Digital Security
Progress. Protected.

Threat Report

H2 2024

June 2024 – November 2024

(eset):research

Contents

Executive summary

Infostealers Malware as a service

A tale of two stealers: Upheaval in the infostealer threat landscape

RedLine Stealer taken down while Lumma Stealer detections soar.

Infostealers Email threats

Formbook's return to form

Formbook dethrones Agent Tesla as number one infostealer in ESET telemetry data.

Cryptostealers macOS Windows Android

Digital treasure hunters: Bitcoin's surge fuels cryptostealer rise

Cryptostealers grow across the board as bitcoin exchange rates reach an all-time high.

Android iOS Financial threats

Is it an app or a website? Attackers find a shortcut to steal mobile banking credentials

A new mobile threat vector allows attackers to bypass traditional security measures of mobile operating systems and trick users into compromising their Android and iOS devices.

Web threats Scams Deepfakes

Invest with the rich and famous, end up with Nomani

New investment scam ads are filling social media news feeds, using deepfake videos and company-branded posts to lure victims, leading to financial harm and data loss.

Web threats Scams Phishing

Online marketplace fraudsters diversify, scamming tourists via fake hotel bookings

H2 2024 gave rise to a new scam targeting users of popular accommodation booking platforms. The scammers use Telekopye, a toolkit originally developed to defraud people on online marketplaces.

Ransomware

The RaaS war has a clear winner: RansomHub

After LockBit's disruption in H1 2024, a struggle for the leading position in the ransomware-as-a-service market broke out, changing affiliations between criminal groups and sucking in new less-skilled players.

Foreword

Welcome to the H2 2024 issue of the ESET Threat Report!

In the usual cat-and-mouse game with defenders, the second half of 2024 has seen the cybercriminals keeping busy, finding security loopholes and innovative ways to expand their victim pool. As a result, we've seen new attack vectors and social engineering methods, new threats skyrocketing in our telemetry, and takedown operations leading to shake-ups of established cybercriminal ranks.

Infostealers are one of the threat categories to experience a reshuffle, with the long-dominant Agent Tesla malware dethroned by Formbook – a well-established threat designed to steal a wide variety of sensitive data. Despite being around for almost a decade, Formbook continues to attract a wide criminal user base thanks to its malware-as-a-service (MaaS) model and continuous development.

Lumma Stealer, a newer addition to the infostealer scene, and another MaaS, is becoming increasingly sought after by cybercriminals: appearing in several notable malicious campaigns in H2 2024, ESET telemetry saw its detections shoot up almost 400% between reporting periods. RedLine Stealer, another notorious "infostealer as a service", met a very different fate: after a takedown by international authorities in October 2024, RedLine Stealer appears to have reached the end of its line. We can, however, expect that its demise will lead to the expansion of other similar threats, eager to fill its place.

Unsurprisingly, with cryptocurrencies reaching record values in H2 2024, cryptocurrency wallet data was one of the prime targets of malicious actors. In our telemetry, this was reflected in a rise in cryptostealer detections across multiple platforms. Curiously, the increase was the most dramatic on macOS, where so-called Password Stealing Ware – heavily targeting cryptocurrency wallet credentials – more than doubled compared to H1. Further, Android financial threats, targeting banking apps as well as cryptocurrency wallets, grew by 20%.

Android and iOS users alike should be on the lookout for a novel attack vector, caught in the wild and analyzed by ESET researchers in H2 2024. In these attacks, cybercriminals have leveraged Progressive Web App (PWA) and WebAPK technologies to bypass traditional security measures tied to mobile apps. Since neither PWAs nor WebAPKs require users to grant explicit permissions to install apps from unknown sources, mobile users may end up unwittingly installing malicious apps that steal banking credentials. And unless there's a change in how mobile platforms approach these technologies, we anticipate that more sophisticated and varied phishing campaigns utilizing PWAs and WebAPKs will emerge.

Social media waters have become even more murky recently, with a flood of new scams cropping up, using deepfake videos and company-branded posts to lure victims into fraudulent investment schemes. These scams, tracked by ESET as HTML/Nomani, saw a 335% increase in detections between reporting periods, and we don't expect their growth to slow down.

H2 2024 also gave rise to a new scam targeting users of popular accommodation booking platforms, such as Booking.com and Airbnb. Using a toolkit named Telekopye, originally developed to defraud people on online marketplaces, the scammers use compromised accounts of legitimate accommodation providers to single out people who have recently booked a stay, then target them with fraudulent payment pages.

The ransomware landscape was reshaped by the takedown of former leader LockBit, creating a vacuum to be filled by other actors. RansomHub, a ransomware as a service first spotted in H1 2024, stacked up hundreds of victims by the end of H2 2024, establishing itself as the newly dominant player.

I wish you an insightful read.

Jiří Kropáč
ESET Director of Threat Detection

Threat landscape trends

Infostealers Malware as a service

A tale of two stealers: Upheaval in the infostealer threat landscape

RedLine Stealer taken down while Lumma Stealer detections soar.

RedLine Stealer and Lumma Stealer are well-known to the readers of ESET Threat Reports: already covered in past issues, both of these infostealers operate under the malware-as-a-service (MaaS) model.

RedLine Stealer, used for collecting a large variety of data, from saved credit card details to local cryptocurrency wallets, was discovered in 2020 and quickly became one of the most detected infostealers in ESET telemetry.

Lumma Stealer first appeared in the wild in 2022 and also started climbing the ranks rapidly, eventually appearing on the list of top ten infostealers detected by ESET products in H2 2024. Among other things, it targets two-factor-authentication browser extensions, user credentials, and, as with RedLine Stealer, cryptocurrency wallets.

With the MaaS model granting them a wide criminal user base, both of these infostealers seemed to be set for the foreseeable future. However: while Lumma Stealer did indeed continue to thrive, RedLine Stealer did not last through the end of the year, thanks to law enforcement efforts.

RedLine Stealer taken down by international authorities

In October 2024, the Dutch National Police, alongside the FBI, Europol, and several other law enforcement organizations, managed to take down RedLine Stealer and its clone META Stealer during Operation Magnus. Aside from making several arrests and disrupting the stealers' infrastructure, the authorities also retrieved a database of RedLine and META's criminal clients.

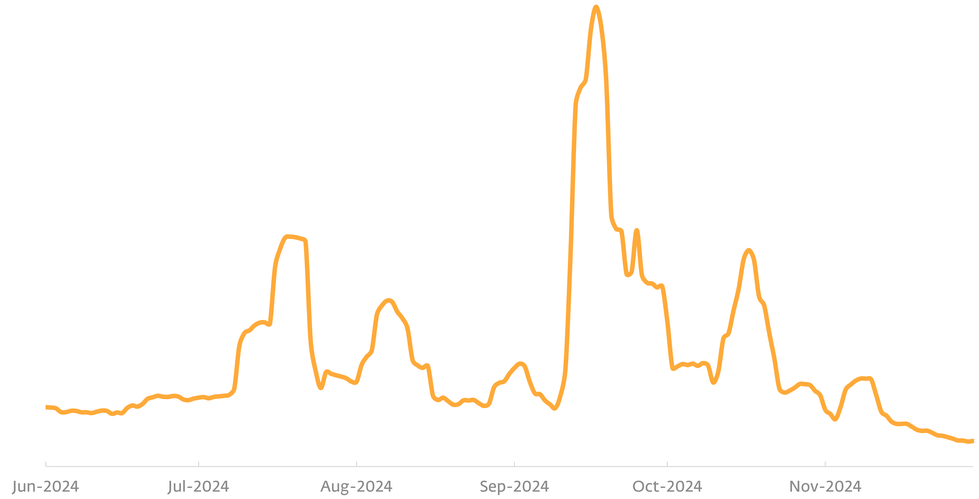
We can be quite certain that Operation Magnus spelled the end of RedLine Stealer. Even though the creator of RedLine has not been arrested yet, it is unlikely that he would try to resurrect the malware. While he could, in theory, buy or rent new servers and use the existing code to set up new infrastructure and distribute panels to affiliates, he has been identified and charged by law enforcement, so he will probably want to keep a low profile.

RedLine affiliates will also probably want to move on, since law enforcement now has the database with their usernames and last-used IP. While this might not be enough to identify the people behind those aliases in every case, they are now considered "Very Important to the Police". All in all, we can expect that the power vacuum left by RedLine's takedown will lead to a bump in the activity of other MaaS infostealers.

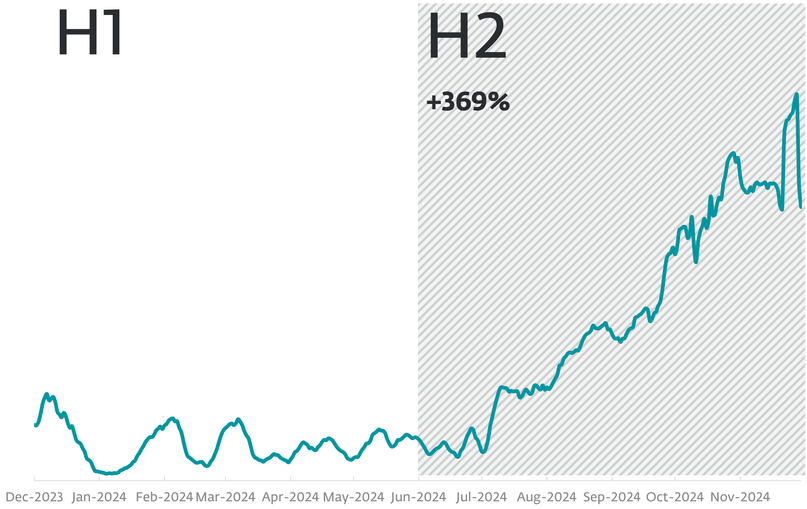
Alexandre Côté Cyr, ESET Malware Researcher

Following Operation Magnus, ESET publicly released the results of an investigation into RedLine's backend modules we performed in 2023 alongside the researchers at Flare. Along with the 2023 findings, our blogpost included some new information gleaned from the source code that the Dutch National Police shared with us after the takedown.

As our statistics show, even though RedLine Stealer detections have dropped, they have not disappeared completely yet. The main reason behind this is that a lot of RedLine samples are still out there. Even though the affiliates were not actively spreading them, there are many passive phishing campaigns delivering RedLine via YouTube comments or GitHub repositories. Another cause for ongoing detections is the existence of older, cracked RedLine Stealer versions, some of which might still be functional. If you suspect that your system has been compromised by either RedLine Stealer or META Stealer, ESET provides an online scanner specifically for the two threats.



RedLine Stealer detection trend in H2 2024, seven-day moving average



Lumma Stealer detection trend in H1 and H2 2024, seven-day moving average

Lumma Stealer detections grow like never before

Lumma Stealer is becoming more and more in demand by cybercriminals: as we already stated, in H2 2024, it managed for the first time to get into the top 10 infostealers detected by ESET products. Its growth between periods was also the highest ever, amounting to 369% with almost 50,000 detections registered in total in H2 2024.

As seen in news reports, Lumma Stealer was used in several notable campaigns in H2 2024. To mention some of them, the infostealer was being pushed as fake fixes in thousands of project comments in many GitHub repositories, and also found masquerading as the AI image and video editor EditPro. In another campaign discovered in October, threat actors used creative deception tactics that redirect their targets to fake CAPTCHA sites. Completing the verification steps would lead to Lumma Stealer being delivered to the victims' systems.

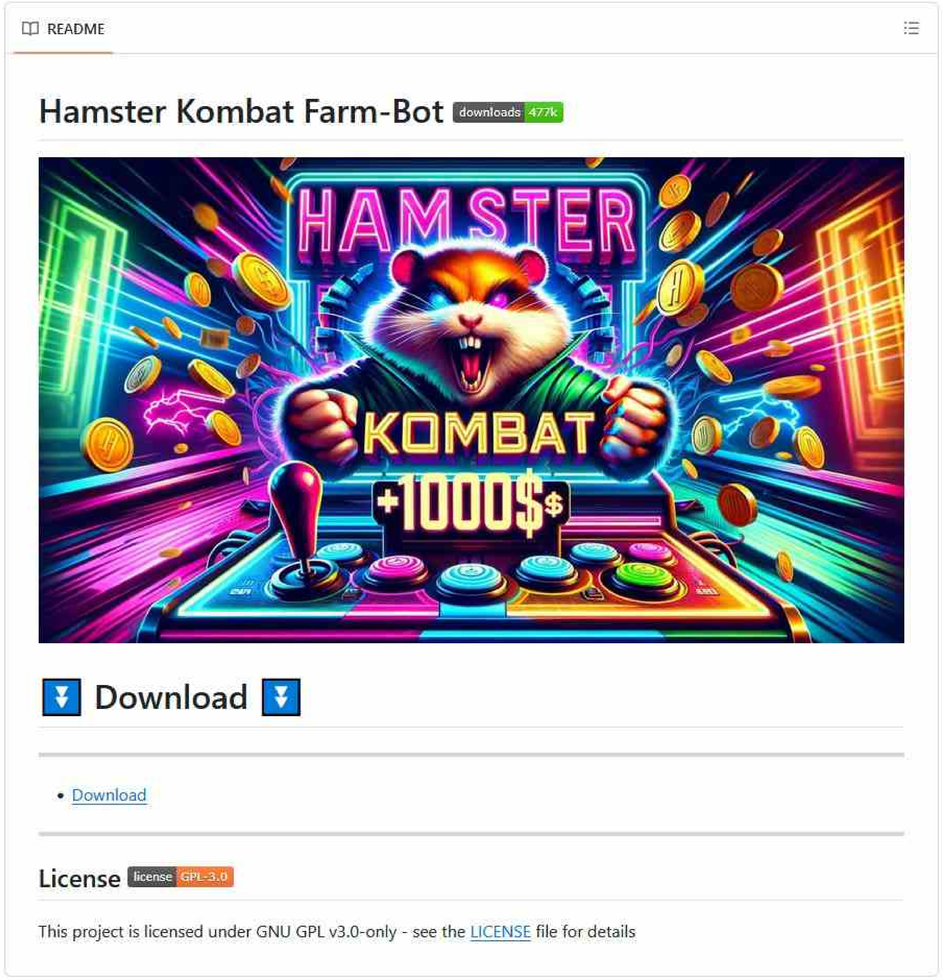
ESET telemetry data confirms that Lumma Stealer had its virtual fingers in many pies in the latter half of 2024. In the Cryptostealer category, where we detect

it as Win/PSW.Agent.OGR trojan, the malware accounted for three fourths of H2 2024 detections. The stealer showed particularly high activity in July through October, when it was distributed in the form of patched popular files and installers, mainly Key Management Service (KMS) activators for activating pirated copies of Windows.

We also detected a campaign of the Win/Rozena.ADZ injector, which in the majority of cases was delivering Lumma Stealer. Spreading via compromised videos on online marketplaces and websites with adult content, the campaign was visible mainly in October and November.

As described in a **blogpost** published in July, ESET researchers also discovered cryptors that contain embedded Lumma Stealers that target players of the mobile clicker game Hamster Kombat. We found several GitHub repositories claiming to offer farm bots and autoclickers (both are tools that automate gameplay to produce results faster) to help Hamster Kombat players maximize their in-game profits. These repositories were actually hiding cryptors containing Lumma Stealer, either directly in the release files, or as links to external file-sharing services.

In H2 2024, ESET telemetry registered the highest number of Lumma Stealer attack attempts in Peru, Poland, Spain, Mexico, and Slovakia.



One of the GitHub repositories discovered spreading Lumma Stealer

Infostealers Email threats

Formbook's return to form

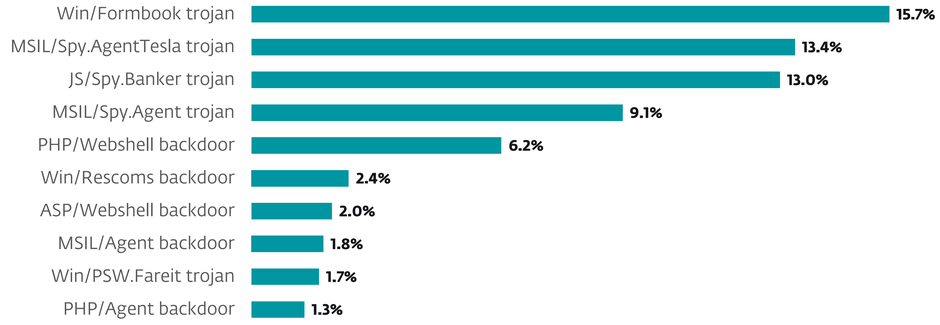
Formbook dethrones Agent Tesla as number one infostealer in ESET telemetry data.

H2 2024 delivered an interesting upset in the top ten infostealers when the Formbook malware managed to oust the notorious Agent Tesla from the **number one position**. While Agent Tesla detections decreased by 26% between H1 and H2 2024, ESET telemetry shows that Formbook numbers shot up by more than 200% in that same period.

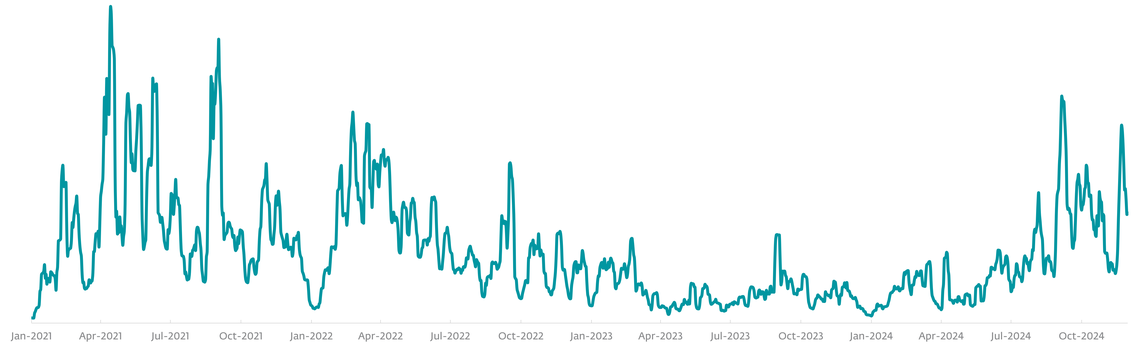
A look at our Formbook trend data between 2021 and 2024 reveals that this threat was especially **sought-after in 2021**, some days even surpassing 10,000 hits per day. While later on, its numbers gradually decreased, it always remained a potent threat, never leaving ESET's top five detected infostealers. During the latter half of 2024, we saw a Formbook resurgence, with the malware returning to 2022 numbers. Its most significant daily detections occurerd on September 5 with more than 7,000 detections, about half of which were registered in Japan.

Formbook was also found among the payloads of significant campaigns of the ModiLoader downloader, overwhelmingly targeting Poland (80% of registered attack attempts), that we described in a **blogpost** in

First discovered in 2016, Formbook is a well-established threat. This malware is an infostealer that collects, among other things, clipboard data, keystrokes, screenshots, and cached browser data. It is a malware-as-a-service (MaaS) solution, sold on underground forums, that spreads as malicious attachments in phishing emails. Since 2020, this infostealer has sometimes been referred to as XLoader. Because this name can also refer to a macOS version of the malware, ESET continues to track the Windows threat as Formbook under the detection name Win/Formbook trojan.



Top 10 infostealer detections in H2 2024

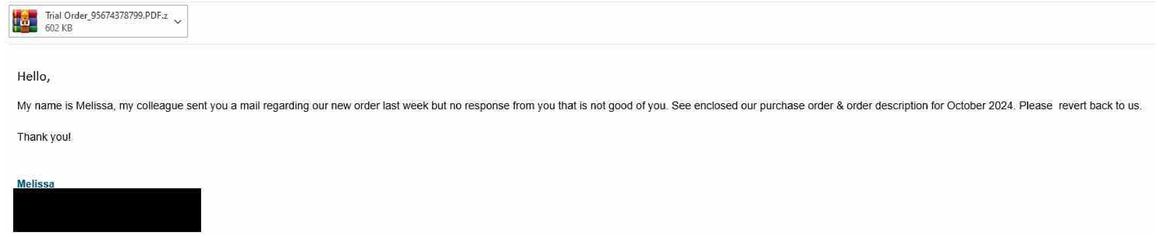


Formbook detection trend from H1 2021 to H2 2024, seven-day moving average

Timeline of the most significant ModiLoader and AceCryptor campaigns in Central and Eastern Europe delivering Formbook

July. During these campaigns, the attackers spread ModiLoader via malicious attachments in phishing emails impersonating existing companies and their employees. Apart from Formbook, the other frequently delivered payloads were infostealers Agent Tesla and Rescoms (also known as Remcos).

Our more recent findings show that Formbook continues to be distributed in further ModiLoader campaigns, as well as several **AceCryptor** campaigns. In June through October, ESET products protected almost 34,000 users against ModiLoader and AceCryptor attacks in Eastern and Central Europe. During this time, we saw a total of 24 campaigns; while at the start of H2 2024, they were delivering mainly Rescoms and Agent Tesla, later on the payloads shifted primarily to contain Formbook. Poland remained the most targeted country of these attacks.



One of the phishing emails with an attachment delivering ModiLoader in H2 2024

Large-scale campaigns such as the ModiLoader ones meant that 2024 was a rather prosperous time for infostealers in general. Since the end of 2021 until recently, their numbers always decreased between our reporting periods. Their detections only started picking up in H1 2024, when this category experienced a slight, 4% increase. It seems this trend has accelerated in H2 2024, which brought 12% growth for infostealers.

The rather significant decrease in Agent Tesla detections should not be taken to mean that this infostealer is on its death bed, though. Since there's been no takedown of this malware's operations, this lull in activity most probably signifies that the operators behind Agent Tesla are working on new and improved malicious features. Therefore, we can almost certainly expect Agent Tesla to return in full force.

No matter which infostealer is currently ascendant, you should always be on the lookout for suspicious emails, and protect your data with up-to-date security solutions. Since infostealers such as Formbook are often after user passwords, we recommend not storing credentials in your browser but using a dedicated password manager.

EXPERT COMMENT

Despite being relatively old, Formbook continues to be used frequently by cybercriminals because, as malware-as-a-service, it's under continuous development. Just in H2 2024, we have seen this threat use more and more sophisticated obfuscation techniques, in order to make its analysis, along with automatic sample collection, significantly more difficult.

Juraj Horňák, ESET Malware Analyst

Cryptostealers macOS Windows Android

Digital treasure hunters: Bitcoin's surge fuels cryptostealer rise

Cryptostealers grow across the board as bitcoin exchange rates reach an all-time high.

In 2024, especially its second half, exchange rates were exceptionally generous to cryptocurrency. By March, bitcoin had already managed to surpass its previous all-time high rate of US$69,000, with its rate continuing to climb even higher through the rest of the year. Then, following a surge after Donald Trump's victory in the US presidential election in November 2024, the cryptocurrency traded for more than US$90,000. As might be expected, cybercriminals were also eager to profit from this development, which translated into significant growth for cryptostealers.

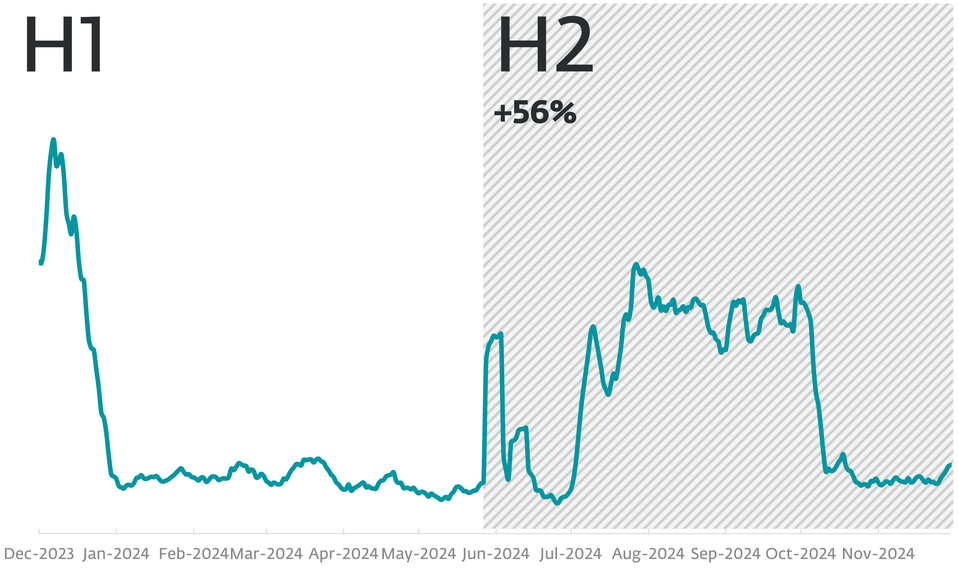
According to ESET telemetry data from H2 2024, cryptostealer numbers were up across multiple platforms, specifically Windows, macOS, and Android. The increase was the most dramatic on macOS, where password stealers targeting cryptocurrency wallets more than doubled in detections compared to H1.

Meanwhile, Windows cryptostealers grew by 56%, and Android financial threats, which include cryptostealing malware, by 20%.

macOS

On the macOS platform, ESET telemetry recorded a 127% increase in Password Stealing Ware (PSW), which frequently targets credentials related to cryptocurrency wallets, among others. Although these threats cannot be classified solely as cryptostealers due to their broader functionality, they are indicative of the rising trend in cryptostealing activities on macOS.

A significant contributor to this surge is **AMOS** (also known as Atomic Stealer), along with its numerous versions and imitators. Initially designed as a malware family to collect and exfiltrate sensitive data from Mac devices, AMOS was marketed as malware as a service



Cryptostealer detection trend in H2 2024, seven-day moving average

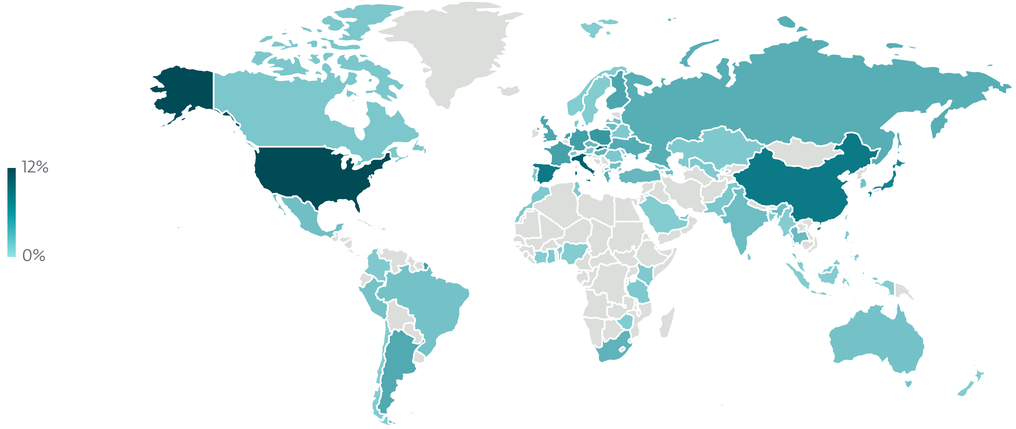
on Telegram. Since its inception in 2023, various AMOS variants and copycats have appeared both for sale on the black market and in the wild. ESET detects these as variants of the OSX/PSW.Agent trojan.

Devices are typically compromised with AMOS via Google ad poisoning or social engineering. Attackers use legitimate-looking malicious ads on Google's network, leading users to a site that prompts the target to download malware posing as legitimate software. Victims have also reported on social media and online forums that they were approached by individuals posing as representatives of cryptocurrency investment entities. After gaining the victims' trust, these representatives recommended installing specific software, such as a videoconferencing app, that turned out to be AMOS.

OSX/PSW.Agent trojan detection trend in H2 2024, seven-day moving average

ESET telemetry registered most PSW detections in H2 2024 in the United States, Italy, China, Spain, and Japan.

Interestingly, there has also been a notable increase in cryptominers on macOS. Despite their detections skyrocketing by over 320%, their absolute numbers remain relatively small, especially when compared to the aforementioned PSWs. Unlike the rise in PSWs, this growth can not be attributed to a specific macOS detection because, according to ESET telemetry, the increase is evenly distributed across most macOS cryptominer families, probably influenced by fluctuations in the bitcoin exchange rate.



Geographic distribution of macOS PSWs in H2 2024

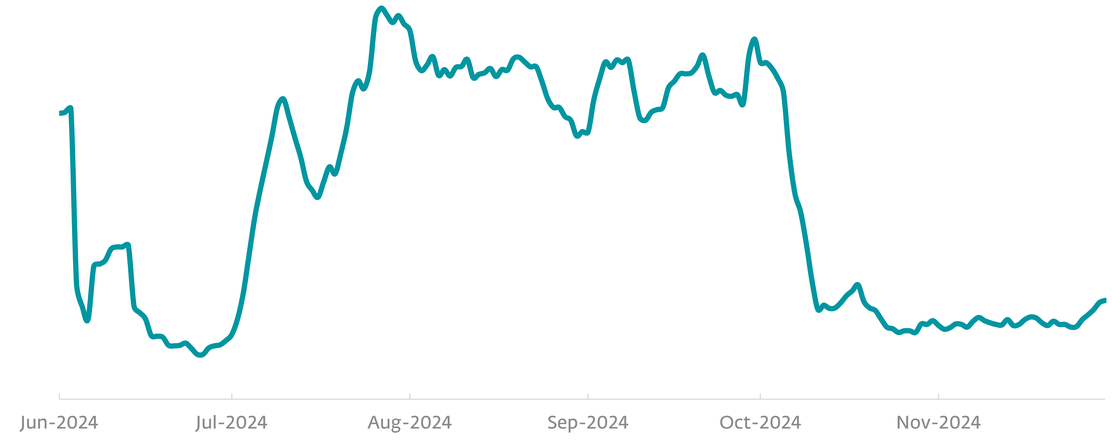
Windows

PSW threats were also behind the growth of cryptostealers that target the Windows platform. The two most frequently detected malware groups in this category were Win/PSW.Agent trojan and Win/PSW.Delf trojan, which together made for almost 90% of cryptostealer detections in H2 2024.

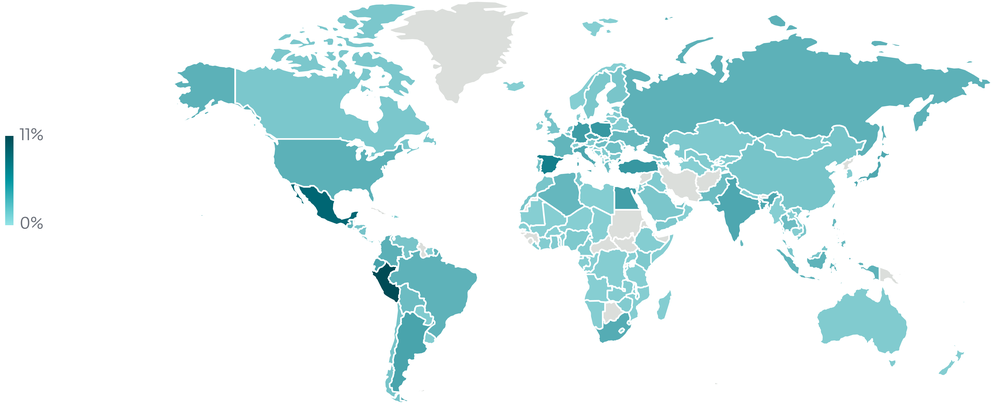
Win/PSW.Agent detections skyrocketed from a couple of hundred in H1 2024 to several thousand in H2 2024. An examination of the samples we detected revealed that the most prevalent Win/PSW.Agent group is actually one of the many variants of the infamous malware-as-a-service Lumma Stealer, which explains the elevated number of detections. Our latest findings on Lumma Stealer can be found in **A tale of two stealers: Upheaval in the infostealer threat landscape** section of this report.

Unlike Win/PSW.Agent, the Win/PSW.Delf trojan did not experience growth in detections in H2 2024. However, we still noted two significant spikes in the malware's activity: one on June 7, targeting mainly Türkiye, and another on September 2. In September, the malware was being delivered in a spam campaign impersonating Fujifilm.

Phishing email delivering Win/PSW.Delf trojan, pretending to be from Fujifilm



Detection trend of cryptostealers targeting the Windows platform in H2 2024, seven-day moving average



Geographic distribution of cryptostealers targeting the Windows platform in H2 2024

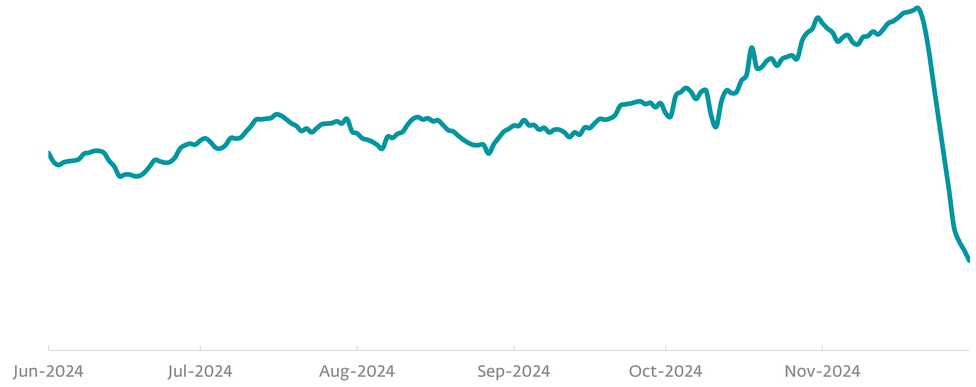
Countries that saw the highest number of Windows cryptostealer attack attempts in this reporting period were Peru, Mexico, Spain, Türkiye, and Poland.

Android

On the Android platform, cryptostealers are part of a broader category of financial threats that also includes Android banking malware. This amalgamation reflects a growing trend where many banking trojans have incorporated functionalities to steal credentials related to cryptocurrency wallets and trading apps, private keys, and cryptocurrency recovery phrases when found on the device.

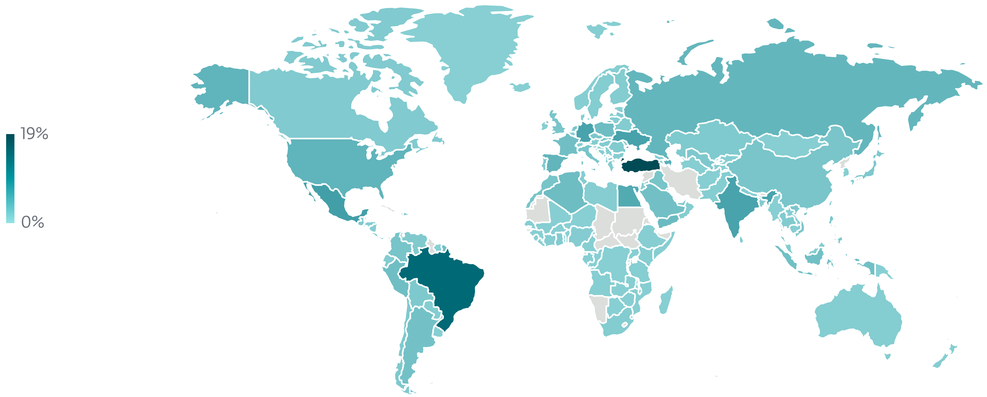
ESET telemetry shows that Android financial threats grew by 20% in H2 2024. Although this percentage increase is not substantial, the trend on the graph on the next page indicates an upward trajectory. This increase is primarily driven by Cerberus, a sophisticated banking trojan that, while primarily targeting banking apps, also extends its capabilities to cryptocurrency wallets and exchanges.

Cerberus operates by overlaying fake login screens on legitimate apps. When a victim attempts to log into a targeted app, Cerberus captures the entered credentials and sends them to the attackers. ESET telemetry recorded a 56% increase in Cerberus detections in H2 2024; however, it is important to note that an Android device can be compromised by Cerberus (or any other threat) via a dropper that is able to "drop" additional malicious code onto the already compromised device.



Android Financial threats detection trend in H2 2024, seven-day moving average

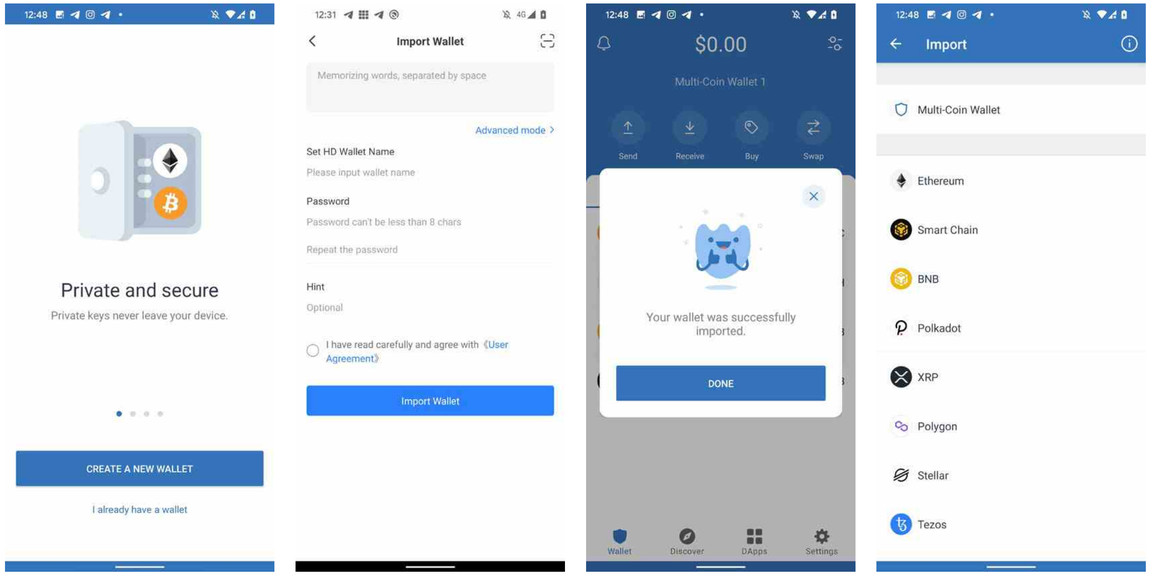
According to ESET telemetry, droppers are responsible for over 53% of all Android Financial threat detections. Countries where ESET products detected the highest numbers of Android Financial threats in H2 2024 are Türkiye, Brazil, Mexico, India, Germany, and Ukraine.



Geographic distribution of Android Financial threats detections in H2 2024

One notable Android cryptostealer identified by fellow researchers is **WalletConnect**, a malicious app masquerading as a legitimate tool to act as a proxy between cryptocurrency wallets and decentralized apps. Upon installation, WalletConnect directs its targets to a fraudulent website where they are tricked into authorizing transactions, leading to the theft of their sensitive wallet information and digital assets. ESET detects this threat as Android/FakeWallet.KH.

Additionally, researchers have **discovered** malware that employs optical character recognition (OCR) to extract cryptocurrency wallet recovery phrases from screenshots saved on the device. Some users take screenshots of their recovery phrases and save them as images on their mobile devices, so that they are not stolen from their clipboard or notes. By obtaining these recovery phrases, the malware allows threat actors to restore and gain control of the victim's cryptocurrency wallet, enabling them to steal all funds contained within it. ESET products detect this threat as Android/Spy.OcrSpy.A and Android/Spy.Banker.CTP.



Example of a trojanized crypto wallet app that sends the recovery phrase to the attacker's command and control server

Android iOS Financial threats Attack vectors

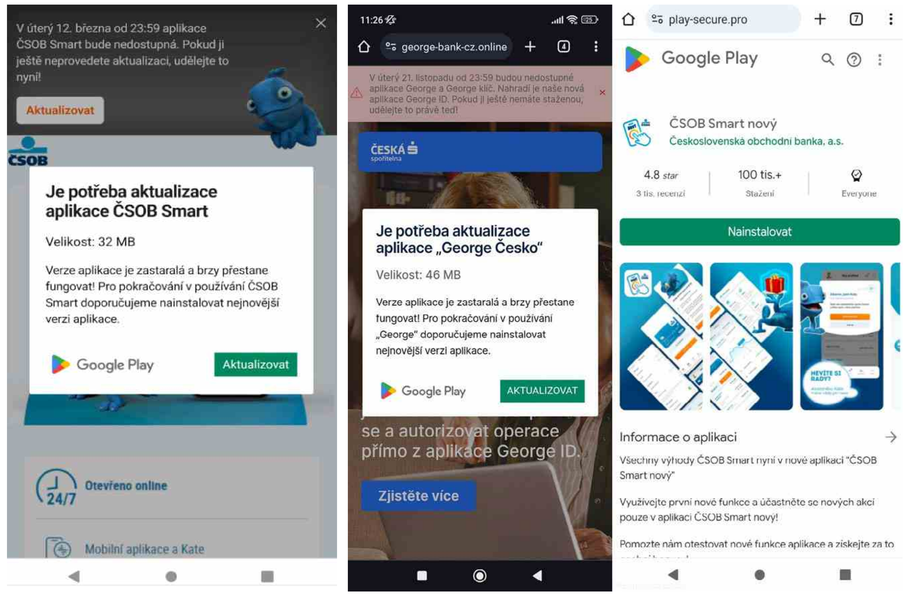
Is it an app or a website? Attackers find a shortcut to steal mobile banking credentials

A new mobile threat vector allows attackers to bypass traditional security measures of mobile operating systems and trick users into compromising their Android and iOS devices.

ESET researchers analyzed campaigns utilizing a novel attack vector targeting mobile devices, with significant potential for further exploitation by cybercriminals. This method leverages Progressive Web Apps (PWAs) and WebAPKs (Android Package Kits generated by the Chrome browser) – technologies allowing their users to install apps directly from websites via supported browsers. Essentially, PWA and WebAPK users can access web-based services from their mobile phone screen, via an icon resembling a native app.

A critical aspect of this technique is that neither PWAs nor WebAPKs require users to grant explicit permissions to install apps from unknown sources or allow the browser to install unknown apps. As a result, device owners may end up installing apps from untrusted sources without realizing it. Once installed, the malicious apps ESET researchers analyzed behave like standard mobile banking malware and present fake banking login interfaces, prompting victims to enter their credentials. The stolen credentials, including login details, passwords, and two-factor authentication codes, are then transmitted to the attackers' command and control servers, so that the attackers can gain unauthorized access to victims' accounts.

In 2024, ESET research uncovered campaigns targeting clients of major banks in Czechia, as well as one bank in Hungary and another bank in Georgia. However, this tactic was first reported by the Computer Security Incident Response Team of the Polish financial sector (CSIRT KNF) in July 2023, following an attack on a Polish bank. In one campaign in Czechia, attackers used the stolen data to withdraw funds from ATMs using NFC data relayed from a compromised phone to an attacker's rooted mobile device. This is the first time that we have seen Android malware with this NFC data relay capability being used in the wild.



Examples of fake download websites, the one on the right mimics Google Play visuals

Countries where ESET research and CSIRT KNF detected malicious PWAs and WebAPKs targeting clients of local banks

The initial phishing messages were delivered through various methods, including SMS, automated voice calls, and social media malvertising. Victims received messages or calls suggesting the need to update their mobile banking applications or informing them of potential tax refunds. These messages, sent to presumably random numbers, contained links directing victims to phishing websites mimicking legitimate banking sites. Malvertising on Facebook and Instagram promoted a fake banking app, falsely claiming that the official app was being decommissioned.

Once on the phishing site, Android users were prompted to install a WebAPK, while iOS users were instructed to add the PWA to their home screen, mimicking native system prompts. In both cases, the installed application looks and behaves like a legitimate banking app, complete with official logos and design elements. This process bypasses the usual warnings associated with installations from untrusted sources, making the phishing attempt much more convincing.

While ESET researchers are actively monitoring and analyzing these threats, showcasing a trend graph (such as those in other sections of this report) for mobile threats utilizing PWAs and WebAPKs is challenging. Unlike traditional apps, these malicious PWAs and WebAPKs are essentially phishing websites packaged to look like legitimate applications. This means that they do not exhibit the typical behaviors or characteristics associated with malware. Their ability to bypass traditional security warnings of a mobile operating system, and total sidestepping of app store vetting processes is particularly concerning. Therefore, it is anticipated that more sophisticated and varied phishing campaigns utilizing PWAs and WebAPKs will emerge, unless mobile platforms change their approach towards them.

Difference between PWAs/WebAPKs and native apps

PWAs are basically local copies of web pages that function much like native apps, but are built using standard web technologies such as HTML, CSS, and JavaScript. They are cross-platform and can be installed directly from the browser, bypassing app stores and the vetting they perform. WebAPKs are a step further in this evolution. They are native Android applications generated from PWAs by the Chrome browser, appearing more legitimate because their icons lack the small, telltale, browser logo overlay typically found on PWA icons.

Comparison of icons of a legitimate app for a bank in Czechia (left), malicious WebAPK (middle), and malicious PWA (right)

The installation process does not require explicit permissions for third-party apps, and the apps themselves do not display the usual indicators of being untrusted. This makes it challenging for users to recognize these apps as malicious. Additionally, the seamless integration of these apps into the device's operating system enhances their apparent legitimacy, making it difficult to distinguish between genuine and malicious applications.

ESET telemetry detects the described attacks in Czechia, Hungary, Poland, and Georgia as Android/Spy.NGate (variants .A, .B, and .C) and Android/Spy.Banker (variants .CIC, .CLW, and .BWW).

EXPERT COMMENT

As cybercriminals continue to innovate, the use of PWAs and WebAPKs for malicious purposes is likely to increase. These technologies provide a convenient and effective means for attackers to distribute phishing applications without needing app store approvals. The cross-platform nature of PWAs also allows attackers to target a broader audience, making these types of attacks more scalable and versatile. Thankfully, existing tools and advice – such as installing apps only from official app stores and using a reputable security app – also apply to staying safe from this novel threat.

Lukáš Štefanko, ESET Senior Malware Researcher

Web threats Scams Deepfakes

Invest with the rich and famous, end up with Nomani

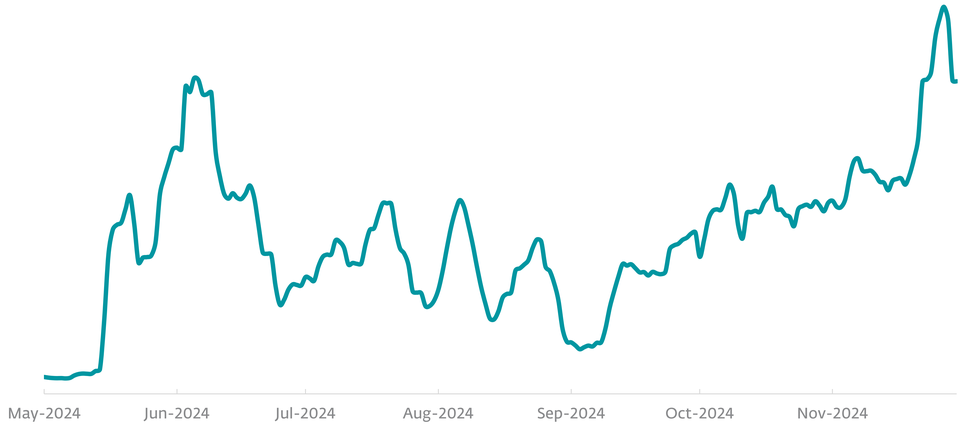
A new type of investment scam ads are filling social media news feeds, using deepfake videos and company-branded posts to lure victims, leading to financial harm and data loss.

In 2024, social media has been flooded with scam ads propagating "secret" investment opportunities, miraculous dietary supplements, and legal or law enforcement assistance. To make these offers appear credible, criminals abuse brands of local and global businesses or use AI-generated deepfake videos featuring famous personalities apparently guaranteeing the legitimacy of the advertised products.

The main goal of the fraudsters is to lead victims to phishing websites and forms that harvest their personal information. The contents of these websites – as with the bogus ads – visually imitate local news media; abuse logos, branding and colors of specific brands and organizations; or use a generic, financially themed visual with ever-changing names such as Quantum Bumex, Immediate Mator, or Bitcoin Trader.

ESET detects this threat as HTML/Nomani trojan – a name chosen by ESET detection engineers as a derivate of the English words "no money". According to our telemetry, HTML/Nomani initially spiked in May 2024 and grew by over 335% between H1 and H2 2024. In May to November 2024, ESET blocked over 8,500 domains and tens of thousands of attempts to access them. On average, our systems identify more than 100 such new URLs daily. Countries with the most H2 2024 detections are Japan (11.5%), Slovakia (11%), Canada and Spain (both 9%), and Czechia (7%).

Fake website promoting nonexistent investment product, detected as HTML/Nomani



Detection trend for HTML/Nomani from May 2024 to November 2024, seven-day moving average

Fraudsters use the data gathered from the phishing domains to directly call the victims and manipulate them into investing their money into fraudulent products that show phenomenal gains. Some victims are even tricked into taking out loans or installing remote access apps on their devices. When these victim "investors" request payout of the promised profits, the scammers force them to pay additional fees and to provide further personal information such as ID and credit card information. In the end, the fraudsters take both the money and data and disappear – following the typical pig butchering scam.

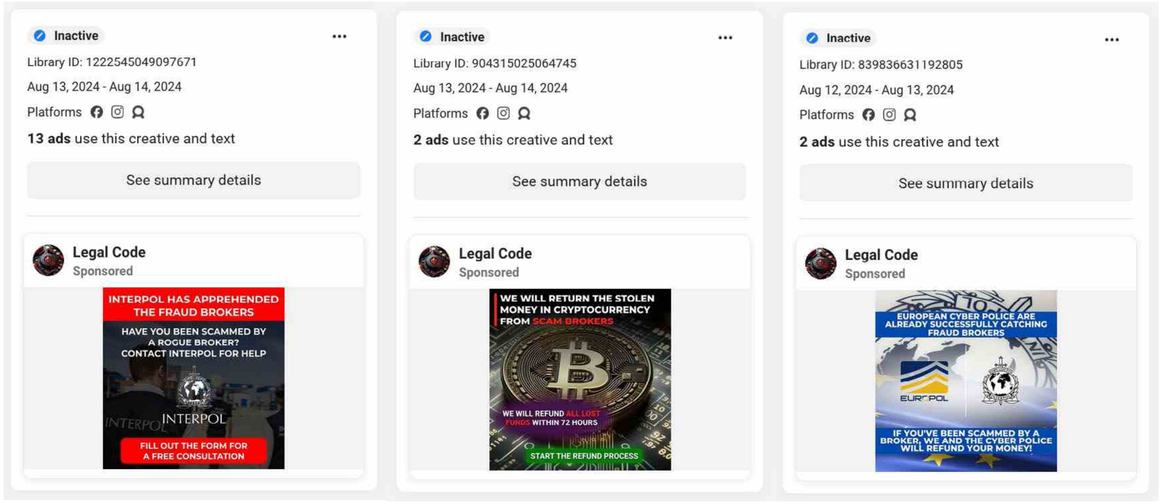
Localized, continuously updated content

An attentive viewer can identify Nomani-related ads based on several red flags. The videos in the ads are low-resolution – a "feature" masking the rendering glitches, making them harder to spot on small smartphone displays. The sentence structure is often odd, the breathing of the generated personality is unnatural, keywords are repeated annoyingly often, or the audio-video sync is poor. Yet in an era of declining attention span and an unfortunate habit to accept cookies, terms and conditions, and other prompts without reading them, the risk that users will click on these ads almost automatically is relatively high.

Analysis of several hundred of these fraudulent ads shows that the attackers use a highly localized version of the content for each country. In Slovakia, the current head of state, energy companies, or businesses such as ESET are among the top candidates to fake. In Germany, attackers put their money on the leader of the German political party Christian Democratic Union (CDU) or fake investments abusing the Lufthansa brand. In the US and Canada, most people have probably seen deepfakes of Elon Musk offering unique cryptoinvestment opportunities.

Ads on Meta; fake reviews on X, YouTube, and Google

The main distribution channels for these fake ads are Facebook and Instagram, but according to the ad details available via Meta Ad Library, many of the posts were also distributed via Messenger and Threads as well. X and YouTube were previously used primarily for fake reviews and deepfake video testimonials for the "investment platforms", but recently, fraudulent ads have been appearing on the video platform.



Examples of fraudulent Nomani ads as listed in the Meta Ad Library; ironically, the ads target people who have previously been scammed

Deceptively positive reviews are abundant – and ranking high – in Google search as well. We haven't seen this type of fraudulent content on TikTok.

To increase reach on Meta platforms, scammers use a mix of fake and stolen legitimate profiles to run the ads. The hacked accounts include pages of small businesses, governmental entities, and micro-influencers with tens of thousands of followers. One outlier spotted by ESET Research was an account of a popular actor with over 300,000 followers. According to the EU transparency info, it was controlled from dozens of countries and spreading hundreds of fake ads in different regions of Europe.

Another large group of accounts frequently spreading Nomani ads are newly created profiles with easy-to-forget names, a handful of followers, and very few posts. We've also documented a few duplicate or lightly altered versions of already existing accounts of legitimate companies or news media, typically abusing their official colors, logos, and even older social media content.

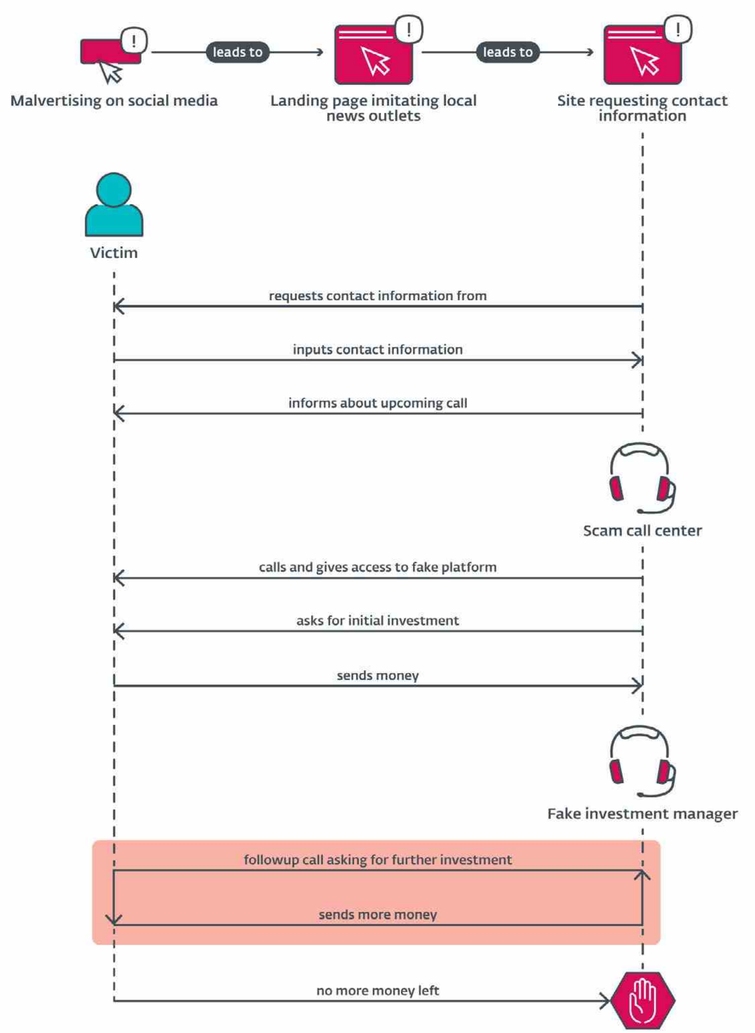
Division of labor(?)

After analyzing HTML/Nomani samples, there are several artifacts leading us to believe that the threat actors come from Russian-speaking countries. Many of the detected phishing websites – including investment, snake oil, legal, and other topics – shared templates and callbacks to the same Russian servers. The scripts

and code used in the pages contained comments in Cyrillic and used Yandex tools for visitor tracking. Some of the groups and actors involved in the scams were also seen using Telegram for coordination, which is typical – but not exclusive – for Russian-speaking cybercriminals.

HTML/Nomani scams show signs of labor division, with different groups being responsible for different parts of the attack chain. For example, one group manages the theft, creation, and (ab)use of Meta accounts and ads, while others build the phishing pages and fake investment platforms, run the call centers, or control the money laundering part of the operation. Distributed structure complicates tracking and attribution and limits the potential impact of any future law enforcement takedown.

In their public statements, several financial institutions confirmed that these types of manipulative attacks are on the rise or have already become the most frequent scenario. In other words, Nomani-style fraud is replacing "traditional" phishing scenarios, in which cybercriminals aim to steal victim's credentials and try to make the transactions themselves. By using social engineering techniques and building trust with the victims, scammers often outmaneuver even the authorization mechanisms and verification phone calls the banks use to prevent fraud.



Nomani scam overview

Web threats Scams Phishing

Online marketplace fraudsters diversify, scamming tourists via fake hotel bookings

H2 2024 gave rise to a new scam targeting users of popular accommodation booking platforms. The scammers use Telekopye, a toolkit originally developed to defraud people on online marketplaces.

Let's say you've just booked a winter holiday stay online. You're already counting down the days to your cozy retreat, when you get a message from the hotel. There's been a problem with your payment – you can resolve it at the link below. Suspicious? A little, but you click the link anyway to see what the issue is about.

The page that opens looks like the real deal: besides the expected website design, all your information is listed correctly, as well as the details of the booking you've made – including the amount to pay.

Filling out the payment form on the page seems like the reasonable thing to do – until the card details you put in get stolen by an organized scammer group.

Scam with a troubling twist

So, what exactly are we dealing with here?

ESET researchers have written extensively about scams plaguing online marketplaces, targeting buyers and sellers alike, using a "Swiss Army knife" scam toolkit named **Telekopye**.

In 2024, our researchers found that the groups running these scams have **expanded their playbook** with schemes targeting users of popular online platforms handling hotel and apartment reservations, such as Booking.com and Airbnb.

The new scam comes with a troubling twist: the information provided on the fraudulent payment pages matches real bookings made by the targeted users.

TELEKOPYE

- A toolkit operating as a Telegram bot enabling simple generation of phishing features, serving as a Swiss Army knife for turning online marketplace scams into an organized illicit business.
- Discovered by ESET Research in 2023 and in use since at least 2016, likely originating in Russia.
- Designed to target a large variety of online services in Europe and North America, with victims all over the world.

Mammoths: The scammers' name for targeted buyers and sellers.

Neanderthals: ESET Research name for the scammers – members of any Telegram group utilizing Telekopye.

Online marketplace scams come in two main scenarios – the scammers posing as sellers and (more commonly) as buyers. Both scenarios lead to a phishing web page mimicking a payment gateway.

Accommodation booking scams are the newest addition to the Telekopye scam repertoire.

To achieve this level of plausibility, scammers use compromised accounts of legitimate hotels and accommodation providers on the platforms, most likely accessed using purchased, stolen credentials. The scammers then single out users who recently booked a stay with that provider and haven't paid yet – or paid very recently – and contact them via in-platform chat. Depending on the platform and the victim's settings, this may also lead to the victim receiving an email or SMS from the booking platform.

As we tried to illustrate in the beginning of this article, this makes the scam much harder to spot. The information provided is personally relevant to the victims, arrives via the expected communication channel, and the linked, fake websites look as expected. So how can holiday goers recognize that they are being tricked before it's too late?

The devil's in the domains

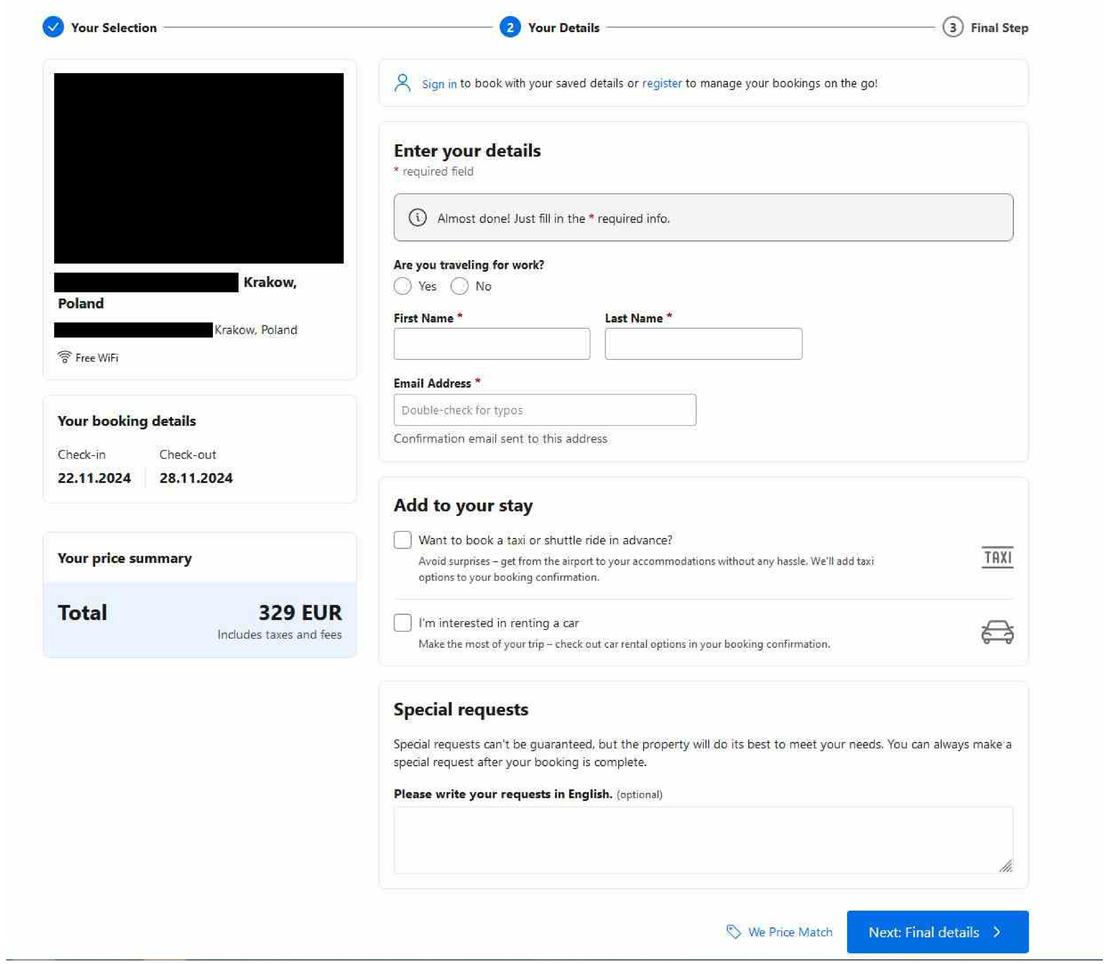
Very often, the only visible signs of something being amiss are domain names in the websites' URLs, which do not match those of the impersonated, legitimate websites. However, even here, the fraudsters put some effort into making the URLs appear legitimate – the name of the targeted platform is frequently used as a subdomain, with the actual domain name being something generic, seemingly representing the step in the payment process the victims are asked to complete. Examples of such URLs, impersonating Booking.com, seen in ESET telemetry include[1]:

- `https://booking.support-ticketapp[.]com/confirm/login`
- `https://booking.com-extra-check[.]quest/confirm/login`
- `https://booking.processord-user[.]com/order`

Were, say, Booking.com to create dedicated domains for such purposes, these would most likely be created as subdomains of their established domain, and be of the form `<task_name>.booking.com`, so in this case `support-ticketapp.booking.com`, `extra-check.booking.com`, etc.

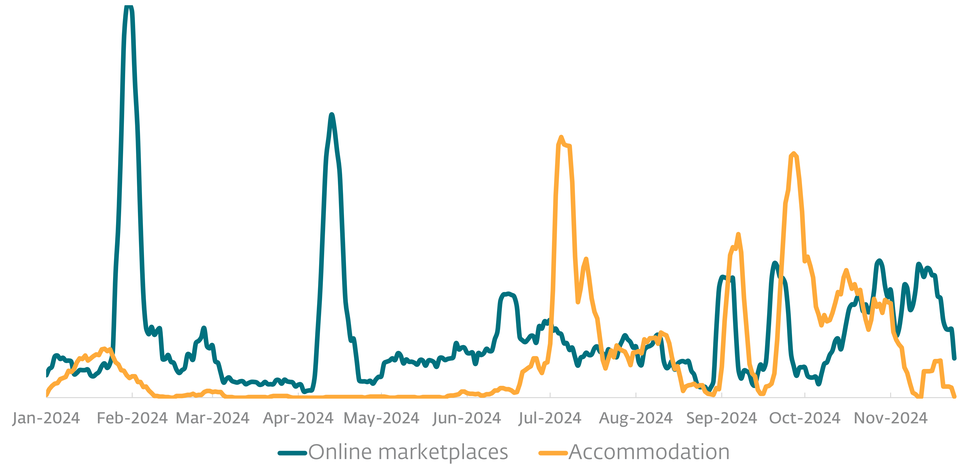
Once targeted users fill out the forms on the phishing pages, they are taken to the final step of the "booking" – a form requesting payment card information. Card details entered into the form are harvested by the scammers and used to steal money from the victims.

According to ESET telemetry, this type of scam started gaining traction in 2024. As seen in the trend chart, the accommodation-themed scams saw a sharp uptick in July, surpassing the original Telekopye online marketplace scams for the first time, with more than double the detections during that month. Another uptick was recorded in October. The detection peaks appear to be connected to busier seasons for holiday booking, but we might also be looking at random increases in activity.



Example of a fake Booking.com form created by Telekopye, prefilled with real booking details

[1] The original URLs include unique alphanumeric identifiers for each target at the end of the URL path; these have been removed from the example URLs.



Types of online services targeted by Telekopye in 2024, seven-day moving average detection trend

EXPERT COMMENT

With this new booking scam, criminals using the Telekopye toolkit have managed to expand their well-established scam operation to a whole new sphere – potentially widening their victim pool.

Since the scammers already have their tried and true tools and processes readily available for use, we expect to see more of these scams in the future – and our trend data suggests that the targeting of accommodation booking platforms will grow more prevalent. Given how prolific these scammers are, and the relatively high sophistication of their tactics, awareness is crucial for staying safe.

It remains to be seen whether the recent changes to the Telegram policy[2] regarding cooperation with law enforcement will shake things up in any way for these scammer groups.

Radek Jizba, ESET Malware Researcher

How to stay safe

The best way to stay protected against scams driven by Telekopye is being aware of the scammers' tactics and exercising caution on the affected platforms.

- Before filling out any forms related to your booking, always make sure you haven't left the official website or app of the platform in question. Being directed to an external URL to proceed with your booking and payment is an indicator of a likely scam.
- Because this scam uses compromised client accounts (property owners) at accommodation booking services, contacting the property owners directly is not a reliable way of verifying the legitimacy of payment requests. When in doubt, contact the official customer support of the booking service provider you used for booking your stay (**Booking.com**, **Airbnb**) or report a security issue (**Booking.com**, **Airbnb**).
- To protect your account from compromise, whether you're booking accommodation or renting one out, use a strong password and enable two-factor authentication wherever available.

Besides knowing what red flags to pay attention to, we strongly recommend using a reputable antimalware solution on your device to step in if you do end up being lured to a phishing website.

To learn more about Telekopye and the modus operandi of the scammer groups using it, read our recent **white paper** on the topic.

[2] https://thehackernews.com/2024/09/telegram-agrees-to-share-user-data-with.html

Ransomware

The RaaS war has a clear winner: RansomHub

After LockBit's disruption in H1 2024, a struggle for the leading position in the ransomware-as-a-service market broke out, changing affiliations between criminal groups and sucking in new less-skilled players.

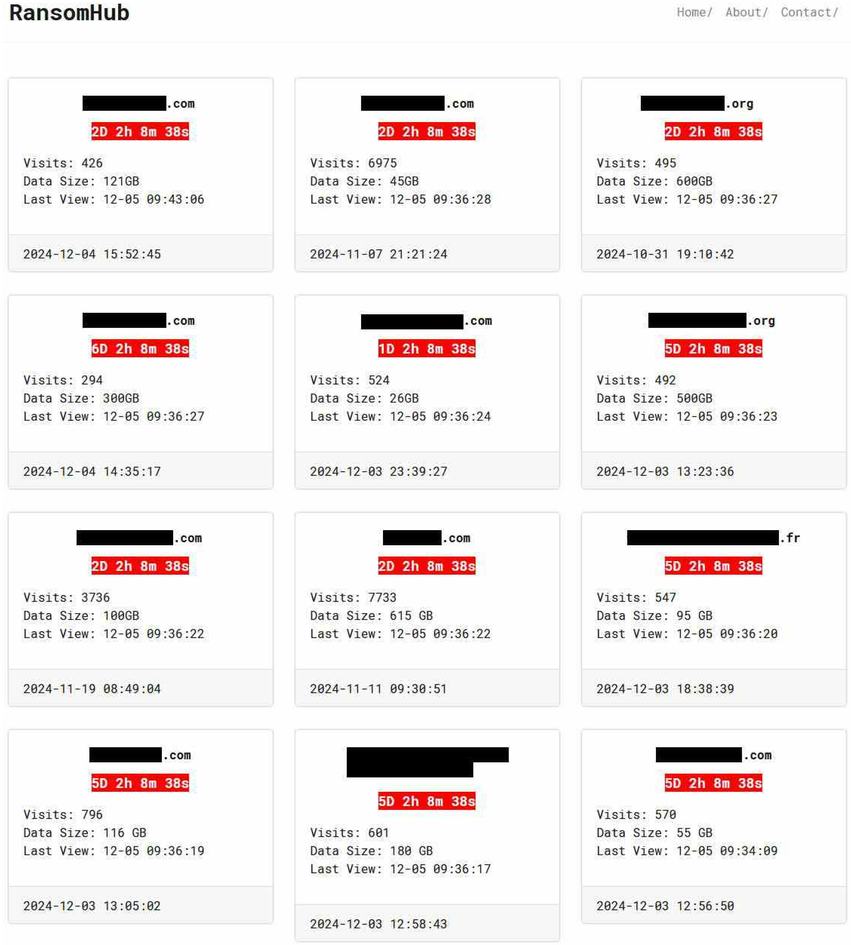
While H1 2024 was dominated by the news of Operation Cronos, which took down LockBit – the number one ransomware as a service (RaaS) on the market at the time – H2 2024 brought several follow-up actions by law enforcement. This included arrests of one developer, one bulletproof hosting admin, and two other people as well as the arrest of LockBit's cryptor specialist. On top of that, the FBI successfully recovered 7,000 decryption keys, making decryption possible for many victims.

The criminal gang behind LockBit didn't seem to want to give up so easily: it rebuilts its infrastructure and restarted its leak site. However, the gang's reputation and "business" relationships were disrupted to a point where it even resorted to posting fake victims on the leak site in an attempt to appear relevant.

The sudden swoop of the former top RaaS created a short-lived vacuum, one that many ransomware groups tried to fill. The most successful in this endeavor was RansomHub, occupying the prime spot among RaaS since July 2024. And if no dramatic event shakes up the landscape, this gang will also remain the leader until the end of the year.

RansomHub leading the pack

RansomHub is a relatively new RaaS; it was first spotted in February 2024 but quickly ranked among the most active groups. In the following six months, over 200 victims were listed on RansomHub's leak site and today the number is close to 500, which include such prominent brands such as Halliburton and Kawasaki Europe.



RansomHub leak site

Its main payload is written in Go, and targets both Linux and Windows systems. Like other advanced ransomware actors, RansomHub uses endpoint detection and response (EDR) killers to strip the targeted system of detection and protection capabilities. To achieve that goal, the gang either abuses legitimate tools designed to remove very low-level, persistent software, such as Kaspersky's antirootkit tool TDDSKiller, or uses malware of its own making, known as **EDRKillShifter**.

Considering the steep increase in activity of RansomHub and the ever-growing number of its victims, it is highly likely that this RaaS attracted the former top tier affiliates from the now disrupted LockBit and **defunct BlackCat** services. To establish its brand, we believe that RansomHub is also opening its doors to less-experienced ransomware players.

EXPERT COMMENT

In 2024, RansomHub has established itself as the leading RaaS group in the market, replacing the disrupted LockBit service. We expect RansomHub to stay in that position well into 2025. However, RaaS is a very competitive cybercriminal environment where gangs often come up with innovations and changes to their affiliate programs, trying to attract more partners and grow in profitability. If some of the competitors turn out to be more profitable, skilled affiliates may very well modify their alliances.

Jakub Souček, ESET Senior Malware Researcher

CosmicBeetle's fail, RansomHub's win?

One example of the latter is **CosmicBeetle** (also known as NONAME), a relatively low-skilled actor operating since 2020. According to ESET research observations, this group started its career by spreading the old Scarab ransomware but switched to its own Delphi-based, GUI-controlled ransomware ScRansom in 2023. Due to the combination of bugs in its code, manual control of the malware during an attack, and overcomplicated encryption routine, the success rate of the ScRansom malware has been severely limited.

Even in cases where CosmicBeetle was able to compromise interesting targets, the gang could not provide reliable decryption tools for the affected data. That was probably the reason why it attempted to polish its image by impersonating LockBit, both in ransom notes and by copying some of the victims and the design of its leak site.

The connection between RansomHub and CosmicBeetle popped up on our radar during an attack on an Indian manufacturing company in June 2024. In this instance, CosmicBeetle operators attempted to deploy their ScRansom, but were unsuccessful. Following this failure, they tried using various third-party EDR killing tools. When these attempts also proved futile, they went looking for other options and returned with RansomHub's EDR disabling tool and payload a few days later.

What was particularly noteworthy was the manual extraction of the EDR disabling tool from an archive stored in `C:\Users\Administrator\Music\1.0.8.zip`. This method is atypical for RansomHub affiliates but is a very common approach employed by CosmicBeetle.

Ransomware is typically the final payload preceded by other threats including phishing, exploitation, brute-force attacks, compromised credentials, downloaders, or custom malware. Many would-be ransomware attacks are caught early in the attack lifecycle. Only if attackers manage to circumvent their victims' defenses and finally attempt to deploy ransomware, will security products label these attacks as ransomware.

Embargo cutting its EDR killing teeth

Another emerging competitor in the RaaS space that caught the attention of ESET researchers in H2 2024 is the **Embargo group**. It was first observed in June 2024 and following the growing trend on the ransomware scene, it is writing its tools in Rust.

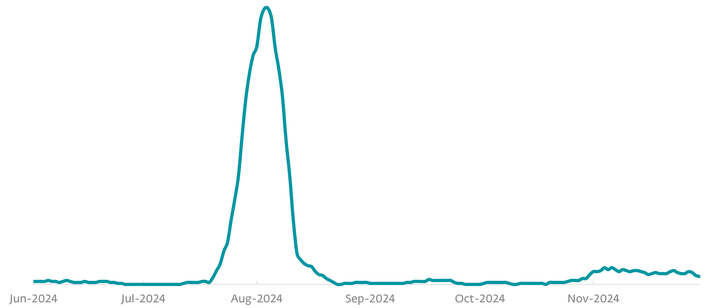
The main toolkit consists of a loader we have named MDeployer, and another EDR killer named MS4Killer. The latter is especially noteworthy, as it is custom compiled for each victim's environment, targeting only the installed security solutions. To assure that MS4Killer can terminate security-related processes running in the kernel, Embargo uses a technique known as bring your own vulnerable driver (BYVOD).

What makes Embargo stand out is its operators' ability of quickly modify their tooling – even during an active intrusion. This was demonstrated by Embargo using several variants of MDeployer in the same incident, probably replacing earlier, buggy versions that failed to fulfill the original goal.

Magniber wave hits end users, not business

As for ESET telemetry, ransomware detections in H2 2024 have globally decreased by over 23% compared to H1 2024.

We also observed an unusual uptick in activity in July and August 2024, when Magniber ransomware ran a **campaign** aiming to extort thousands of dollars from end users instead of larger sums from companies. This is not unprecedented, as other mass spreading attacks using CryptoWall, DejaVu (STOP), or LockBit built with the leaked builder appear regularly.



Win/Filecoder.Magniber spike in July and August 2024

What makes Magniber's campaign rather atypical is the scale and wide distribution of the attack, attempting to encrypt data of people worldwide, although although we have seen most detections in Poland, Slovakia, Taiwan, Hungary, and Czechia.

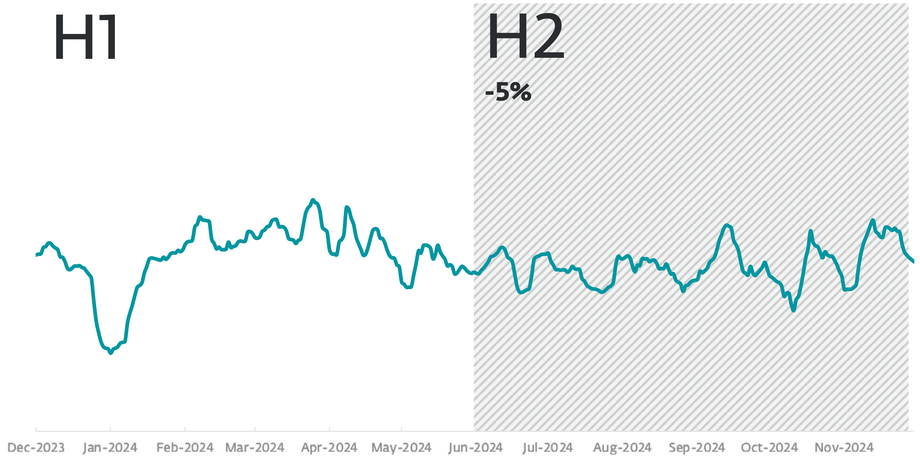
Ransomware schemes of APT groups

H2 2024 also produced more evidence that state-aligned cyberespionage groups are becoming more and more involved in ransomware attacks. Some deploy custom malware, such as the North Korean **Moonstone Sleet** with its FakePenny ransomware. Others, such as the China-aligned **ChamelGang**, utilize encrypting malware to distract from their covert operations.

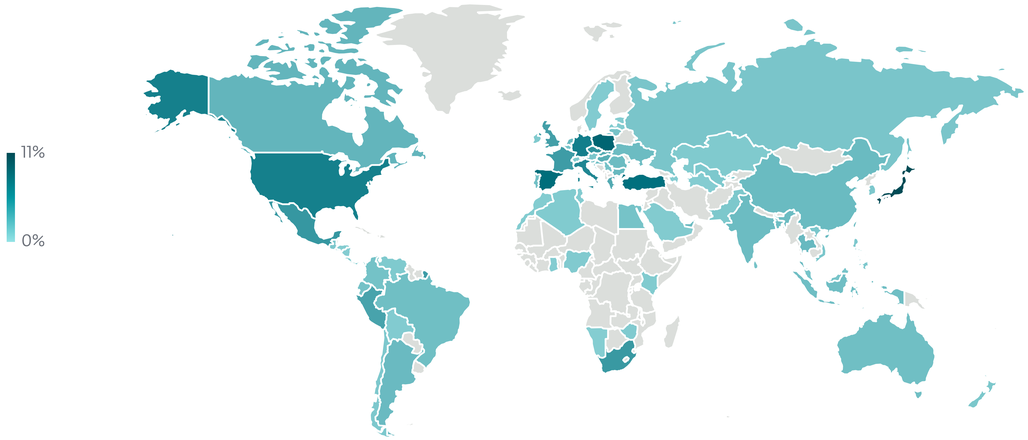
Then there are groups that want to make an "extra buck" on the side, one of them being Iran-aligned **Pioneer Kitten** that acted as initial access broker (IAB) and collaborated with several groups, including Ransomhouse as well as the now defunct NoEscape and BlackCat. North Korea-aligned **Andariel** is also suspected of providing initial access or affiliate services to the Play gang, as deployment of Play ransomware was spotted at a target previously compromised by Andariel. Interestingly, the Play gang officially denies operating as RaaS, making the connection to the North Korean actor appear at least as strange.

Threat telemetry

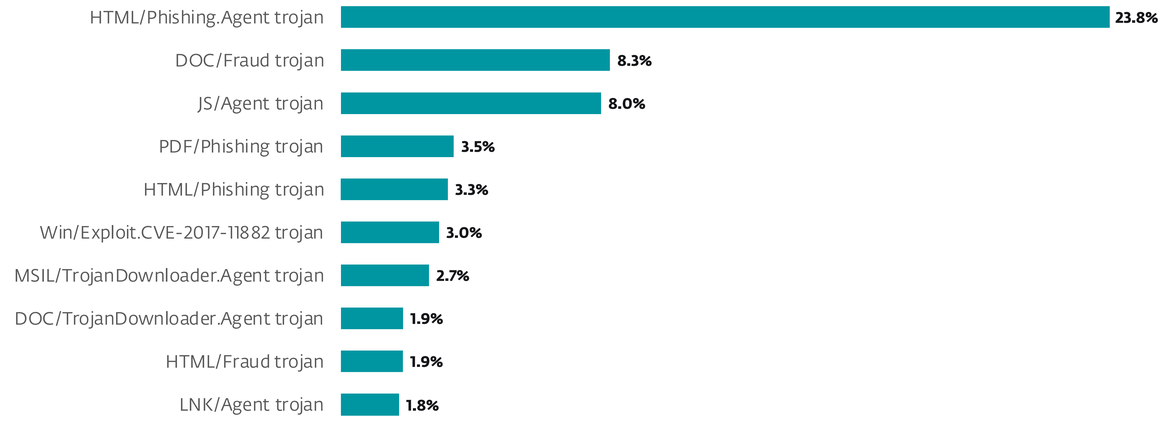
All threats



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

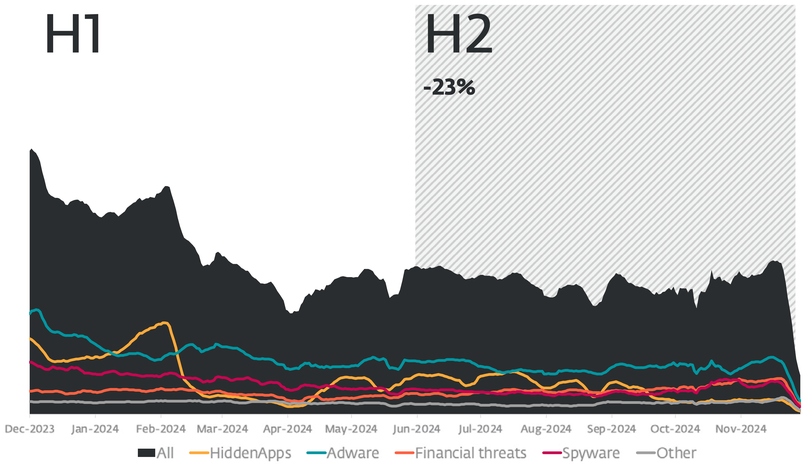


Geographic distribution of malware detections in H2 2024

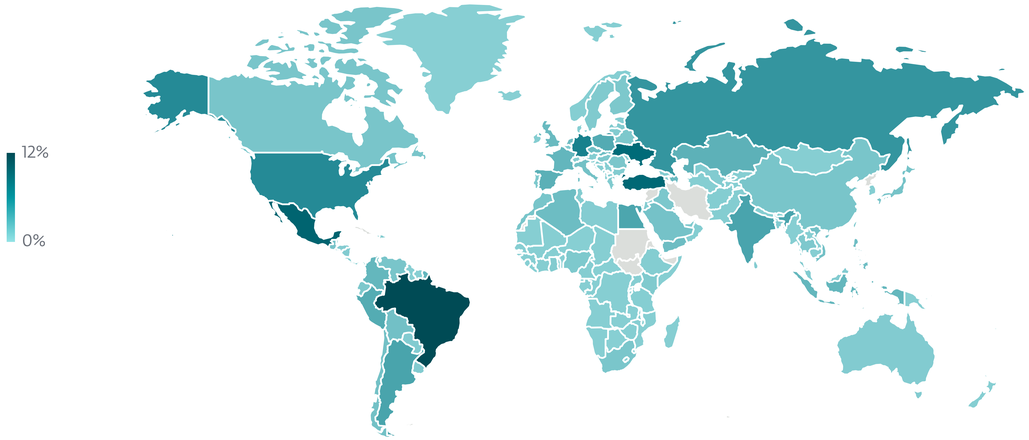


Top 10 malware detections in H2 2024 (% of malware detections)

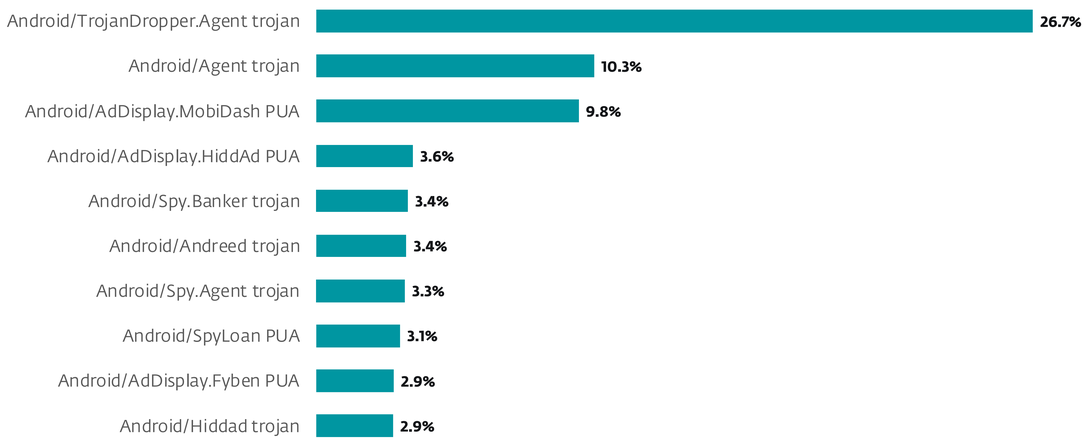
Android



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

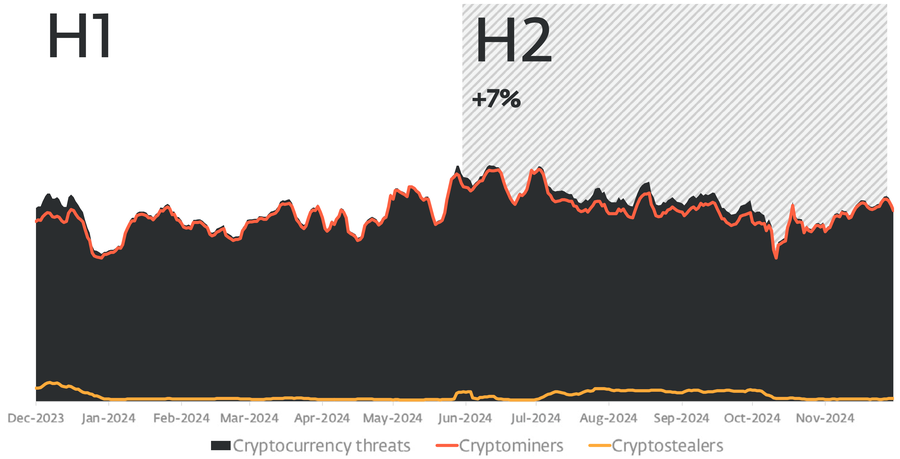


Geographic distribution of Android detections in H2 2024

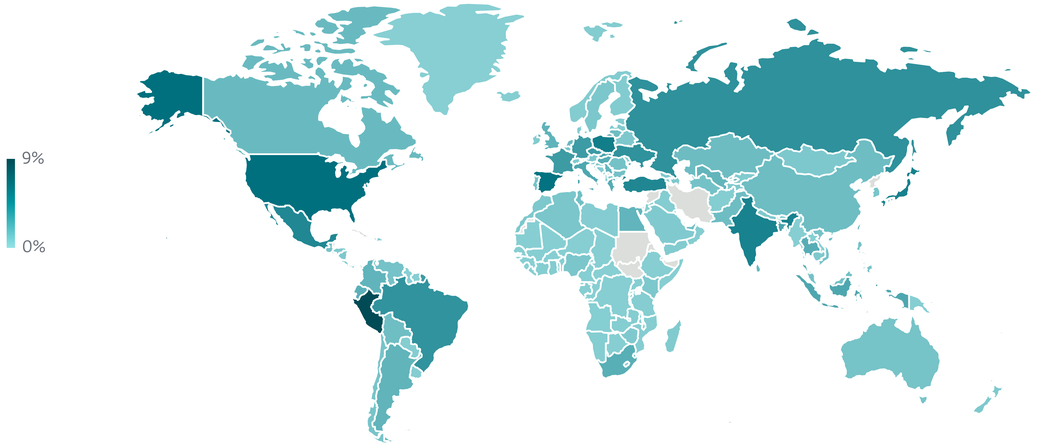


Top 10 Android detections in H2 2024 (% of Android detections)

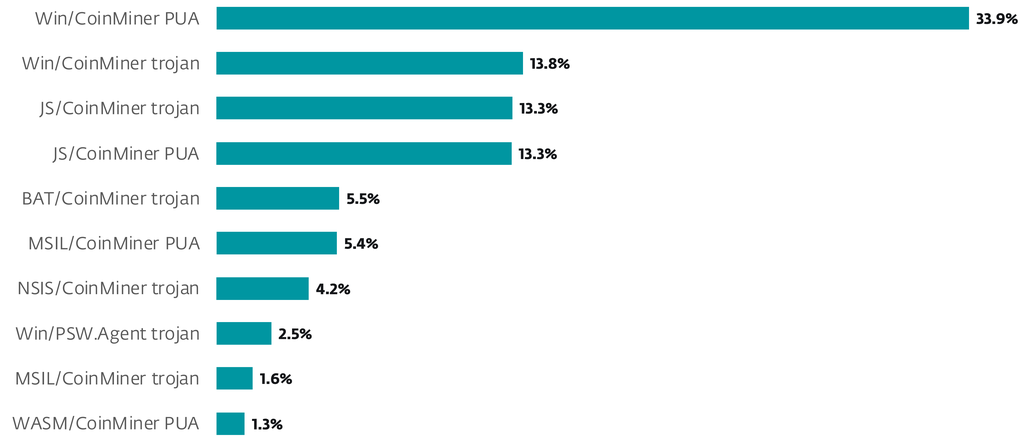
Cryptocurrency threats



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

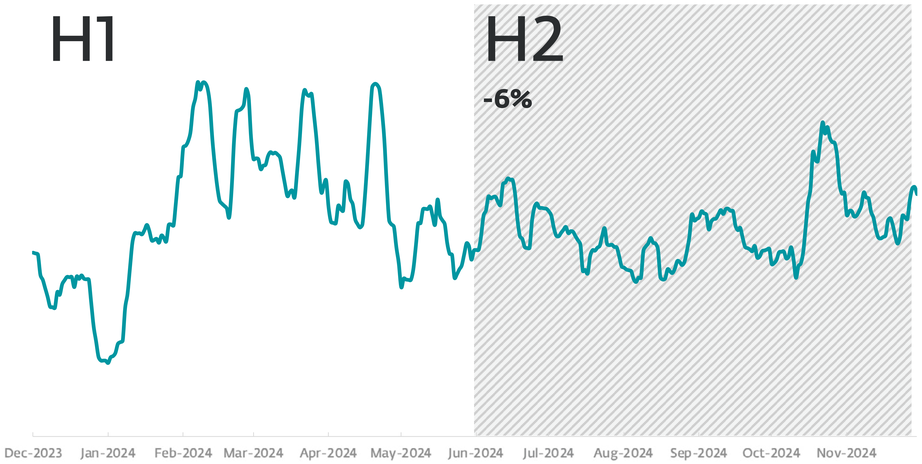


Geographic distribution of Cryptocurency threat detections in H2 2024

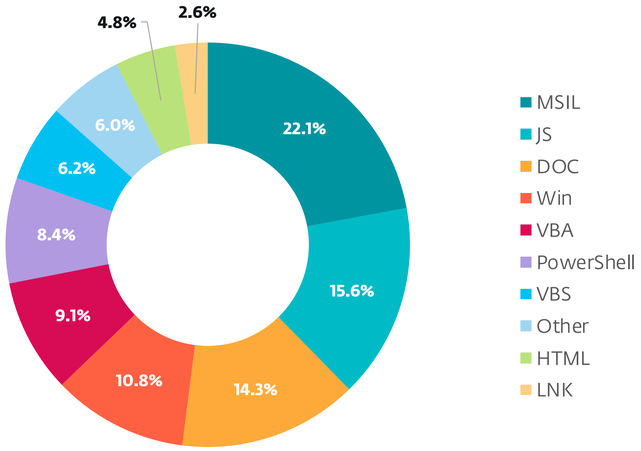


Top 10 Cryptocurrency threat detections in H2 2024 (% of Cryptocurrency threat detections)

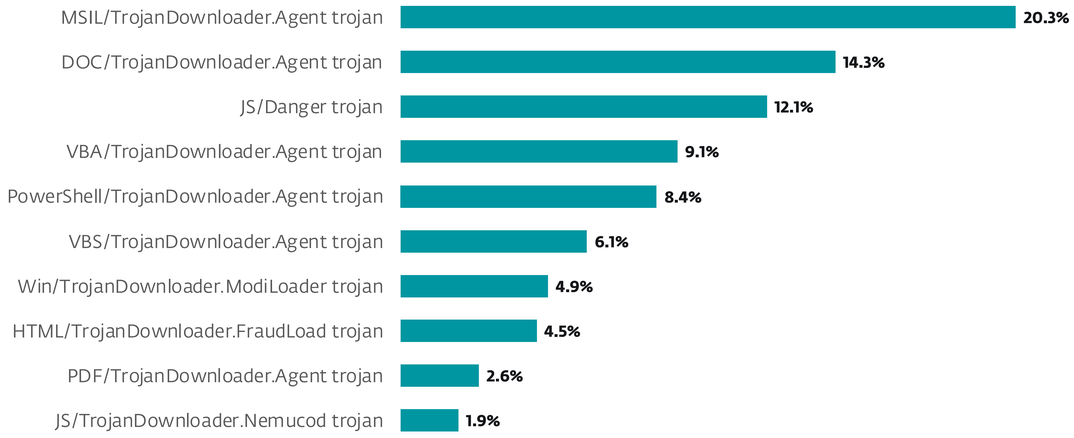
Downloaders



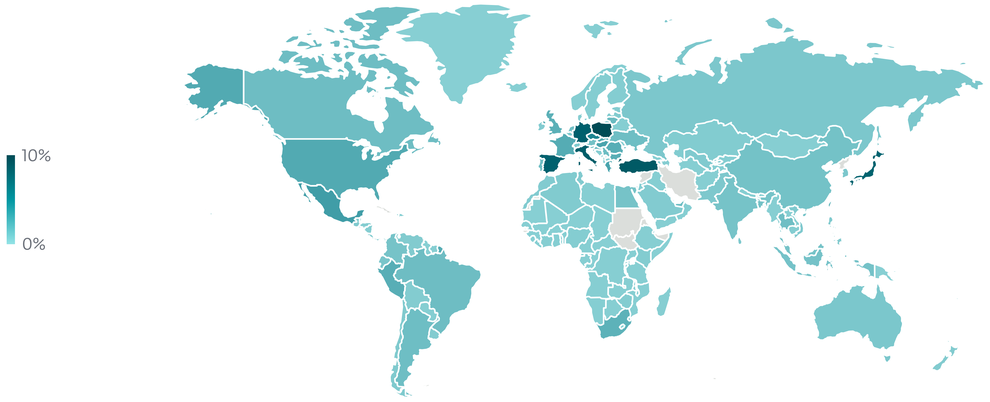
Downloader detection trend in H1 2024 and H2 2024, seven-day moving average



Downloader detections per detection type in H2 2024

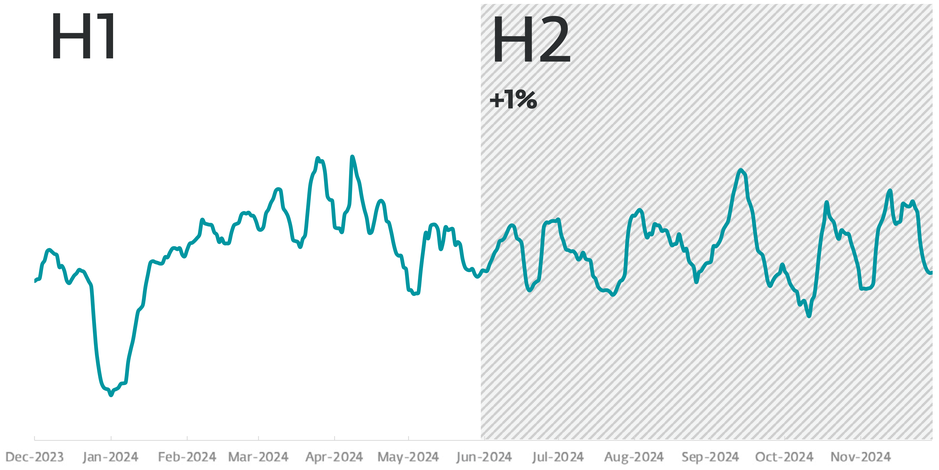


Top 10 Downloader detections in H2 2024 (% of Downloader detections)

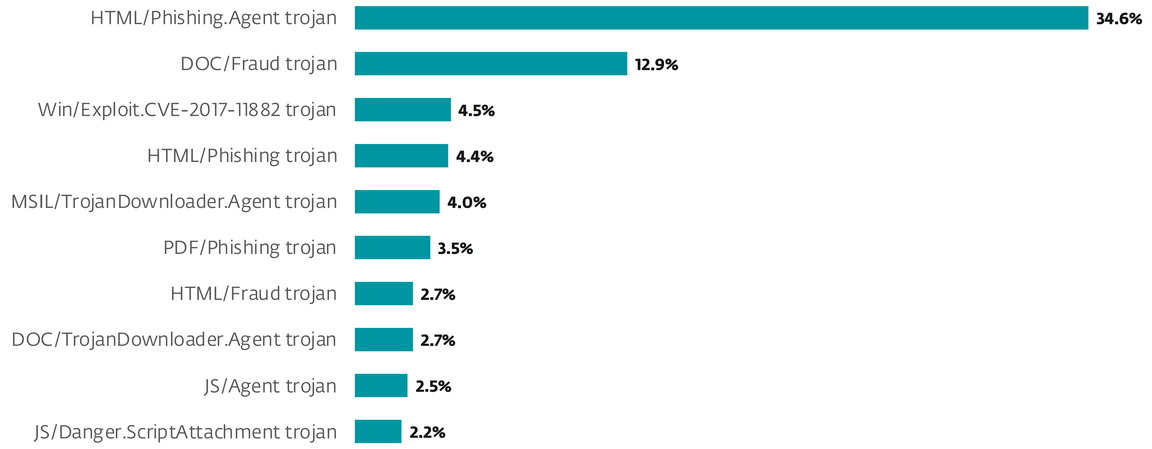


Geographic distribution of Downloader detections in H2 2024

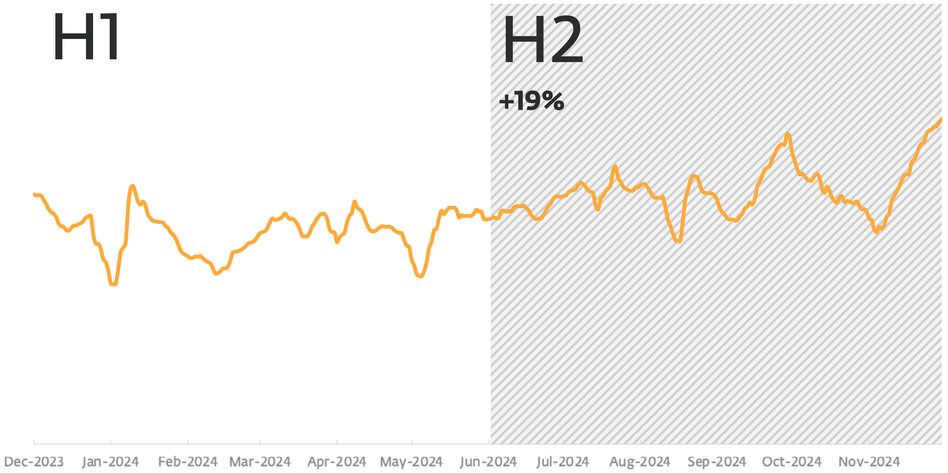
Email threats



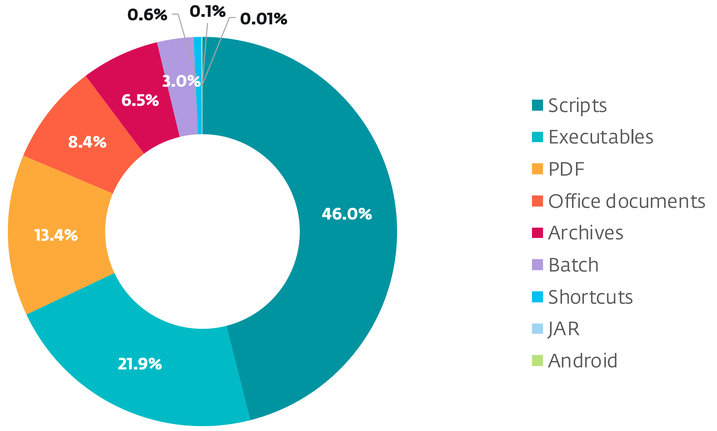
Malicious email detection trend in H1 2024 and H2 2024, seven-day moving average



Top 10 threats detected in emails in H2 2024

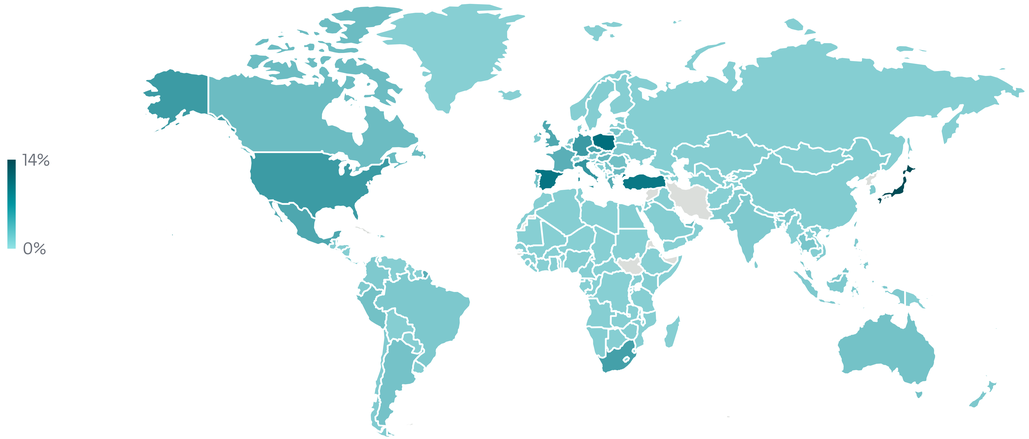


Spam detection trend in H1 2024 and H2 2024, seven-day moving average



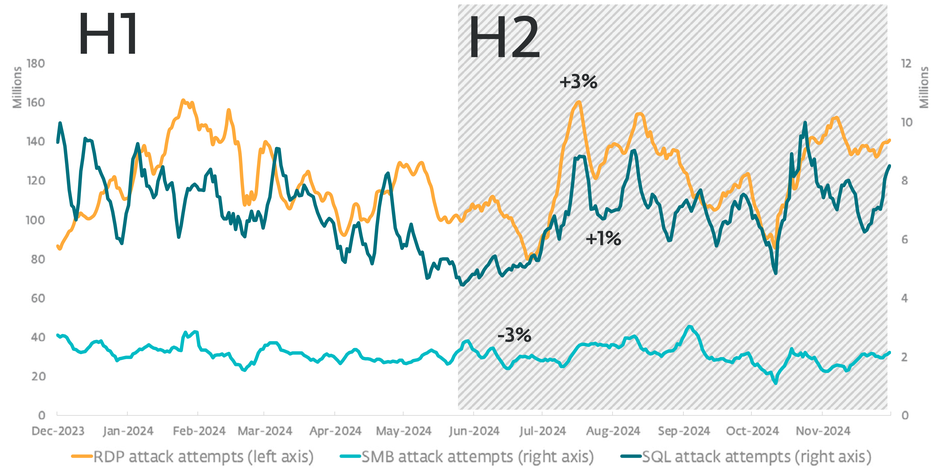
Top malicious email attachment types in H2 2024

Email threats

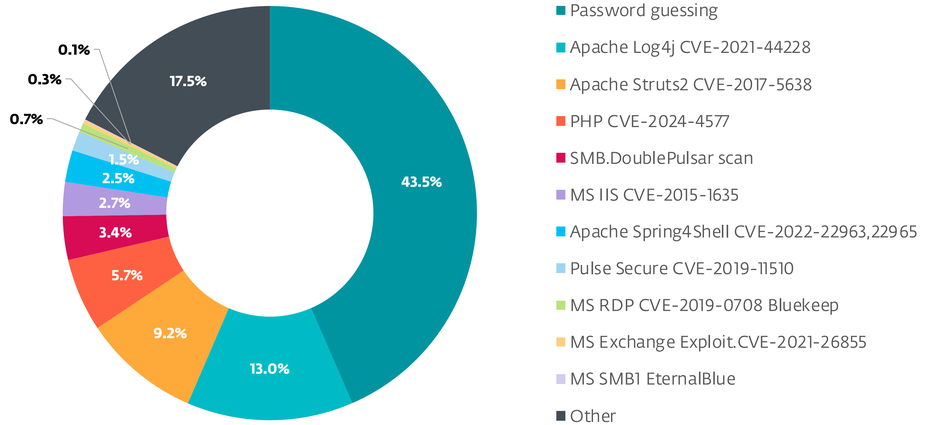


Geographic distribution of Email threat detections in H1 2024

Exploits

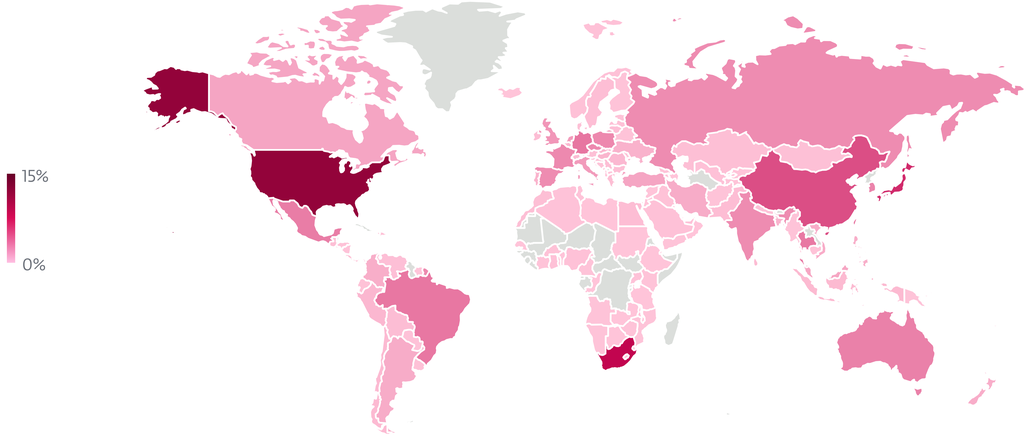


Trends of RDP, SMB, and SQL attack attempts in H1 2024 and H2 2024, seven-day moving average

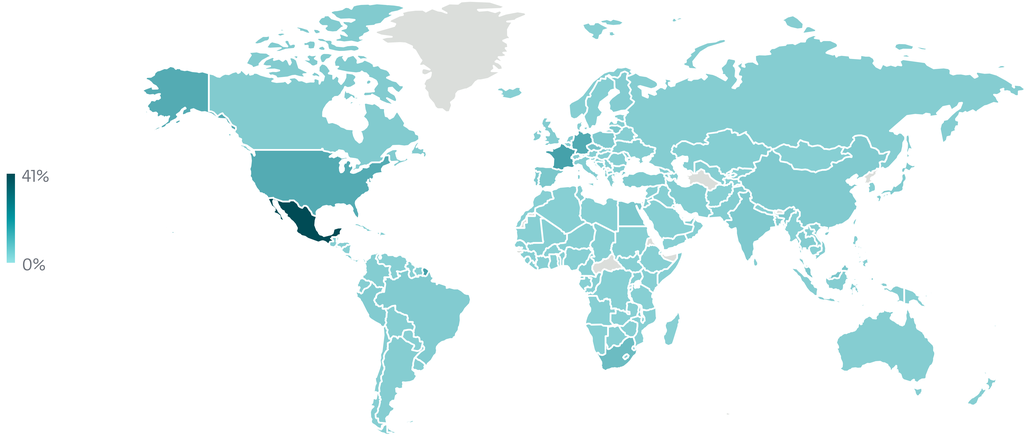


External network intrusion vectors reported by unique clients in H2 2024

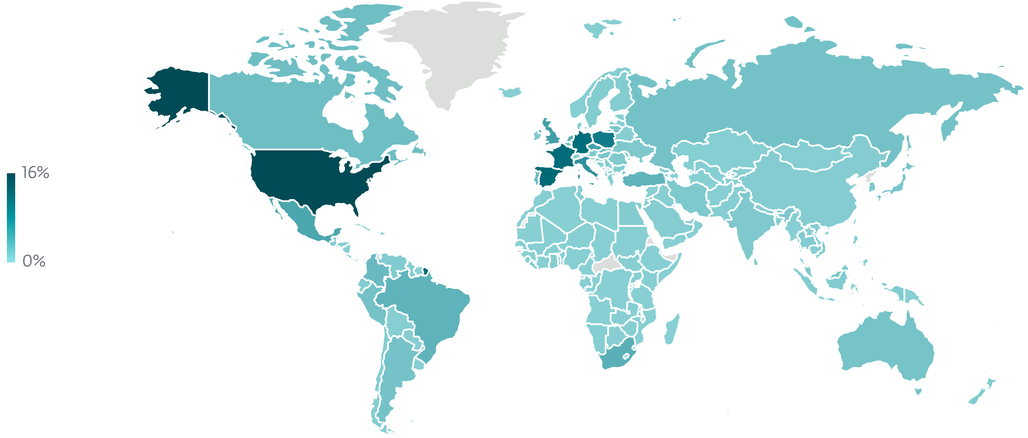
Exploits



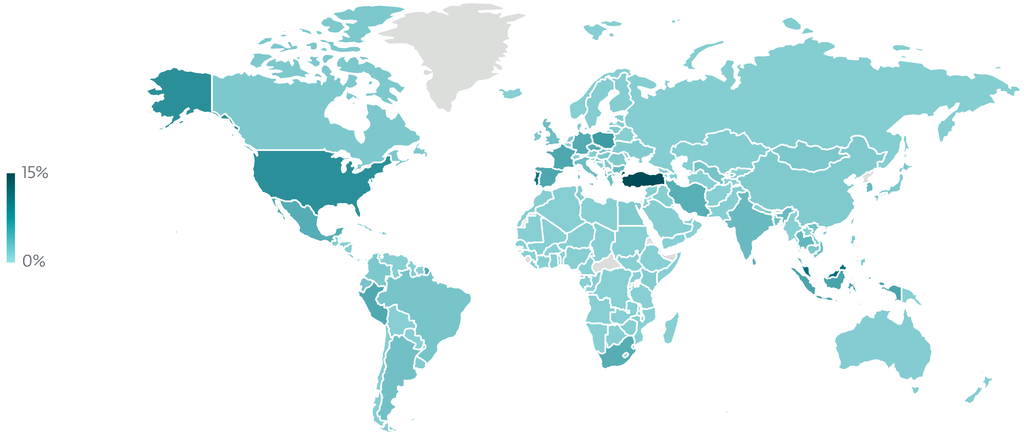
Geographic distribution of RDP password guessing attack attempt sources in H2 2024



Geographic distribution of SMB password guessing attack attempt targets in H2 2024

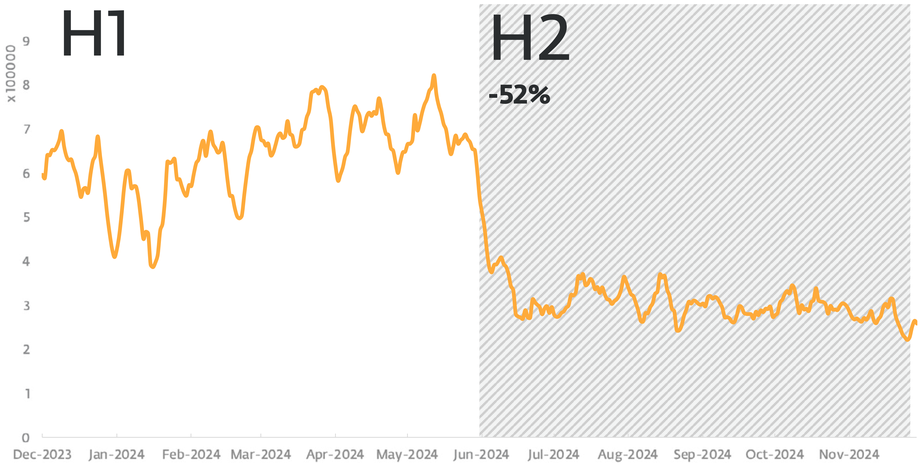


Geographic distribution of RDP password guessing attack attempt targets in H2 2024

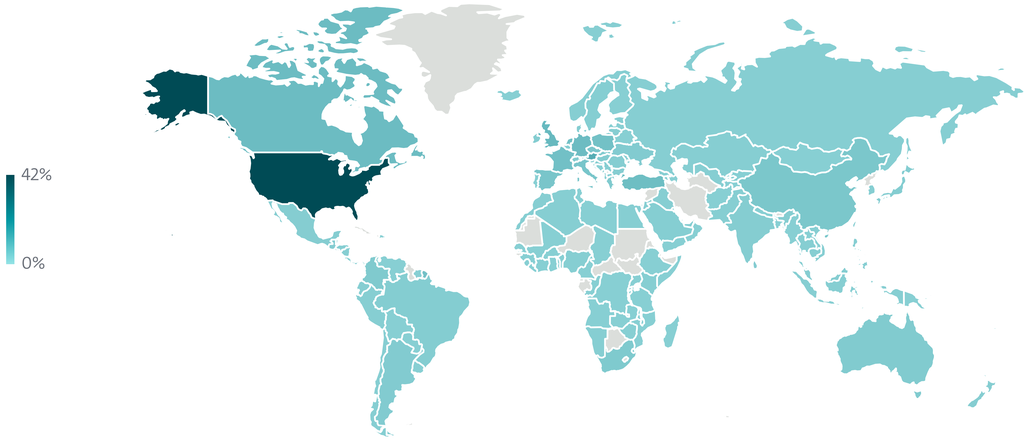


Geographic distribution of SQL password guessing attack attempt targets in H2 2024

Exploits

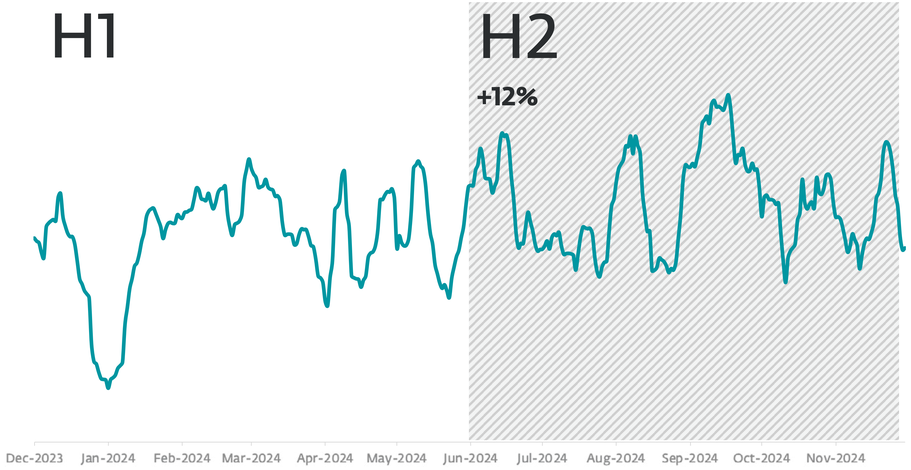


Detection trend of Log4Shell exploitation attempts in H1 2024 and H2 2024, seven-day moving average

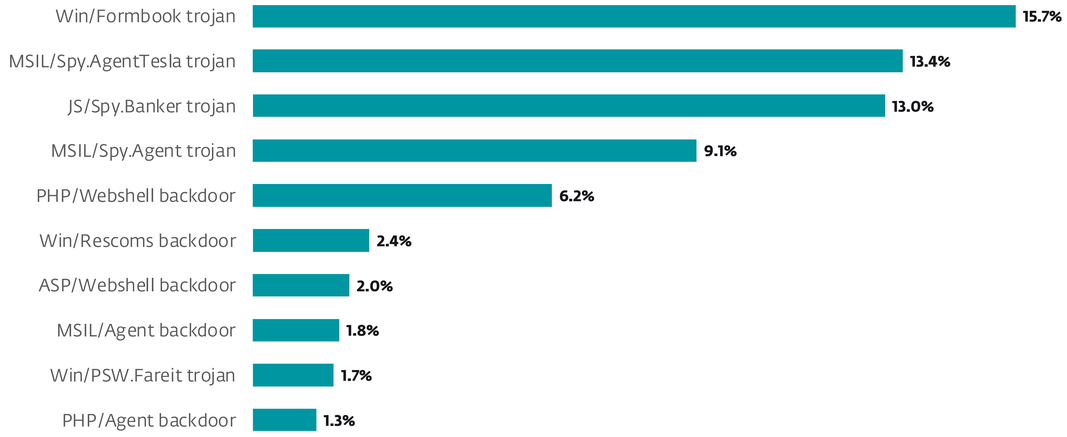


Geographic distribution of Log4Shell exploitation attempts in H2 2024

Infostealers

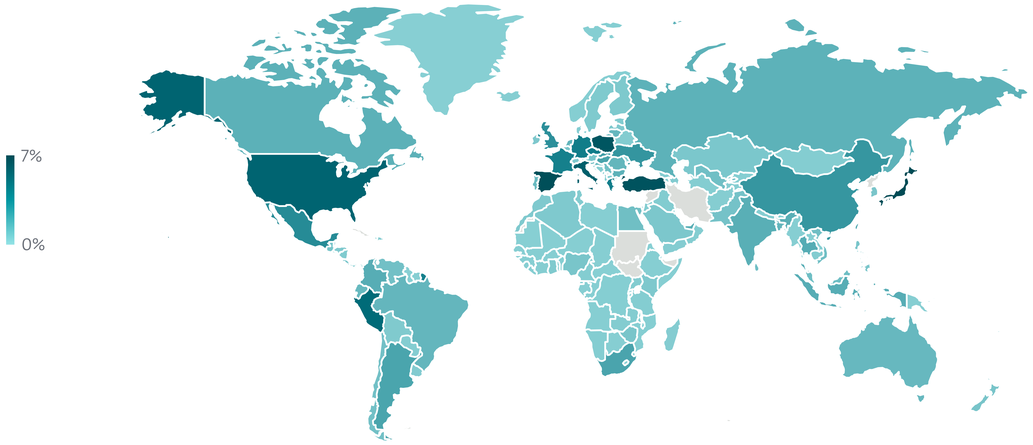


Infostealer detection trend in H1 2024 and H2 2024, seven-day moving average



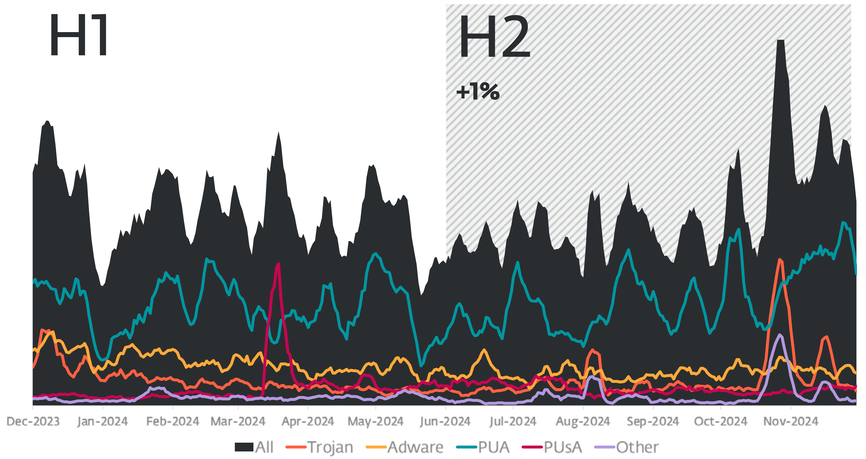
Top 10 Infostealer families in H2 2024 (% of Infostealer detections)

Infostealers

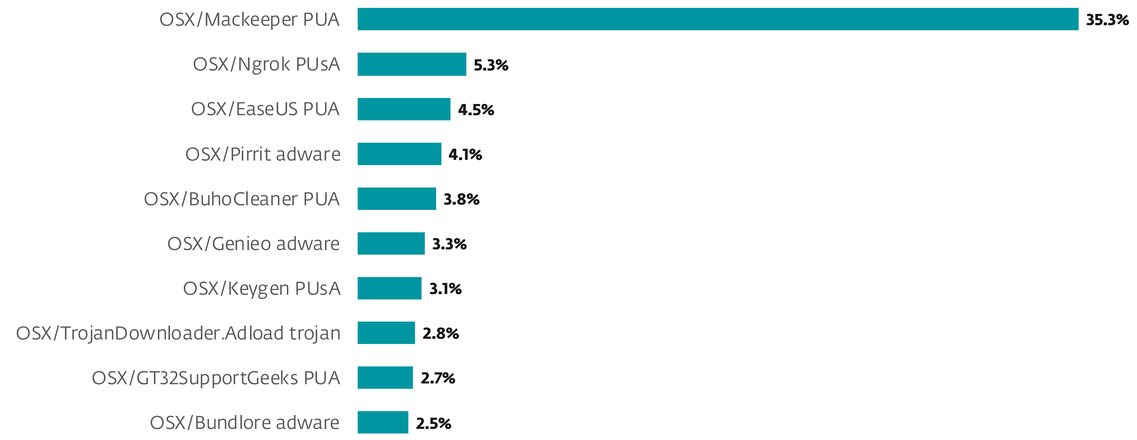


Geographic distribution of Infostealer detections in H2 2024

macOS

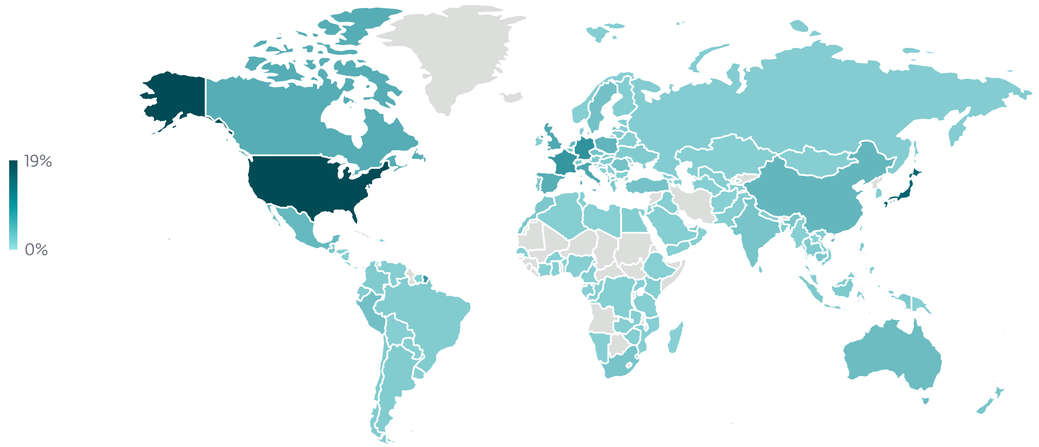


macOS detection trend in H1 2024 and H2 2024, seven-day moving average



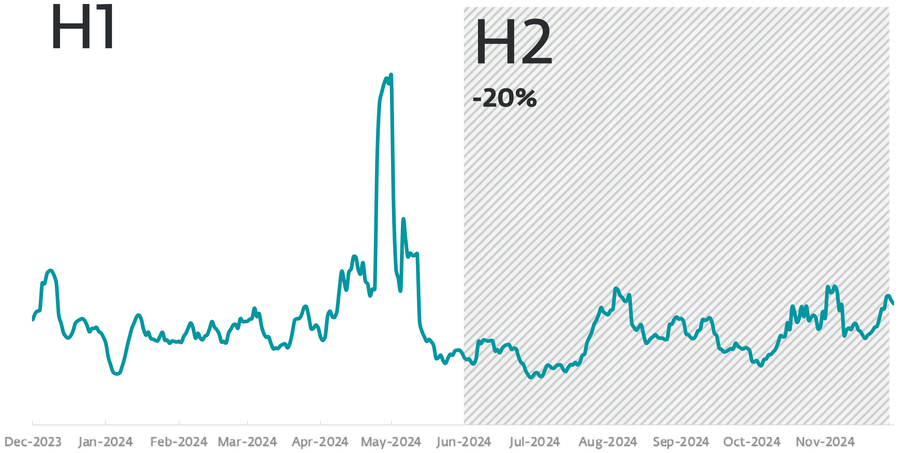
Top 10 macOS detections in H2 2024 (% of macOS detections)

macOS

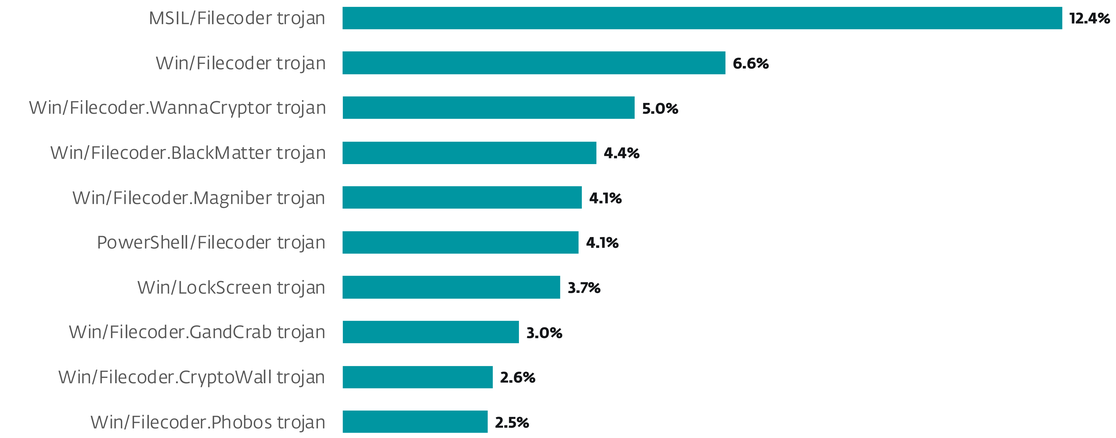


Geographic distribution of macOS detections in H2 2024

Ransomware

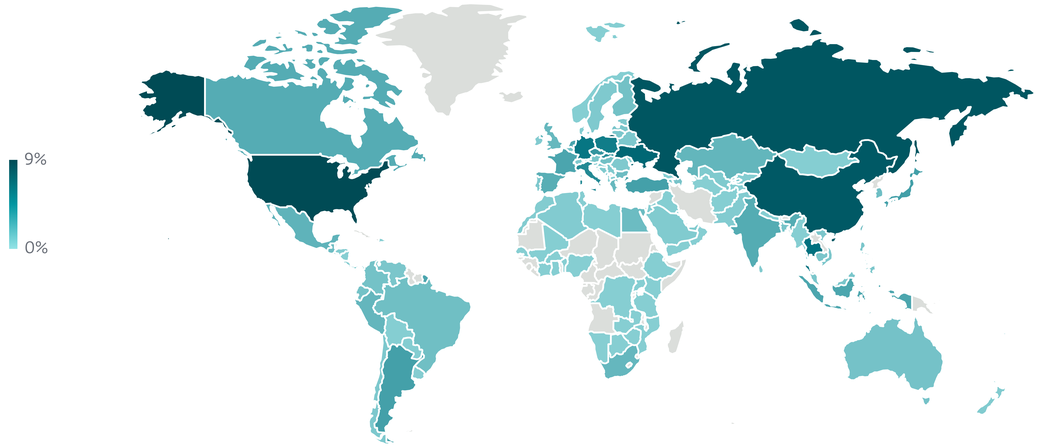


Ransomware detection trend in H1 2024 and H2 2024, seven-day moving average



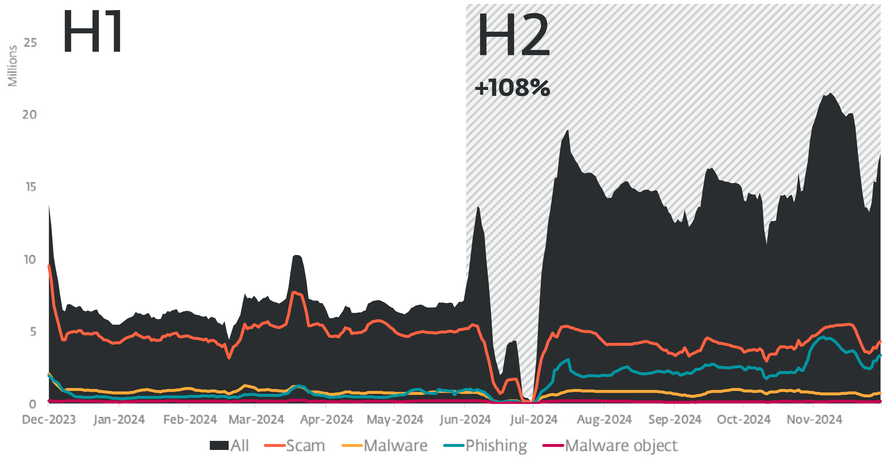
Top 10 Ransomware detections in H2 2024 (% of Ransomware detections)

Ransomware

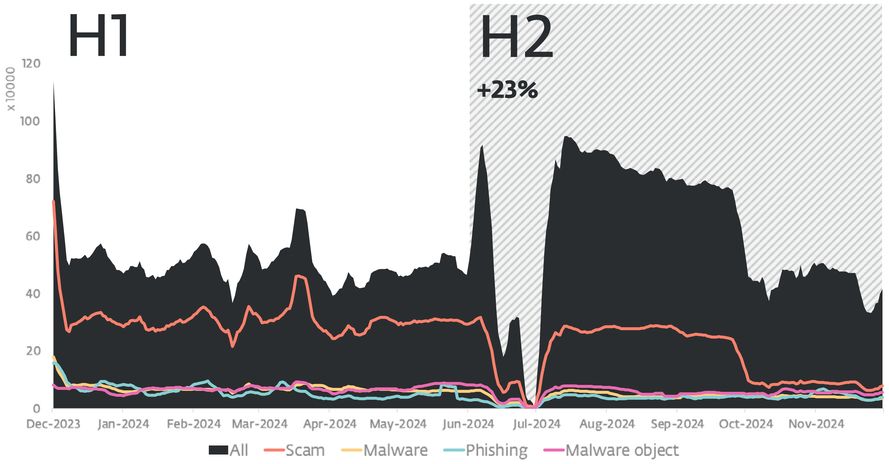


Geographic distribution of Ransomware detections in H2 2024

Web threats



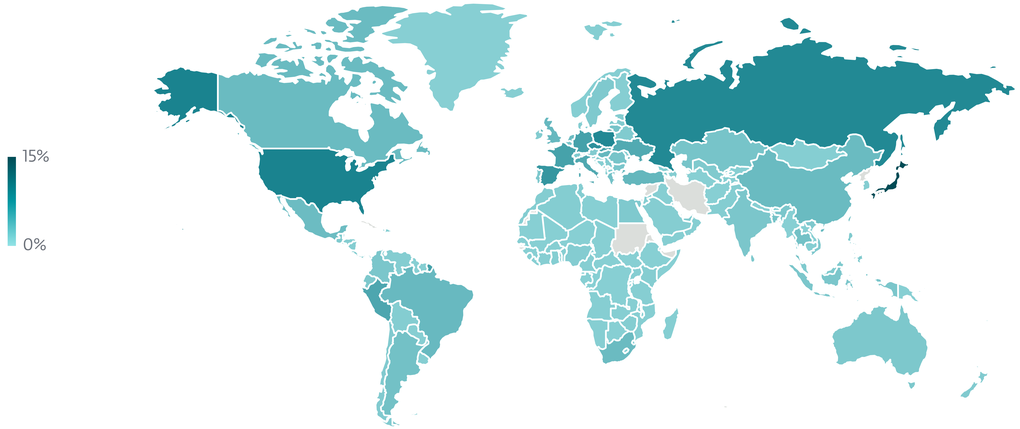
Web threat block trend in H1 2024 and H2 2024, seven-day moving average[3]



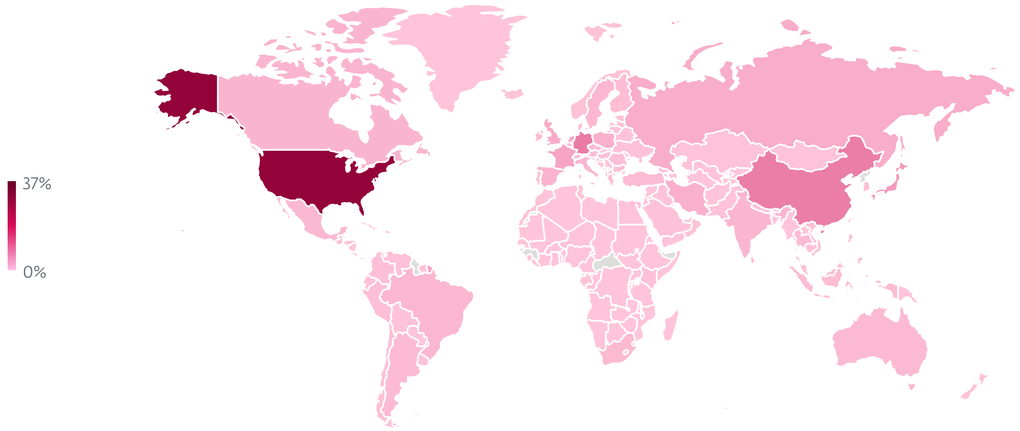
Unique URL block trend in H1 2024 and H2 2024, seven-day moving average[3]

[3] 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.

Web threats



Global distribution of Web threat blocks in H2 2024



Global distribution of blocked domain hosting in H2 2024

Research publications

Arid Viper poisons Android apps with AridSpy

ESET researchers discovered Arid Viper espionage campaigns spreading trojanized apps to Android users in Egypt and Palestine

The tap-estry of threats targeting Hamster Kombat players

ESET researchers have discovered threats abusing the success of the Hamster Kombat clicker game

Analysis of two arbitrary code execution vulnerabilities affecting WPS Office

Demystifying CVE-2024-7262 and CVE-2024-7263

ESET Research Podcast: APT Activity Report Q4 2023–Q1 2024

The I-SOON data leak confirms that this contractor is involved in cyberespionage for China, while Iran-aligned groups step up aggressive tactics following the Hamas-led attack on Israel in 2023

Phishing targeting Polish SMBs continues via ModiLoader

ESET researchers detected multiple, widespread phishing campaigns targeting SMBs in Poland during May 2024, distributing various malware families

ESET Research Podcast: HotPage

ESET researchers discuss HotPage, a recently discovered adware armed with a highest-privilege, yet vulnerable, Microsoft-signed driver

HotPage: Story of a signed, vulnerable, ad-injecting driver

A study of a sophisticated Chinese browser injector that leaves more doors open!

Be careful what you pwish for – Phishing in PWA applications

ESET analysts dissect a novel phishing method tailored to Android and iOS users

CosmicBeetle steps up: Probation period at RansomHub

CosmicBeetle, after improving its own ransomware, tries its luck as a RansomHub affiliate

Cursed tapes: Exploiting the EvilVideo vulnerability on Telegram for Android

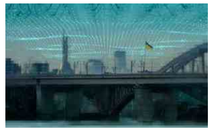
ESET researchers discovered a zero-day Telegram for Android exploit that allows sending malicious files disguised as videos

NGate Android malware relays NFC traffic to steal cash

Android malware discovered by ESET Research relays NFC data from victims' payment cards, via victims' mobile phones, to the device of a perpetrator waiting at an ATM

ESET Research Podcast: EvilVideo

ESET researchers discuss how they uncovered a zero-day Telegram for Android exploit that allowed attackers to send malicious files posing as videos



Cyberespionage the Gamaredon way: Analysis of toolset used to spy on Ukraine in 2022 and 2023

ESET Research has conducted a comprehensive technical analysis of Gamaredon's toolset used to conduct its cyberespionage activities focused in Ukraine

Separating the bee from the panda: CeranaKeeper making a beeline for Thailand

ESET Research details the tools and activities of a new China-aligned threat actor, CeranaKeeper, focusing on massive data exfiltration in Southeast Asia

Mind the (air) gap: GoldenJackal gooses government guardrails

ESET Research analyzed two separate toolsets for breaching air-gapped systems, used by a cyberespionage threat actor known as GoldenJackal

Telekopye transitions to targeting tourists via hotel booking scam

ESET Research shares new findings about Telekopye, a scam toolkit used to defraud people on online marketplaces, and newly on accommodation booking platforms

ESET Threat Report H1 2024

A view of the H1 2024 threat landscape as seen by ESET telemetry and from the perspective of ESET threat detection and research experts

ESET Research Podcast: CosmicBeetle

Learn how a rather clumsy cybercrime group wielding buggy malicious tools managed to compromise a number of SMBs in various parts of the world

CloudScout: Evasive Panda scouting cloud services

ESET researchers discovered a previously undocumented toolset used by Evasive Panda to access and retrieve data from cloud services

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

Following the takedown of RedLine Stealer by international authorities, ESET researchers are publicly releasing their research into the infostealer's backend modules

ESET Research Podcast: Gamaredon

ESET researchers introduce the Gamaredon APT group, detailing its typical modus operandi, unique victim profile, vast collection of tools and social engineering tactics, and even its estimated geolocation

ESET APT Activity Report Q2 2024–Q3 2024

An overview of the activities of selected APT groups investigated and analyzed by ESET Research in Q2 2024 and Q3 2024

Embargo ransomware: Rock'n'Rust

Novice ransomware group Embargo is testing and deploying a new Rust-based toolkit

Unveiling WolfsBane: Gelsemium's Linux counterpart to Gelsevirine

ESET researchers analyzed previously unknown Linux backdoors that are connected to known Windows malware used by the China-aligned Gelsemium group, and to Project Wood

RomCom exploits Firefox and Windows zero days in the wild

ESET Research details the analysis of a previously unknown vulnerability in Mozilla products exploited in the wild and another previously unknown Microsoft Windows vulnerability, combined in a zero-click exploit

Bootkitty: Analyzing the first UEFI bootkit for Linux

ESET researchers analyze the first UEFI bootkit designed for Linux systems

Credits

Team

Peter Stančík, Team Lead
Klára Kobáková, Managing Editor

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

Contributors

Alexandre Côté-Cyr
Dušan Lacika
Igor Kabina
Jakub Kaloč
Jakub Osmani
Jakub Souček
Jan Holman
Juraj Horňák
Lukáš Štefanko
Martin Jirkal
Michal Malík
Ondřej Novotný
Radek Jizba

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