Digital Security
Progress. Protected.

Threat Report

H1 2025

December 2024 – May 2025

(eset):research

Contents

Executive summary

Attack vectors | Social engineering

ClickFix: Fake errors, real threats

A novel social engineering technique called ClickFix is taking the threat landscape by storm, becoming the second most prevalent attack vector after phishing.

Infostealers | Malware as a service

Double trouble befalls prominent infostealers

ESET participated in disruption operations aimed at two notable infostealers: Lumma Stealer and Danabot.

Infostealers | Malware as a service

SnakeStealer slithers to the top

In the wake of Agent Tesla's creators abandoning their malware, SnakeStealer claims its place as the most-detected infostealer in ESET telemetry data.

Android | Adware

Kaleidoscope and its evil twin scheme flood Android with ads

Android adware detections jump by 160%, fueled by new evil twin fraud and the rise of potentially unwanted apps.

Android | NFC | Scams

The evolution of NFC fraud: From NGate to GhostTap to relay scams

NFC-based fraud soared more than thirty-five-fold, fueled by phishing campaigns and inventive relay techniques.

Ransomware

Get your popcorn: it's time for ransomware deathmatch

While the number of ransomware attacks and gangs has been growing, ransomware groups are increasingly fighting each other, impacting several players including the top ransomware as a service – RansomHub.

Foreword

Welcome to the H1 2025 issue of the ESET Threat Report!

From novel social engineering techniques to sophisticated mobile threats and major infostealer disruptions, the threat landscape in the first half of 2025 was anything but boring.

One of the most striking developments this period was the emergence of ClickFix, a new, deceptive attack vector that skyrocketed by over 500% compared to H2 2024 in ESET telemetry. Now the second most common attack vector after phishing, ClickFix manipulates internet users into executing malicious commands under the guise of fixing a fake error. The payloads at the end of ClickFix attacks vary widely – from infostealers to ransomware and even to nation-state malware – making this a versatile and formidable threat across Windows, Linux, and macOS.

The infostealer landscape also saw significant shifts. With Agent Tesla fading into obsolescence, SnakeStealer (also known as Snake Keylogger) surged ahead, becoming the most detected infostealer in our telemetry. Meanwhile, ESET contributed to major disruption operations targeting Lumma Stealer and Danabot, two prolific malware-as-a-service threats.

On the Android front, adware detections soared by 160%, driven largely by a sophisticated new threat dubbed Kaleidoscope. This malware uses a deceptive "evil twin" strategy to distribute malicious apps that bombard users with intrusive ads, degrading device performance. At the same time, NFC-based fraud shot up more than thirty-five-fold, fueled by phishing campaigns and inventive relay techniques. While the overall numbers remain modest, this jump highlights the rapid evolution of the criminals' methods and their continued focus on exploiting NFC technology. Each new iteration of NFC threats – from NGate to GhostTap, and most recently SuperCard – demonstrates how attackers adapt to new security measures.

The ransomware scene descended (even further) into chaos, with fights between rival ransomware gangs impacting several players including the top ransomware as a service – RansomHub. Yearly data shows that while ransomware attacks and the number of active gangs have grown, ransom payments saw a significant drop. This discrepancy may be the result of takedowns and exit scams that reshuffled the ransomware scene in 2024, but also partially due to diminished confidence in the gangs' ability to keep their side of the bargain.

I wish you an insightful read.

Jiří Kropáč
ESET Director of Threat Prevention Labs

Threat landscape trends

Attack vectors Social engineering

ClickFix: Fake errors, real threats

A novel social engineering technique called ClickFix is taking the threat landscape by storm, becoming the second most prevalent attack vector after phishing.

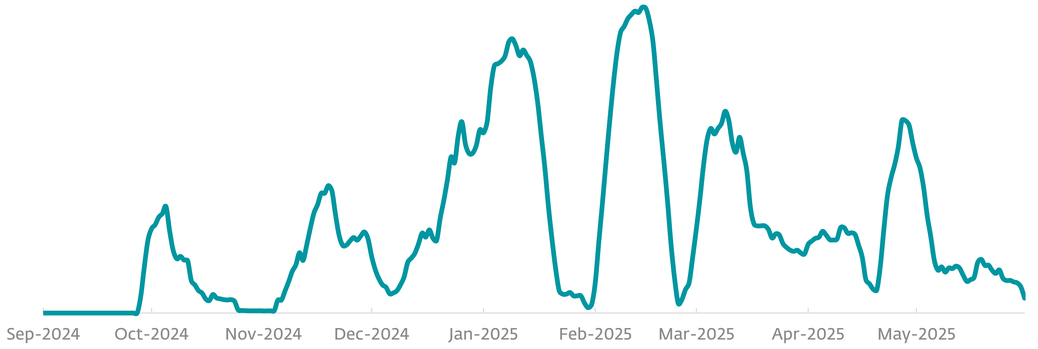
Proving, online, that you are human can take on many forms. At times, you may need to transcribe blurry text into a blank field, while on other occasions you're asked to select all images of buses, traffic lights, or stairs. Every now and then a website will have you drag a puzzle piece to its correct location within an image. As the variety of reCAPTCHA checks has grown, users have become accustomed to the process, and few would question encountering a new type of challenge, such as copying and pasting something onto their device. And that is precisely what cybercriminals have thought, weaponizing one of the web's most frustrating features into a new intrusion avenue.

ClickFix is a new type of social engineering that uses a fake error or verification message to manipulate victims into copying and pasting a malicious script and then running it. The list of threats that ClickFix leads to is growing by the day, currently including infostealers, ransomware, remote access trojans, cryptominers, post-exploitation tools, and even custom malware from nation-state-aligned threat actors.

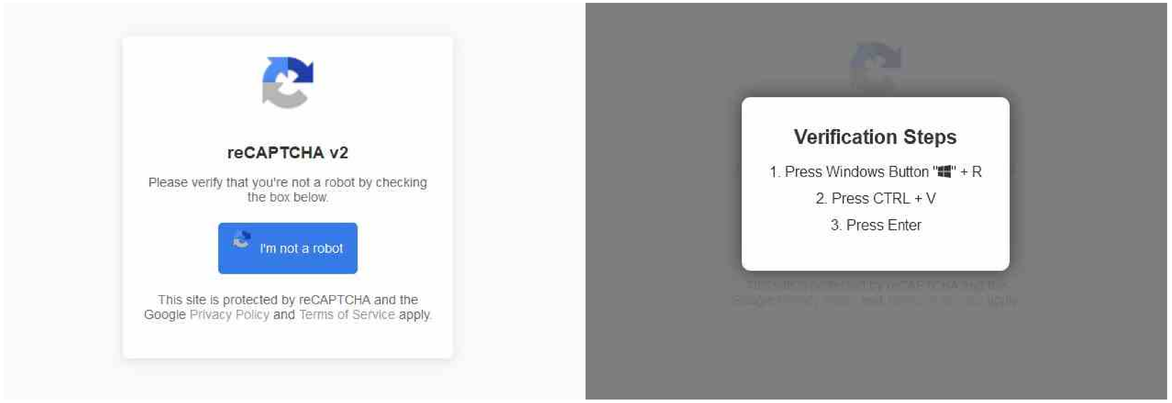
While virtually nonexistent a year ago, ESET's detection for ClickFix, HTML/FakeCaptcha, grew by 517% between H2 2024 and H1 2025. This makes it one of the fastest rising threats, accounting for nearly 8% of all blocked attacks and placing it second **in our top 10**.

It is important to note that the multiple stages of the attack, including the copied PowerShell commands or scripts, executables, malicious "envelopes", and final payloads, are covered by dozens of other detection names. Therefore, the real prevalence of this threat is probably even higher than the HTML/FakeCaptcha numbers. Countries reporting the highest volume of detections in ESET telemetry are Japan (23%), Peru (6%), and Poland, Spain and Slovakia (each over 5%).

ClickFix emerged in March 2024, in a campaign **documented** by Proofpoint, being used by ClearFake and TA571. This campaign used phishing emails delivering malicious HTML attachments that displayed a page imitating Microsoft Word or OneDrive. A pop-up shown on those pages falsely claims that an



HTML/FakeCaptcha detection trend in H2 2024 and H1 2025, seven-day moving average



Fake reCAPTCHA check instructing the victim to paste and execute a malicious command on their device

error needs to be resolved before the content can be accessed. The victim is then instructed to click a "Fix it" button – copying a PowerShell command to their clipboard – open a PowerShell terminal, and then paste it there to execute the command. Instead of resolving the made-up error, this starts a chain of downloading and executing other malicious scripts that ultimately lead to compromise by DarkGate or Matanbuchus malware offered as a service on the dark web.

By the end of 2024, attacks using the same social engineering technique flooded the web. Threat actors have been creating fake websites mimicking popular services – such as Booking.com or Google Meet – compromising legitimate websites with fake browser update prompts, fake Cloudflare verifications or reCAPTCHA checks, and distributing links leading to ClickFix pages via email campaigns. As reported in a recent **ESET APT Activity Report**, the North Korea-aligned DeceptiveDevelopment group also used this social engineering tactic by creating issues in popular GitHub repositories, proposing a "fix" that instead delivered the group's WeaselStore malware.

Prompted by the effectiveness of the ClickFix approach, threat actors have now **reportedly** started selling builders that provide other attackers with ClickFix-weaponized landing pages.

As the number of ClickFix variants has grown, so have a variety of threats being delivered using this technique. Currently the list includes popular infostealers such as **Lumma Stealer**, VidarStealer, StealC, and **Danabot**; remote access trojans such as VenomRAT, AsyncRAT, and NetSupport RAT; remote monitoring and management tools such as MeshAgent; post-exploitation frameworks such as Havoc and Cobalt Strike; and cryptominers, loaders, clipboard hijackers, and much more. In early 2025, attacks were spotted that attempted to deploy Interlock (formerly Rhysida) ransomware.

Nation-state-aligned threat actors also quickly jumped on the bandwagon, incorporating this social engineering technique into their toolsets for gaining initial access. North Korea-aligned Kimsuky, Lazarus, and DeceptiveDevelopment were the first, targeting Windows, Linux, and macOS users. Other actors soon followed, including Russia-aligned Callisto and Sednit, Iran-aligned MuddyWater, and Pakistan-aligned APT36.

While Windows users are the largest group affected, macOS and Linux users have also come into the crosshairs. For macOS, public reports reveal that ClickFix campaigns dropped AMOS stealer. For Linux, APT36 was seen redirecting victims to a counterfeit CAPTCHA page that instructed them to run the malicious code via the Alt+F2 shortcut that, on most Linux distributions, opens a Run Command dialog.

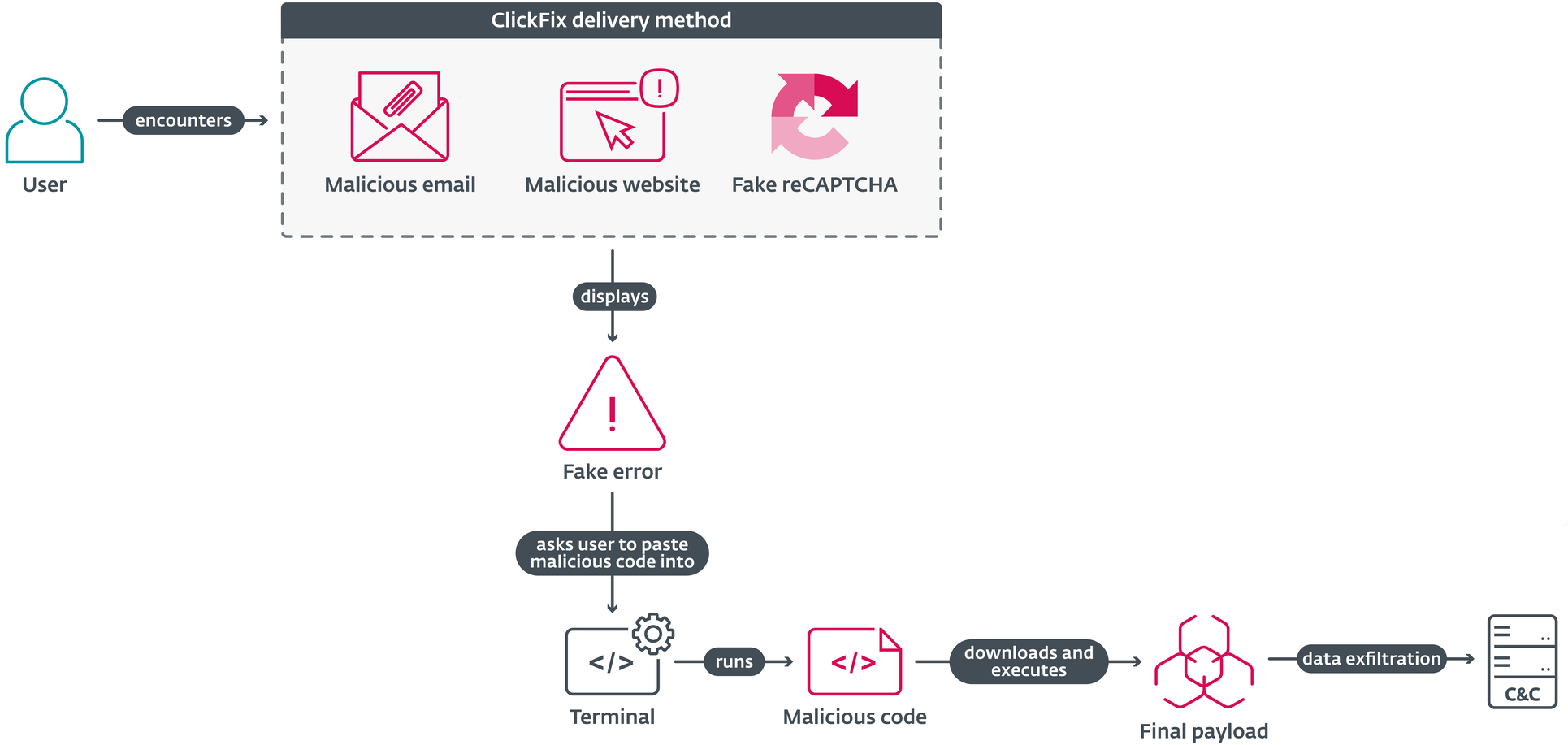
EXPERT COMMENT

Looking at ESET telemetry data, ClickFix has quickly become one of the most prominent cybercriminal intrusion vectors. What makes this new social engineering technique effective is that it is simple enough for the victim to follow the instructions, believable enough to look like it might fix a made-up problem, and abuses the probability that victims won't pay much attention to the exact commands they have been asked to paste and execute on their device. It is also a good example of how threat actors quickly adopt new techniques, once they prove to yield results. With its growing popularity, it is possible that Microsoft and Apple, but also the open-source community, will add some kind of security warning like the one used for macros in Word or Excel, or for files copied from the internet, notifying users that they are about to execute a potentially dangerous script.

Dušan Lacika, ESET Senior Detection Engineer

However, in that specific case, the compromise only led to fetching a hidden JPEG file from the attacker's server and opening it in the background without causing any damage or taking other malicious actions.

As mentioned before, ClickFix attacks can be intercepted by security solutions at several stages. These include the malicious and compromised website URLs, HTML email attachments, HTA files, JavaScript files, PowerShell scripts, and command line programs used to deliver the payloads. Reliable security solutions should also block "envelopes" used by the attackers to obfuscate or otherwise mask secondary payloads (detected by ESET as Win/Kryptik or Win/GenKryptik), recognize malicious activity in memory, and identify suspicious network behavior like data exfiltration. Users should also remain vigilant whenever anyone is offering "one-click" or "copy-and-paste" fixes to unknown issues. In corporate environments, endpoint detection and response (EDR) tools can flag anomalous PowerShell usage – especially on machines that rarely need it – and thus improve visibility into and protection against such attacks.



Simplified ClickFix attack flow

Infostealers Malware as a service

Double trouble befalls prominent infostealers

ESET participated in disruption operations aimed at to two notable infostealers: Lumma Stealer and Danabot.

The world is full of gloomy and disturbing news lately, so how about something positive for a change? Months of hard work on the part of law enforcement and cybersecurity companies, ESET included, paid off and resulted in not one, but two prominent infostealers disrupted by the authorities. Both Lumma Stealer, a malware-as-a-service (MaaS) behemoth, and Danabot, another MaaS operation of considerable malicious influence, had their infrastructure largely taken down in May 2025.

Here, we bring you an overview of the two disruptions, as well as some recent data from ESET telemetry regarding both infostealers. Our in-depth research and reporting on these recent events can be found in the respective **Lumma Stealer** and **Danabot** blogposts on WeLiveSecurity.

Lumma Stealer steals no more?

Just half a year after we published the article covering the unprecedented growth of Lumma Stealer in the H2 2024 **Threat Report**, a reckoning has arrived for this malware-as-a-service powerhouse. In May 2025, ESET, alongside Microsoft, BitSight, Lumen, Cloudflare, CleanDNS, and GMO Registry, took part in a coordinated global effort to disrupt Lumma Stealer. The operation targeted all known Lumma Stealer C&C servers from the past year, taking out a large part of the malware's exfiltration network. As part of the disruption effort, ESET supplied technical analysis and statistical information. Using our automated systems, we also extracted essential data, such as C&C servers and affiliate identifiers, from tens of thousands of malware samples.

Lumma Stealer detection trend in H1 2025, seven-day moving average

EXPERT COMMENT

We can certainly call the Lumma Stealer disruption a success. The malware suffered a considerable technical blow, taking it out of commission for some time after the operation occurred. While we now see that the threat actors have started rebuilding Lumma Stealer infrastructure using DNS servers located in Russia, the reputation of this cybercriminal endeavor has undoubtedly taken a hit. The ongoing success of Lumma Stealer is very much reliant on the trust of its affiliates. This means that even if Lumma Stealer were to succeed in the rebuilding effort, its user base might just straight up abandon it for another infostealer. In that case, the most likely path for the malware's operators would be to completely rebrand their service.

Jakub Tomanek, ESET Malware Analyst

Looking at our telemetry data, before the disruption, Lumma Stealer activity in H1 2025 was even higher than in H2 2024. We have registered a 21% increase in the malware's detections. During this period, there was also a considerable spike in the malware's numbers following a spam email campaign on April 11 mainly targeting Mexico, which saw more than 40% of Lumma Stealer attack attempts that day. While the takedown took place very close to the end of the reporting period, we are already seeing a drop off in Lumma Stealer detections.

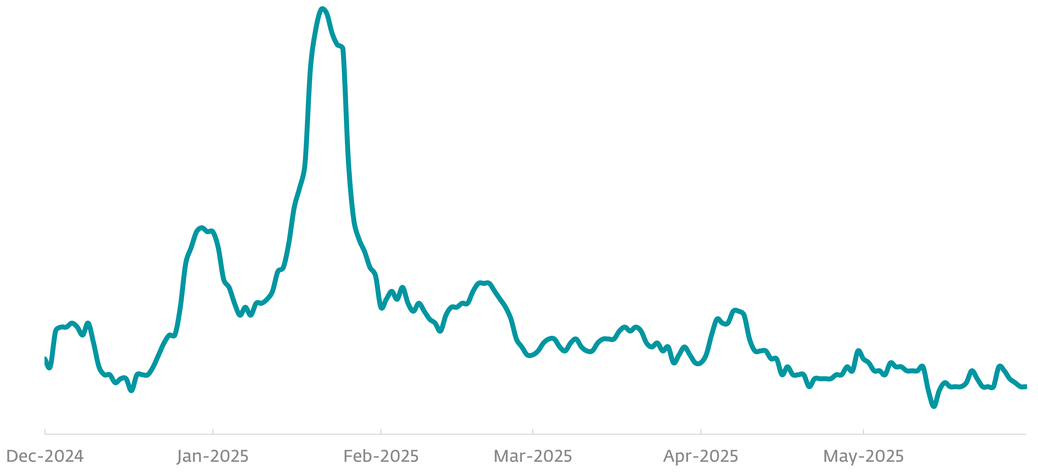
The in-depth research we conducted as part of the disruption effort reveals the degree of threat actor activity happening behind the scenes: between June 17, 2024 and May 1, 2025, we observed 3,353 new unique C&C domains, which means about 74 new domains per week. We also noticed regular code updates being pushed during this period. This shows that Lumma Stealer is a hugely prolific threat, making its disruption that much more important.

ESET telemetry also points towards Lumma Stealer being the primary payload of the HTML/FakeCaptcha trojan, used in ClickFix social engineering attacks described in **the previous section of this report**. However, even if this method might have mainly been used to distribute Lumma Stealer in the past, its use has already spread far and wide to other threats. Therefore, this takedown operation will most likely only have a temporary effect on FakeCaptcha and other varieties of ClickFix attacks.

Danabot brought to its knees

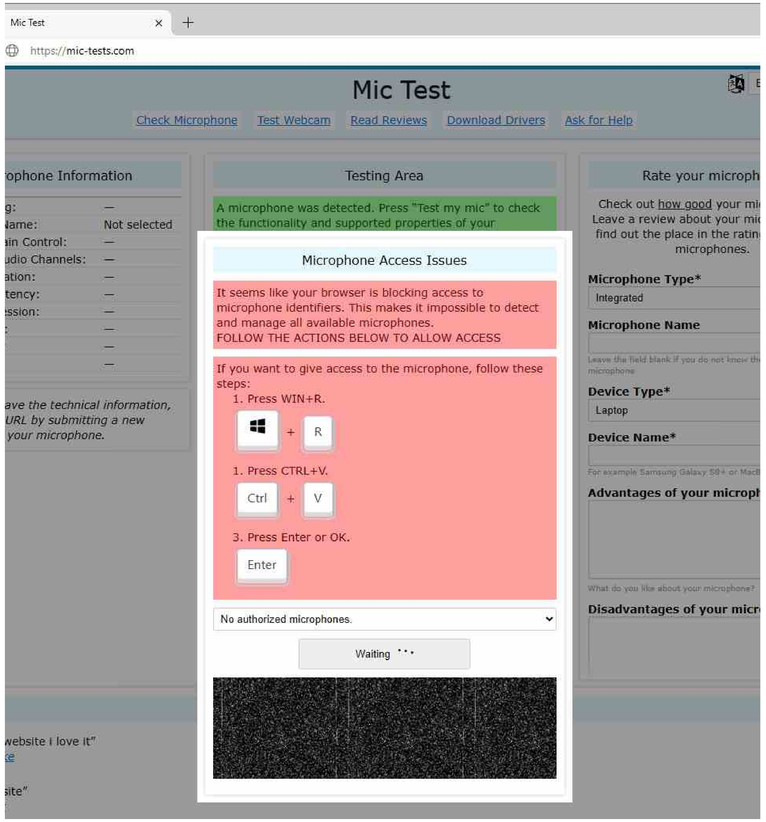
Just a couple of days after Lumma Stealer's disruption, the notorious infostealer Danabot also got its comeuppance, having been **targeted** by the FBI and US DoD's Defense Criminal Investigative Service (DCIS), in conjunction with **Operation Endgame** coordinated by **Europol and Eurojust**.

ESET took part in this undertaking alongside Amazon, CrowdStrike, Flashpoint, Google, Intel471, PayPal, Proofpoint, Team Cymru, Zscaler, and several law enforcement agencies across the globe. The takedown was a culmination of a years-long effort on the part of the involved parties – ESET's participation in this endeavor began as early as 2018. Our contribution included providing technical analyses of the infostealer and its backend infrastructure, as well as identifying its C&C servers. This coordinated operation resulted in the disruption of a large part of Danabot's infrastructure, impacting the malware significantly.



Danabot detection trend in H1 2025, seven-day moving average

Danabot is an infostealer written in Delphi that, same as Lumma Stealer, operates as malware as a service. It is available for rent on underground forums, putting a variety of tools at the malware affiliates' disposal, who can then establish and manage their own botnets.



Website luring the victim into executing malicious code copied into the clipboard

Cybercriminals have employed Danabot in quite a number of ways: apart from the typical data exfiltration capabilities, such as keylogging, screen recording, and file grabbing, the malware is also used to distribute further malware – even ransomware – to compromised systems. We have observed it pushing, among other payloads, LockBit, Buran, and Crisis. Additionally, machines compromised by the infostealer have been employed to launch DDoS attacks.

The malware itself is distributed using a variety of means. Apart from being spread through attachments in phishing emails, it is also delivered by other malware, as well as via malicious sponsored links in Google search results. As of late, this malware has also started to be distributed via the **ClickFix** method: the potential victim is presented with a fake technical issue, with the "solution" being running a command in a terminal window. The command contains malicious PowerShell code that ultimately downloads Danabot.

While, according to ESET telemetry data, Danabot is not as widespread as Lumma Stealer, it is still a MaaS operation of a considerable scale. Over the years of tracking this infostealer, ESET analyzed a large number of distinct samples, and identified more than 1,000 unique C&C servers. Before the disruption, the malware was on the rise, growing by more than 50% in H1 2025. Countries most affected by Danabot attack attempts during this period were the US (44%) and Poland (29%). Thankfully, as can be seen in the trend data on the previous page, Danabot detections have started to decline following the disruption.

Infostealers Malware as a service

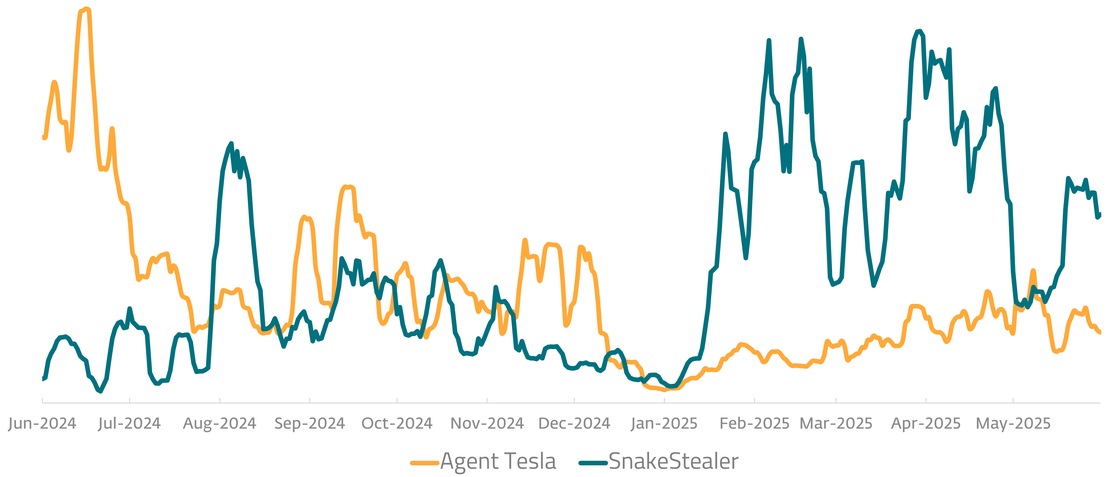
SnakeStealer slithers to the top

In the wake of Agent Tesla's creators abandoning their malware, SnakeStealer claims its place as the most-detected infostealer in ESET telemetry data.

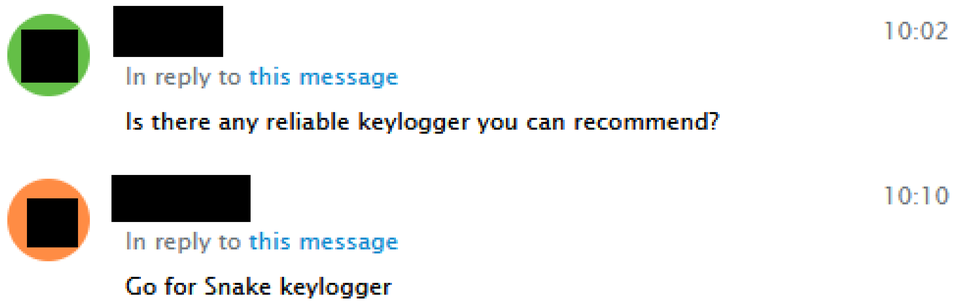
After several years of dominance in ESET's top infostealer statistics, it seems that the era of Agent Tesla has come to an end. It had already slipped into second place in H2 2024, when it was surpassed by Win/Formbook, and its downward trajectory has since continued. Now sitting in fourth place, the H1 2025 Agent Tesla detections have decreased by 57% compared to the previous period. Based on the claims of the threat actors responsible for this notorious malware-as-a-service (MaaS) operation, the reason behind the decline is quite prosaic: the operators have lost access to the servers with the infostealer's source code, and have therefore decided to stop its development indefinitely. This is why the drop in the malware's numbers has been gradual rather than dramatic – it is not completely gone; new versions are just not being developed.

While Agent Tesla is slowly waning, it has already been replaced by a new rising star: another MaaS threat, named SnakeStealer and tracked by us mainly as MSIL/Spy.Agent.AES trojan, is now the number one infostealer according to ESET telemetry data. SnakeStealer has actually been recommended as a suitable replacement for Agent Tesla in the latter's own Telegram channel. It seems that the recommendations were key to the malware's success, as the first surge of SnakeStealer detections from the end of July 2024 roughly coincides with the time that Agent Tesla's development was discontinued.

SnakeStealer, also known as Snake Keylogger or 404 Keylogger, is .NET malware that first appeared in 2019. Sold via a Telegram group, this infostealer is capable of logging keystrokes, stealing saved credentials, capturing screenshots, and collecting clipboard data.



SnakeStealer and Agent Tesla detection trends in H2 2024 and H1 2025, seven-day moving average



Member of the Agent Tesla Telegram channel recommending SnakeStealer

EXPERT COMMENT

While it is certainly possible that SnakeStealer will replace Agent Tesla as the dominant infostealer, we have to keep in mind that the competition is fierce and there are various other prevalent infostealers offered on the market. One such example is the Pure Logs infostealer, which has also been rising in prominence since Agent Tesla stopped updating. On the other hand, we cannot discount the power of word of mouth, since we have noticed multiple individuals on the dark web recommending SnakeStealer as an alternative to Agent Tesla. By itself, however, there is not much else that makes SnakeStealer stand out in the sea of its competitors.

Jakub Kaloč, ESET Malware Analyst

The data is then exfiltrated via FTP, SMTP, or Telegram bots. The malware is distributed mainly as malicious attachments in phishing emails. SnakeStealer's operators also offer a VIP version of the malware that contains additional features for a higher fee. As these two versions are quite similar to each other from a technical point of view, our MSIL/Spy.Agent.AES detection covers both of them.

Looking at ESET telemetry data, we see that SnakeStealer accounted for almost a fifth of all infostealer detections we registered in H1 2025. After an end-of-year holiday lull, there has been a steady influx of detections of this malware from mid-January onwards. The infostealer's numbers more than doubled between H2 2024 and H1 2025. We saw the highest rate of SnakeStealer activity in the spring after it launched three successive email campaigns, with detection spikes occurring close to each other on March 25, April 3, and April 9. Each of those dates, the malware hit more than 6,000 detections per day. The countries that have seen the highest numbers of attempted SnakeStealer attacks are Türkiye (15%), Japan (13%), and Spain (11%).

Our tracking also managed to catch several SnakeStealer campaigns targeting Central and Eastern Europe. Among the monitored countries, Poland and Latvia saw the highest number of attack attempts: counting only the high-effort attempts that were either targeted or took considerable measures to appear credible, we saw almost 5,000 of them in Latvia, and more than 18,000 in Poland from January to April 2025.

In these campaigns, SnakeStealer was usually packed with either Cassandra Protector or Pure Crypter, which we detect as MSIL/Kryptik trojan and MSIL/TrojanDownloader.Agent trojan. A typical example of such a case is the victim receiving an email with an ISO file attachment, where the attachment contains a Pure Crypter executable, which then downloads, decrypts, and launches SnakeStealer.

Dzień dobry.

Proszę o potwierdzenie realizacji załączonego zamówienia.

--

Pozdrawiam

[redacted]

One of the phishing emails with an attachment delivering SnakeStealer (machine translation: Good day. Please confirm the fulfillment of the attached order. Best regards)

Android Adware

Kaleidoscope and its evil twin scheme flood Android with ads

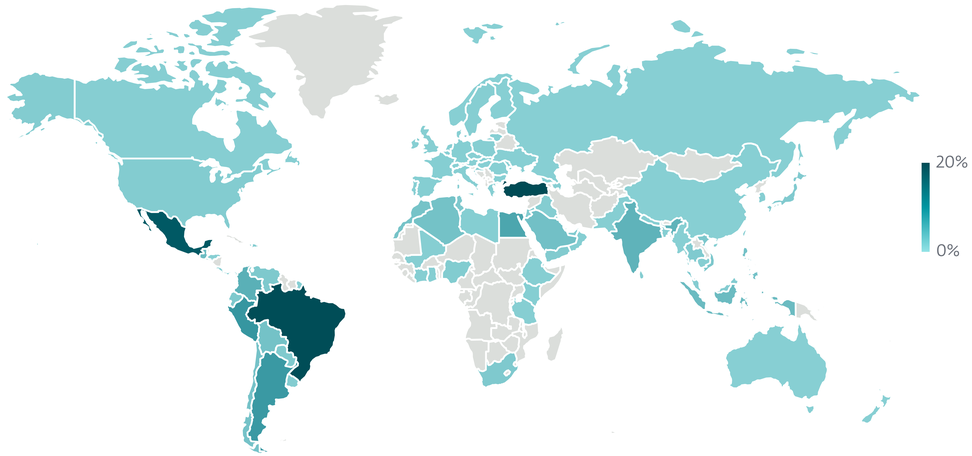
Android adware detections jump by 160%, fueled by new evil twin fraud and the rise of potentially unwanted apps.

A sophisticated new Android threat dubbed Kaleidoscope is flooding devices with intrusive ads through a deceptive evil twin app scheme. While its name seems colorfully harmless, Kaleidoscope is actually a ploy designed to deceive advertisers and app stores.

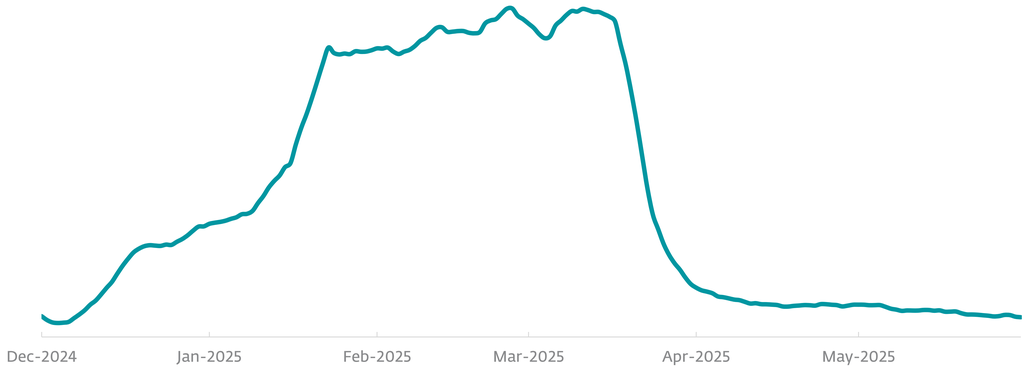
Kaleidoscope is an Android-based ad fraud operation uncovered by **IAS Threat Lab**. Cybercriminals behind this operation create two nearly identical versions of the same app – a harmless one available on official app stores (decoy twin) and a malicious version distributed through third-party app stores (evil twin). The evil twin generates intrusive, unwanted ads to fraudulently earn advertising revenue.

ESET detects this threat as the .MPP variant of Android/TrojanDropper.Agent; it accounts for 28% of detections across the whole Android adware category. Kaleidoscope impacts a large number of Android users worldwide each month: according to ESET telemetry, most victims are in Latin America, Türkiye, Egypt, and India, where third-party app stores are popular. Users in these regions unintentionally install evil twin apps, resulting in intrusive ads and degraded device performance.

The evil twin method used by Kaleidoscope is a clever deception tactic that pursues the steps described in the next four sections.



Geographic distribution of Kaleidoscope in H1 2025



Kaleidoscope detection trend in H1 2025, seven-day moving average

Creating a decoy twin app

First, attackers upload a legitimate app (the decoy twin) to official app stores. This app is genuinely harmless; it might be a simple puzzle game or a utility app. Because it's on the official store, users trust it.

Creating the evil twin

Next, the attackers create another version of the same app – but this version is malicious (the evil twin). This malicious app uses the same app name and unique identifier, called an app ID, but contains additional code that generates fraudulent ad impressions. These fraudulent ads appear unexpectedly and intrusively, even when the user isn't actively using the app.

Distributing the evil twin

Since official app stores actively block known malicious apps, attackers distribute the evil twin through third-party app stores or websites. Often, they use deceptive ads and offers to trick users into believing it to be the legitimate one found on official app stores, leading them to download the evil twin version.

Connecting the evil twin to the decoy twin

The key to Kaleidoscope's success lies in how the evil twin "pretends" to be the legitimate decoy app. Both twins share the same unique app ID, which advertisers and automated systems use to identify apps. As a result, fraudulent traffic generated by the evil twin appears to originate from the harmless and legitimate version. In reality, the intrusive ads are real – but unauthorized – and are generated by the evil twin, tricking advertisers into paying fraudsters for illegitimate ad views.

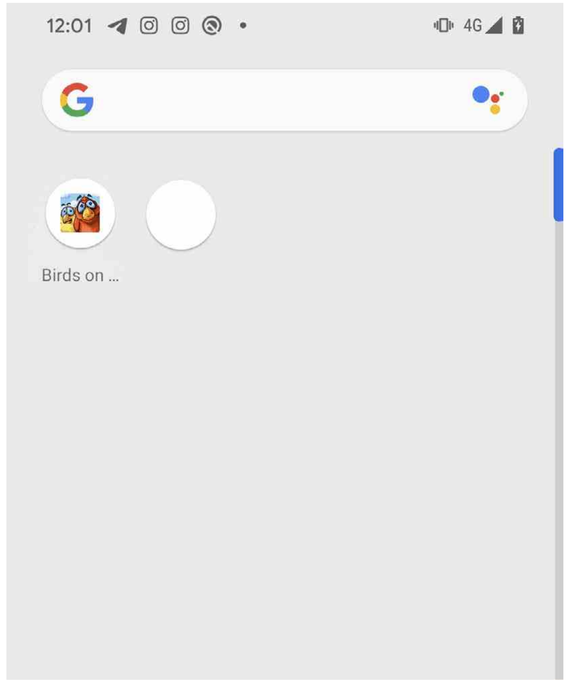
Simply put, the evil twin app steals the legitimate app's identity, allowing fraudsters to profit from ads that appear genuine yet are deceptively intrusive.

Interestingly, when compared, the icons of some evil twin apps are very different from their decoy twins' icons – for example, a white circle without a name, while the decoy twins have a more standard app icon.

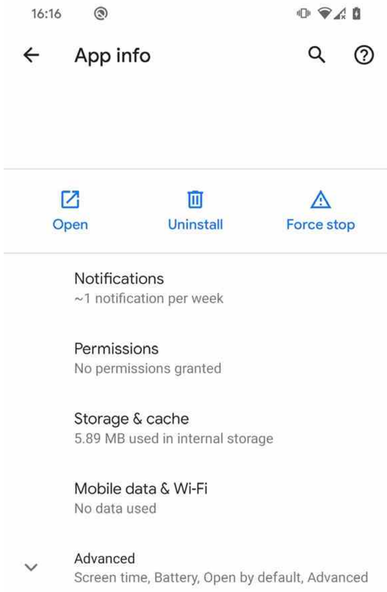
When opened, these apps also function differently. For instance, tapping the decoy twin app icon launches the Birds on a Wire game. In contrast, tapping the white evil twin icon only brings up the App Info screen without the user interface. Both apps are shown in the images to the right.

Kaleidoscope isn't entirely new. It evolved from a similar fraud discovered earlier, named **Konfety**, which abused an advertising framework called CaramelAds. After Konfety was exposed, attackers changed their strategy. They removed references to CaramelAds and created new, rebranded software tools (SDKs) with different names. These new SDKs allowed Kaleidoscope to continue undetected, highlighting its ability to constantly adapt.

Users can effectively protect themselves by understanding how this evil twin deception works, sticking to official app sources, paying attention to unusual app behavior, and carefully managing app permissions.



Birds on a wire is the app icon of the decoy twin while the white circle is the app icon of the evil twin



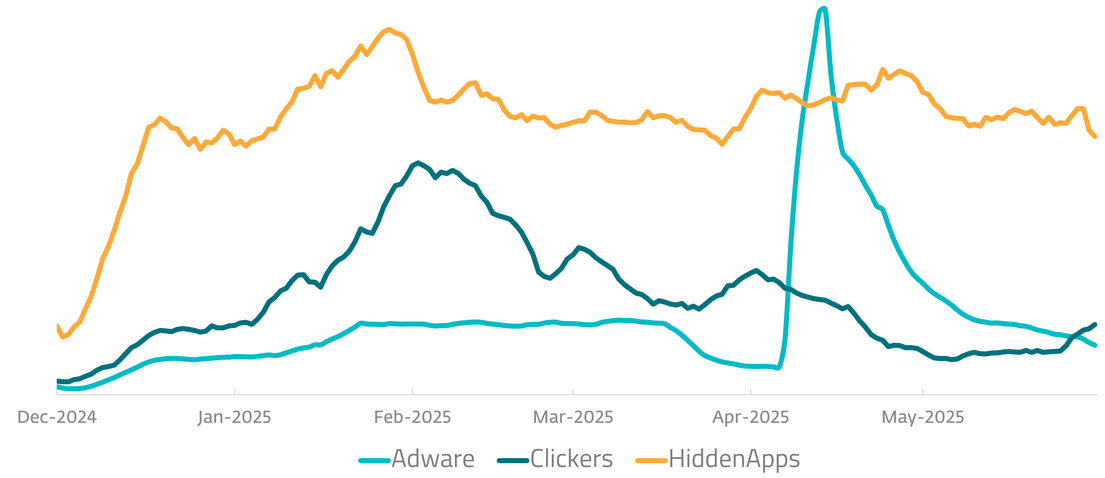
Tapping the decoy twin app icon launches the Birds on a Wire game (top); tapping the white evil twin icon only brings up the App Info screen (bottom)

Ad-fueled threats still cashing in on mobile users

In H1 2025, ESET observed a significant rise in two types of Android detections that profit from advertisements: Adware and Clickers. Combined, these categories surged by 160%, far outpacing the 50% increase seen across all types of Android detections. Adware shows unsolicited ads on users' devices, while Clickers generate fraudulent ad revenue by automatically clicking on ads without the user's knowledge. A third category, HiddenApps, hides itself after installation and can perform various malicious actions – such as displaying intrusive ads – but saw a 60% decrease in detections during this period. Altogether, Adware, Clickers, and HiddenApps accounted for 48% of all Android detections in H1 2025.

Some apps exhibiting such behavior are classified by ESET as potentially unwanted applications (PUAs). While they may not meet the criteria for malicious software, PUAs can still exhibit intrusive or misleading behavior, such as displaying excessive ads, device slowdowns, battery drain, and unauthorized data collection, negatively affecting user experience and potentially exposing users to privacy or security risks.

ESET Mobile Security allows users to choose whether to block or allow PUAs, offering flexibility for those willing to tolerate certain intrusive behaviors to use an app's primary functions. However, we strongly recommend enabling PUA detection to protect your device, privacy, and security.



Android Adware, Clicker, and HiddenApp detection trends in H2 2024 and H1 2025, seven-day moving average

Android NFC Scams

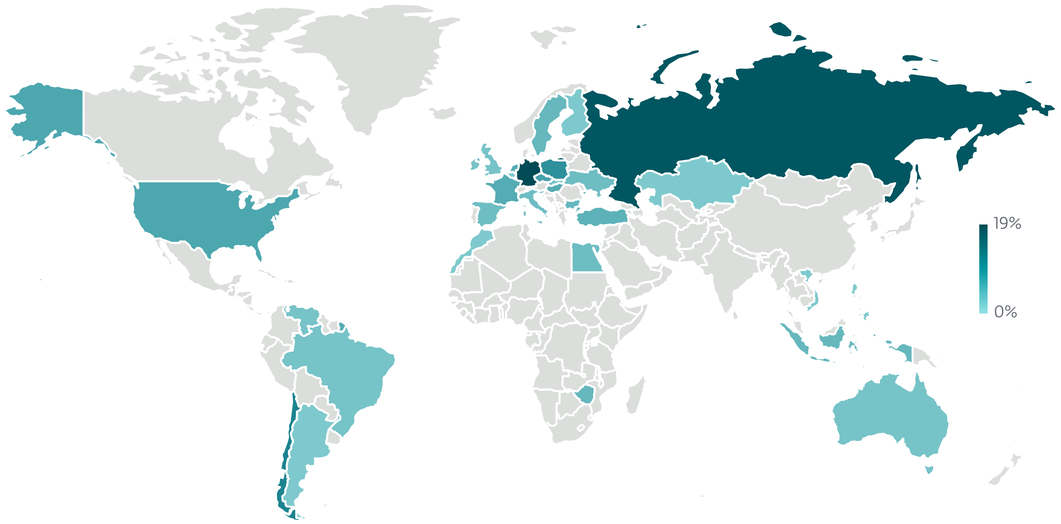
The evolution of NFC fraud: From NGate to GhostTap to relay scams

NFC-based fraud soared more than thirty-five-fold, fueled by phishing campaigns and inventive relay techniques.

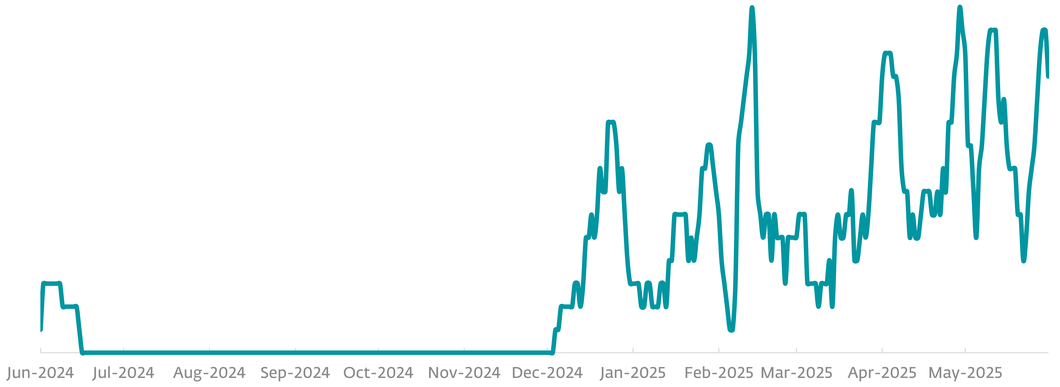
Near-Field Communication (NFC) technology has transformed how millions of people make payments and use banking apps. By simply hovering a phone or tapping a contactless card, in-store purchases and even ATM withdrawals can be completed within seconds. NFC technology enables two devices, such as a smartphone and a payment terminal, to communicate when placed close together. Mobile payment apps like Google Pay and Apple Pay rely on NFC to let users pay easily by tapping their phone or smartwatch at a checkout terminal.

When used legitimately, NFC allows for faster, more secure payments compared to older methods like magnetic stripes. Unfortunately, cybercriminals have also set their sights on NFC, creating a wave of highly specialized malware and new fraud schemes that exploit this technology.

According to ESET telemetry, NFC-related scams surged more than thirty-five-fold in H1 2025 compared to H2 2024. In the previous reporting period, covered in the ESET Threat Report H2 2024, we typically saw



Geographic distribution of NFC-related Android malware and scams in H1 2025



NFC-related Android malware detection trend in H2 2024 and H1 2025, seven-day moving average

only about one detection each week, and the scams affected only a limited group of cardholders in a few regions. By H1 2025, however, detections had grown to dozens per week. While the overall numbers remain modest, this jump highlights the rapid evolution of the criminals' methods and their continued focus on exploiting NFC technology.

NGate: An NFC malware pioneer

In 2024, ESET researchers **described** a novel mobile threat, which we named NGate. Once installed on a victim's device, it relays NFC signals from the victim's payment card through the compromised phone to attacker-controlled devices, enabling criminals to withdraw cash from ATMs remotely. This represented one of the first documented cases of mobile malware using NFC data relay functionality to steal directly from victims' bank accounts.

At that time, NGate was targeting clients of specific banks in Czechia, Poland, Hungary, and Georgia. NGate abuses an open-source tool called NFCGate, initially intended for academic use. NFCGate allows users to capture, analyze, and modify NFC data between devices, but cybercriminals quickly recognized its malicious potential.

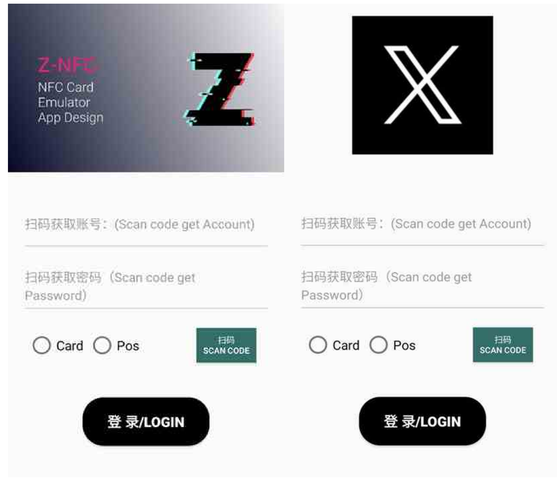
ESET telemetry has since also detected NGate in Russia, Germany, and Chile.

Malicious app, detected by ESET as **Android/NGate**, pretending to be the app of the Central Bank of Russia

GhostTap: Relay scams targeting digital wallets

Unfortunately, threat actors were inspired by the success of NGate and evolved this method further. One novel technique, dubbed **GhostTap**, involves cybercriminals secretly using stolen card data stored in digital wallets like Google Pay and Apple Pay. Criminals deploy, for instance, convincing phishing messages that prompt victims to enter their payment card details on fake websites, then trick them into sharing the one-time passcode meant to confirm transferring a card into a digital wallet. With the card data and code, the attackers register the stolen credentials in their own Apple or Google wallets. Then they relay these loaded wallets for fraudulent contactless payments anywhere in the world.

GhostTap attackers create fraudulent transactions by tapping compromised mobile devices against NFC-enabled payment terminals. These transactions appear legitimate, bypassing traditional security checks, and allowing criminals to cash out quickly. GhostTap shows how NFC fraud could scale massively, with criminals organizing farms of Android phones loaded with compromised card data, automating fraudulent transactions against banks and merchants worldwide, which have already suffered losses due to GhostTap-related fraud campaigns.



GhostTap tools

Several Chinese-speaking cybercriminal groups actively promote **GhostTap tools** on Telegram and dark-web markets. Criminals now operate NFC fraud farms that automate transactions, targeting financial institutions in the US, UK, Australia, Canada, UAE, and Saudi Arabia.

SuperCard X: Malware with a business model

This year, researchers at **Cleafy** reported on a new threat called SuperCard X, which exhibits significant code overlap with NGate. SuperCard X is delivered via sophisticated social engineering attacks. Victims

SuperCard X captures NFC data when victims tap their payment cards against their compromised phones

receive convincing SMS messages, impersonating bank security alerts, prompting them to call attackers posing as bank representatives. During these calls, criminals gain victims' trust, instructing them to install a malicious app disguised as a security tool.

Once installed, SuperCard X quietly captures NFC data when victims tap their payment cards against their compromised phones, relaying this data instantly to another attacker-controlled device. Criminals then use this relayed data to make fraudulent contactless payments at stores or withdraw cash from ATMs.

Unlike previous NFC attacks, it leverages a malware-as-a-service (MaaS) business model. This means that cybercriminals without deep technical skills can easily access and deploy NFC fraud tools. SuperCard X offers criminals two distinct Android applications: the Reader app installed on victims' devices and the Tapper app, controlled by attackers. These two apps communicate via a secure command and control server, allowing the seamless, real-time relay of NFC data from victim to attacker.

One critical innovation of SuperCard X is its minimalistic design, requesting only basic NFC permissions. Unlike traditional mobile banking malware, SuperCard X can remain undetected because it appears as a harmless NFC app without extensive permission demands. Additionally, SuperCard X employs a sophisticated encryption method that makes it harder for researchers and security tools to analyze and detect malicious traffic. These advanced tactics give SuperCard X a significant advantage over older threats.

EXPERT COMMENT

Each iteration of NFC fraud demonstrates how attackers adapt to new security measures. Even advanced solutions – like multifactor authentication or real-time transaction monitoring – face challenges when criminals physically relay the card data in seconds. Meanwhile, organized smishing campaigns, combined with highly polished malware interfaces, make it even harder for typical users to spot fraud.

We expect these criminal techniques to evolve further. Some groups already combine NFC theft with other capabilities, such as smishing or call-center scams, to keep tricking victims. Nonetheless, vigilant financial institutions, device manufacturers, and the cybersecurity community are monitoring and reacting to these threats. Aware and informed cardholders can also block a large portion of attacks by downloading apps only from official app stores, screening app permissions, ignoring suspicious links, and never tapping their physical card unless they are absolutely certain of its legitimate use.

Lukáš Štefanko, ESET Senior Malware Researcher

Ransomware

Get your popcorn: It's time for ransomware deathmatch

While the number of ransomware attacks and gangs has been growing, ransomware groups are increasingly fighting each other, impacting several players including the top ransomware as a service – RansomHub.

In H1 2025, summarized 2024 data of the **ecrime.ch** service showed ransomware attacks growing by 15% and the number of ransomware gangs increasing by 43% compared to the previous year. Surprisingly, according to **Chainalysis**, the total value of payments went in the opposite direction, dropping by a stunning 35%. This discrepancy can be attributed to takedowns and exit scams that reshuffled the whole ransomware scene in 2024, but also partially to uncertainty and diminished confidence in the gangs' longevity and ability to keep their side of the bargain.

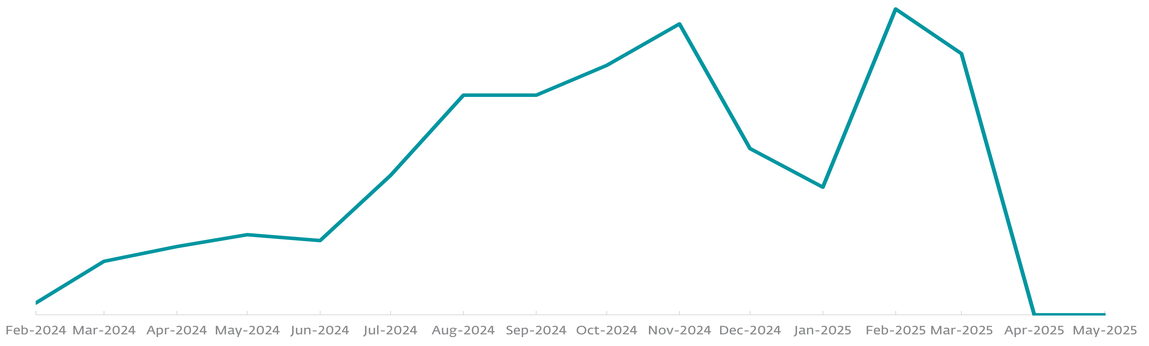
Let the fights begin!

Looking at H1 2025 developments, that assessment holds firm. The recently established "new order", where RansomHub amassed a large pool of affiliates and dominated the arena, was once again disrupted. However, this time it was due to infighting and defacements that ransomware operators inflicted on each other.

The most visible clashes are attributed to the DragonForce gang – a very vocal and brazen threat actor with dozens of victims on its data leak site (DLS). Despite only being a minor player with little trust among affiliates, it was this group that went on a defacement spree in March, taking down the dark web sites of BlackLock, Mamona, and of the number one RaaS at that time – RansomHub.

DragonForce even went so far as to claim that RansomHub had voluntarily joined its cartel, but without proof. This was also contradicted in a heated public exchange on the notorious RAMP forum. Importantly,

Defaced RansomHub data leak site



RansomHub remained inactive after the attack and defacement by DragonForce

note that RansomHub's service, DLS, and operations have not recovered since the attack. This leaves affiliates of the leader – often former coconspirators of the disrupted LockBit – without a central operator again.

Ransomware leaks left and right

A few days after the RansomHub defacement, the DLS of Everest ransomware was targeted too, although by a different threat actor, who left a sarcastic message "Don't do crime CRIME IS BAD xoxo from Prague". Then, the same wording replaced content on LockBit's recently restarted DLS, adding a link to a dump of the gang's information. The leaked database included names and plaintext passwords of dozens of admins and affiliates using the RaaS service, almost 60,000 unique bitcoin addresses, builds and configurations used by the affiliates, and over 4,400 messages documenting negotiations between the criminals and their victims.

Defaced LockBit data leak site

Another leaker – possibly a disgruntled gang member or a researcher who breached the group's systems – also **dumped** weeks' worth of internal messages of the Black Basta ransomware operation. Leaked data contained insights into the gang's phishing templates, cryptocurrency addresses, data drops, and victims' credentials.

Towards the end of H1 2025, a new account on X.com, **@GangExposed**, revived the 2022 ContiLeaks and 2023 TrickLeaks and used the material to dox

Sinbad[.]io cryptomixer domain seized by the law enforcement

leaders and members of the notorious cybercriminal gang. This includes the alleged masterminds known by the nicknames Stern, Tramp and Target, with ties to other malware operations online such as TrickBot, Black Basta, and Royal ransomware. The identity of at least one of the mentioned perpetrators has been **confirmed** by German law enforcement.

Apart from the "deathmatch" in the ransomware arena, operators and affiliates also faced active pursuit by law enforcement. In H1 2025, suspects linked to several gangs such as **DoppelPaymer**, **Nefilim**, **LockBit**, and **Phobos/8Base** have been either arrested, extradited to the US, or indicted. Authorities also went after the supporting infrastructure, charging operators of **cryptomixers** Blender.io and Sinbad.io for helping launder ransomware proceedings, and **sanctioning** and **dismantling** the ZServers/XHost bulletproof hosting provider. A Romanian affiliate of **Netwalker** ransomware was handed a 20 year sentence.

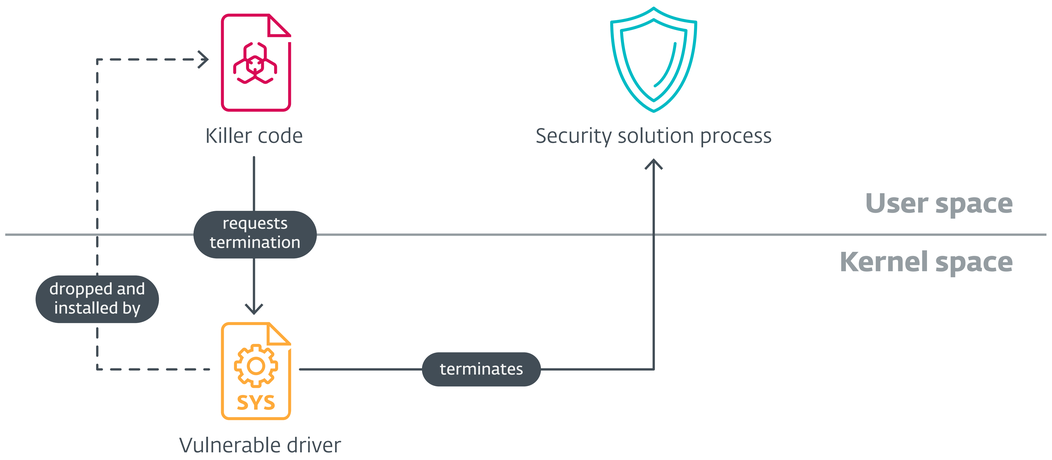
In another bit of positive news, security researcher Yohanes Nugroho developed a new nonconventional **Akira decryptor**. It exploits specifics of this ransomware strain and uses high-powered GPUs to brute-force the decryption keys. The catch is in its deployment, which might be a bit complicated for less technically savvy victims.

Expanding toolkits: EDR killers and abuse of RMM tools

Ransomware gangs often boast that they can circumvent any security measures of their victims. And yet, endpoint detection and response (EDR) solutions seem to be thorns in their sides. Thorns so big, in fact, that several ransomware operators developed new tools – so called EDR killers – designed to terminate, blind, or crash the security product installed on a victim's system.

Less mature actors have attempted to achieve this goal by using simple scripts or by abusing legitimate tools such as the GMER rootkit detector or PC Hunter. More advanced ransomware operators, however, build their EDR killers around the bring your own vulnerable driver (BYOVD) technique. These tools typically consist of two parts: a user mode "killer code" component orchestrating the attack, and a legitimate, vulnerable, signed driver that is dropped and exploited by the killer component to terminate security-related processes from kernel mode.

In H1 2025, ESET researchers put one such EDR killer – **EDRKillShifter** – under the microscope. It was created and maintained by the number one RaaS at that time: RansomHub. While EDRKillShifter's functions do not deviate from other EDR-killing malware, there is a notable distinction in the code's protection. The shellcode, serving as the middle layer of the execution



Sophisticated EDR killers use BYOVD, dropping and installing a known vulnerable kernel driver that they can exploit to terminate security-related processes

chain, is protected by a 64-character password. Without that password, security researchers cannot access the list of targeted processes or the misused driver. Even so, taking advantage of EDRKillShifter's distinctive nature, ESET researchers were able to identify links between RansomHub's affiliates and the rival gangs that some of those affiliates also work for – namely Play, Medusa, and BianLian.

But EDRKillShifter is not the only tool on the market targeting EDR solutions. After its popularity grew, we observed an increase in the number and variety of these killers used by ransomware affiliates. Apart from RansomHub's EDRKillShifter, other well-known EDR killers include MS4Killer from Embargo, BadRentdrv2, and TFSysMon-Killer – the latter two being publicly available on GitHub.

Another continuing trend among ransomware groups being observed by ESET researchers is the abuse of legitimate remote monitoring and management (RMM) tools, which companies typically use to remotely manage endpoints and prevent insider threats and data leaks. Some of the frequently abused tools include Anydesk, MeshAgent, and SimpleHelp. Apart from the case where such tools are legitimately deployed by the organization, installation of these tools in the environment should serve as a red flag and trigger an immediate response to mitigate their possible misuse by an adversary.

Interlock ransomware adopting ClickFix

Ransomware gangs are trying to keep up with the latest developments; therefore it comes as no surprise that ClickFix – a rising social engineering technique – caught their attention. As described in an earlier section of this report, these attacks display a fake error that manipulates victims into copying, pasting, and executing malicious commands on their devices.

Used originally by initial access brokers, ClickFix has probably contributed to ransomware attacks before but it took until H1 2025 for a ransomware actor to use it directly in a **campaign**. Interlock ransomware leveraged ClickFix to impersonate IT tools such as MS Teams and Advanced IP Scanner, with malicious commands downloading fake installers and opening legitimate sites in the foreground, while dropping secondary payloads or creating PowerShell backdoors in the background.

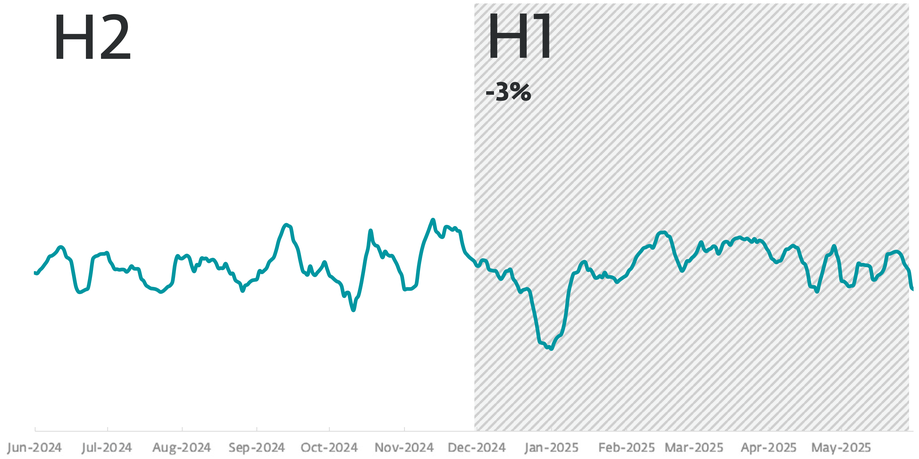
EXPERT COMMENT

While Q1 2025 displayed a massive growth in the number of reported attacks, the sudden cessation of RansomHub's operation put a hard stop to that. When RansomHub emerged in 2024 and swayed LockBit's and BlackCat's affiliates, its timing and attractive conditions set it up for quick growth. Now, in contrast, the ransomware landscape is in chaos; this disruption was caused by rivals, not law enforcement. We expect that, over time, a new dominant player will arise, but also that the current infighting won't stop any time soon. DragonForce may have grabbed the spotlight, but what it definitely didn't earn is trust. Its false claims of RansomHub voluntarily joining its "cartel" only increase its untrustworthiness.

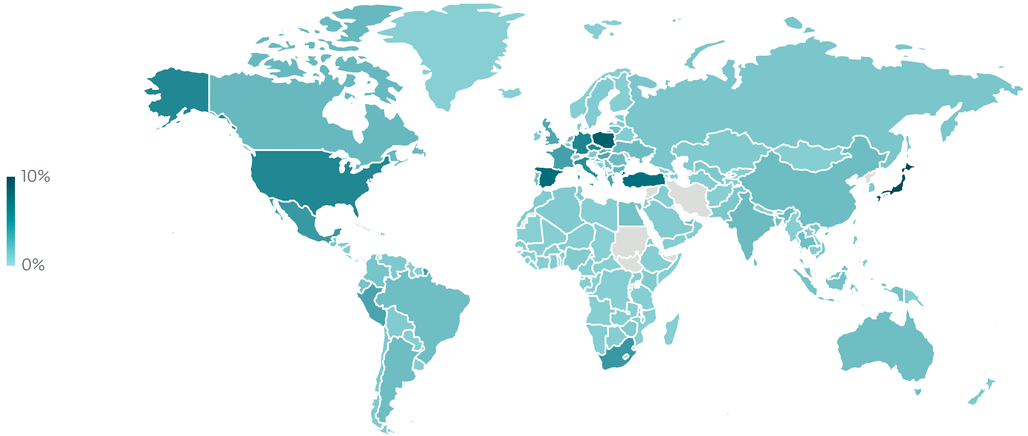
Jakub Souček, ESET Senior Malware Researcher

Threat telemetry

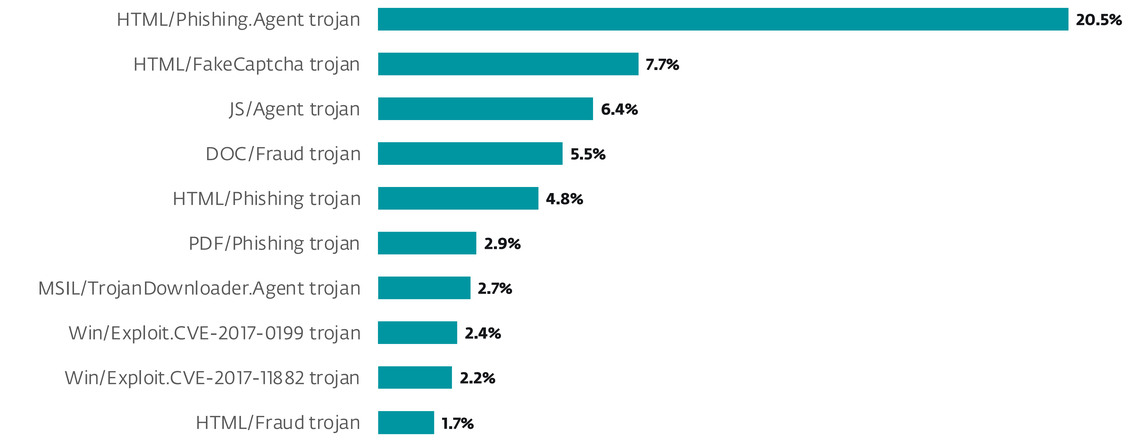
All threats



Overall threat detection trend in H2 2024 and H1 2025, seven-day moving average

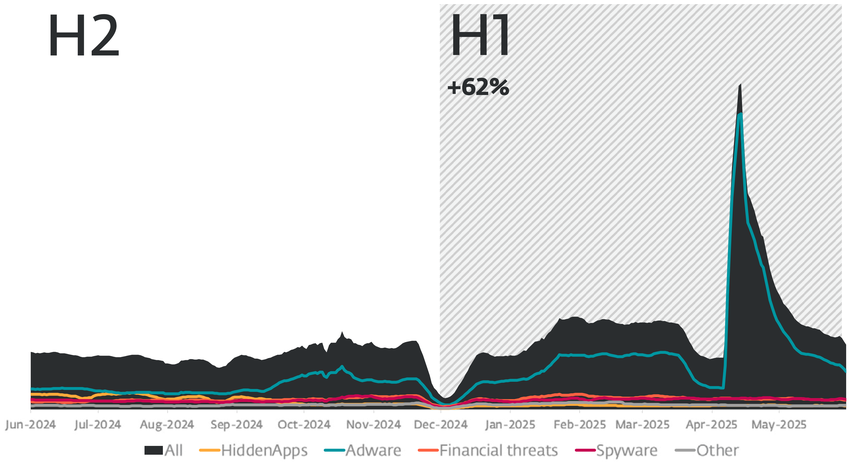


Geographic distribution of malware detections in H1 2025

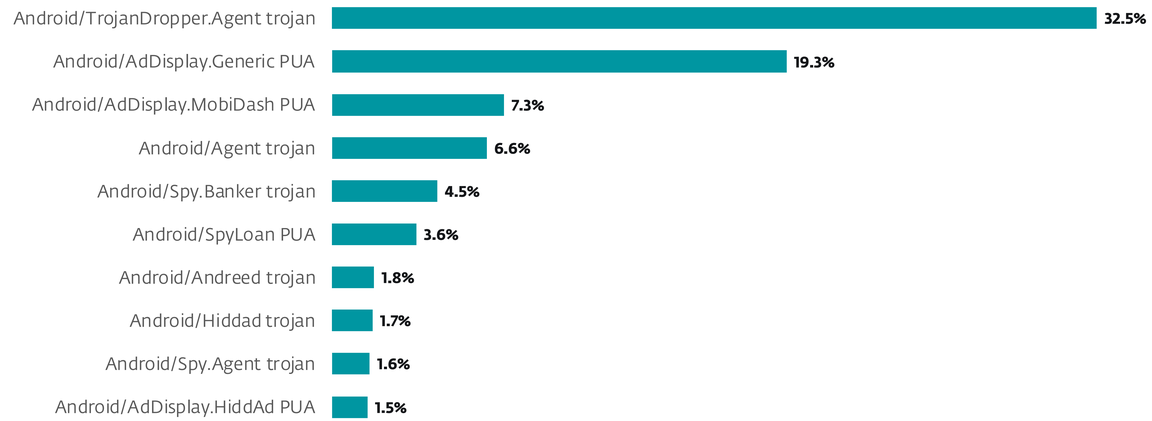


Top 10 malware detections in H1 2025 (% of malware detections)

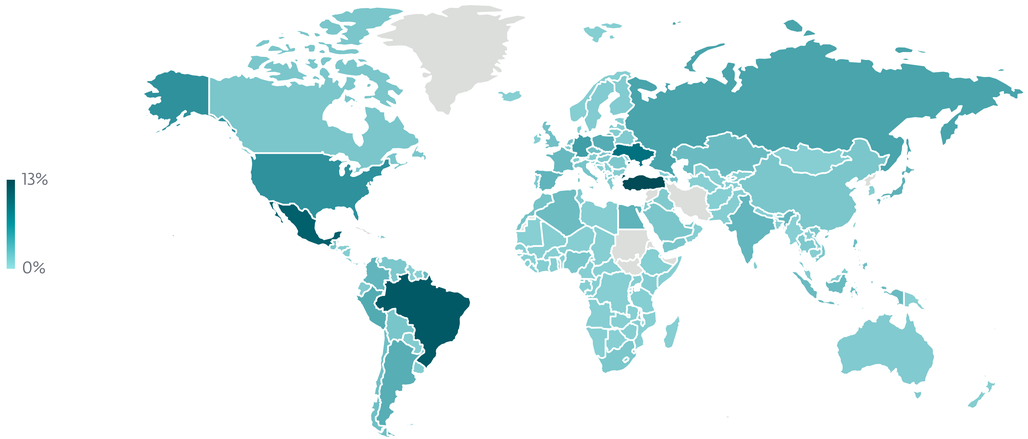
Android



Detection trends of selected Android detection categories in H2 2024 and H1 2025, seven-day moving average (Clickers, Cryptominers, Ransomware, Scam apps, SMS trojans, and Stalkerware are combined in the trendline Other)[1]



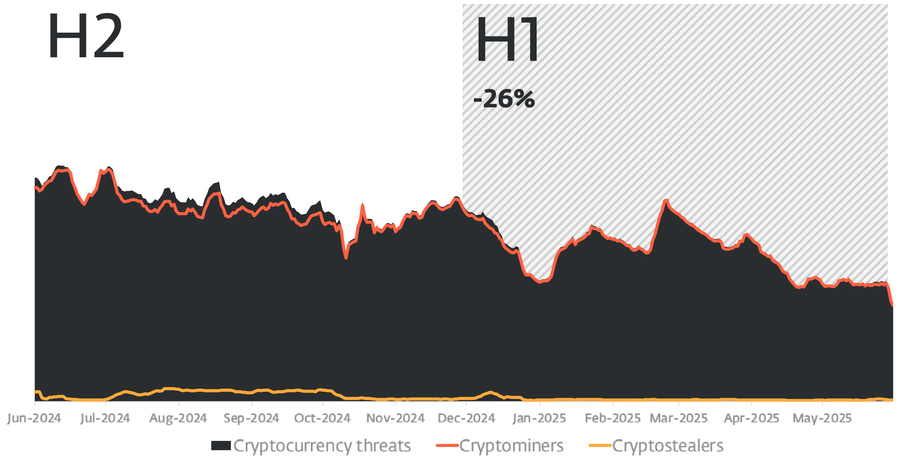
Top 10 Android detections in H1 2025 (% of Android detections)



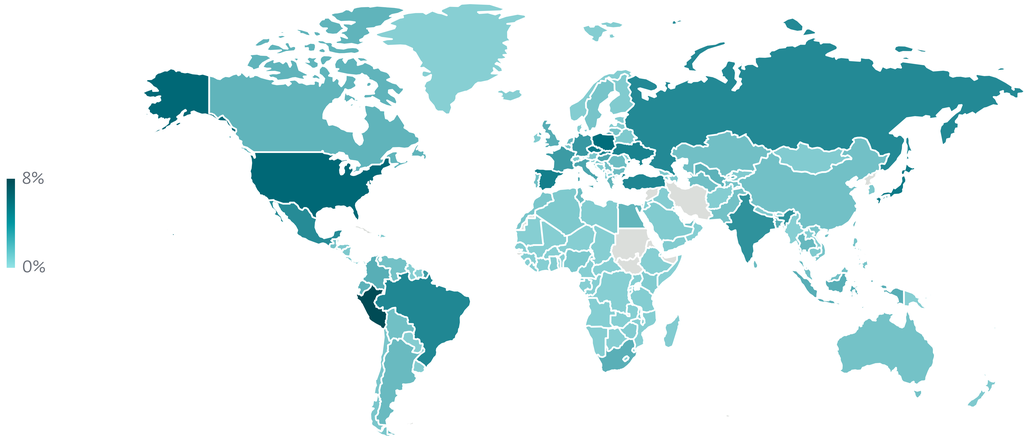
Geographic distribution of Android detections in H1 2025

[1] The dip in detection numbers in December 2024 was caused by a miscommunication within one of the modules included in our mobile cybersecurity products. Despite this issue, the security and protection of Android devices remained fully effective and uncompromised during this period.

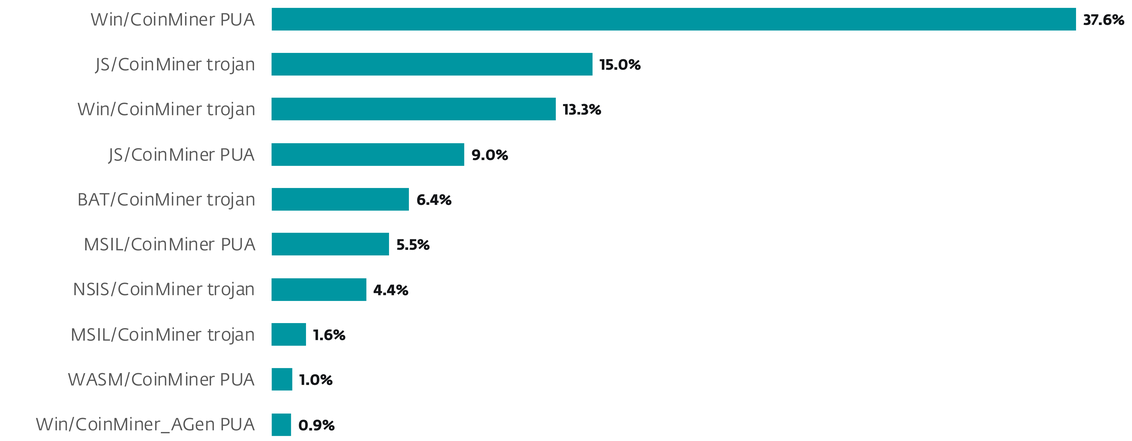
Cryptocurrency threats



Cryptocurrency threat detection trend in H2 2024 and H1 2025, seven-day moving average

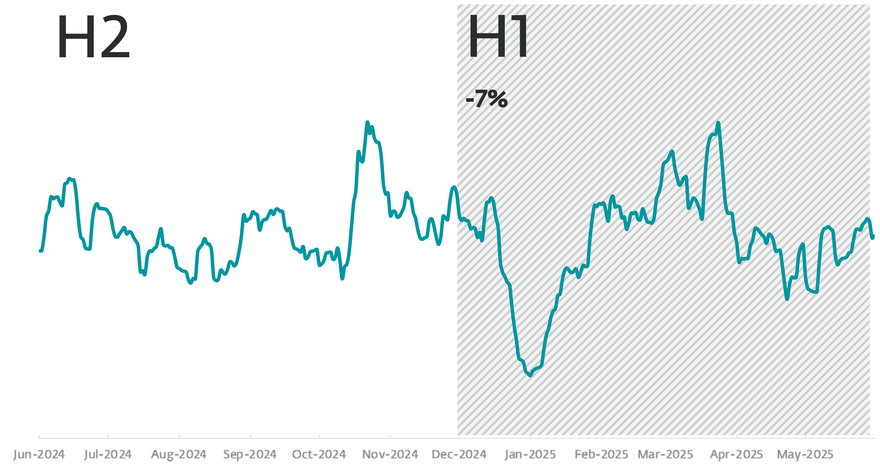


Geographic distribution of Cryptocurency threat detections in H1 2025

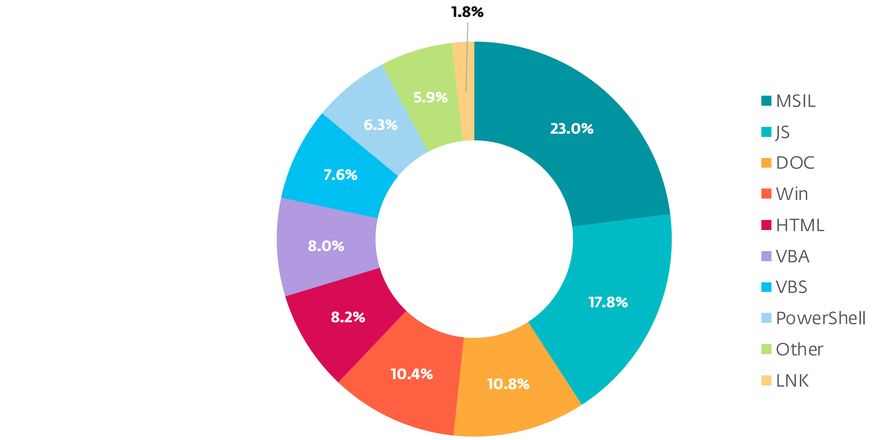


Top 10 Cryptocurrency threat detections in H1 2025 (% of Cryptocurrency threat detections)

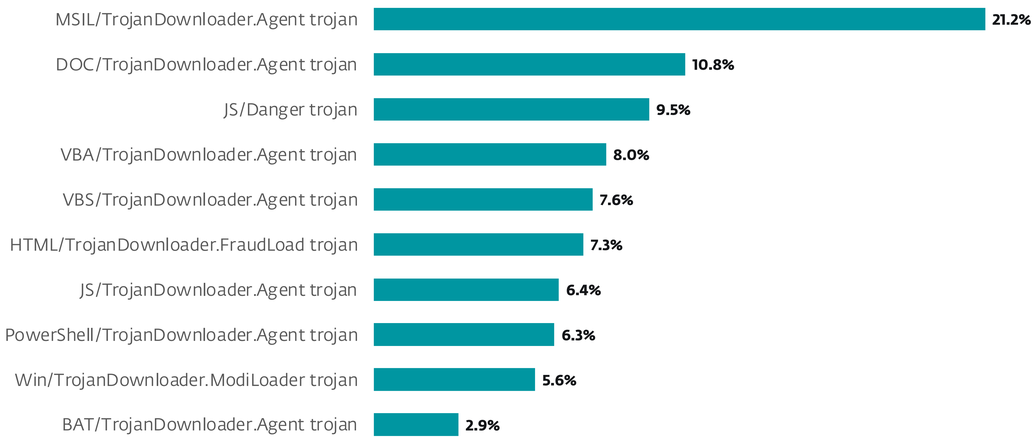
Downloaders



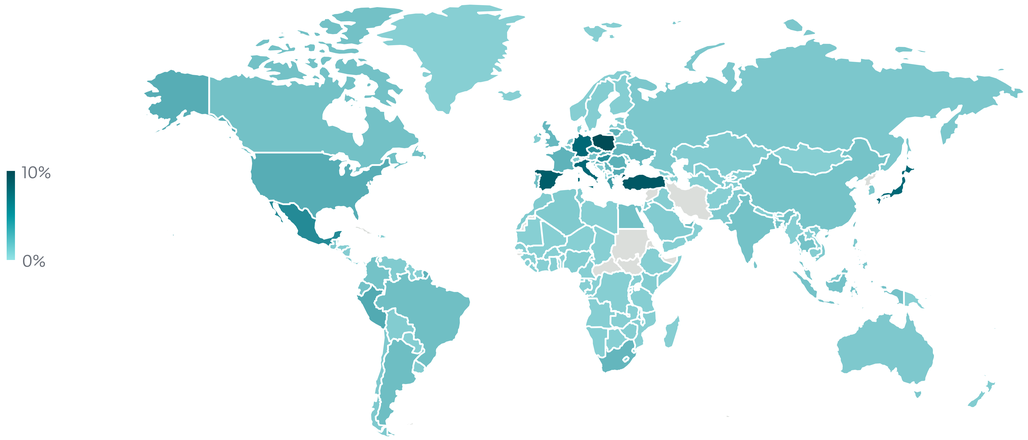
Downloader detection trend in H2 2024 and H1 2025, seven-day moving average



Downloader detections per detection type in H1 2025

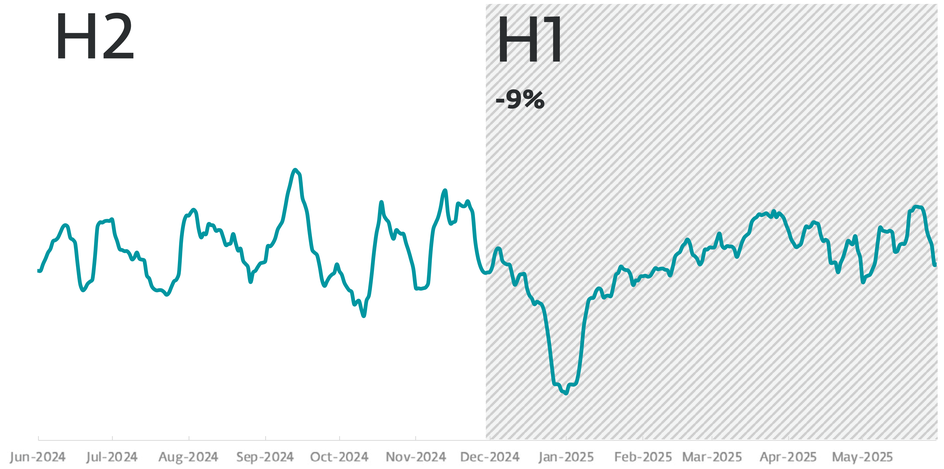


Top 10 Downloader detections in H1 2025 (% of Downloader detections)

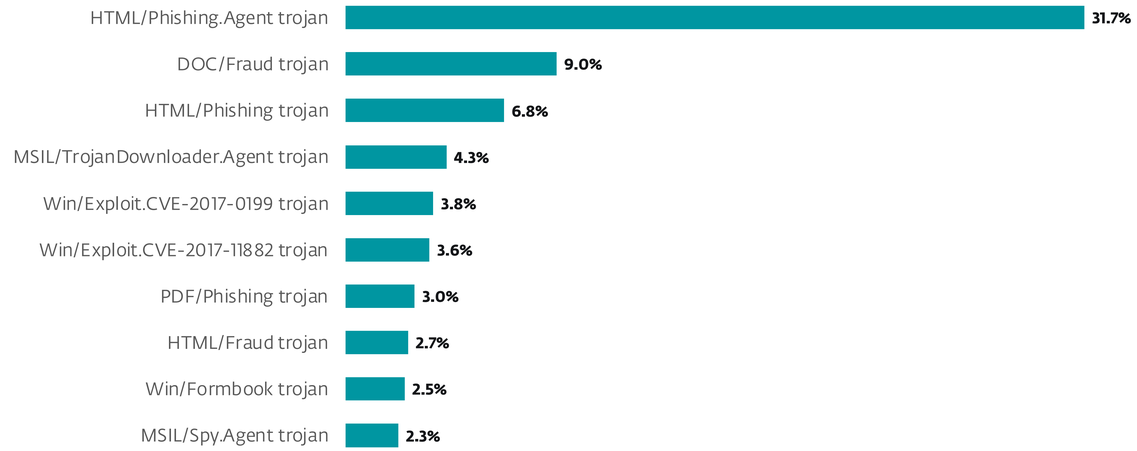


Geographic distribution of Downloader detections in H1 2025

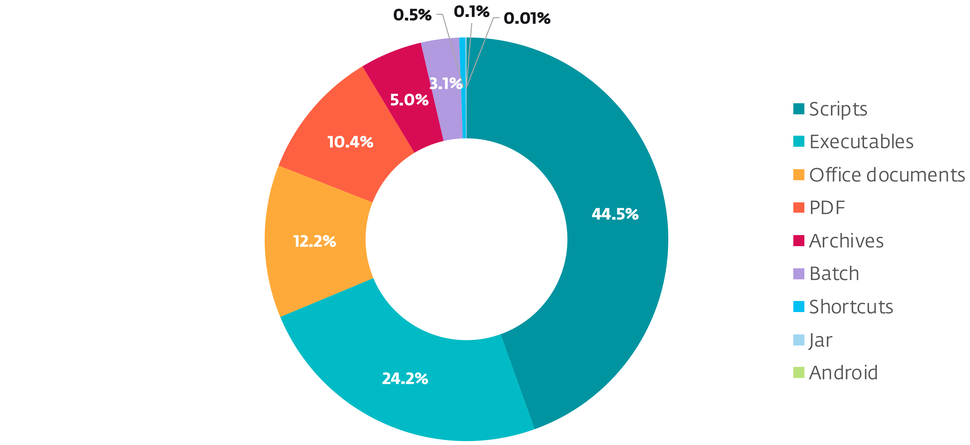
Email threats



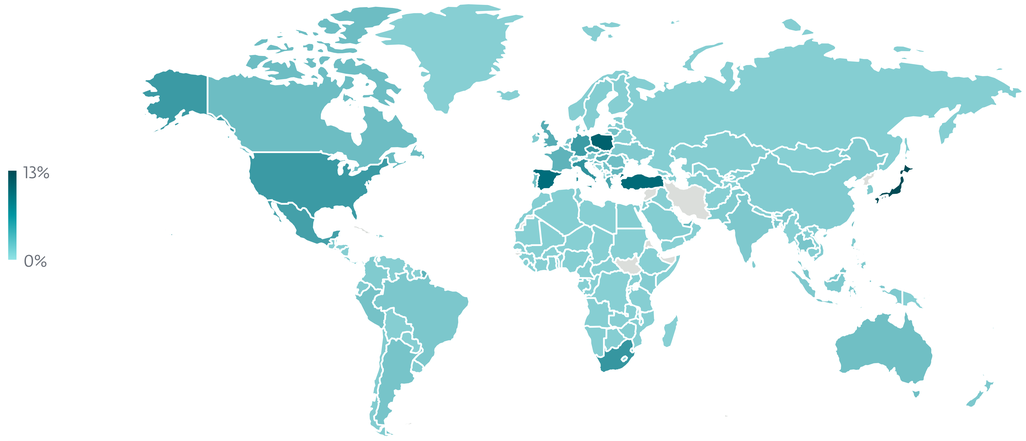
Malicious email detection trend in H2 2024 and H1 2025, seven-day moving average



Top 10 threats detected in emails in H1 2025

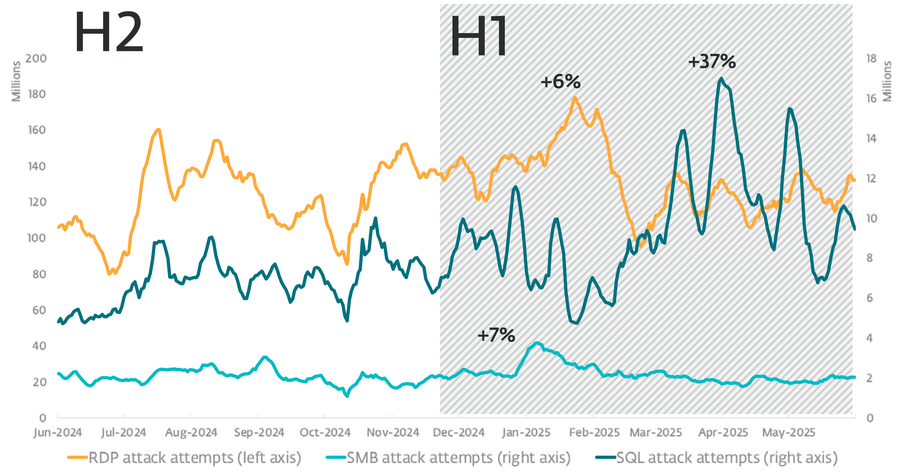


Top malicious email attachment types in H1 2025

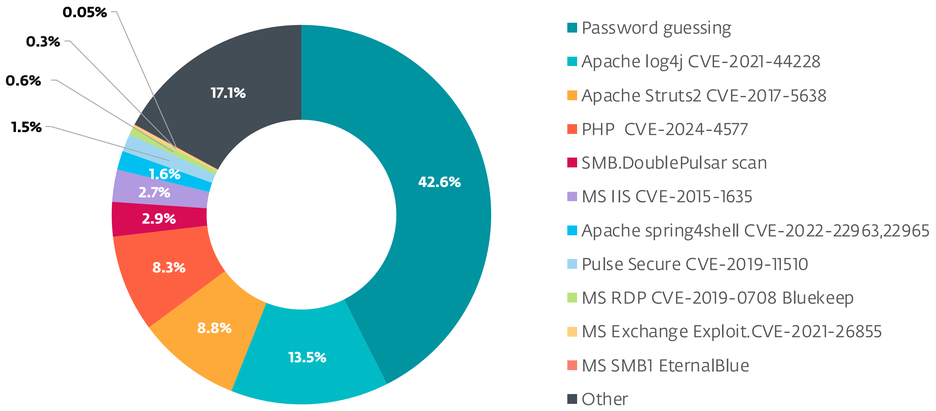


Geographic distribution of Email threat detections in H1 2025

Exploits

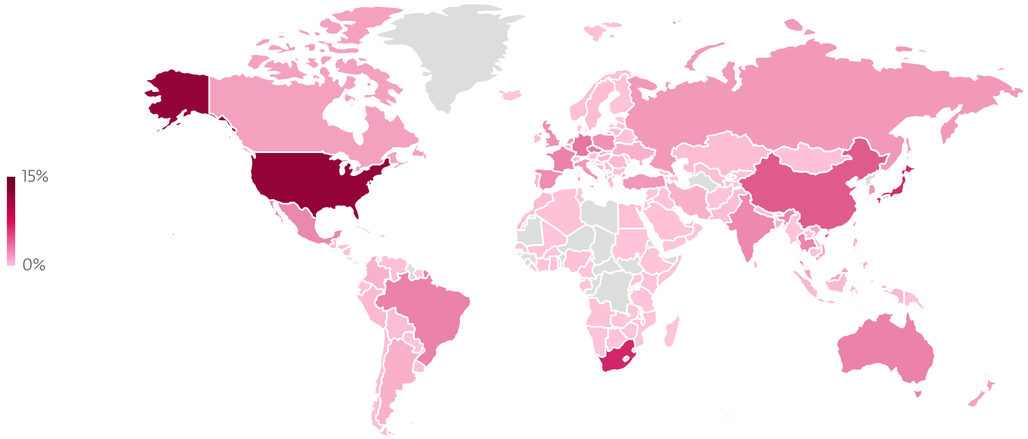


Trends of RDP, SMB, and SQL attack attempts in H2 2024 and H1 2025, seven-day moving average

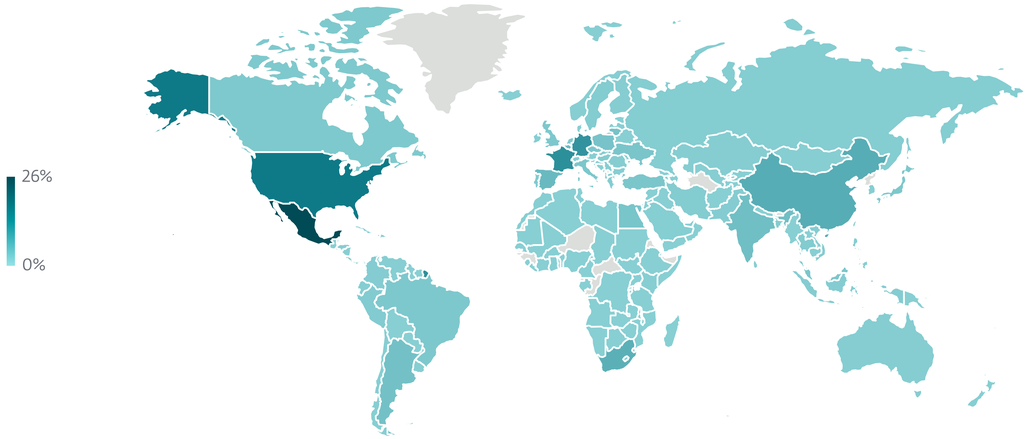


External network intrusion vectors reported by unique clients in H1 2025

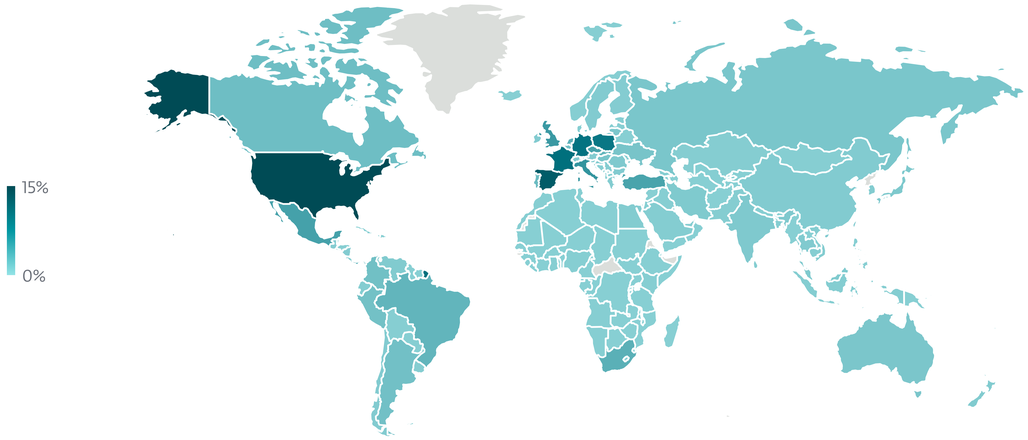
Exploits



Geographic distribution of RDP password guessing attack attempt sources in H1 2025



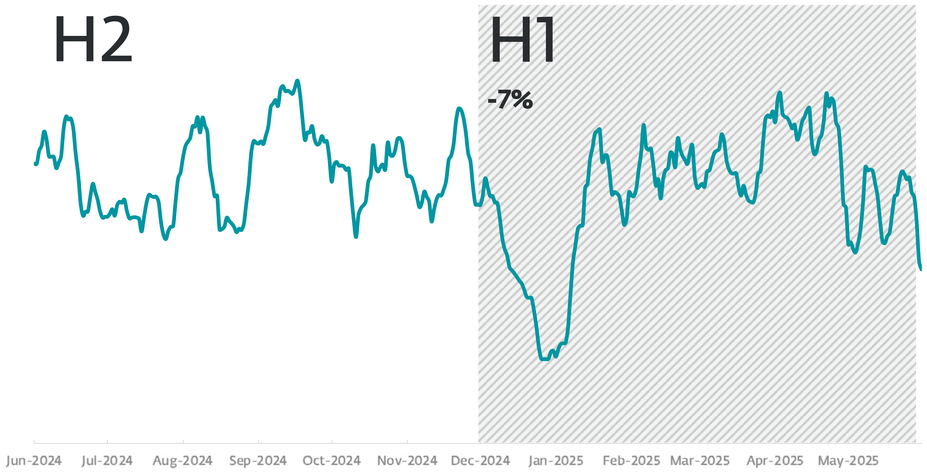
Geographic distribution of SMB password guessing attack attempt targets in H1 2025



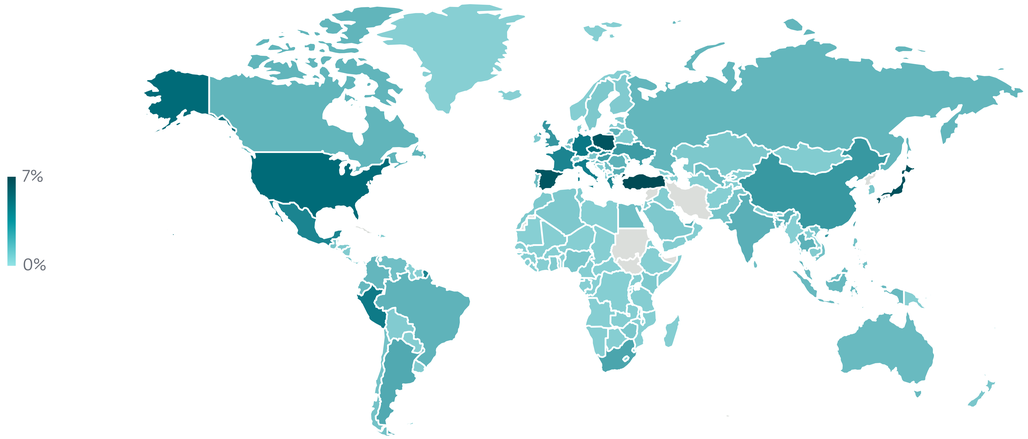
Geographic distribution of RDP password guessing attack attempt targets in H1 2025

Geographic distribution of SQL password guessing attack attempt targets in H1 2025

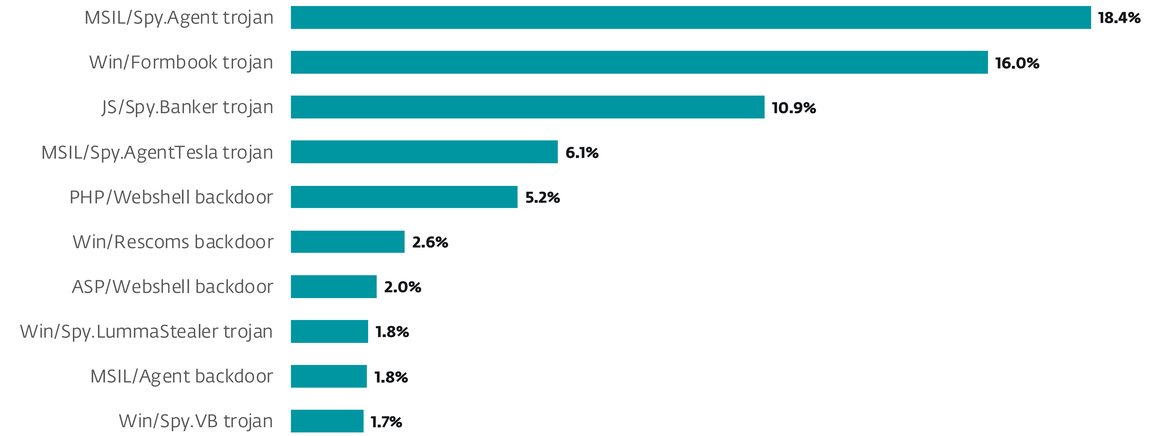
Infostealers



Infostealer detection trend in H2 2024 and H1 2025, seven-day moving average

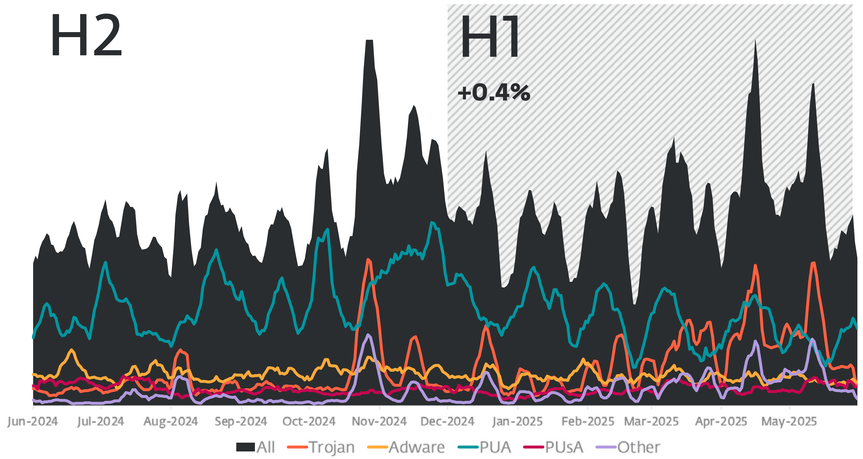


Geographic distribution of Infostealer detections in H1 2025

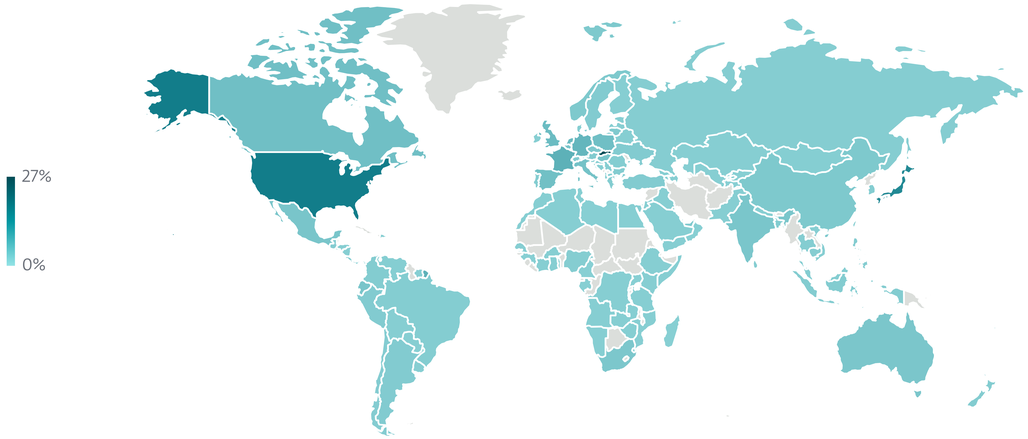


Top 10 Infostealer families in H1 2025 (% of Infostealer detections)

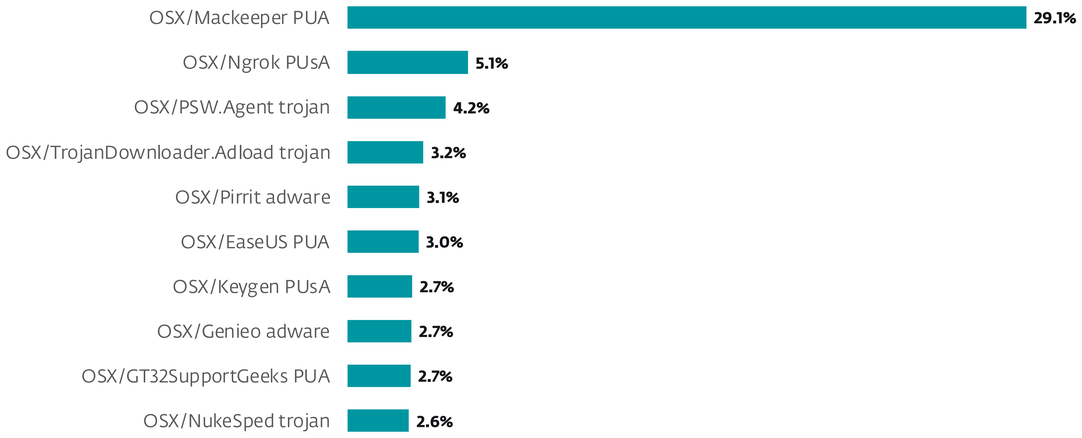
macOS



macOS detection trend in H2 2024 and H1 2025, seven-day moving average

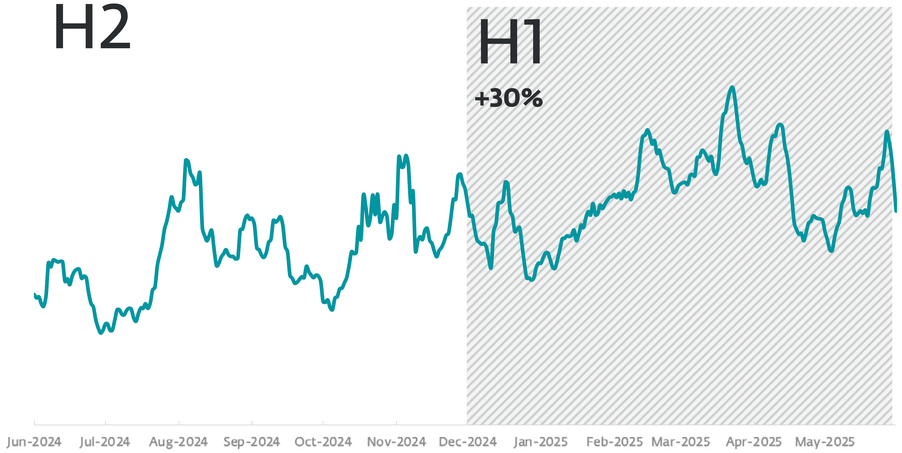


Geographic distribution of macOS detections in H1 2025

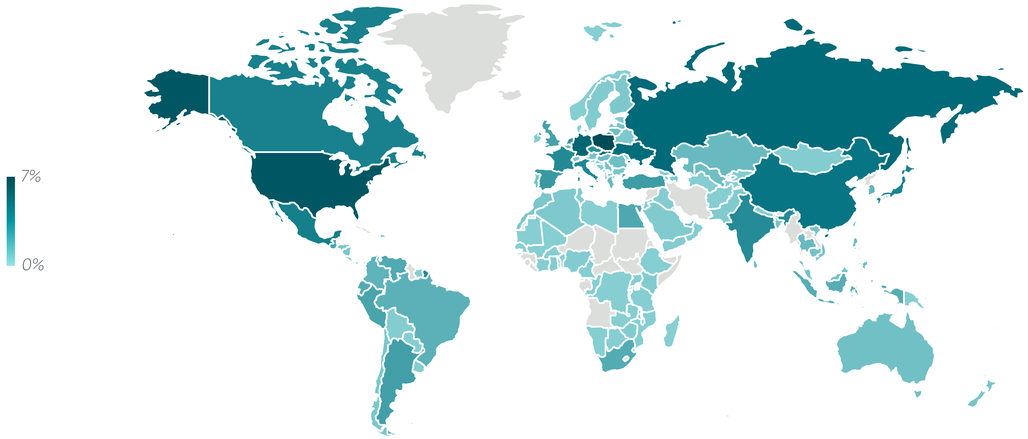


Top 10 macOS detections in H1 2025 (% of macOS detections)

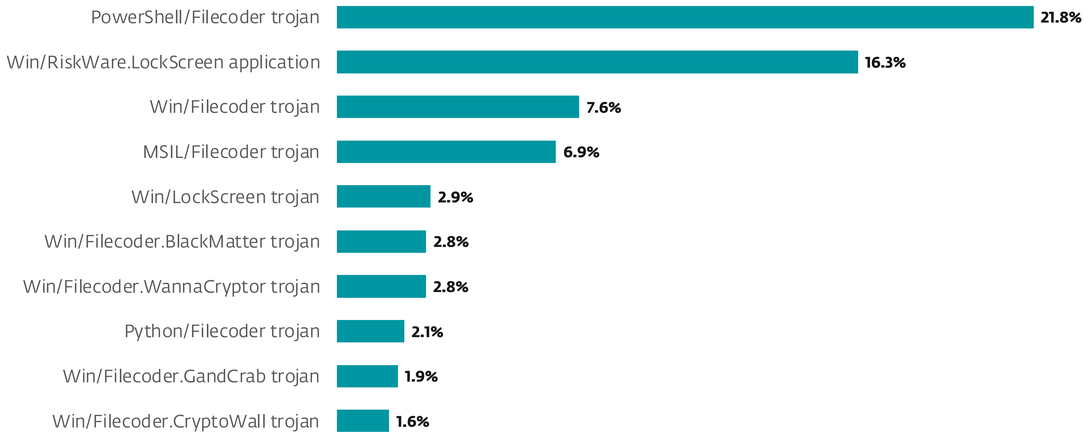
Ransomware



Ransomware detection trend in H2 2024 and H1 2025, seven-day moving average

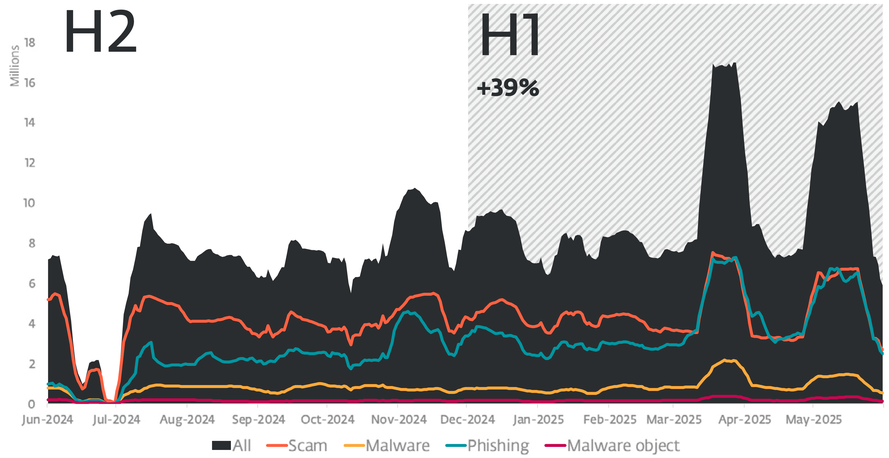


Geographic distribution of Ransomware detections in H1 2025

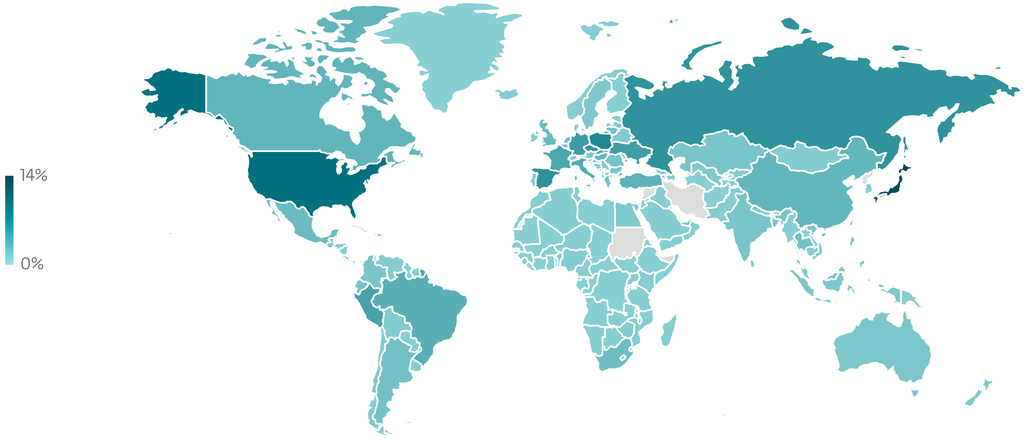


Top 10 Ransomware detections in H1 2025 (% of Ransomware detections)

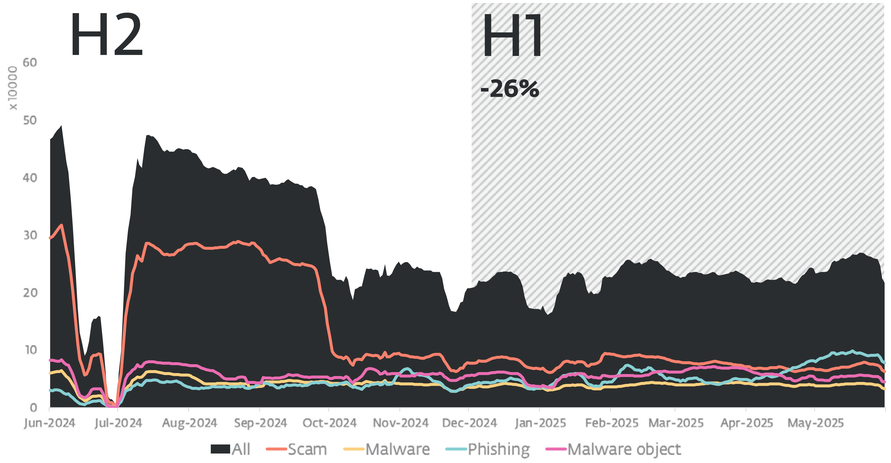
Web threats



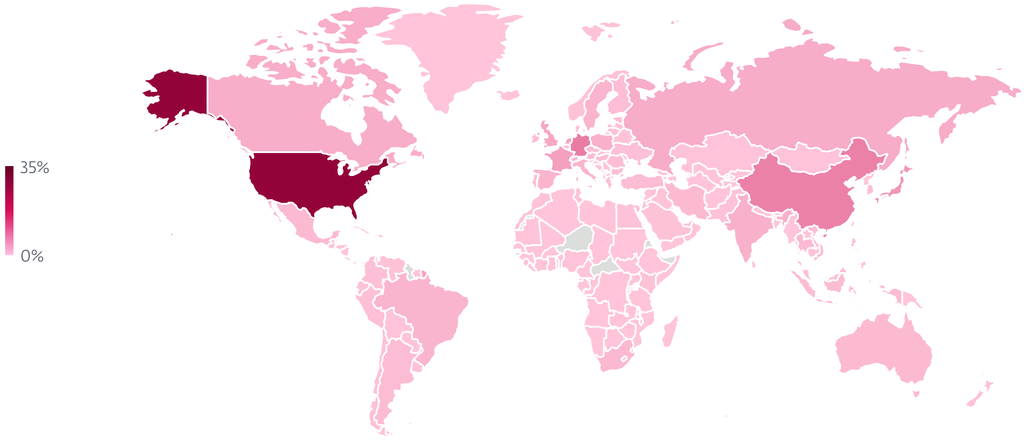
Web threat block trend in H2 2024 and H1 2025, seven-day moving average[2]



Global distribution of Web threat blocks in H1 2025



Unique URL block trend in H2 2024 and H1 2025, seven-day moving average[2]



Global distribution of blocked domain hosting in H1 2025

[2] The sharp decline in detection numbers from late June to early July 2024 was caused by a short-lived problem with connections to our statistical databases; this had no impact on threat protection.

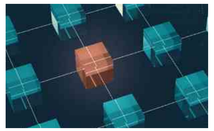
Research publications

ESET Research Podcast: Telekopye, again

Take a peek into the murky world of cybercrime where groups of scammers who go by the nickname of 'Neanderthals' wield the Telekopye toolkit to ensnare unsuspecting victims they call 'Mammoths'

Under the cloak of UEFI Secure Boot: Introducing CVE-2024-7344

The story of a signed UEFI application allowing a UEFI Secure Boot bypass



PlushDaemon compromises supply chain of Korean VPN service

ESET researchers have discovered a supply-chain attack against a VPN provider in South Korea by a new China-aligned APT group we have named PlushDaemon

DeceptiveDevelopment targets freelance developers

ESET researchers analyzed a campaign delivering malware bundled with job interview challenges

Danabot: Analyzing a fallen empire

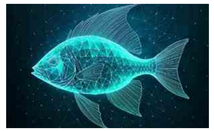
ESET Research shares its findings on the workings of Danabot, an infostealer recently disrupted in a multinational law enforcement operation

Threat Report H2 2024: Infostealer shakeup, new attack vector for mobile, and Nomani

Big shifts in the infostealer scene, novel attack vector against iOS and Android, and a massive surge in investment scams on social media

Operation AkaiRyū: MirrorFace invites Europe to Expo 2025 and revives ANEL backdoor

ESET researchers uncovered MirrorFace activity that expanded beyond its usual focus on Japan and targeted a Central European diplomatic institute with the ANEL backdoor



Operation FishMedley

ESET researchers detail a global espionage operation by FishMonger, the APT group run by I-SOON

You will always remember this as the day you finally caught FamousSparrow

ESET researchers uncover the toolset used by the FamousSparrow APT group, including two undocumented versions of the group's signature backdoor, SparrowDoor

BladedFeline: Whispering in the dark

ESET researchers analyzed a cyberespionage campaign conducted by BladedFeline, an Iran-aligned APT group with likely ties to OilRig

Shifting the sands of RansomHub's EDRKillShifter

ESET researchers discover new ties between affiliates of RansomHub and of rival gangs Medusa, BianLian, and Play

TheWizards APT group uses SLAAC spoofing to perform adversary-in-the-middle attacks

ESET researchers analyzed Spellbinder, a lateral movement tool used to perform adversary-in-the-middle attacks

Operation RoundPress

ESET researchers uncover a Russia-aligned espionage operation targeting webmail servers via XSS vulnerabilities

ESET takes part in global operation to disrupt Lumma Stealer

Our intense monitoring of tens of thousands of malicious samples helped this global disruption operation

ESET Threat Report H2 2024

A view of the H2 2024 threat landscape as seen by ESET telemetry and from the perspective of ESET threat detection and research experts

ESET APT Activity Report Q4 2024–Q1 2025

An overview of the activities of selected APT groups investigated and analyzed by ESET Research in Q4 2024 and Q1 2025

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

Dušan Lacika
Jakub Kaloč
Jakub Souček
Jakub Tomanek
Lukáš Štefanko
Tomáš Procházka

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

Digital Security
Progress. Protected.

(eset):research