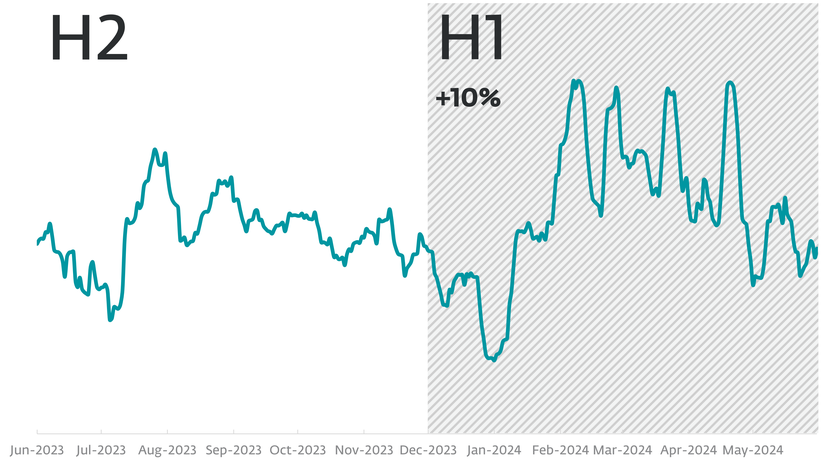


Geographic distribution of Cryptocurency threat detections in H1 2024

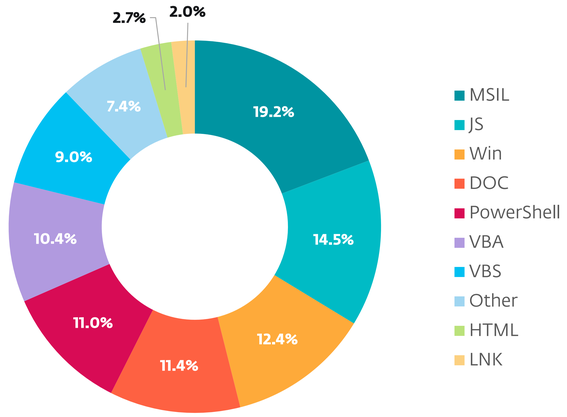


Top 10 Cryptocurrency threat detections in H1 2024 (% of Cryptocurrency threat detections)

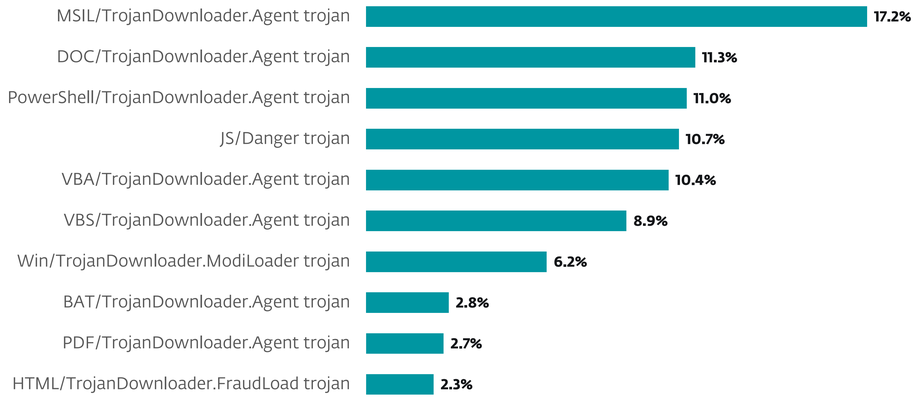
Downloaders



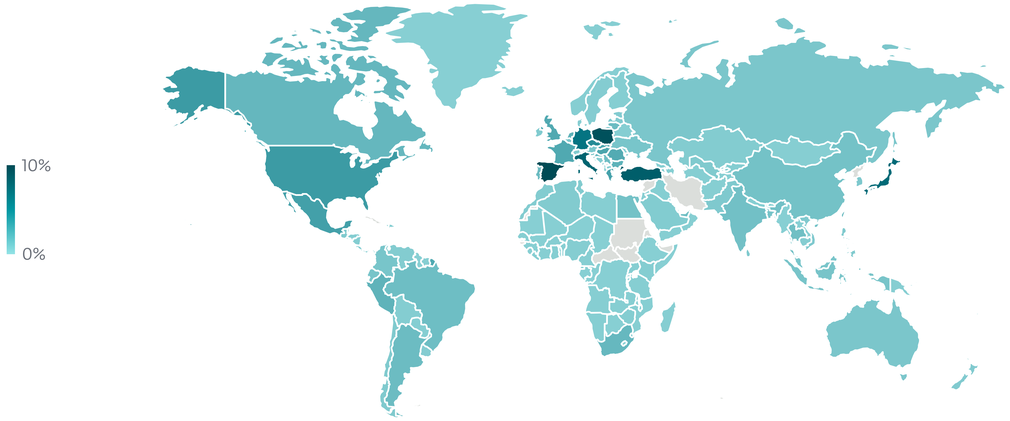
Downloader detection trend in H2 2023 and H1 2024, seven-day moving average



Downloader detections per detection type in H1 2024

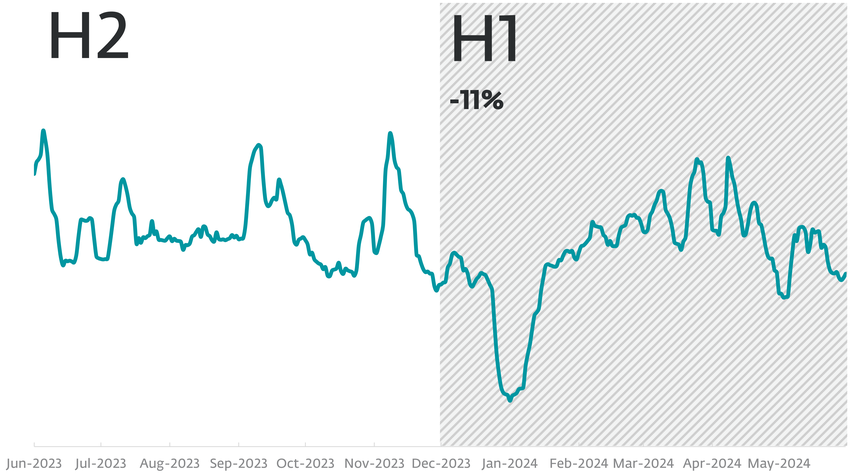


Top 10 Downloader detections in H1 2024 (% of Downloader detections)

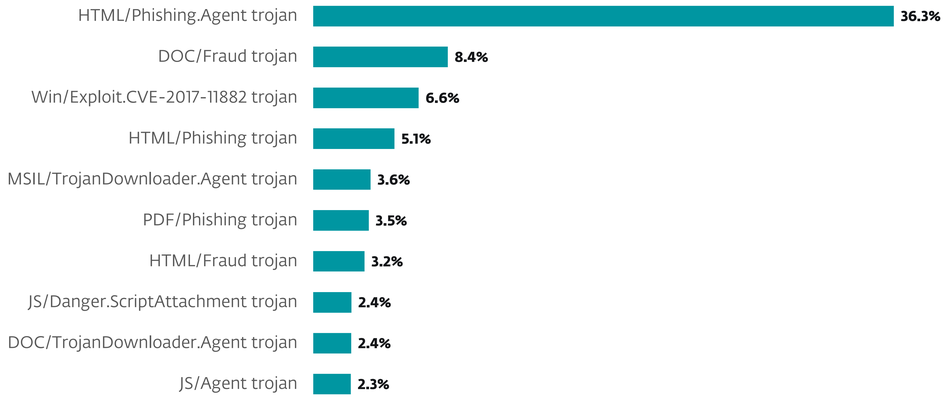


Geographic distribution of Downloader detections in H1 2024

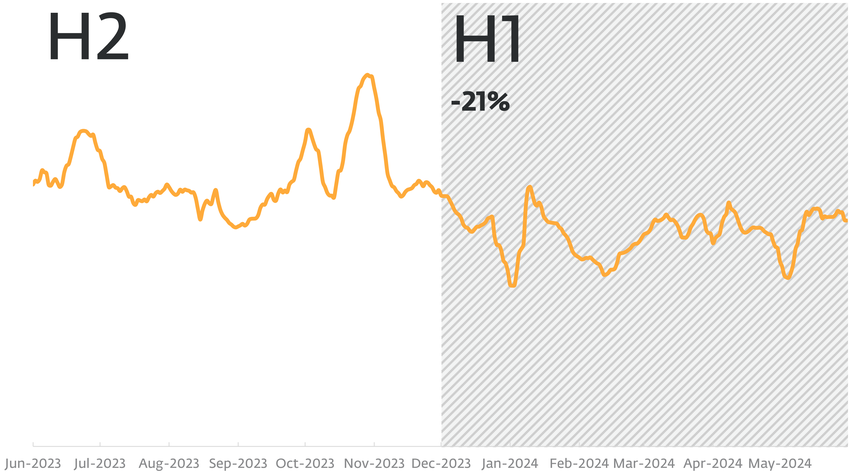
Email threats



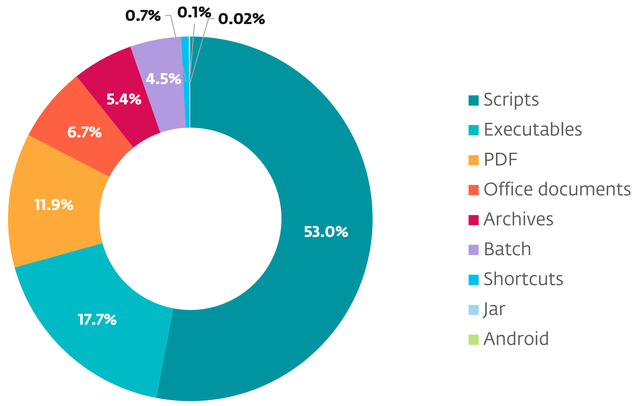
Malicious email detection trend in H2 2023 and H1 2024, seven-day moving average



Top 10 threats detected in emails in H1 2024

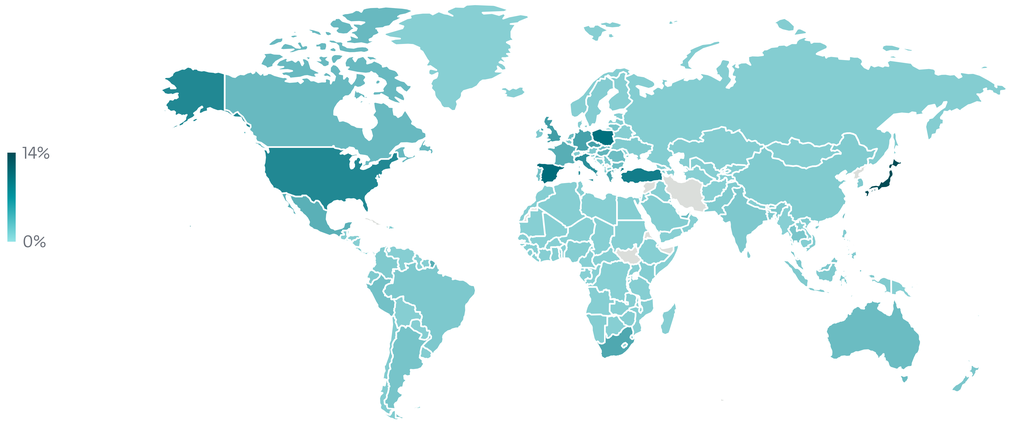


Spam detection trend in H2 2023 and H1 2024, seven-day moving average



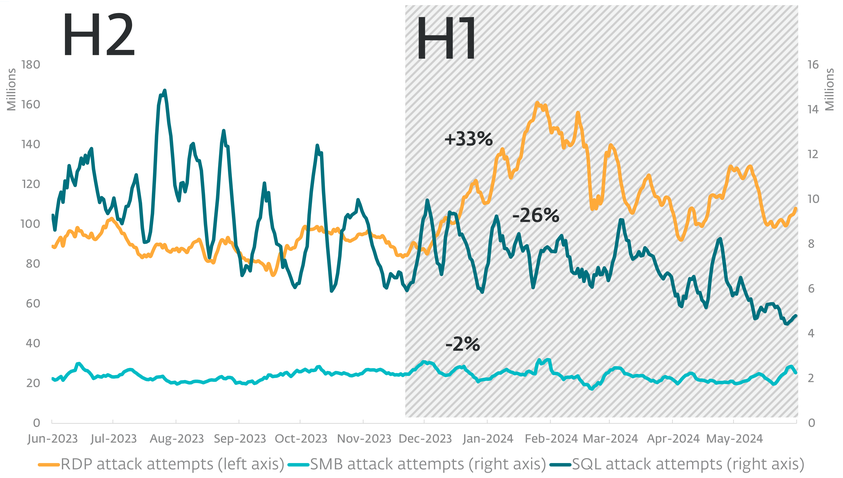
Top malicious email attachment types in H1 2024

Email threats

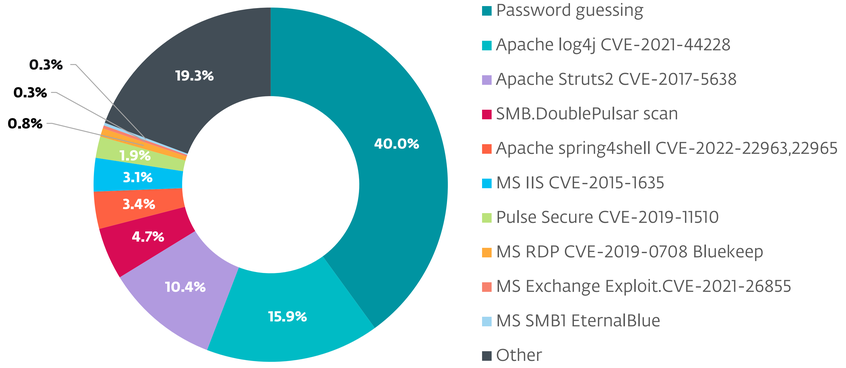


Geographic distribution of Email threat detections in H1 2024

Exploits

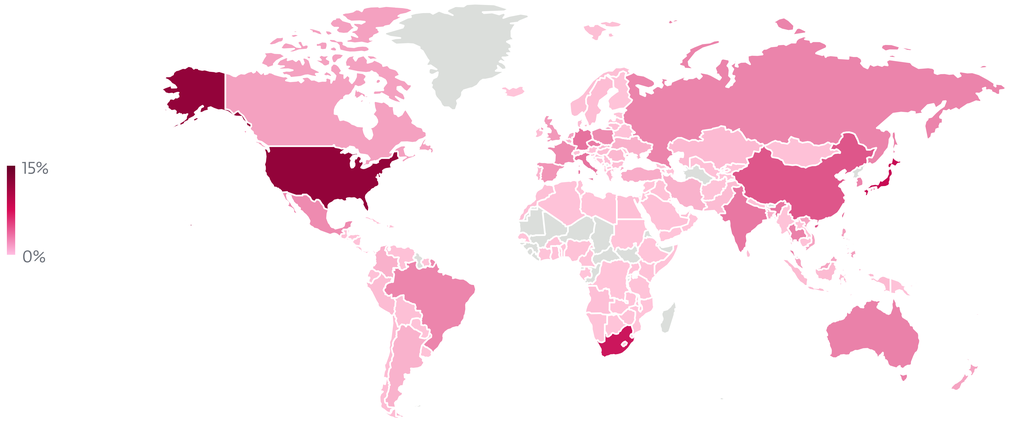


Trends of RDP, SMB and SQL attack attempts in H2 2023 and H1 2024, seven-day moving average

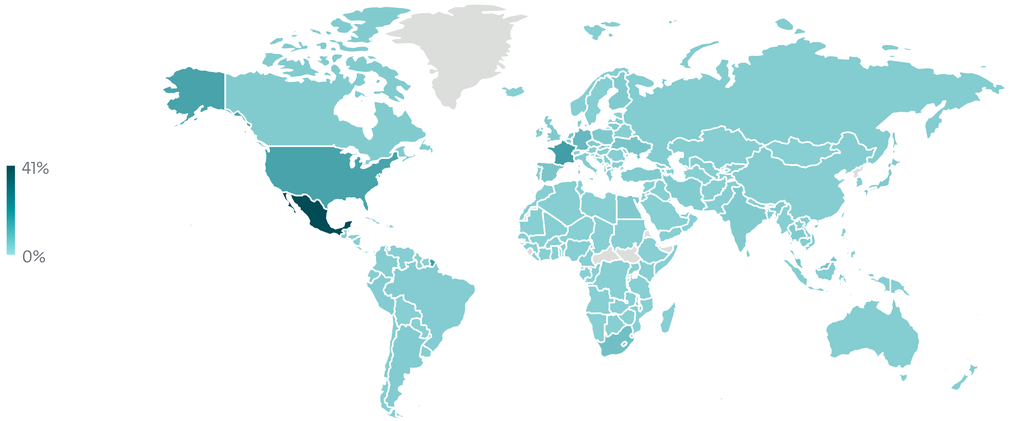


External network intrusion vectors reported by unique clients in H1 2024

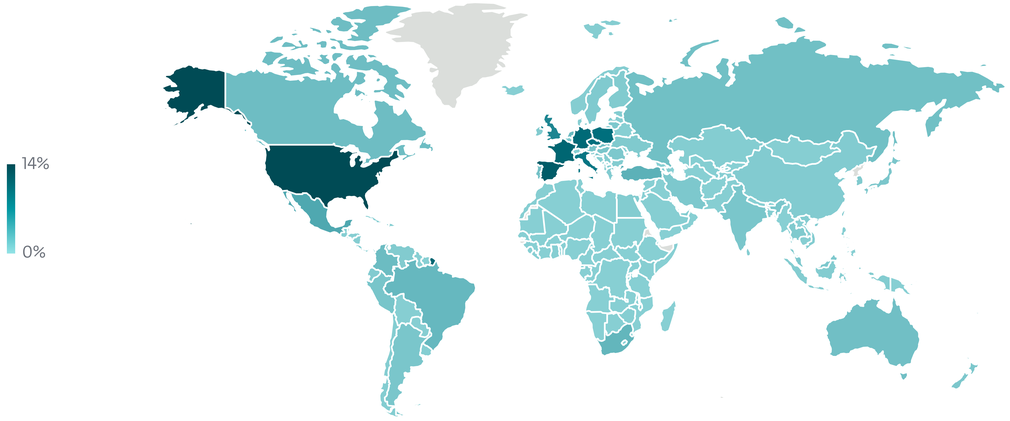
Exploits



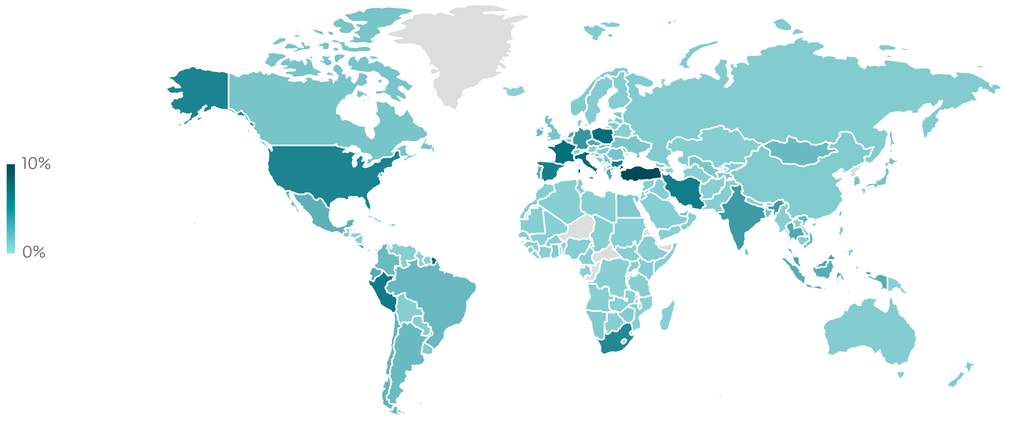
Geographic distribution of RDP password guessing attack attempt sources in H1 2024



Geographic distribution of SMB password guessing attack attempt targets in H1 2024

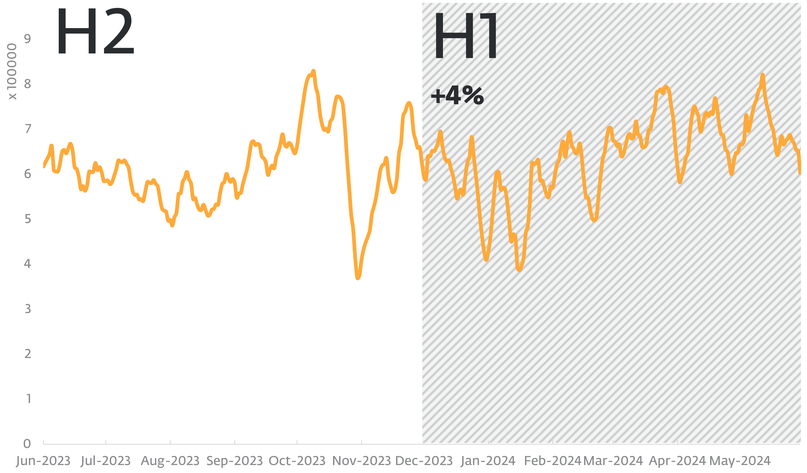


Geographic distribution of RDP password guessing attack attempt targets in H1 2024

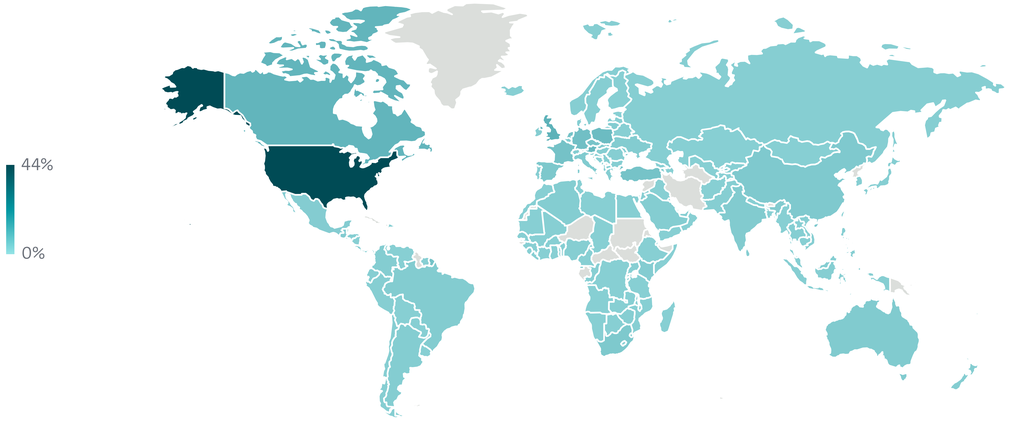


Geographic distribution of SQL password guessing attack attempt targets in H1 2024

Exploits

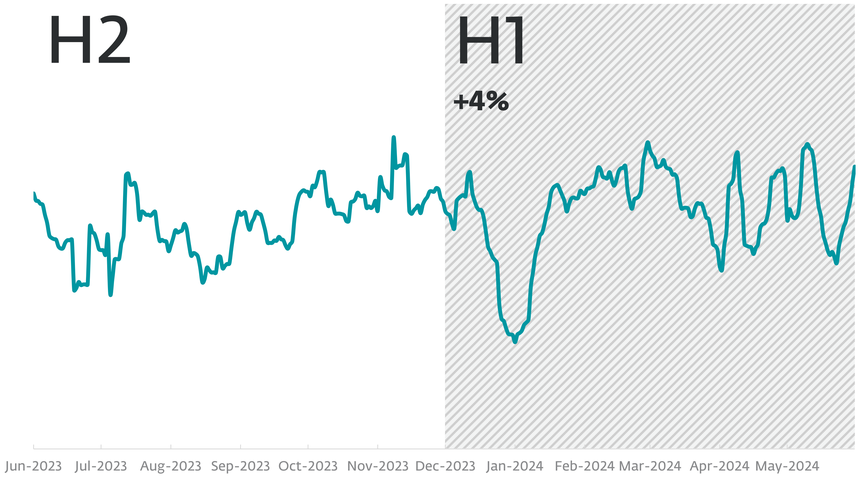


Detection trend of Log4Shell exploitation attempts in H2 2023 and H1 2024, seven-day moving average

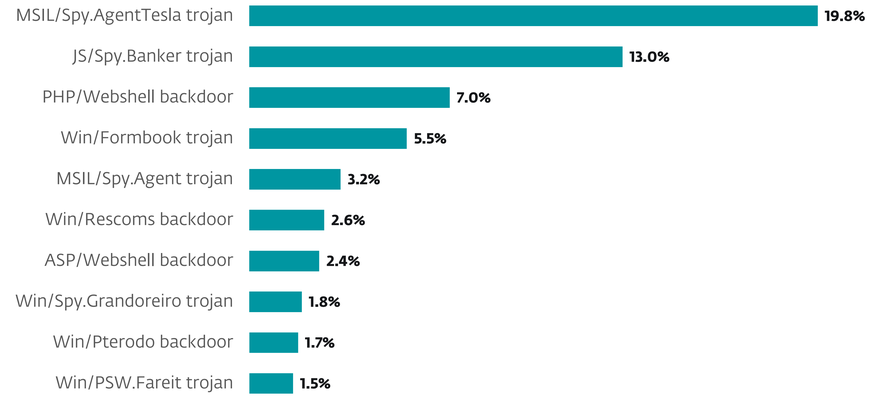


Geographic distribution of Log4Shell exploitation attempts in H1 2024

Infostealers

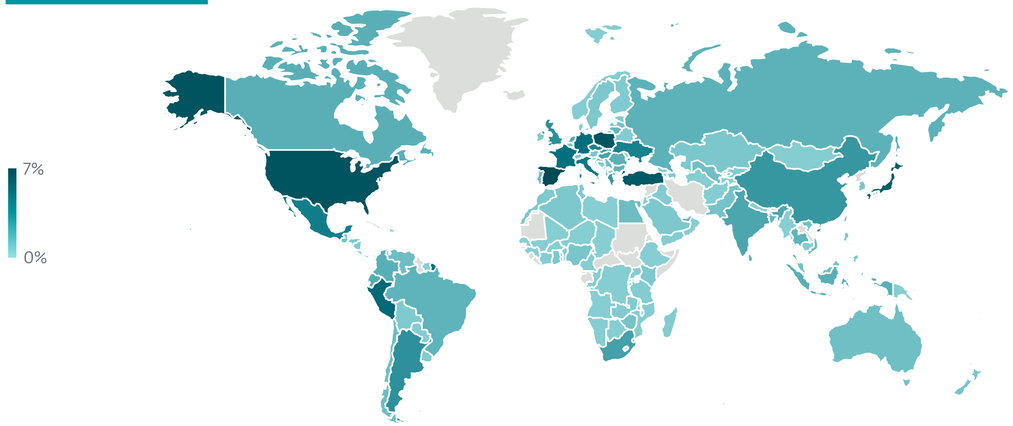


Infostealer detection trend in H2 2023 and H1 2024, seven-day moving average



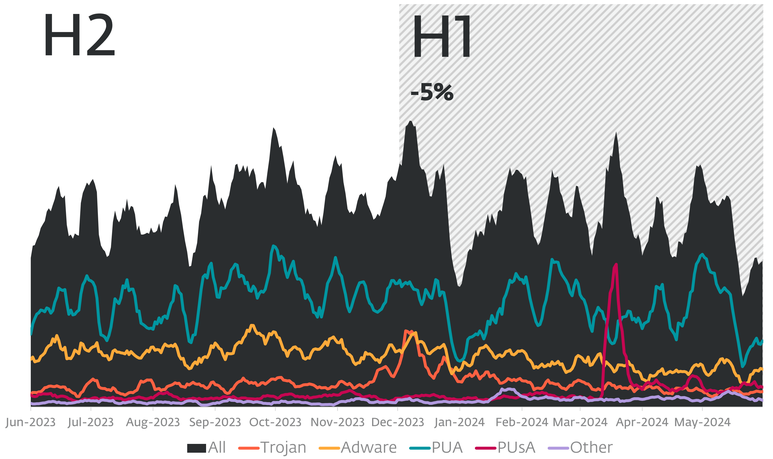
Top 10 Infostealer families in H1 2024 (% of Infostealer detections)

Infostealers

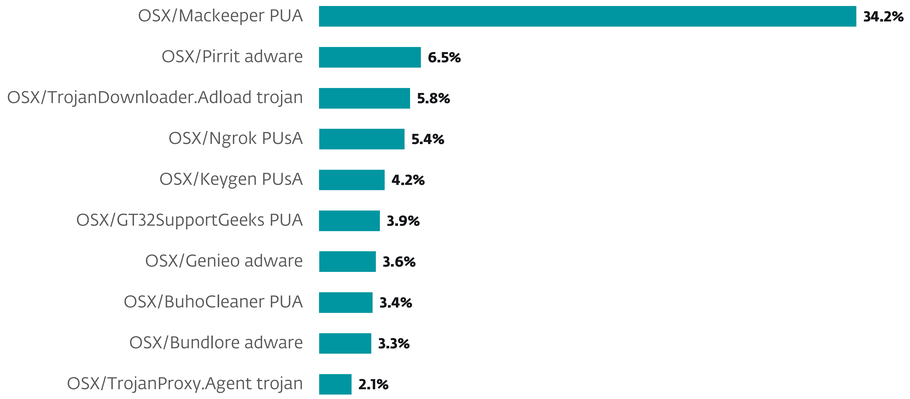


Geographic distribution of Infostealer detections in H1 2023

macOS

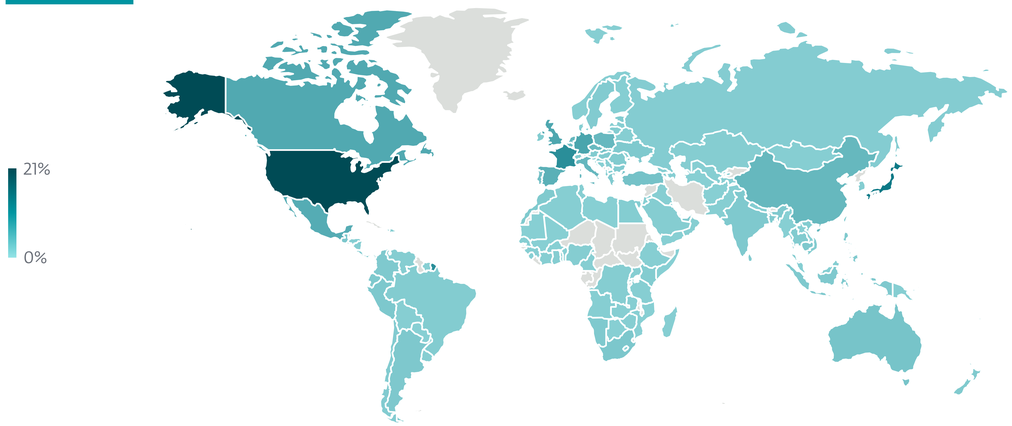


macOS detection trend in H2 2023 and H1 2024, seven-day moving average



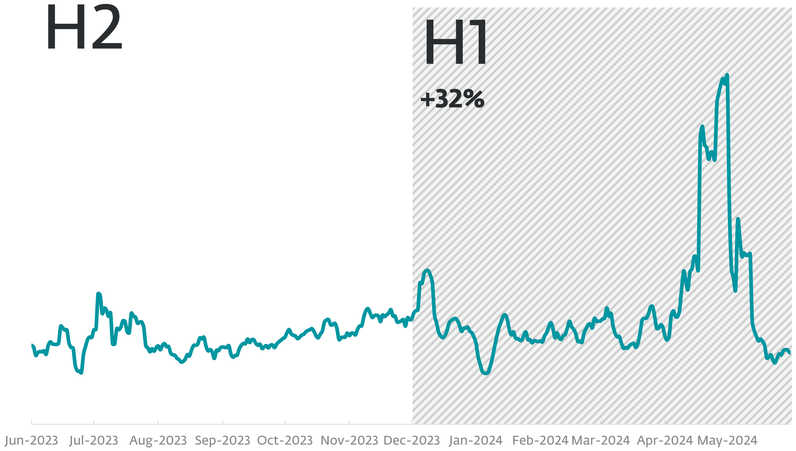
Top 10 macOS detections in H1 2024 (% of macOS detections)

macOS

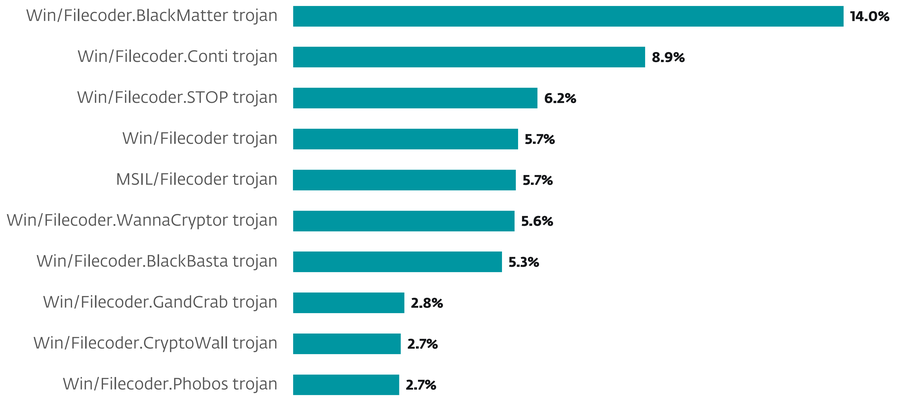


Geographic distribution of macOS detections in H1 2024

Ransomware

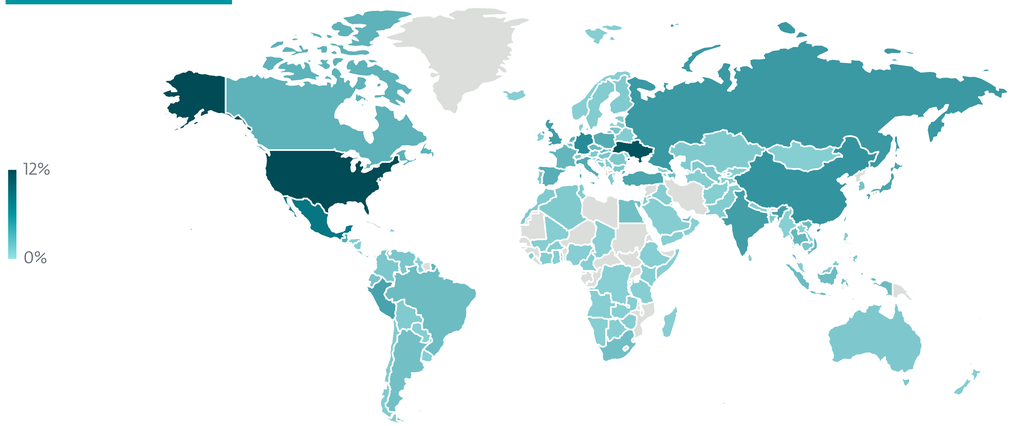


Ransomware detection trend in H2 2023 and H1 2024, seven-day moving average



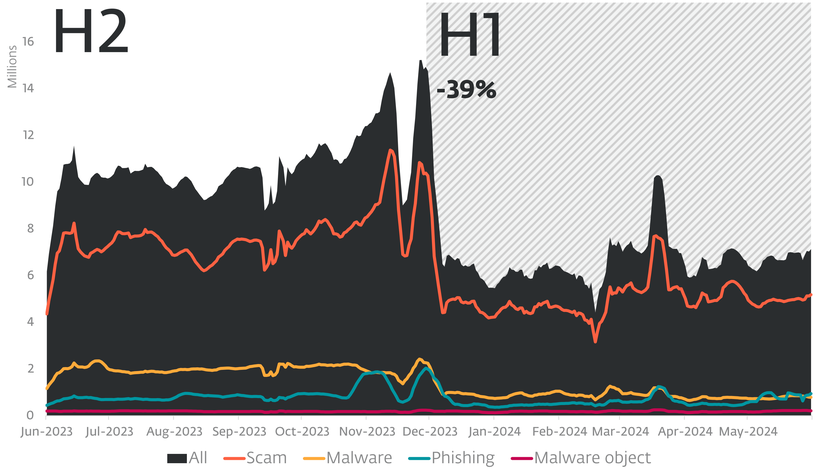
Top 10 Ransomware detections in H1 2024 (% of Ransomware detections)

Ransomware

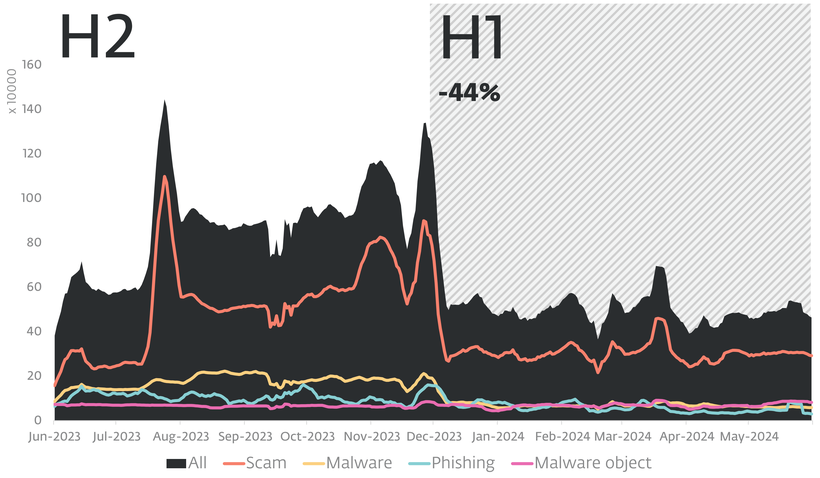


Geographic distribution of Ransomware detections in H1 2024

Web threats

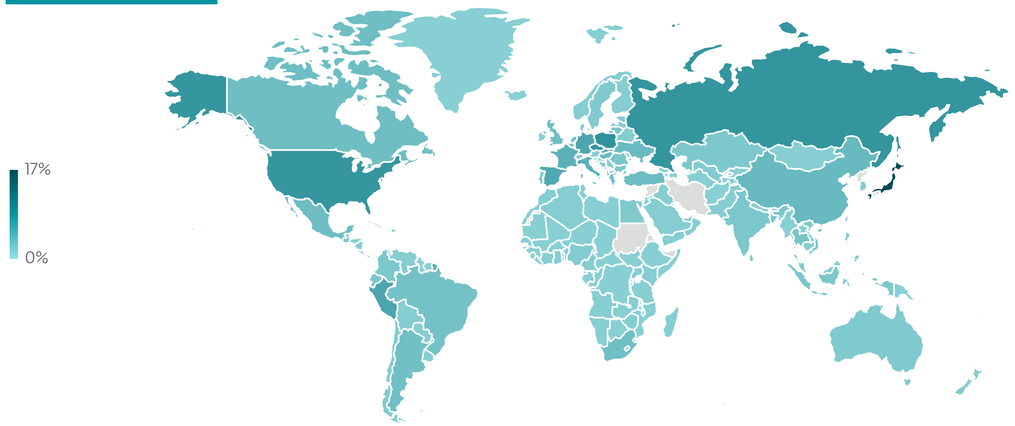


Web threat block trend in H2 2023 and H1 2024, seven-day moving average

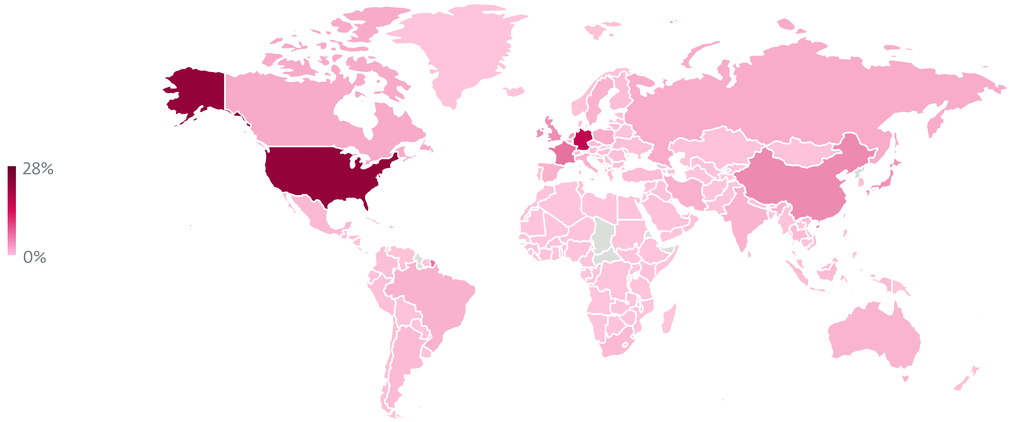


Unique URL block trend in H2 2023 and H1 2024, seven-day moving average

Web threats



Global distribution of Web threat blocks in H1 2024

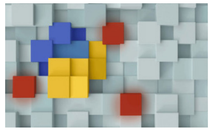


Global distribution of blocked domain hosting in H1 2024

Research publications

Beware of predatory fin(tech): Loan sharks use Android apps to reach new depths

ESET researchers describe the growth of deceptive loan apps for Android and techniques they use to circumvent Google Play



A pernicious potpourri of Python packages in PyPI

The past year has seen over 10,000 downloads of malicious packages hosted on the official Python package repository

OilRig's persistent attacks using cloud service-powered downloaders

ESET researchers document a series of new OilRig downloaders, all relying on legitimate cloud service providers for C&C communications

ESET Research Podcast: Neanderthals, Mammoths and Telekopye

ESET researchers discuss the dynamics within and between various groups of scammers who use a Telegram bot called Telekopye to scam people on online marketplaces

NSPX30: A sophisticated AitM-enabled implant evolving since 2005

ESET researchers have discovered NSPX30, a sophisticated implant used by a new China-aligned APT group we have named Blackwood

ESET takes part in global operation to disrupt the Grandoreiro banking trojan

ESET provided technical analysis, statistical information, known C&C servers and was able to get a glimpse of the victimology

ESET Research Podcast: ChatGPT, the MOVEit hack, and Pandora

An AI chatbot inadvertently kindles a cybercrime boom, ransomware bandits plunder organizations without deploying ransomware, and a new botnet enslaves Android TV boxes

VajraSpy: A Patchwork of espionage apps

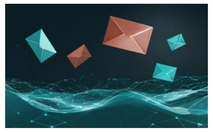
ESET researchers discovered several Android apps carrying VajraSpy, a RAT used by the Patchwork APT group

Operation Texonto: Information operation targeting Ukrainian speakers in the context of the war

A mix of PSYOPs, espionage and ... fake Canadian pharmacies!

Evasive Panda leverages Monlam Festival to target Tibetans

ESET researchers uncover strategic web compromise and supply-chain attacks targeting Tibetans



Rescoms rides waves of AceCryptor spam

Insight into ESET telemetry statistics about AceCryptor in H2 2023 with a focus on Rescoms campaigns in European countries

eXotic Visit campaign: Tracing the footprints of Virtual Invaders

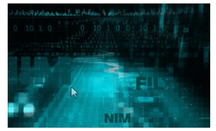
ESET researchers uncovered the eXotic Visit espionage campaign that targets users mainly in India and Pakistan with seemingly innocuous apps

Ebury is alive but unseen: 400k Linux servers compromised for cryptocurrency theft and financial gain

One of the most advanced server-side malware campaigns is still growing, with hundreds of thousands of compromised servers, and it has diversified to include credit card and cryptocurrency theft

To the Moon and back(doors): Lunar landing in diplomatic missions

ESET researchers provide technical analysis of the Lunar toolset, likely used by the Turla APT group, that infiltrated a European ministry of foreign affairs



Introducing Nimfilt: A reverse-engineering tool for Nim-compiled binaries

Available as both an IDA plugin and a Python script, Nimfilt helps to reverse engineer binaries compiled with the Nim programming language compiler by demangling package and function names, and applying structs to strings

ESET APT Activity Report Q4 2023–Q1 2024

An overview of the activities of selected APT groups investigated and analyzed by ESET Research in Q4 2023 and Q1 2024

Credits

Team

Peter Stančík, Team Lead
Hana Matušková, Managing Editor

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

Contributors

Alexandre Côté-Cyr
Dušan Lacika
Igor Kabina
Jakub Souček
Jan Holman
Ján Adámek
Ján Šugarek
Jiří Kropáč
Ladislav Janko
Lukáš Štefanko
Marc-Étienne Léveillé
Martin Červeň
Mathieu Tartare
Vladimír Šimčák
Yevhenii Fomiachenko

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

ESET® provides cutting-edge digital security to prevent attacks before they happen. By combining the power of AI and human expertise, ESET stays ahead of known and emerging cyberthreats — securing businesses, critical infrastructure, and individuals. Whether it's endpoint, cloud, or mobile protection, our AI-native, cloud-first solutions and services remain highly effective and easy to use. ESET technology includes robust detection and response, ultra-secure encryption, and multifactor authentication. With 24/7 real-time defense and strong local support, we keep users safe and businesses running without interruption. An ever-evolving digital landscape demands a progressive approach to security: ESET is committed to world-class research and powerful threat intelligence, backed by R&D centers and a strong global partner network. For more information, visit **www.eset.com** or follow us on **LinkedIn**, **Facebook**, and **X**.

WeLiveSecurity.com

@ESETresearch

ESET GitHub

ESET Threat Reports and APT Activity Reports

© 2024 ESET, spol. s r.o. - All rights reserved.

Trademarks used herein are trademarks or registered trademarks of ESET, spol. s r.o.

All other names and brands are registered trademarks of their respective companies.