Gen™

Q4/2024 Threat Report

The Dark Side of Social Media, CryptoCore Deepfakes Stole $7 Million, and More than 4 Million Users Protected from Scam-Yourself-Attacks

norton™ Avast™ LifeLock™ by norton Avira™ AVG™ REPUTATION DEFENDER™ by norton CCleaner

Table of Contents

Gen Threat Report

Q4/2024

All values are sum of monthly unique counts. Risk ratios values are monthly averages.

GLOBAL RISK RATIO

27.7%

-0.17% Q/Q change

BLOCKED ATTACKS

2.55B

-0.96% Q/Q change

BLOCKED URLS

388M

-12.7% Q/Q change

BLOCKED FILES

200M

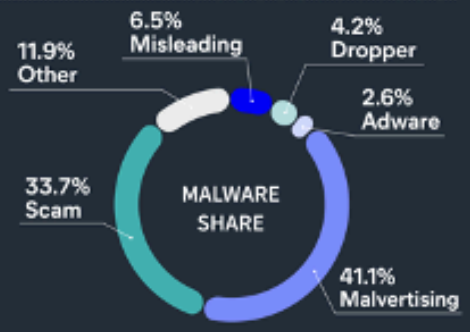
3.1% Q/Q change

AV SHIELDS BLOCKED ATTACKS

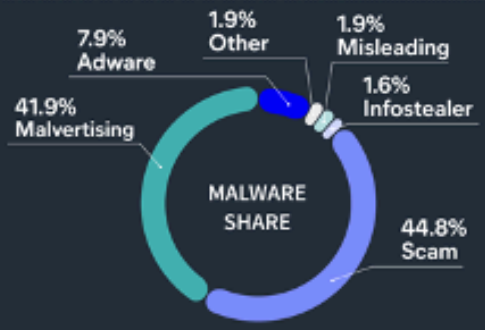
Web	File	Network	Mail	Behavioral	Script	Exploit	SMS Security	Other
2.3B	96M	75M	26M	21M	7.4M	5.4M	1.4M	0.2M

DESKTOP DEVICES

MALWARE TYPES	Risk ratio	Q/Q change
Malvertising	17.2%	30.2%
Scam	14.1%	-13.2%
Misleading	2.7%	37%
Dropper	1.8%	13.8%
Adware	1.1%	49.3%



MOBILE DEVICES



MALWARE TYPES	Risk ratio	Q/Q change
Scam	5.7%	-17.4%
Malvertising	5.3%	58.6%
Adware	1.0%	22%
Misleading	0.2%	50%
Infostealer	0.2%	5.3%

Foreword

The year is over, and we can confidently conclude that 2024 was record-breaking. In Q4 alone, **we successfully blocked 2.55 billion threats**—equivalent to **321 attacks every second.** This 9% increase compared to 2023. Social engineering threats, particularly scams, dominated the landscape, making up 86% of all attacks.

Some of you might recall what we mentioned back in 2021, when we launched this series: the threat landscape is highly dynamic and constantly evolving. At that time, we were witnessing one of the major shifts – the move beyond malware and attacks on devices (e.g., exploits, droppers, banking trojans) to more human-centric attacks. While malware threats remain as we enter 2025 and continue to require robust defenses, today's scam-related threats are far more dangerous, both technically and psychologically.

As we step into the new year, we see new threats on the horizon. Rapid advancements in AI and large language models (LLMs), such as OpenAI's Operator, capable of automating our daily online tasks (e.g., paying invoices, placing online orders), are being eyed by attackers as the next frontier. Imagine the risks when malicious actors attack or manipulate these AI agents. It's a shift that would redefine the threat landscape yet again.

But before we look forward, let's review the key developments in the final quarter of 2024. Our featured story, **The Dark Side of Social Media**, delves into how cybercriminals target billions of users across social platforms. Social media threats have evolved beyond traditional malware, with scams such as malvertising, fake e-shops, and phishing becoming prevalent. Facebook emerges as the dominant source of these attacks, followed by YouTube. We also showcase how each platform faces different types of threats, influenced by their unique purposes and user bases, with cybercriminals tailoring their tactics accordingly.

he social media threat landscape is closely linked to campaigns targeting personal data, which grew in complexity and scale in the last quarter. Campaigns like ClickFix and FakeCaptcha – what we call "Scam-Yourself Attacks" - continued to psychologically manipulate users. We safeguarded over 4.2 million unique users from FakeCaptcha scams alone, a staggering 130% increase compared to the previous quarter. To help protect people from this growing threat, we introduced a Clipboard Protection feature that blocks clipboard-based threats before execution.

The attackers linked to these scams deployed the NetSupport remote access trojan (RAT) with iterative improvements to its script, reportedly developed using AI tools like ChatGPT, highlighting the dual role of AI in cybersecurity.

While scams dominated the quarter, ransomware threats continued to escalate, with attacks surging by 50% in Q4/2024 building on a staggering 100% increase in Q3/2024. Magniber emerged as the most prevalent ransomware family, accounting for 62% of all detected cases. We observed notable increases in regions such as Mexico (+230%), Japan (+180%), and parts of Europe (e.g., Austria and France, both +100%). Furthermore, Advanced Persistent Threats (APTs) also remained a critical concern, as groups like Lazarus Group employed zero-day exploits and sophisticated social engineering tactics to steal sensitive information from high-value targets.

Financial threats demonstrated both persistence and innovation in the fourth quarter, with mobile banking trojans like DroidBot and ToxicPanda targeting EU users across advanced techniques such as NFC relay attacks and the disabling of system monitoring. The BankBot banker also saw a 236% increase in protected users compared to Q3/2024. In India, attackers used WhatsApp to distribute trojans disguised as utility payment apps. Unfortunately, they left the database unsecured, allowing access to thousands of stolen victim credentials. Spyware threats also surged, with SpyLoans campaigns causing spikes in several regions, despite law enforcement crackdowns. Furthermore, Crypto scams evolved further, with campaigns like CryptoCore leveraging high-profile events and deepfake technology to defraud victims of millions. The CryptoCore attackers targeted individuals through fake investment schemes tied to newsworthy subjects including the U.S. presidential election and Elon Musk announcements. These deepfakes and manipulated narratives enabled attackers to gain victims' trust and convince them to transfer funds. This marked the attackers' largest campaign to date, stealing over $7 million in Q4/2024 alone.

Scams remained widespread, demonstrating remarkable adaptability. Fake e-shops, for instance, were particularly active during Black Friday and Christmas, using poisoned search results, social media ads, and phishing emails to deceive shoppers. Beyond financial losses, these scams often led to compromised personal data, resulting in identity theft and financial fraud or long-term credit damage. Dating scams also gained momentum, particularly in Nordic countries, preying on individuals' emotions and trust. Meanwhile, technical support scams surged in localized areas, such as Switzerland and Japan, with attackers adjusting their methods to align with local preferences and contexts. Malvertising continued to serve as a major vector for scams and malware, comprising 41% of all blocked attacks this quarter, the largest share of any single threat type.

As we enter 2025, these findings highlight three critical areas that are evolving within the threat landscape: APTs and ransomware, scams and fraud, and attacks on AI systems and AI-driven attacks. Threat actors are constantly refining their tactics to exploit vulnerabilities, both human and technological, across each of these areas.

Wishing you an enjoyable read and a safe year ahead in 2025, with security both online and off.

Jakub Křoustek, Malware Research Director

Methodology

This report is structured into three main sections: Desktop-related threats, where we detail our intelligence on attacks targeting the Windows, Linux and Mac operating systems, specifically emphasizing web-related threats; and Mobile-related threats, where we describe the attacks focusing on Android and iOS operating systems.

We use the term “risk ratio” in this report to denote the severity of specific threats. It is calculated as a monthly average of the formula: “Number of attacked users / Number of active users in a given country.” Unless stated otherwise, risk ratios are only reported for countries with more than 10,000 active users per month.

A blocked attack is defined as a unique combination of a protected user and a blocked threat identifier within a specified time frame.

Our quarterly threat reports provide insights about the threat landscape as observed from the Gen family of Cyber Safety brands. We continuously improve our threat telemetry and anticipate further refinements in future reports.

Featured Story: The Dark Side of Social Media: Scams, Threats and Cybercrime

A closer look at how cybercriminals target billions of people through social media platforms

The world is evolving. Today's threats have moved beyond malware, with new forms of scams arising daily, plaguing our digital world and aiming to defraud unsuspecting victims. The days of trojans and worms being the biggest security concerns for people online are gone. Make no mistake, these threats still exist and we need to remain protected against them, but today's threats are far more dangerous, both technically and psychologically.

Adding to this complexity is the rise of Artificial Intelligence (AI), which has recently become a game-changer for cybercriminals. AI-powered tools allow scammers to create highly convincing and adaptive attacks, from deepfake videos and voice synthesis to personalized phishing messages crafted to deceive even the most cautious people. This technological edge makes today's scams much more effective and harder to detect than ever before.

One of the most dangerous playgrounds for today's cybercriminals is social media. It encompasses a wide range of platforms, including traditional social media, video-sharing platforms and messaging apps. These platforms serve different purposes, from connecting friends to sharing content, and their demographics vary significantly.

From a security perspective, it's not just the platforms' user content and functionality that make them unique, it's also the nature of the attacks they attract. Each platform's distinct features and audience shape the strategies cybercriminals use to exploit them. From phishing links on messaging apps to fake profiles on traditional social networks, the variety of scams reflects the diversity of the platforms themselves. In this article, we'll take a look at these threats, specifically pertaining to Facebook, YouTube, Instagram, TikTok, X, LinkedIn and Messenger platforms.

The Latest in Social Scamming

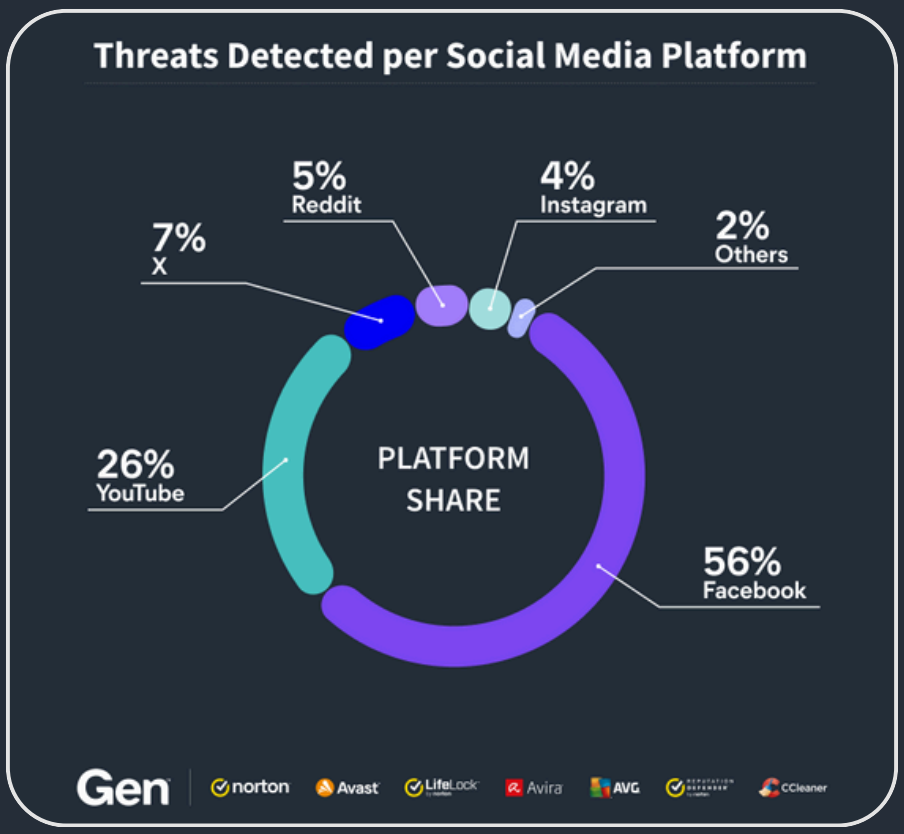
Scammers have found fertile ground in social media, exploiting their massive user bases and diverse functionalities to target unsuspecting individuals. One prominent example is the "TikTok Elon Musk Scam", where fraudsters impersonated the tech billionaire to promote fake cryptocurrency giveaways, enticing people to send funds with the promise of doubling their returns. Particularly, the sophistication of the impersonation made it effective, preying on Musk's real-world influence and TikTok's younger, tech-curious demographic. Meanwhile, fraudulent job offers have surged under the guise of "Part-Time Job Scams", luring individuals with promises of easy income, but ultimately compromising personal information or demanding upfront payments.

Another case, the "Skype Notification Scam", demonstrates how even old-fashioned messaging apps can lead people into costly traps, showcasing the many ways cybercriminals manipulate trust and digital habits. Additionally, phishing attacks often use social media to harvest account credentials, spreading malicious campaigns within the same ecosystem they exploit.

However, beyond the specific stories and articles discussing the general risks and threats in social media, many questions remain unanswered. What are the chances of encountering an attack on social media? Which platforms are the most "dangerous"? What are the actual types of threats we can find there? Our researchers set out to answer these questions.

Threats Across Social Media

When analyzing threats detected across social media platforms, Facebook emerges as the dominant source of detected threats, accounting for an alarming 56.19% of the total. YouTube follows with 25.92%, while platforms like X, Reddit, and Instagram contribute 6.91%, 4.65%, and 3.79%, respectively. The remaining threats are scattered across other platforms. This distribution highlights the disproportionate risk posed by some platforms due to their user base size, engagement patterns, and platform-specific characteristics.



Share of social media platforms where threats have been blocked

Interestingly, we have blocked six times more threats on Telegram than on WhatsApp, despite WhatsApp having a significantly larger user base. This aligns with previous observations, where scammers often redirect victims to continue conversations on Telegram, leveraging its unique features to further their schemes. The chart below provides a visualization of these figures, highlighting how cybercriminals capitalize on the distinct dynamics of each platform to target users effectively.

What are the threats that are targeting people on social media? There is a wide range, including:

1. Malvertising (26.95%): Cybercriminals spread malware or redirects users to malicious websites through deceptive online advertising. These ads often distribute harmful content disguised as legitimate advertisements.

2. **E-shop Scam** (23.47%): Attackers create fake online shops (e-shops) to trick users into making purchases. Victims either receive counterfeit goods or nothing at all, losing money and potentially exposing personal data.

3. **Phishing** (18.07%): Scammers use deceptive messages, emails or websites to steal sensitive information such as credit card numbers, banking credentials or passwords. These campaigns often mimic legitimate communications.

4. **Financial Scam** (10.68%): Attackers trick people into giving money or sensitive financial information. Common examples include fake investment opportunities and fraudulent loan offers.

5. **Generic Scam** (10.24%): This broad category includes scams where attackers aim to deceive victims into sharing personal information or money, without fitting into the more specific categories above.

6. **Tech Scam** (5.43%): Scammers impersonate legitimate technical support providers to gain access to victims' computers and data. These scams typically start with fake error messages or unsolicited calls offering help.

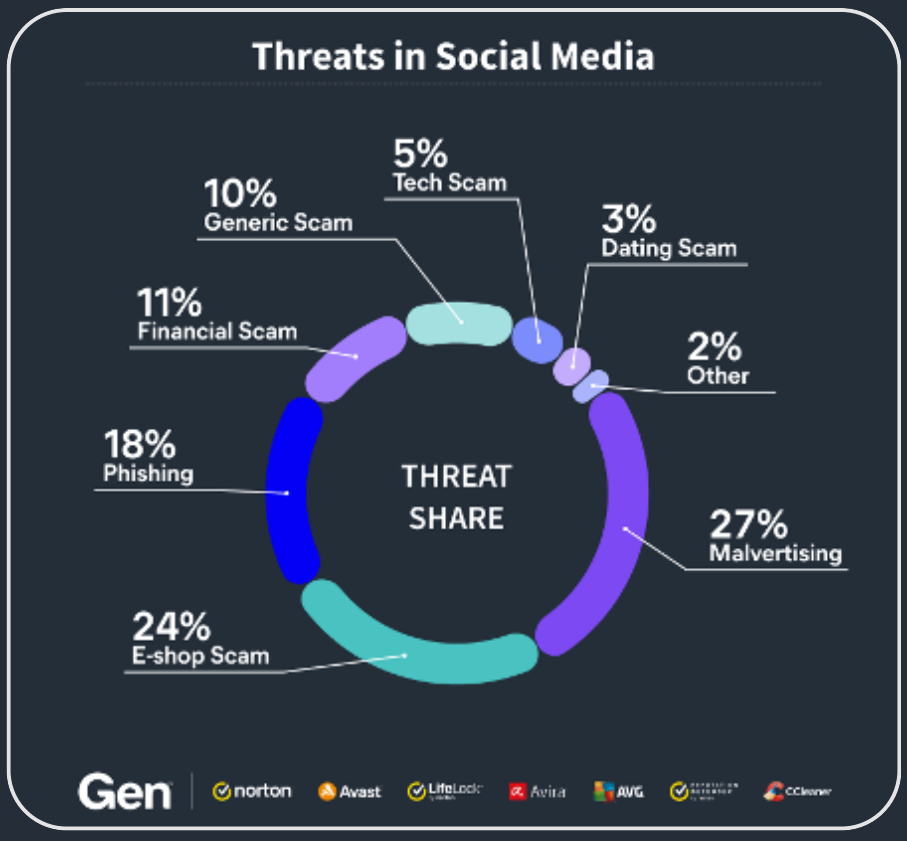
7. **Dating Scam** (2.93%): Cybercriminals establish fake romantic relationships to trick victims into sending money or sharing personal information, typically on dating platforms or social media using fake profiles.

8. **Others** (2.24%): A collection of less common, but still significant, threat types that exploit social media in various ways.

These figures show the diverse strategies used by cybercriminals to exploit users on social media. Malvertising remains the dominant threat at 26.95%, targeting large user bases with scalable attack methods within advertising ecosystems. E-shop scams, accounting for 23.47% of threats, reflect how attackers exploit shopping-centric platforms like Facebook and Instagram to take advantage of users' trust and urgency during transactions. Phishing, at 18.07%, continues to deceive unsuspecting users into revealing sensitive information through deceptive links and messages. Financial scams (10.68%) and generic scams (10.24%) demonstrate the diversity of tactics cybercriminals employ to target victims.

The last quarter of 2024 saw a spike in online shopping activity, and cybercriminals were quick to take advantage of the increased traffic. Platforms like Facebook and Instagram, which promote shopping through integrated features, saw a notable rise in e-shop scams during this period. The urgency of holiday deals and the allure of discounts create the perfect conditions for scammers to thrive.

Each platform is unique, with different types of users and content shared, reflected in the threats that are prevalent in each one. Let's take a closer look at the five social media with more threats detected.



Types of threats blocked on social media

Facebook

The high prevalence of e-shop scams on Facebook, accounting for 26% of all threats, contrasts sharply with their lower representation on other platforms. This is largely due to Facebook's Marketplace and its community-based interactions, which scammers exploit through fake listings and impersonated sellers. Unlike YouTube's ad-centric threats, Facebook's focus on local commerce and its older demographics makes it an ideal ground for e-shop scams, particularly targeting less tech-savvy users.

YouTube

Malvertising dominates YouTube, accounting for 54% of the platform's threats. This is driven by YouTube's platform's ad-based revenue model, which scammers exploit to deliver malicious ads to a vast, engaged audience. Unlike Instagram's visually curated content, YouTube's reliance on long video engagement provides more opportunities for malicious ads to appear, making it a prime target for malvertising campaigns.

X (formerly Twitter)

The overwhelming prevalence of generic scams on X, making up 62% of blocked attacks, reflects the platform's open nature and lack of stringent verification. Unlike Reddit's community-focused structure, X's fast-paced environment and trending hashtags provide scammers with the opportunity to inject fraudulent content, such as cryptocurrency giveaways and donation scams, into high-visibility discussions.

Reddit

Malvertising (66%) and phishing (29%) are the dominant threats on Reddit. Unlike Instagram's shopping-centric scams, Reddit's reliance on user-generated content creates opportunities for malicious actors to embed harmful links in posts and comments. The decentralized nature of Reddit communities amplifies these threats, as scammers target niche audiences with tailored phishing schemes.

Scam giveaway in X using Elon Musk as a lure

Instagram

E-shop scams dominate Instagram, accounting for 42% of threats on the platform. Unlike YouTube's ad-driven ecosystem, Instagram's visual-first design and integrated shopping features make it a prime target for scammers. The ability to create polished, fake product galleries and targeted ads enables fraudulent e-commerce to thrive on the platform, particularly during seasonal shopping periods like Q4.

Conclusion

Social media platforms have evolved into bustling hubs for interaction, commerce and entertainment. However, their growth has also created fertile ground for cybercriminals. The interplay platform-specific features and seasonal trends, such as Black Friday and Christmas shopping frenzies, highlights the adaptability of modern scams.

Looking ahead, the evolving nature of cybercrime on social media calls for innovative and adaptive approaches to security. As platforms integrate more features and users continue to share more of their lives online, finding the right balance between functionality and safety will be crucial. Only through collaboration between platforms, users and security experts can the growing tide of digital threats be effectively countered.

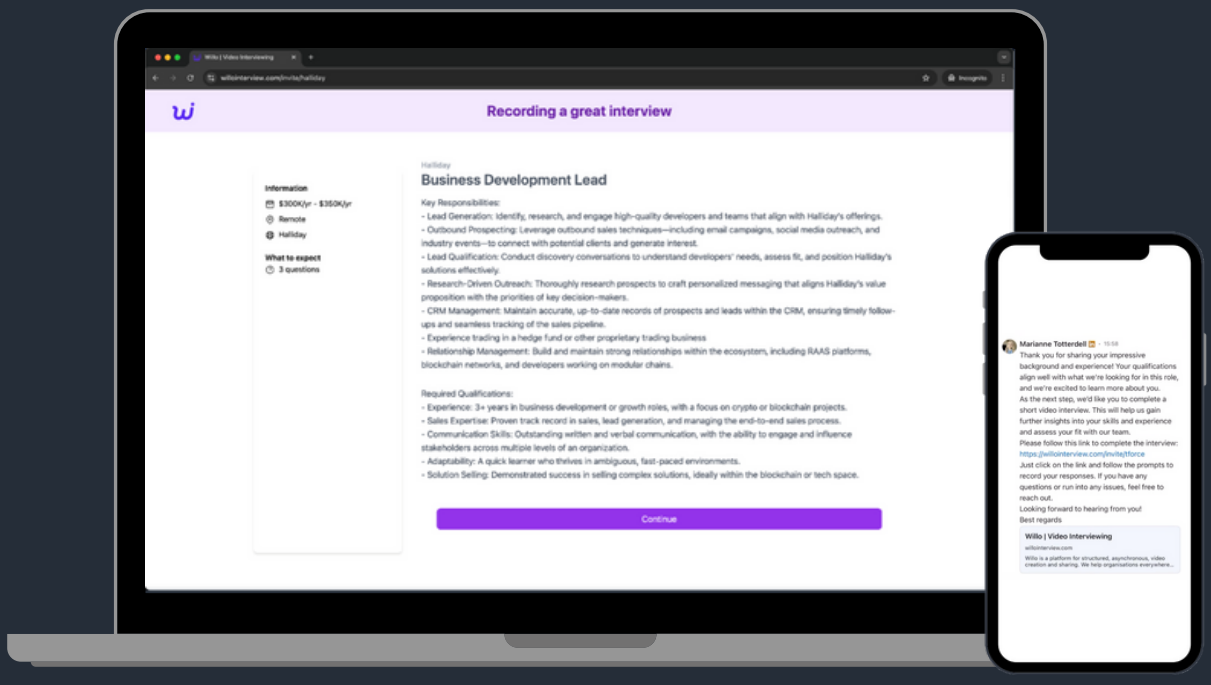
Luis Corrons, Security Evangelist
Patrik Holop, Researcher

Desktop-Related Threats

Advanced Persistent Threats (APTs): From Fake Interviews to Zero-Day Exploits

An Advanced Persistent Threat (APT) is a type of cyberattack that is conducted by highly skilled and determined hackers who have the resources and expertise to penetrate a target's network and maintain a long-term presence undetected.

This quarter, the Lazarus Group, a North Korean advanced persistent threat (APT) actor, continued their stream of attacks by integrating both established and novel malware into its infection chains. In Q4/2024, the group continued to target individuals using compromised archive files masquerading as skill assessment tests for IT professionals, spread by Lazarus through LinkedIn messages. Additionally, Lazarus continues to abuse GitHub repositories to deliver JavaScript-based infostealers and leverage zero-day vulnerabilities to deploy the next stage of the attack chain. One notable example involved a fake job offer shared via a LinkedIn message, which directed recipients to a malicious website "willointerview[.]com". This campaign targeted young IT and cybersecurity professionals who were looking for work.

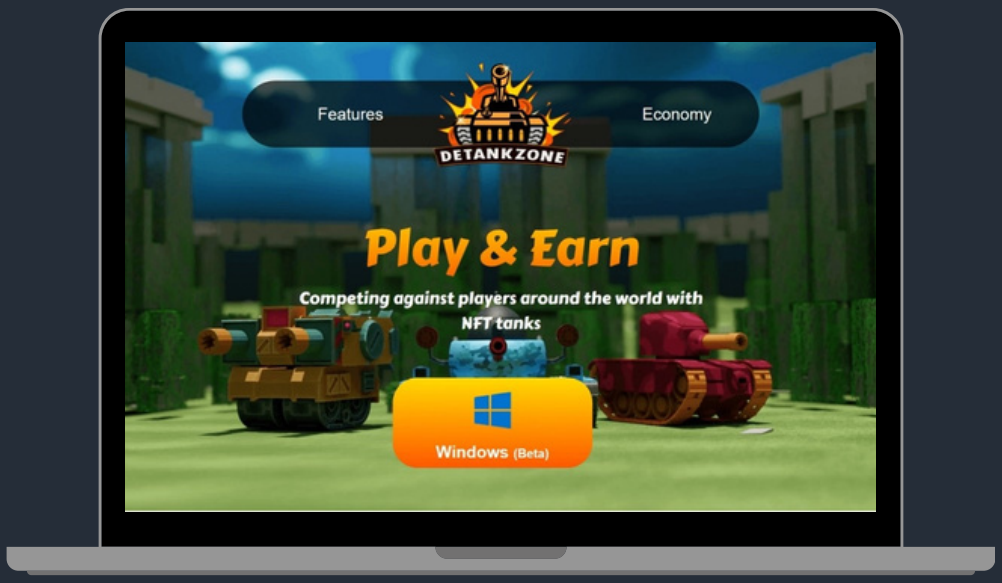


A malicious web page featuring a fabricated job description, prompting the victim to click the "continue" button

A fraudulent job offer presented via message from a recruiter on LinkedIn

The infection sequence employed by Lazarus is intricate, utilizing multiple malware components to establish a foothold within targeted systems. Through our research, combined with insights from Kaspersky, we have identified a new downloader and loader named CookiePlus, which is capable of downloading malicious shellcodes and DLLs. We have also observed Lazarus reusing a loader from a previous campaign, referred to as RollMid.

In another recent campaign, Lazarus targeted cryptocurrency investors by creating a fake multiplayer online battle arena game called detankzone (hosted at "detankzone[.]com"), which it claimed to incorporate both decentralized finance and non-fungible token features. The website of the detankzone game, appearing as a legitimate game, contained hidden scripts that exploited a zero-day vulnerability in Google Chrome (CVE-2024-4947), enabling remote code execution upon visiting the site. After the remote code execution, Lazarus used another exploit to bypass V8 sandboxing.



Website of the Detankzone

This campaign highlights the Lazarus Group's consistent use of advanced tactics, such as zero-day exploits and deceptive lures, to infiltrate systems and steal sensitive information. Their operations remain focused on targeting IT professionals and individuals employed by organizations of strategic interest to the attackers.

Luigino Camastra, Malware Researcher

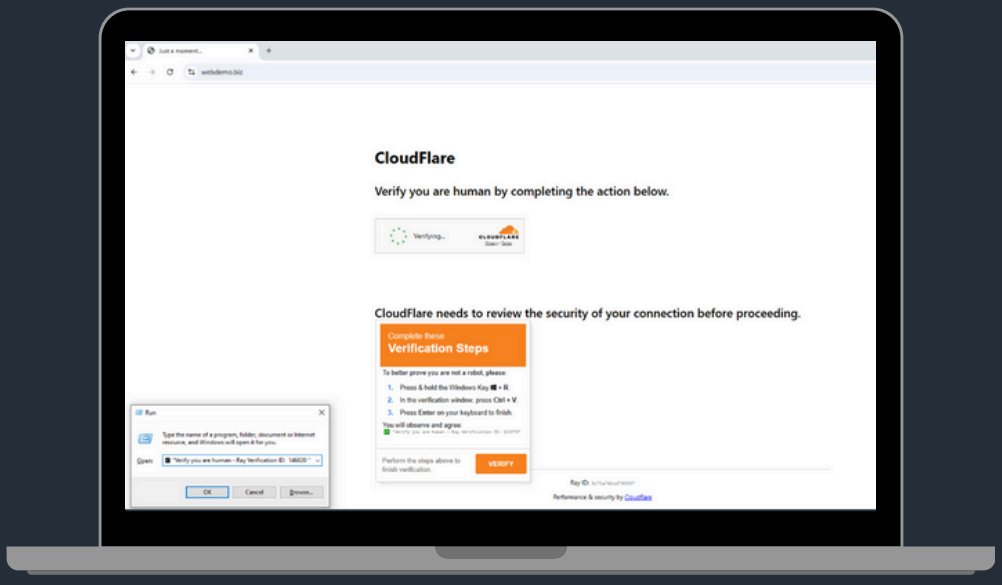
Data-Stealing Threats: Scam-Yourself Attacks Continue to Enable Data Theft

Data-Stealing Threats are dedicated to stealing anything of value from the victim's device. Typically, they focus on stored credentials, cryptocurrencies, browser sessions/cookies, browser passwords and private documents.

The fourth quarter of 2024 saw a number of good-news headlines in the world of cyber gang takedowns. One of the biggest stories was Operation Magnus, a joint effort by the Dutch National Police, the FBI and other partners, resulting in the take down of RedLine and META information stealers.

While the protectors saw success in taking down malicious actors, new data theft threats emerged. Glove Stealer is a newly discovered information stealer written in .NET. In addition to stealing browser data (cookies, autofill information, etc.), it also heavily focuses on cryptocurrency wallets, 2FA authenticators, password managers, email clients, and other sensitive data. This stealer also follows the trend of bypassing App-Bound Encryption, introduced in Google Chrome, using the IElevator service bypass. Note that we described many existing bypasses for the App-Bound Encryption in the previous Q3/2024 report.

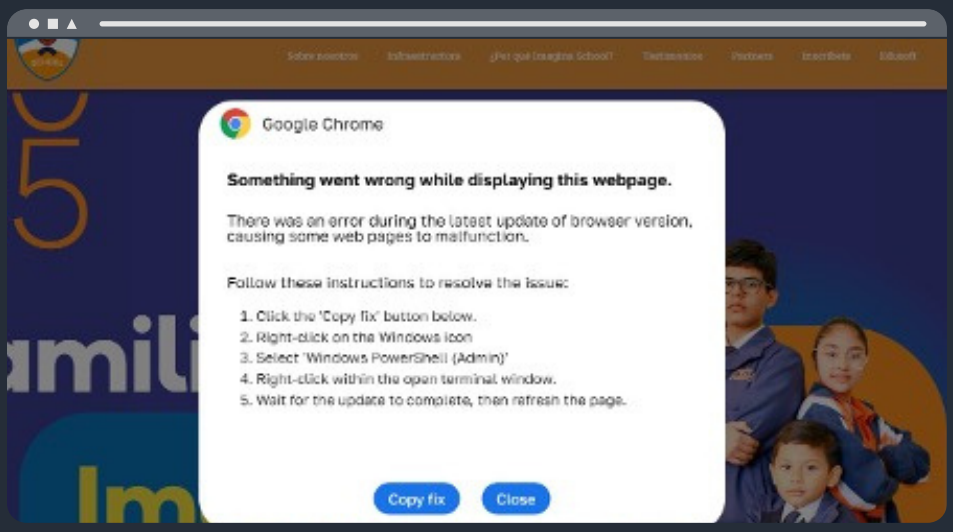
Furthermore, we continued to see many FakeCaptcha campaigns, distributing mostly information stealers and RATs. During Q4/2024, attackers introduced multiple new adaptations of well-known CAPTCHA designs, including CloudFlare.



FakeCaptcha mimicking a typical CloudFlare design of CAPTCHA

Because of the high prevalence of ClickFix and FakeCaptcha campaigns (we will break down the statistics separately below), Gen introduced a brand-new Clipboard Protection feature, available in products across the Norton, Avast and AVG brands. This additional defense layer in our protection stack allows us to better address clipboard threats, including Scam-Yourself Attacks. Ultimately, this protection allows us to eradicate the threat before it even has the chance of being downloaded to the users' systems.

By analyzing content being copied from websites via FakeCaptcha scams, we uncovered an attack chain used for deploying the remote access trojan (RAT) NetSupport. This chain was orchestrated by a script iteratively developed by the attacker using ChatGPT. Findings like these not only highlight a growing trend of enabling low-skill actors to achieve high-impact outcomes, but they also prove that inventions like Clipboard Protection are key in helping make the world a safer place.



ClickFix used by ClearFake, distributing DarkGate

ClearFake, one of the many notoriously known Fake Update actors, continued to use ClickFix to deliver malware. With the assistance of the EtherHiding technique for delivery, we observed the DarkGate information stealer with vast RAT capabilities being distributed.

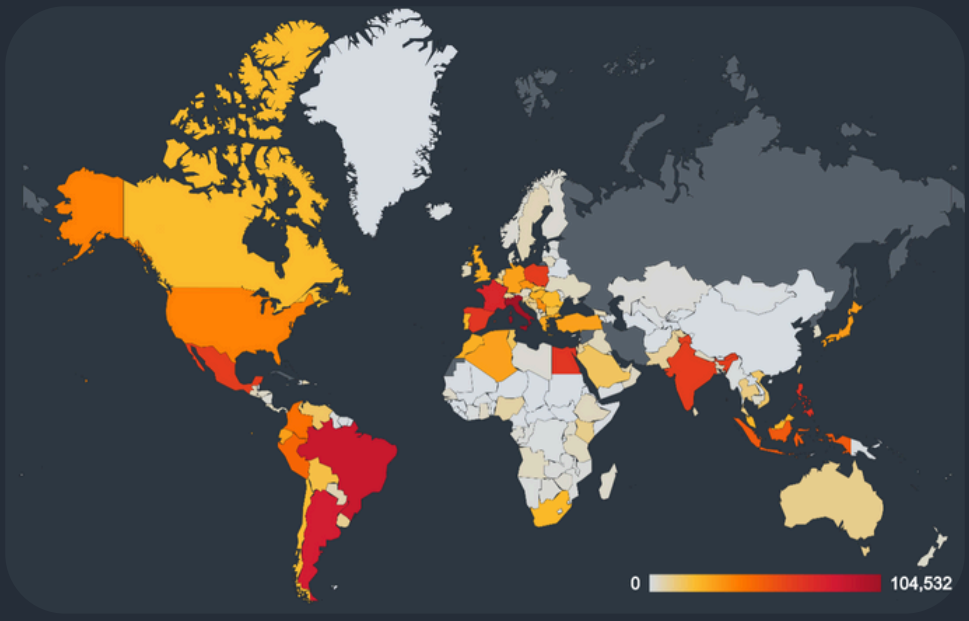
Finally, in Q4/2024 we observed a 17% increase in the activity of AtomicStealer, also known as AMOS, one of the most advanced information stealers targeting macOS. This sophisticated malware is designed to steal a variety of personal information, enabling identity theft, monetization of stolen data, and facilitating more targeted attacks. A rising trend for threats on this platform is the usage of PyInstallers. These provide a way of executing Python scripts even on devices with no Python installed, effectively simplifying the malware distribution.

Statistics

We happily reported a significant 60% decrease in detections of Lumma Stealer in Q4/2024. This was a welcomed break following the previous quarter where Lumma Stealer spiked dramatically and increased its malware share by massive 1154% with data-stealing malware increasing in risk ratio by 32% in general. Additionally, after the aforementioned Operation Magnus, RedLine and META stealers ceased to operate. Even though it might seem like data theft is cooling in terms of the sheer numbers, we need to have a closer look at the threat landscape to understand the changes better.

According to our data and estimations, the decrease of Lumma Stealer and thus information stealer activity overall is due to the protection against typical distribution methods for information stealers, including FakeCaptcha. This is further supported by introducing Clipboard Protection feature to our products. This naturally influences our statistics because we completely eliminate the delivery method at its very origin and thus sooner than the final payload would be delivered to infect the victims' systems.

As described in the previous quarter's featured story, Scam-Yourself Attacks, such as ClickFix and FakeCaptcha, have taken off, launching massive campaigns all around the world. This trend continued in Q4/2024, where we protected more than 4.2M unique users against FakeCaptcha attacks. The risk ratio of encountering FakeCaptcha scams increased by +130% compared to the previous quarter.



Heatmap illustrating the widespread use of FakeCaptcha

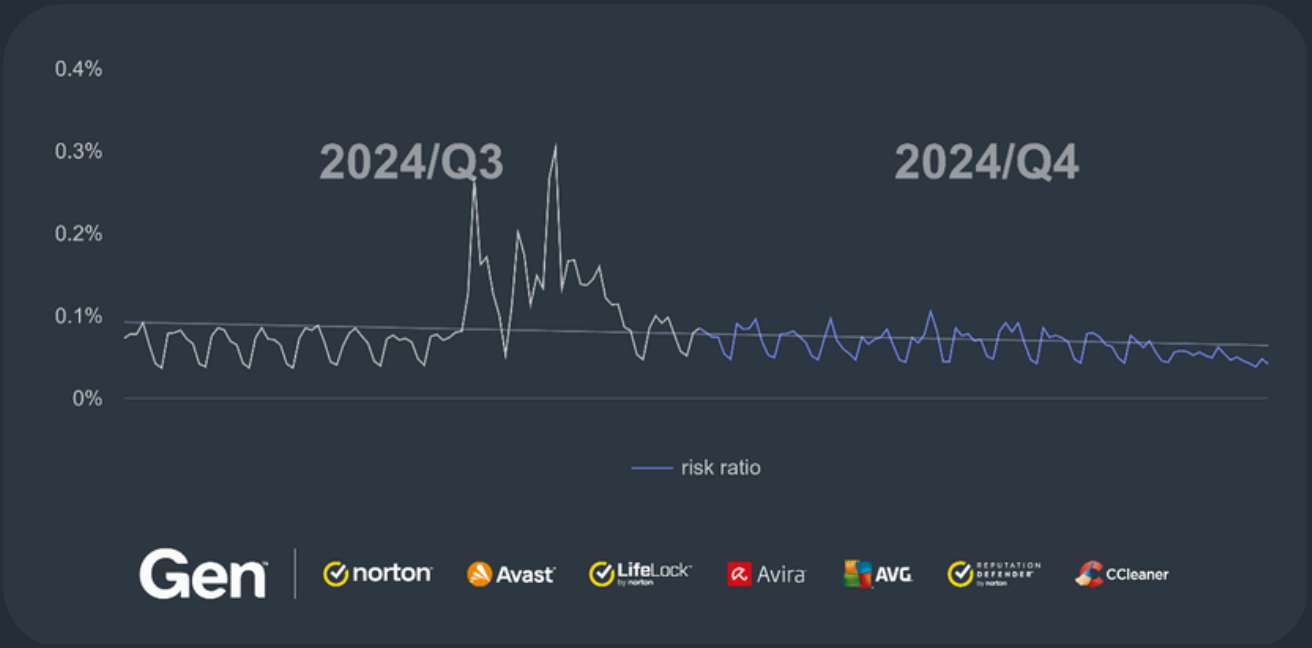
The highest risk ratio of stumbling upon FakeCaptcha was in the Balkan states, including:

- Montenegro (9.76%)
- Serbia (8.94%)
- North Macedonia (8.92%)
- Kosovo (8.51%)

Other countries with a high-risk ratio were:

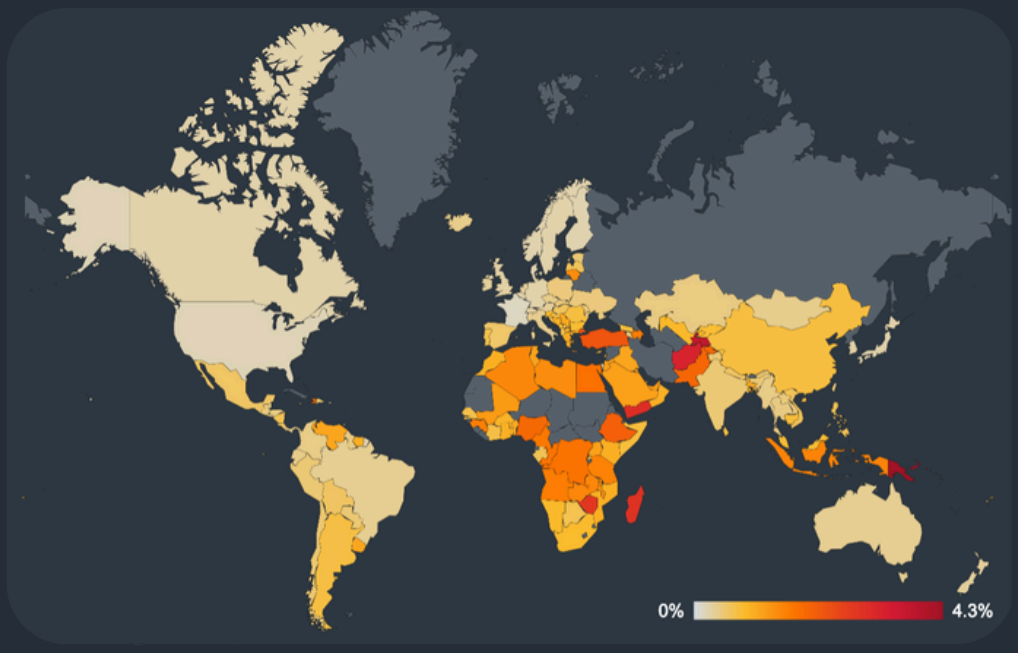
- Egypt (8.31%)
- The Philippines (5.14%)
- Argentina (2.91%)
- Spain (2.17%)
- Italy (2.66%)
- India (1.69%)
- Brazil (1.13%)
- France (1.15%)

Compared to the previous quarter, the overall risk ratio for information stealers decreased by 32% in Q4/2024.



Daily risk ratio in our user base regarding information stealers in Q4/2024

Conversely, the risk ratio in Indonesia experienced a slight increase of 1.53%, while in Turkey, the risk ratio increased by 10%.



Global risk ratio for information stealers in Q4/2024

After losing 60% of its malware share, Lumma Stealer is, according to our data, in the second place in terms of information stealer share behind AgentTesla. However, AgentTesla also lost some presence, decreasing its malware share by 9%. Because of this shift in proportion, every other information stealer increased its malware share in Q4/2024. One of them stands out, however, as MassLogger increased its malware share by massive 437%, ranking amongst the top 10 stealers now.

The most common information stealers with their malware shares in Q4/2024 were:

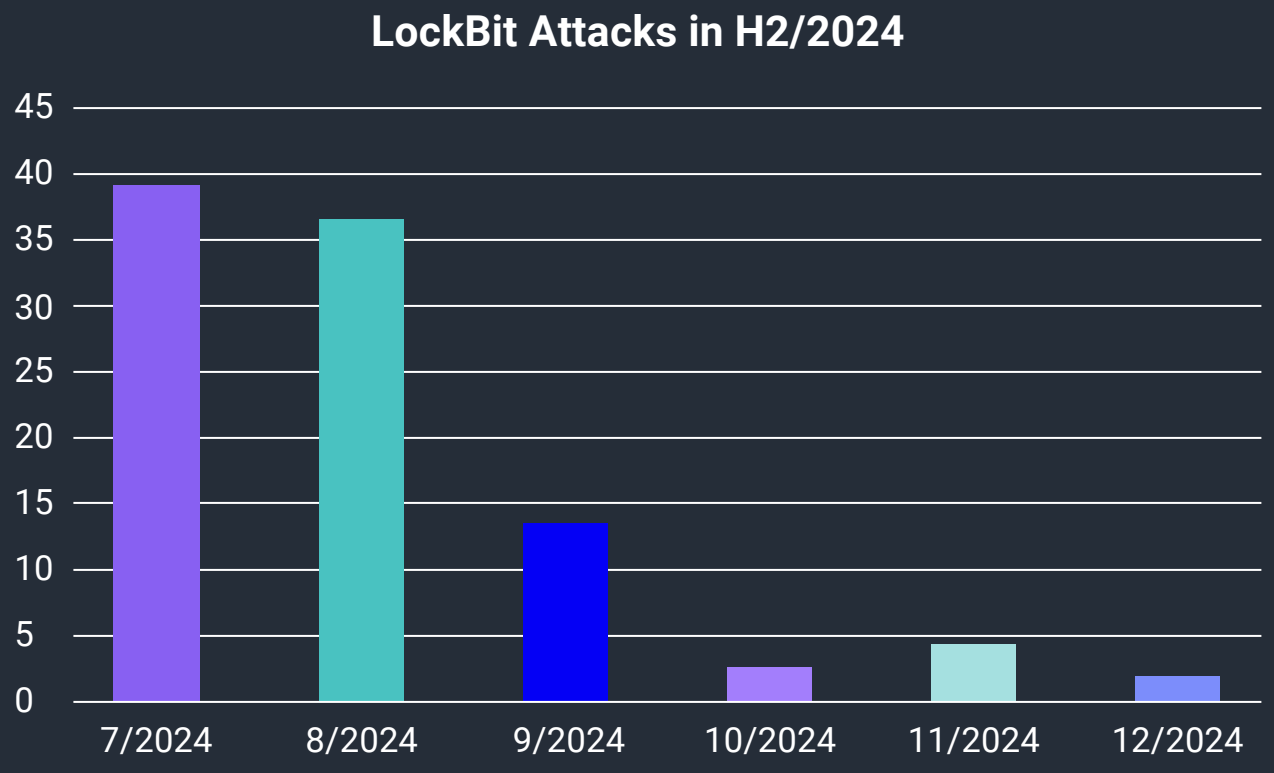
- AgentTesla (16%)
- Lumma (12%)
- FormBook (12%)
- Ramnit (11%)
- Fareit (7%)
- SnakeKeylogger (5%)
- MassLogger (4%)
- Vidar (3%)
- Lokibot (2%)
- ViperSoftX (2%)

Jan Rubín, Malware Researcher

Ransomware:
Third Consecutive Quarter of Growth

Ransomware is any type of extorting malware. The most common subtype is the one that encrypts documents, photos, videos, databases, and other files on the victim's PC. Those files become unusable without decrypting them first. To decrypt the files, attackers demand money, "ransom", hence the term ransomware.

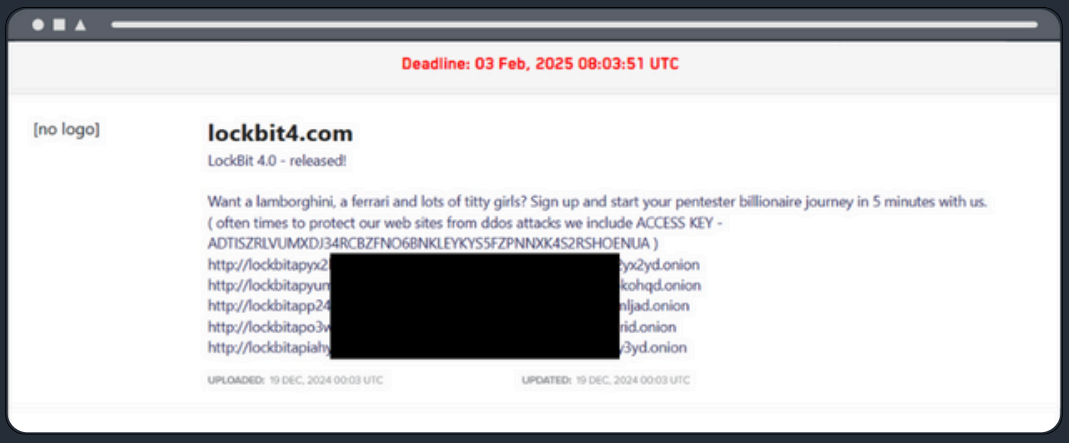
LockBit, one of the biggest players in the ransomware scene, went through some interesting changes in the latter half of 2024, with a significant decrease in the number of (published) attacks over the last 6 months:



Number of LockBit attacks per month in H2/2024

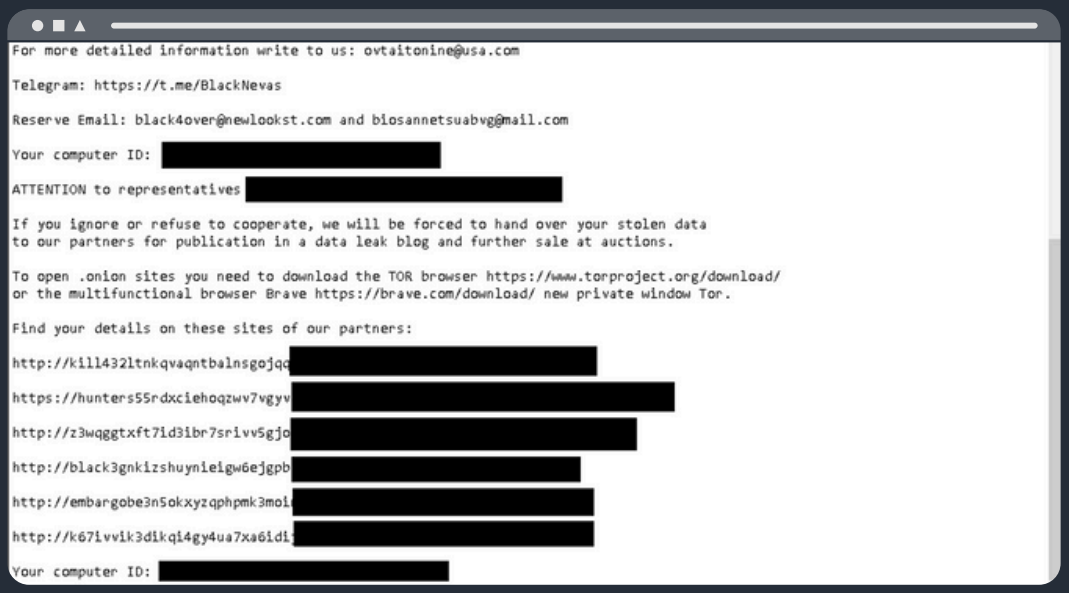
Furthermore, the U.S. Department of Justice announced that they officially charged Rostislav Panev, a LockBit malware developer who was arrested in Israel and is currently awaiting extradition to the USA.

Panev was a key part of the LockBit gang, contributing to their path of destruction which has included attacking children's hospitals amongst other organizations across industries. It seems, though, that the rest of LockBit has moved on from Panev after announcing that an updated version – LockBit 4.0 - is expected to launch in February.



Screenshot of Announcement of LockBit 4.0

Trigona Reemerges with Deceptive Strategy



Heatmap illustrating the widespread use of FakeCaptcha

Trigona ransomware resurfaced in the summer of 2024, but this time with a change in tactics designed to hide its identity. Earlier attacks referenced their own leak site, but recent ransom notes avoid mentioning it altogether. Instead, they point to leak sites belonging to other ransomware groups such as KillSec, Hunters, and DragonForce. However, our analysis has not found any evidence of Trigona victims appearing on these other leak sites, making it unlikely that these groups are actually collaborating. The ransomware group also uses a slightly modified cryptor, which led to it being misclassified as part of a different malware family. Analysis of configuration data inside the binary files confirmed that it is the same Trigona ransomware with some adjustments. This new approach has been observed since June 2024, with additional samples appearing throughout the remainder of the year.

Statistics

For the third consecutive quarter, ransomware has continued its alarming upward trend, with a notable 50% increase in Q4/2024. This follows a staggering 100% rise in Q3/2024 and a 24% jump in Q2/2024. The sustained growth in ransomware activity highlights an ongoing, escalating threat to both individuals and organizations globally.

According to our telemetry, Magniber is still the most prevalent ransomware (62% of malware share). Its high counts come from the previous quarter:

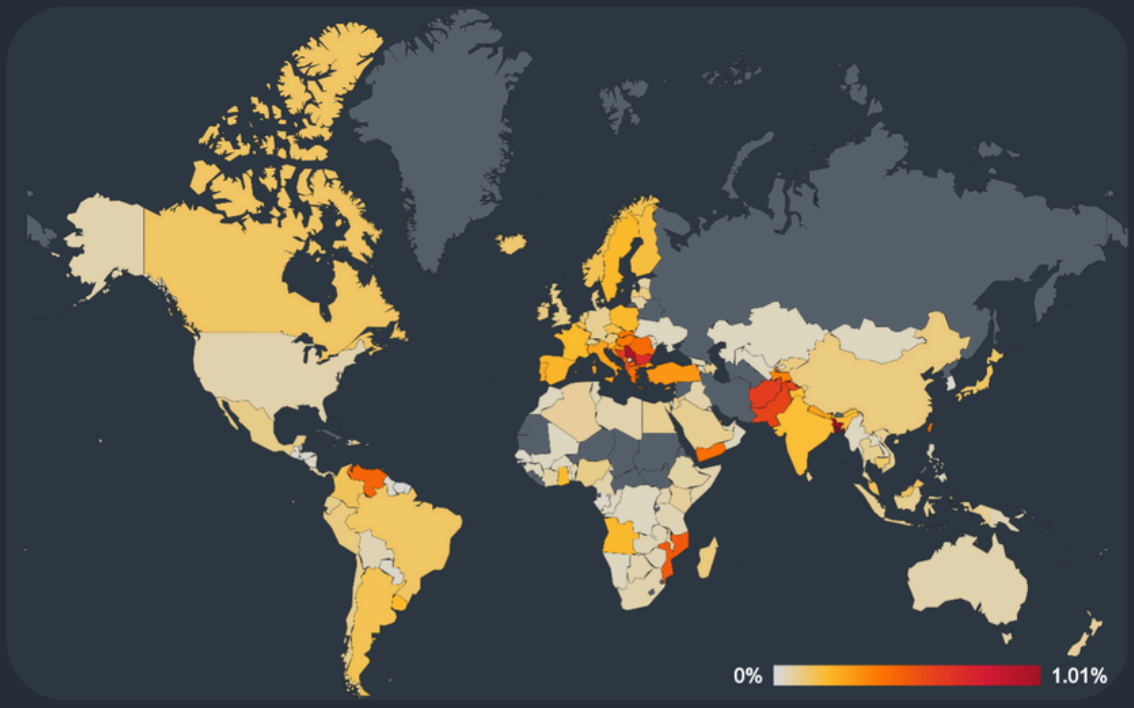
Risk ratio comparison of Q3 and Q4/2024

Countries with the highest increases in risk ratio are in South America, including:

- Colombia (+400%)
- Uruguay (+400%)
- Brazil (+370%)
- Argentina (+300%)
- Venezuela (+290%)
- Peru (+270%)

Risk ratios also increased in Mexico (+230%), Japan (+180%), Austria (+100%), France (+100%), and Canada (+100%).

Absolute risk ratios per country are depicted in the following map:



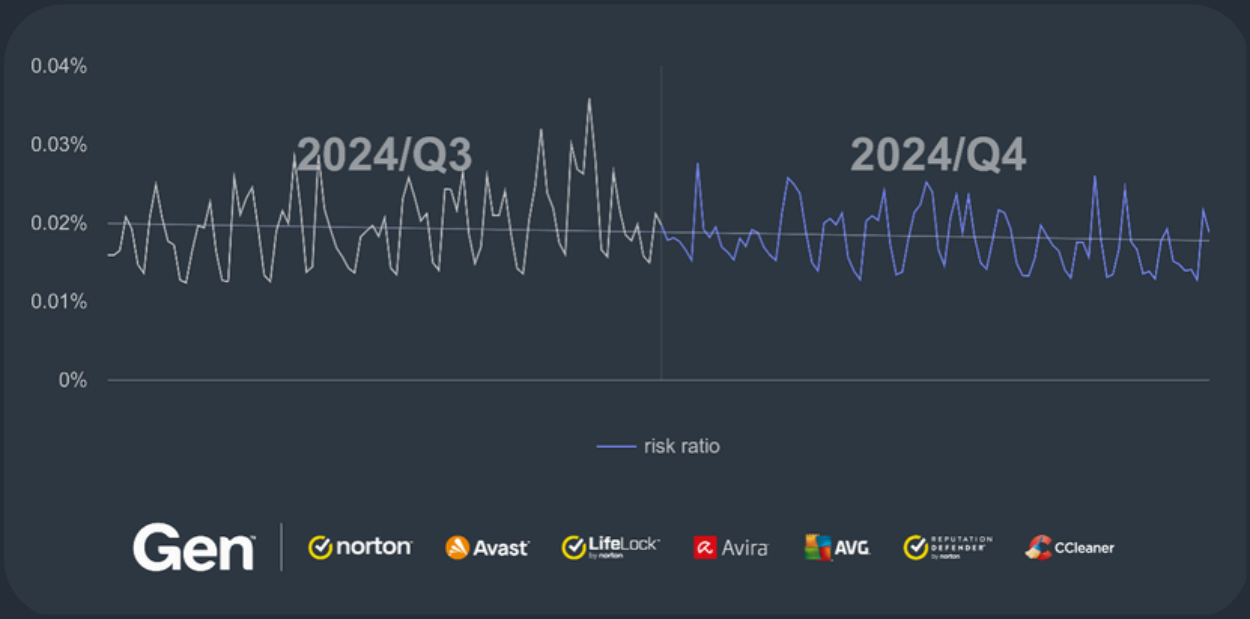
Risk ratio comparison of Q3 and Q4/2024

Ladislav Zezula, Malware Researcher
Samuel Vojtáš, Malware Researcher
Jakub Křoustek, Malware Research Director

Remote Access Trojans (RATs): Remcos Slowing Down

A Remote Access Trojan (RAT) is a type of malicious software that allows unauthorized individuals to gain remote control over a victim's computer or device. RATs are typically spread through social engineering techniques, such as phishing emails or infected file downloads. Once installed, RATs grant the attacker complete access to the victim's device, enabling them to execute various malicious activities, such as spying, data theft, remote surveillance and even taking control of the victim's webcam and microphone.

After a substantial increase in Q3/2024, the activity level of RATs remained consistent throughout Q4/2024. Interestingly compared to what we have seen in previous years, this year there was seemingly no decrease in RAT prevalence towards the end of the year.



FakeCaptcha mimicking a typical CloudFlare design of CAPTCHA

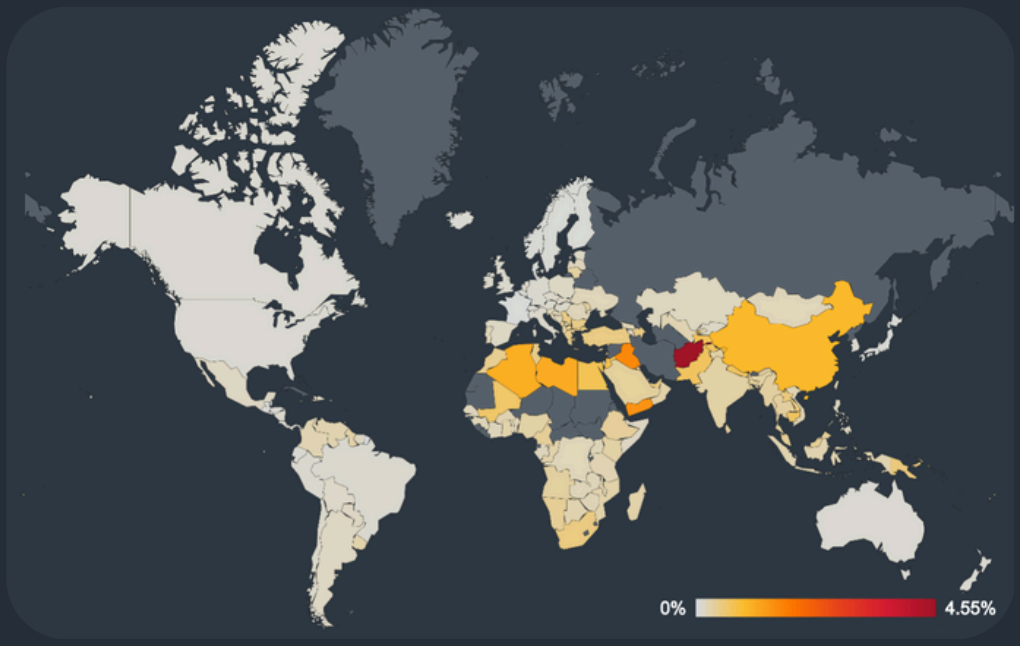
Countries with the largest increases in risk ratio were:

- Algeria +37% (mostly driven by HWorm and njRAT)
- Belgium +33% (AsyncRat, Remcos)
- Netherlands +29% (Remcos, QuasarRAT)

Largest decreases in risk ratio:

- Czechia -35%
- Hungary -31%
- Romania -25%

The list of safest countries includes France , Sweden and Japan. France and Sweden kept their place among the top 3 countries least impacted by RATs from Q3/2024.



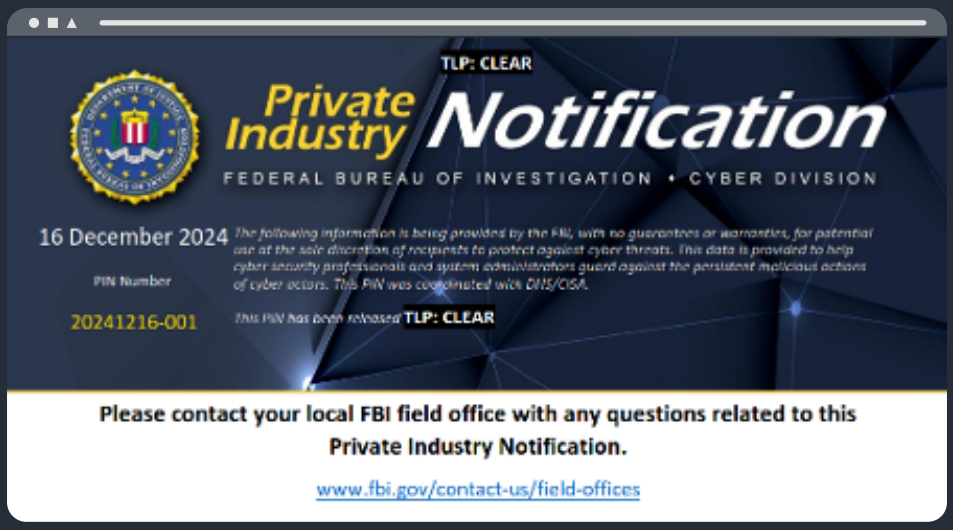
Daily risk ratio in our user base regarding information stealers in Q4/2024

QuasarRAT saw its malware share surge by over 70%, with Turkey, Bulgaria, and Egypt being the most affected countries. Other strains, such as NanoCore and DarkComet, also experienced significant gains, each rising by approximately 30%.

We have seen Remcos decrease in activity mostly in Europe, the United States and Canada losing some of its malware share to other strains in Q4/2024. However, Remcos remains the top strain globally in terms of overall share. Additionally, Remcos has been recently updated to version 6.0 - new features are aimed at operators, mostly simplifying the organization of remote (infected) computers. The update also contains some minor bug fixes. From a defender's perspective, the changes are not significant.

In the Q3/2024 report, we observed that the online shop which previously sold the XWorm RAT had gone inactive. As far as we can tell, it has not been replaced with another one. We also have not seen a more recent version of XWorm following 5.6 which launched in September 2024 and was the last to be advertised on the now defunct site. However, XWorm is not slowing down as its activity remains at approximately the same level as in the previous quarter.

Lesser known RATs are also making their mark, with the FBI issuing a warning regardingHiatusRAT at the end of 2024. Threat actors have been scanning web cameras and DVRs for vulnerabilities using HiatusRAT. Targeted vulnerabilities include CVE-2017-7921, CVE-2018-9995, CVE-2020-25078, CVE-2021-33044 and CVE-2021-36260. While HiatusRAT is not a new threat, being first discovered in early 2023, this warning serves as a reminder of the importance of regularly updating all connected devices, especially those often overlooked like web cameras and DVRs.



Screenshot of Rostislav Panev's profile on Odnoklassniki and Announcement of LockBit 4.0

Ondřej Mokoš, Malware Researcher

Vulnerabilities and Exploits: Chained Exploits and Sandbox Escapes

> *Exploits take advantage of flaws in legitimate software to perform actions that should not be allowed. They are typically categorized into remote code execution (RCE) exploits, which allow attackers to infect another machine, and local privilege escalation (LPE) exploits, which allow attackers to take more control of a partially infected machine.*

In the Q4, two significant local privilege escalation vulnerabilities in Windows were discovered to be actively exploited in the wild. These vulnerabilities highlight critical weaknesses in Windows' security architecture and underscore the need for robust sandboxing mechanisms. Additionally, recent findings have linked some of these exploits to advanced threat actors, further emphasizing the sophistication of modern cyberattacks.

The first vulnerability, CVE-2024-49138, was found in the Windows Common Log File System Driver (CLFS.sys) and reported by CrowdStrike. This vulnerability allowed attackers to escalate their privileges, potentially compromising system security. While CrowdStrike did not provide specific details about the nature of the vulnerability or the identity of the actors exploiting it, the fact that it targeted a core Windows driver underscores its severity.

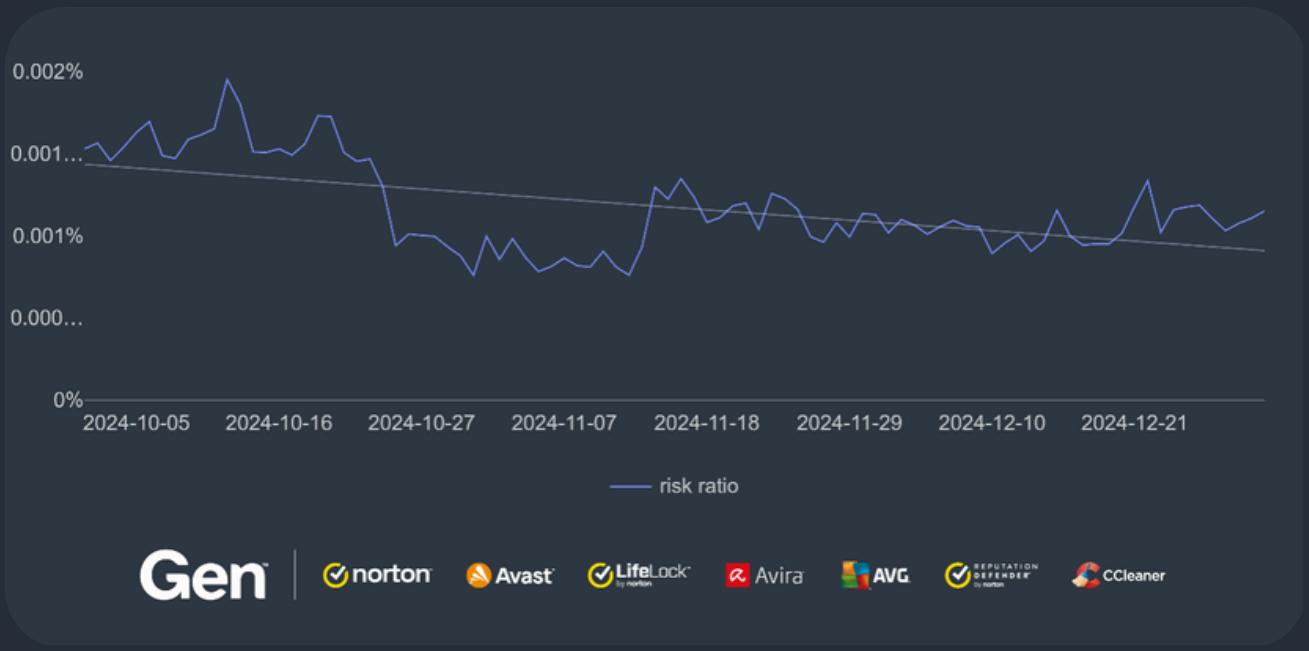
Google reported the second vulnerability, identified as CVE-2024-49039, which involved an escape from the Windows AppContainer sandbox. This security feature in Windows is designed to provide a sandboxed environment for applications, running them with minimal privileges to isolate them from critical system components and each other, thereby reducing the risk of malware or malicious behavior affecting the broader system. However, this vulnerability allowed a low-privileged user to execute code at a medium integrity level, effectively bypassing AppContainer's protections. The discovery of this vulnerability underscores the ongoing challenges in maintaining robust application isolation.

ESET later discovered that CVE-2024-49039 was being exploited in the wild. Attackers were observed chaining this vulnerability with a remote code execution flaw in Firefox, identified as CVE-2024-9680. According to ESET's analysis, the attackers leveraged CVE-2024-49039 to escape the sandbox from the untrusted process level of Firefox's content process to a medium integrity level. This chain of exploits demonstrates the sophistication of modern attacks, where multiple vulnerabilities are combined to achieve a specific goal.

The technical details of CVE-2024-49039 reveal that the vulnerability relied on calling functions from an undocumented Remote Procedure Call (RPC) endpoint. This endpoint allowed the creation of a scheduled task, a function that should not have been callable from the untrusted process level. By exploiting this flaw, attackers were able to create a scheduled task that executed arbitrary applications at a medium integrity level. This action enabled them to elevate their privileges on the system and break out of the sandbox, effectively bypassing the intended security boundaries of the AppContainer.

Adding to this complexity, ESET researchers uncovered a previously unknown vulnerability in Mozilla products that was being exploited in the wild by the Russia-aligned group RomCom. This marks at least the second time that RomCom has been caught exploiting a significant zero-day vulnerability in the wild. Earlier in June 2023, RomCom was linked to the exploitation of CVE-2023-36884 through Microsoft Word. The group's involvement in exploiting CVE-2024-49039 highlights their capability to adapt and weaponize zero-day vulnerabilities for targeted attacks.

The exploitation of these vulnerabilities underscores the importance of continuous monitoring and improvement in security mechanisms. The chaining of CVE-2024-49039 with CVE-2024-9680, along with RomCom's exploitation of Mozilla products, illustrates how advanced threat actors can combine weaknesses in different components to achieve their objectives. Addressing such threats requires a multi-faceted approach, including rigorous patching practices, comprehensive vulnerability assessments, and robust application isolation mechanisms.



Risk ratio of post-exploitation frameworks in Q4/2024

In Q4/2024, we continued evaluating the main exploitation and post-exploitation frameworks targeting our users. While our telemetry indicated that the use of frameworks was on a downward trend for this quarter, Cobalt Strike was again the most prevalent strain, occupying 31% of the hits in this category.

To confirm whether the downward trend that marked this quarter is temporary or significative in time, we will continue to evaluate and monitor the evolution of the exploitation and post-exploitation frameworks in Q1/2025.

Luigino Camastra, Malware Researcher
David Álvarez, Malware Analyst
Michal Salát, Threat Intelligence Director

Web Threats

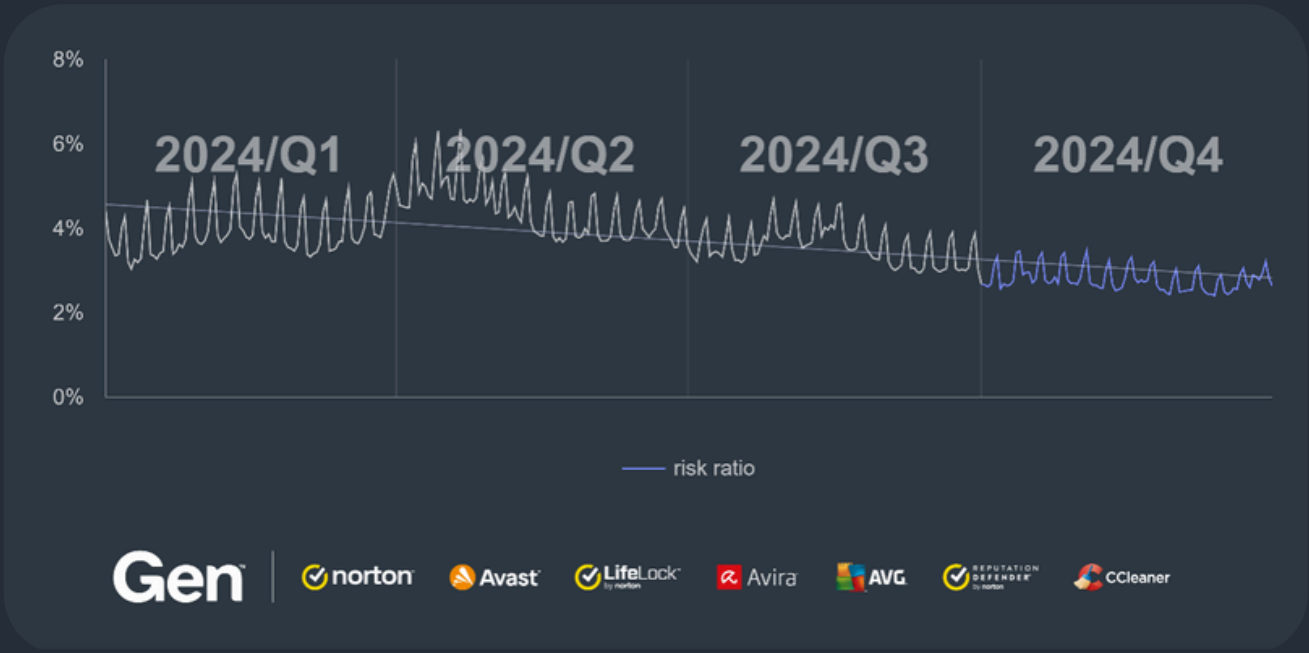
Web threats remain a key focus for our analysts, encompassing numerous sub-categories of scams. Despite attackers continuously introducing modified variations of old scams, the overall downward trend towards the end of the year persisted. The last quarter of the year saw an even further decline, with a 13% drop compared to Q3/2024. This decline was observed in most countries, although there are some exceptions, which we will cover later in the text.

Scams: A Worldwide Challenge

> *A scam is a type of threat that aims to trick people into giving an attacker their personal information or money. We track diverse types of scams which are listed below.*

Despite a downward trend, we observe that certain detections have increased compared to the previous quarter. These detections primarily highlight the main reason for the success of today's scam threats: malvertising.

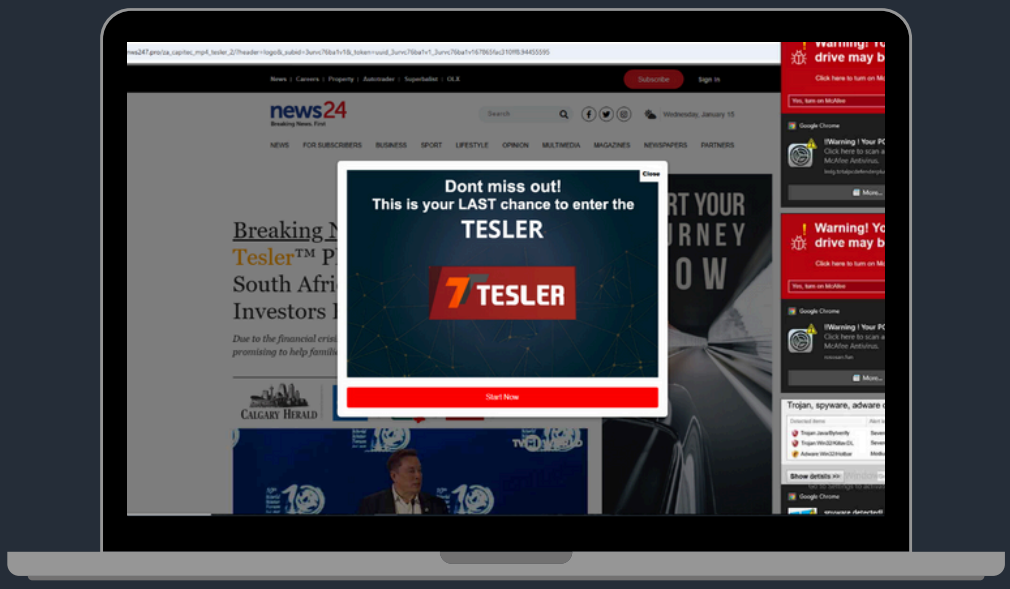
For our regular readers, the concept of malvertising is well-known. However, it's worth reiterating that the key factor in malvertising is its ability to target specific audiences.



Overall scam risk ratio for 2024

When advertisements are presented on social networks, for example, this targeting can be particularly effective because these platforms have access to more accurate and comprehensive user data. Additionally, many users perceive these platforms as safe, which can result in reduced awareness of potential threats. For example, our data indicates that some blocked scams originate from users who have been redirected from Meta's social networks.

In the below screenshot, you can see a notorious landing page. This illustration nicely shows the type of page to which users are redirected by some ads, sometimes resembling a tabloid article. This particular example is a financial scam. The right side of the screenshot shows another way such scams are spread: through push notifications, an increasing threat which we've highlighted in numerous reports and blogs. The screenshot also shows that this is a financial scam.

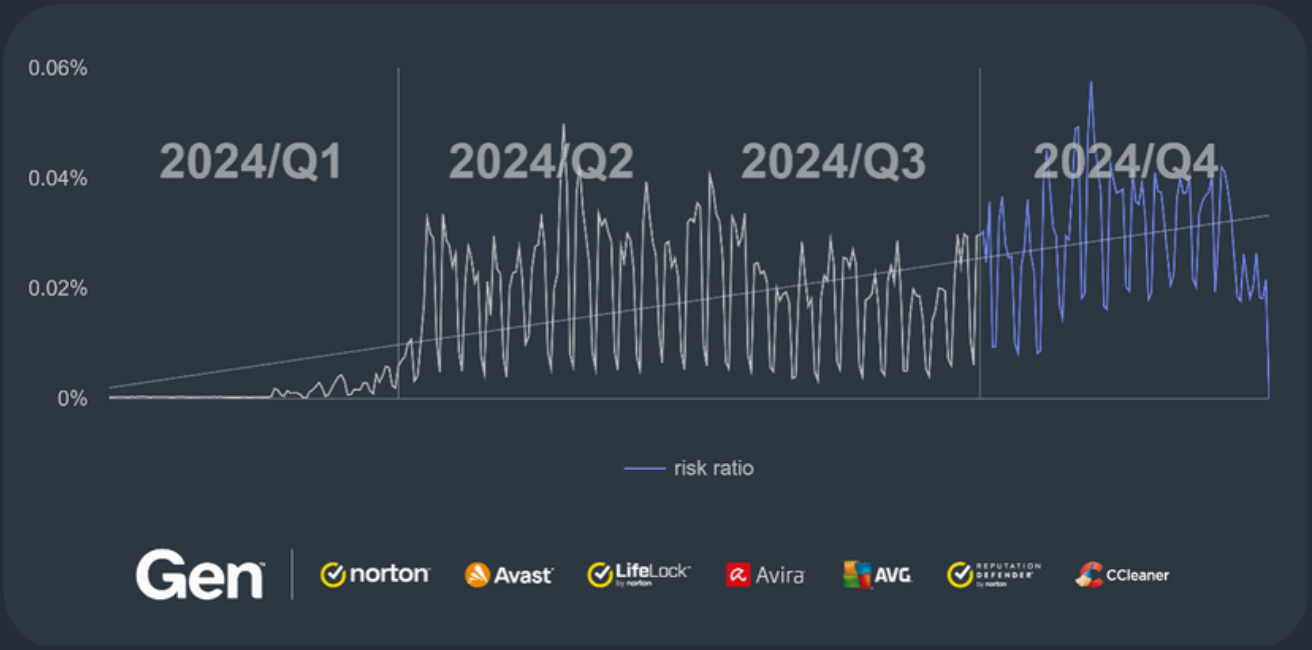


Example of financial scam landing page and malicious push notifications

Financial scams come in many different packages; this constantly recycled social engineering attack can be presented to people, for example, with a narrative of weight loss advice or as medical scams – the ways in which scammers entice their victims is almost endless.

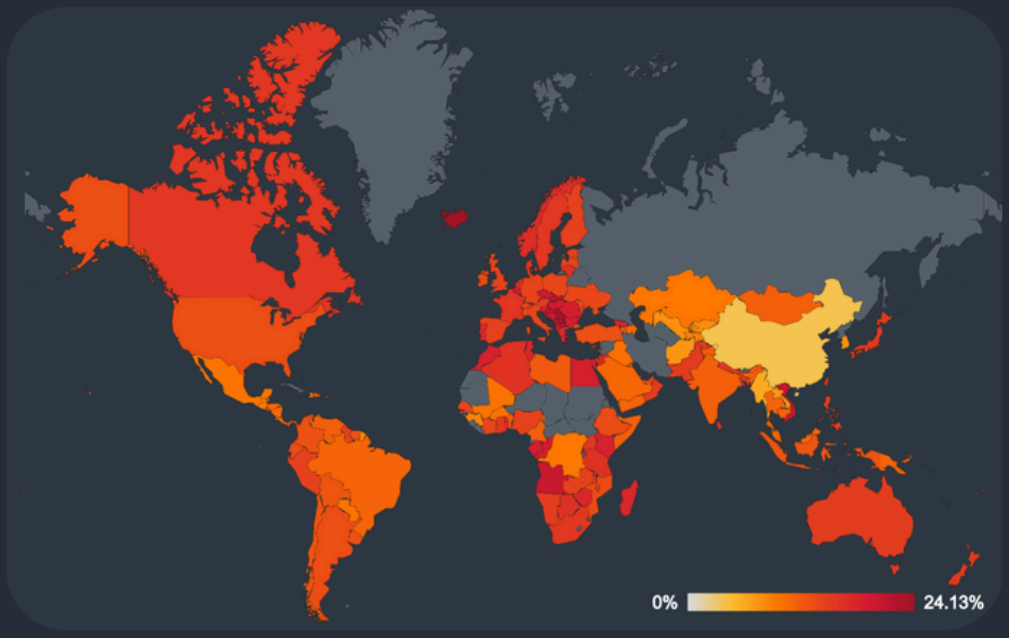
If you look at the global heat map, you'll see there is almost no place in the world that is not impacted by scams as 2024 comes to an end.

If we take a closer look at the chart below, Q4/2024 was the most active quarter for financial scams in 2024.



Risk ratio of financial scams for 2024

If you look at the global heat map, you'll see there is almost no place in the world that is not impacted by scams as 2024 comes to an end.



Example of financial scam landing page and malicious push notifications

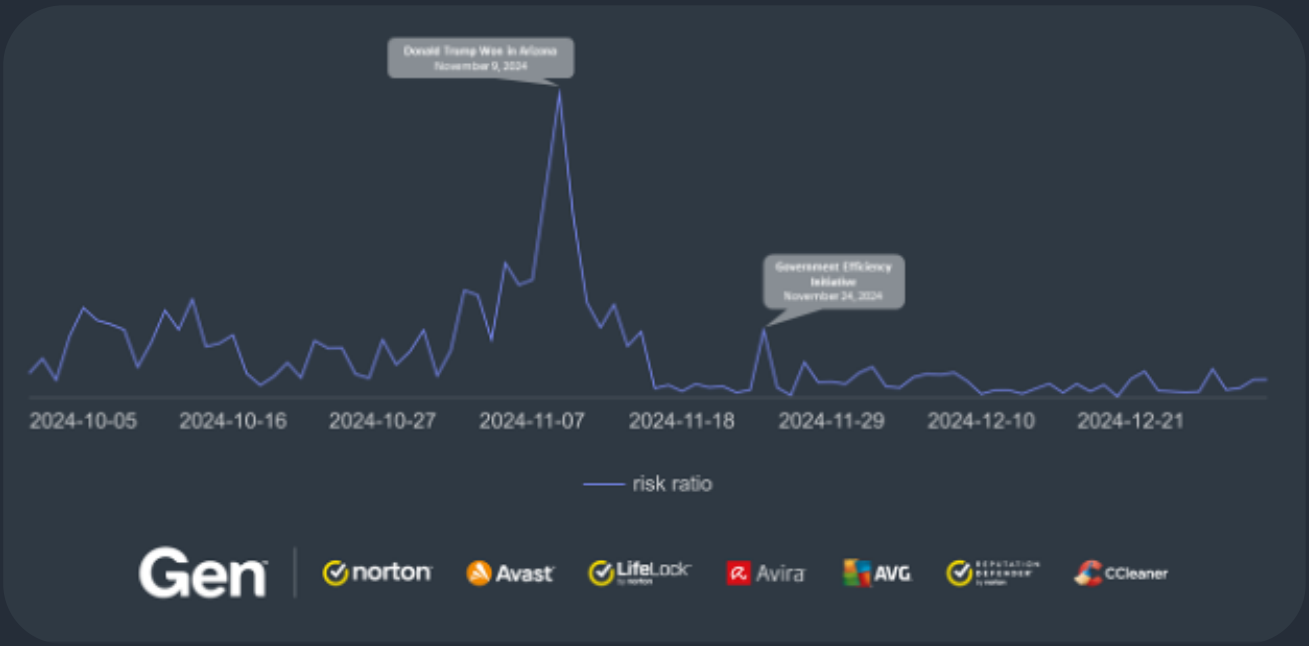
When examining the areas with highest chance of encountering a scam, Slovakia stands out with a risk ratio of 21.30%, although it experienced a slight decrease of 2% compared to the previous quarter. Vietnam follows closely with a risk ratio of 20.69%, showing a significant increase of 6%. Meanwhile, Czechia has a risk ratio of 19.87%, also seeing a 2% decrease from the previous quarter.

Beyond the list of countries with the highest risk, several other countries experienced significant quarter-over-quarter changes. South Korea saw the most substantial increase, with a 20% increase to a final risk ratio of 7.51%. Australia also experienced a notable rise, with a risk ratio of 15.24%, increasing by 6%. The United Kingdom saw a significant increase, with a risk ratio of 14.26%, up by 3%.

CryptoCore Exploits U.S. Election and Elon Musk's Statements – $7M Stolen

A crypto scam is a cyber threat designed to trick individuals into surrendering their cryptocurrency. These scams exploit the anonymity and irreversibility of blockchain transactions, often targeting those with a limited understanding of how cryptocurrency works.

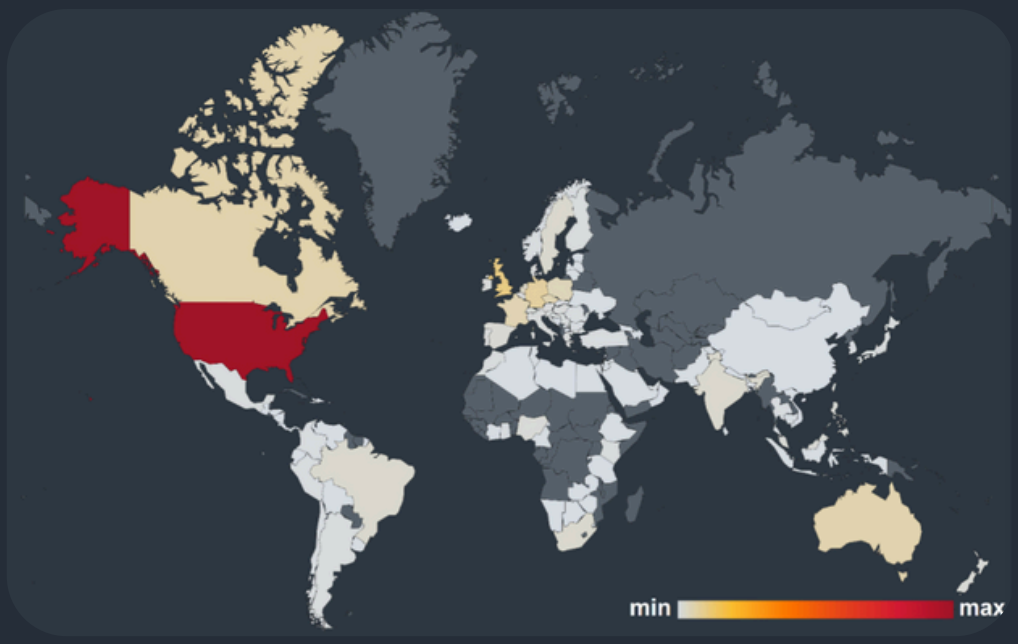
The CryptoCore scam group continued its operations in Q4/2024 with the same modus operandi of abusing high-profile events in the media, luring victims with promises of easy profits using deepfake videos. These attackers also leverage statements and actions by Elon Musk to make their scams appear more legitimate. In Q4/2024, their primary focus, as expected, was the U.S. presidential elections, further amplified by the involvement of Elon Musk.



Daily hits of CryptoCore scam with peaks correspond to U.S. presidential Election in Q4/2024

The CryptoCore activity around the presidential election increased throughout October. The highest threat peak was on November 9, 2024, when Donald Trump won the presidential election in Arizona, completing a clean sweep of all seven battleground states and locking in a decisive electoral college victory over the Democratic Vice President Kamala Harris.

If we compare the activities of CryptoCore across 2024, the presidential campaign was the most dangerous since we began tracking the group. The presidential campaign was even more significant than the highly destructive campaigns abusing the topics of the total solar eclipse and SpaceX flight.

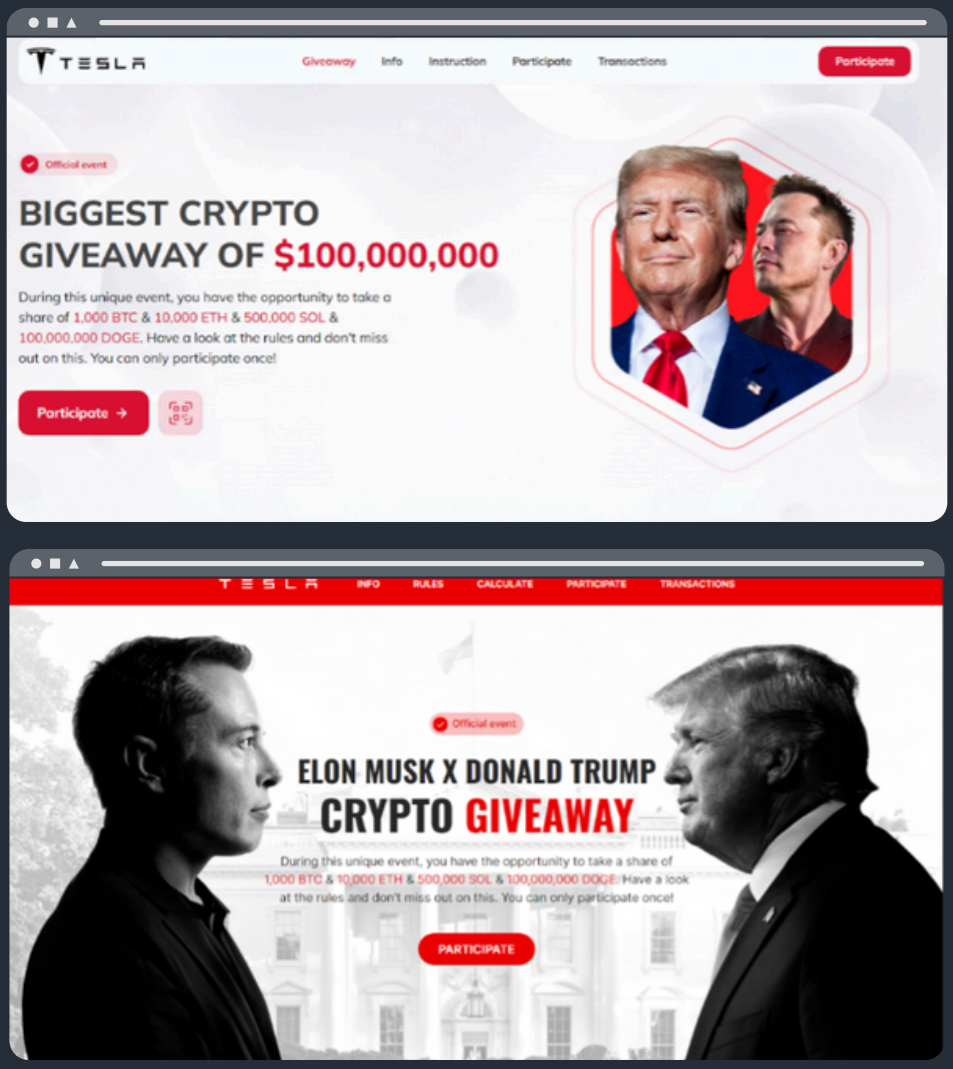


Global risk ratio for CryptoCore Scams for Q4/2024

The United States remains the country most affected by CryptoCore Scams, followed by the United Kingdom and Germany.

Example of a deepfake video related to the U.S. presidential election.

The deepfake videos used as CryptoCore lures used messages emphasizing Donald Trump as a visionary leader who understands innovation and the future of finance, particularly cryptocurrency. They claimed that Trump supports a platform for doubling cryptocurrency investments, presenting it as part of his vision for empowering individuals and revolutionizing financial systems. These scams touted Trump as an advocate for blockchain technology, cryptocurrency adoption, and deregulation to legitimize the fraudulent scheme.



Examples of fraudulent landing pages of CryptoCore

Victims are targeted through hijacked YouTube accounts, which prioritize attackers' videos in search results using specific keywords. These videos typically contain a QR code, which redirects the victim to a well-designed fraudulent website featuring motifs of Elon Musk and Donald Trump.

As CryptoCore's activities escalated dramatically throughout the quarter, and our telemetry captured 3,500 cryptocurrency transactions linked to 500 crypto wallets with a total value of an estimated $7,000,000 in October through December alone. While this figure is a rough estimate, the actual amount could be higher, given the complexity of tracking illicit crypto wallets and abused platforms. Additionally, the sharp rise in the value of most cryptocurrencies used by CryptoCore has significantly increased the group's overall profit in this quarter.

Real Elon Musk's giveaway abused by CryptoCore.

An interesting event exploited by the attackers in Q4/2024 was Elon Musk's promise of a $1 million giveaway per day during the presidential election. Musk's himself added credibility to the CryptoCore scam, because if a real Musk is handing out $1 million checks daily, why couldn't his "official event" be giving away hundreds of thousands in cryptocurrency? The attackers quickly seized the opportunity, creating a fake video based on the official giveaway event. This demonstrates how adept the attackers are at abusing media events to mislead people.

We will repeat ourselves again: Always verify the legitimacy of such claims through official channels and avoid making any financial transactions without confirming the offer's authenticity.

— If it sounds too good to be true, it probably is.

Dating Scams: Love's Illusion

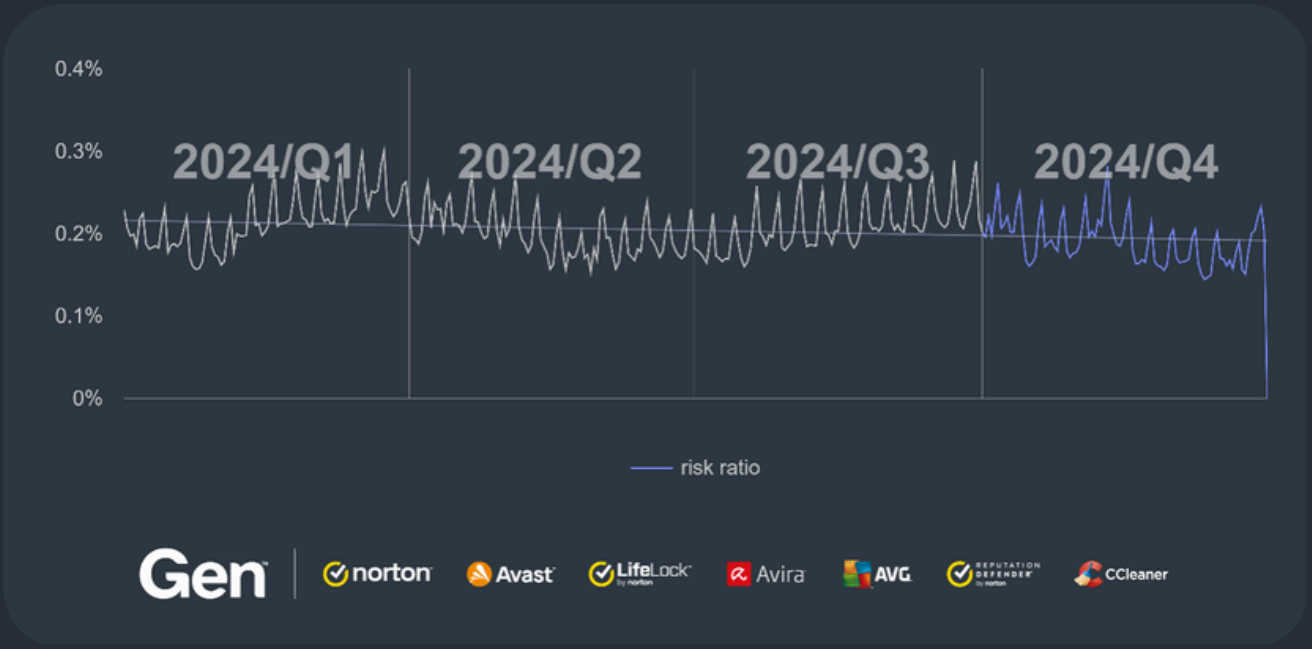
Dating scams, also known as romance scams or online dating scams, involve fraudsters deceiving individuals into fake romantic relationships. Scammers adopt fake online identities to gain the victim's trust, with the ultimate goal of obtaining money or enough personal information to commit identity theft.

When examining the risk ratios for dating scams, several countries have shown significant quarter-over-quarter changes. Iceland experienced the largest increase, with a risk ratio of 5.37%, up by 51%. This substantial rise indicates a growing concern for dating scams in the region.

Risk ratio of dating scams in Iceland in Q4/2024

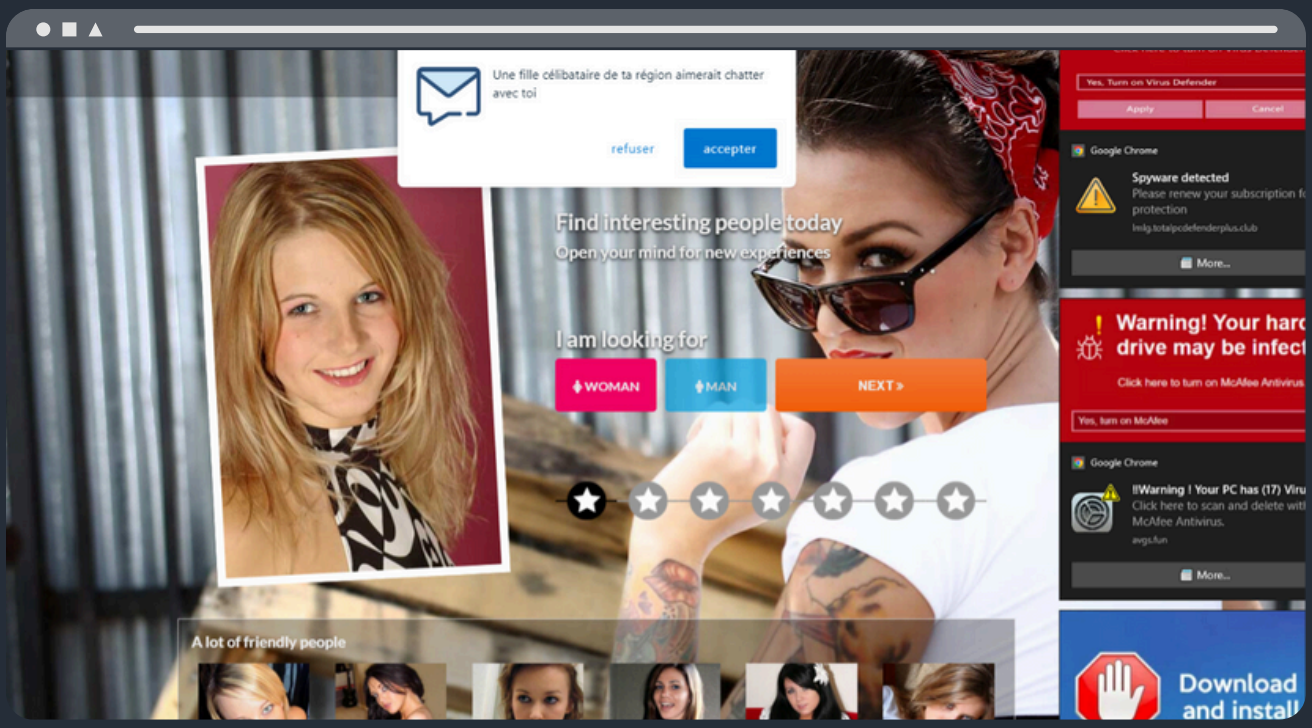
Hungary and Czechia both saw notable increases of 7%, with risk ratios of 4.42% and 3.98%, respectively. Belgium also experienced a significant rise, with a risk ratio of 3.67%, up by 5%.

In contrast, Germany and Norway had minimal changes in their risk ratios, with Germany remaining stable at 4.28% and Norway seeing a slight increase to 4.26%.



Overall risk ratio of dating scams for 2024

Overall, these statistics underscore the varying impact of dating scams across different regions.



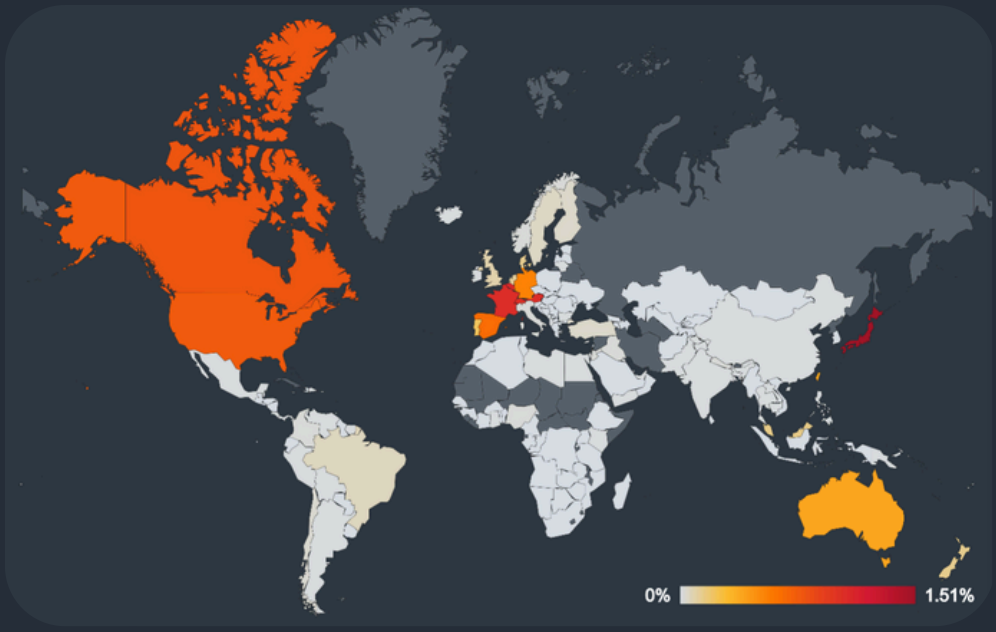
Example of prevalent landing page of a dating scam

Tech Support Scams: Deceptive Assistance

Tech support scam threats involve fraudsters posing as legitimate technical support representatives who attempt to gain remote access to victims' devices or obtain sensitive personal information, such as credit card or banking details. These scams rely on confidence tricks to gain victims' trust and often involve convincing them to pay for unnecessary services or purchase expensive gift cards. It's important for internet users to be vigilant and to verify the credentials of anyone claiming to offer technical support services.

Japan remains a top target for tech support scams, with a risk ratio of 1.51%, up 14% from the previous quarter.

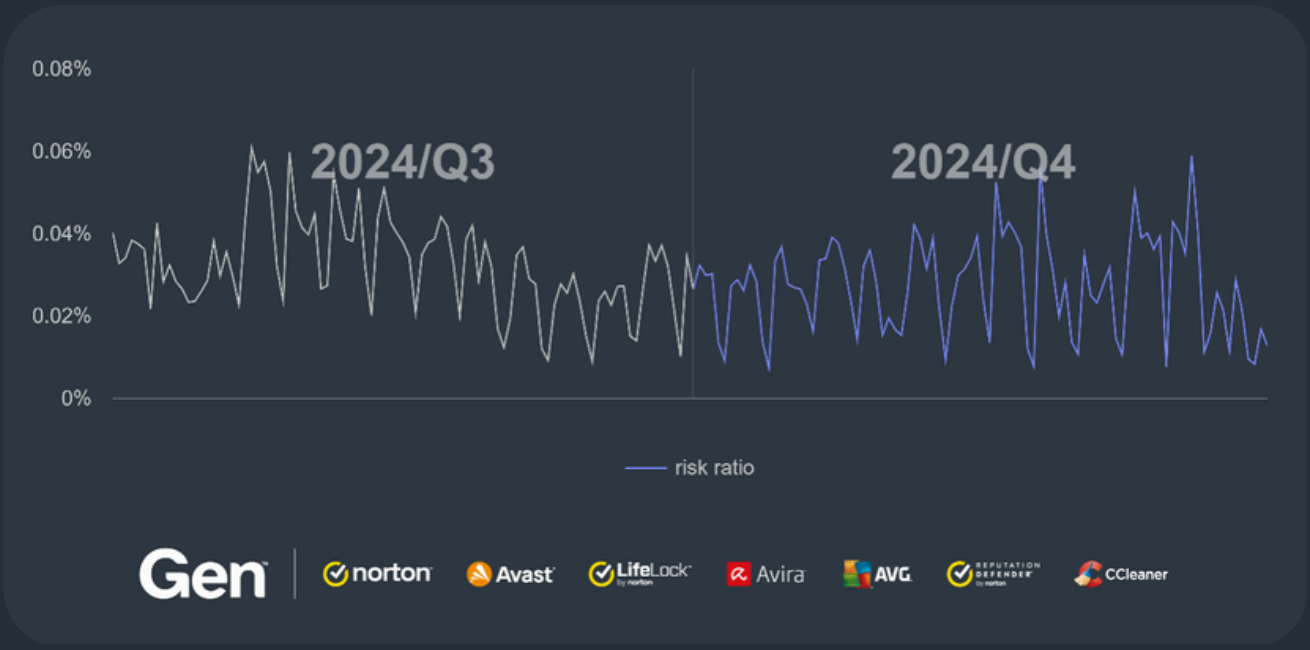
However, the most significant surge in tech support scams this quarter has been observed in Switzerland, where the risk ratio skyrocketed by 114% to 1.05%. This dramatic increase highlights a new hotspot for these scams.



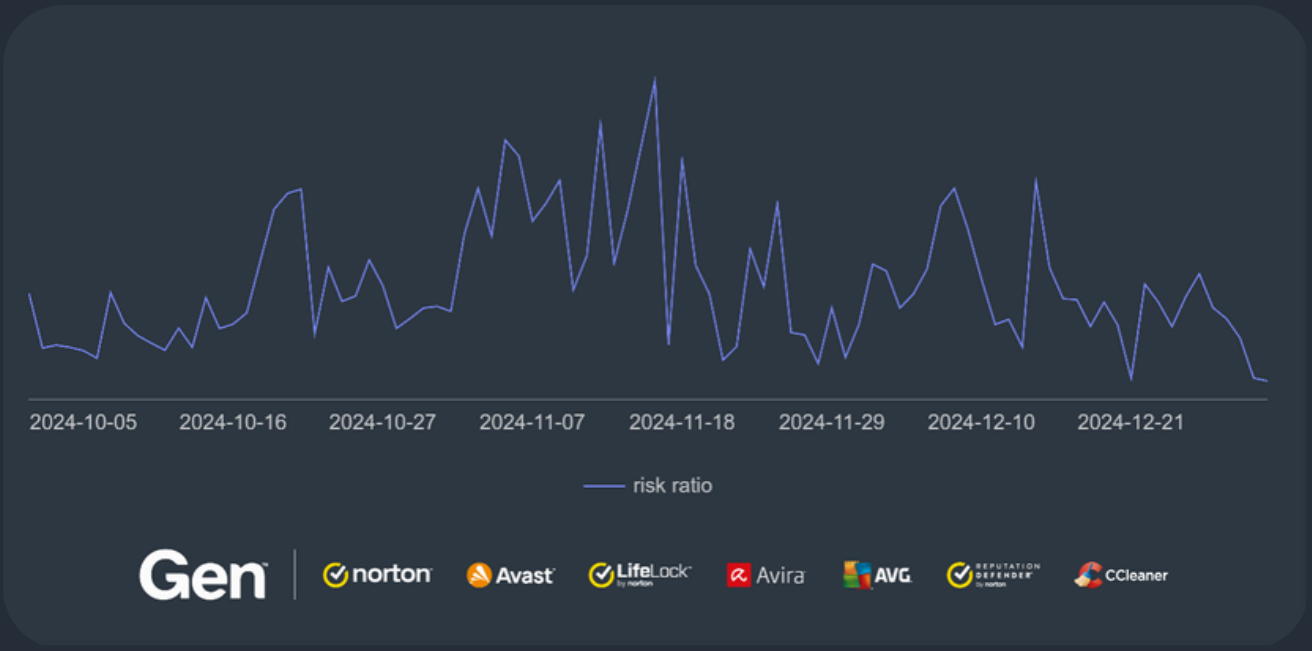
Overall risk ratio of technical support scams in Q4/2024

Austria also experienced a substantial rise, with a risk ratio of 1.06%, up by 68%. Similarly, Hong Kong saw a 43% increase, bringing its risk ratio to 0.96%, and Canada recorded a 35% rise, reaching a risk ratio of 0.80%.

France continues to be a notable target, with a risk ratio of 1.07%, reflecting a 22% increase from the previous quarter.



Activity of technical support scams for Q3/2024 and Q4/2024



Risk ratio of technical support scams for Japan in Q4/2024

Overall, while Japan remains a consistent hotspot, the significant increases in Switzerland, Austria, Hong Kong, Canada, and France indicate a broader and more dynamic threat landscape for tech support scams.

FakeCaptcha mimicking a typical CloudFlare design of CAPTCHA

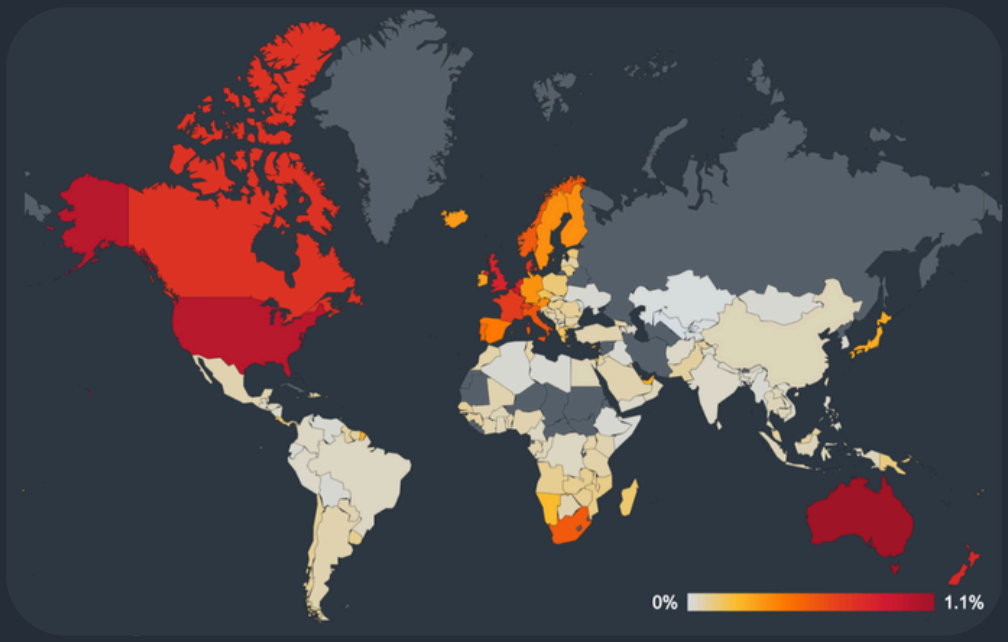
Email Threats: Unwrapping Christmas Email Scams

The Email threats section tends to cover a wide range of scams targeting almost anyone with an email address. These scams take various forms, including fake invoices designed to mimic legitimate brands and trick recipients into making payments to the attackers. Extortion emails attempt to coerce victims into sending cryptocurrency by falsely claiming to have recorded compromising webcam footage. Lottery scams lure users to websites that offer deals too good to be true, while classic phishing emails falsely inform recipients that their password has expired in an attempt to steal credentials. This section will explore the common email scams that can land in your inbox and the tactics used by cybercriminals to exploit unsuspecting users.

Christmas is always a fruitful period, not only for retailers but also for malicious actors. Regarding email scams, the threat intensity remains relatively constant throughout the last quarter of 2024, maintaining a steady threat level. Attackers take advantage of this period to amplify their efforts, primarily because the end of the year is stressful for many people. As a result, individuals often let their guard down when checking their mailboxes, making them more susceptible to scams. This targeted approach likely makes attackers' efforts more effective.

Activity of email threats for Q3/2024 and Q4/2024

As shown on the below map, the red glow is most significant in North America, indicating that the United States and Canada are most affected by email scams. These countries also experienced a notable quarterly increase of 13%. Australia follows this trend closely, with a 10% quarterly rise. The Benelux countries also reported substantial numbers, reflecting high risk ratios. Furthermore, South Africa, France, and the United Kingdom have been significantly impacted.



Overall risk ratio of email threats in Q4/2024

Apple is one of the most targeted brands by email scams, notably iCloud. The reason for this is simple: scammers aim to exploit services that the majority of users rely on. By using notable cloud providers like Microsoft 365 or Google Drive, they increase their chances of success. The example shown below claims that users will lose their cherished data, incorporating a few prominent red flags. Below are three obvious key red flags in the email:

1. **Suspicious Email Address**

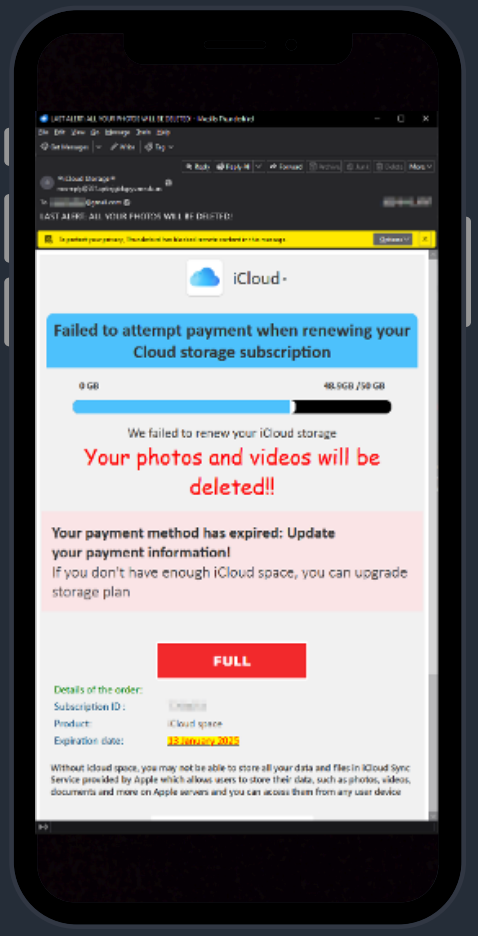
   The sender's email address (no-reply@781[.]qebsjbg...) does not match Apple's official domain (e.g., @apple.com or @icloud.com). A legitimate company like Apple always uses their verified domain.

2. Urgent and Threating language

The subject line and content use panic-inducing phrases like "LAST ALERT: ALL YOUR PHOTOS WILL BE DELETED!" and "Your photos and videos will be deleted!!". Scammers often use fear to pressure victims into acting quickly without verifying details.

3. Poor Grammar

The phrase "Failed to attempt payment" is grammatically incorrect. Professional emails from Apple or any major company are carefully crafted and free of errors. Additionally, the design feels inconsistent, with mismatched fonts, overly bright colors (e.g., "FULL" in red), and unpolished presentation. Furthermore, the email code reveals additional issues that are not immediately apparent.



Example of a recent email threat

4. DKIM Signature Failure

The DKIM signature in the email headers shows an error: dkim=permerror (no key for signature) and the domain 602.qunipameoxsp.us is not a verified or trusted sender. This suggests the email's integrity cannot be verified, which is a common sign of phishing emails.

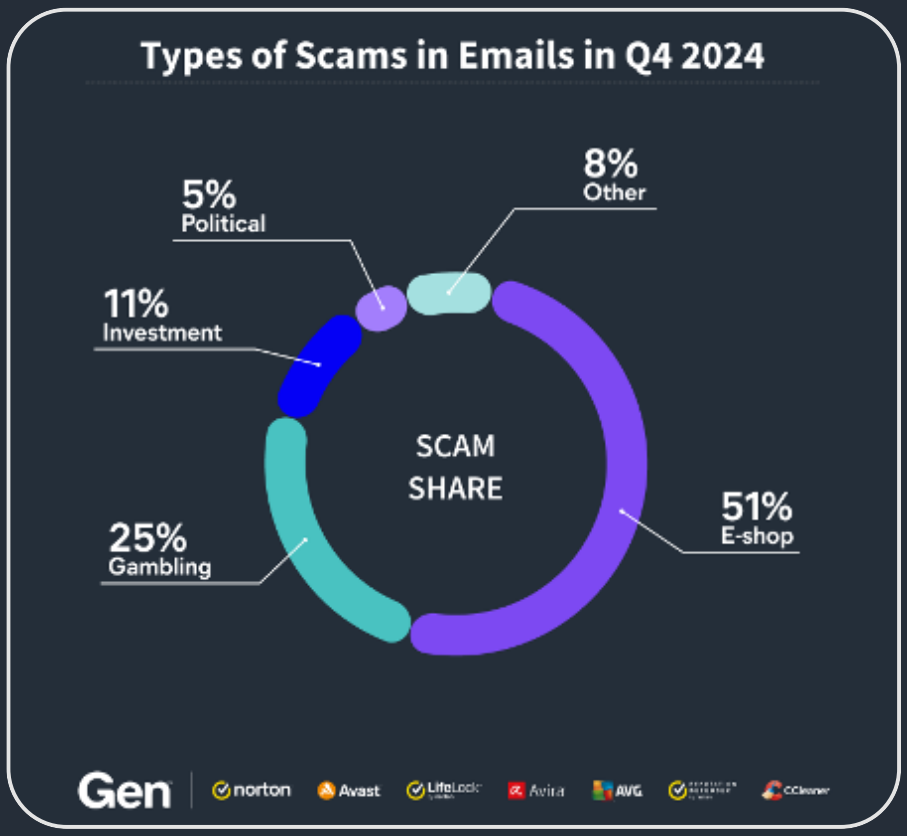
5. Malformed Links

The hyperlink in the code:
(<a href="https://storage[.]googleapis[.]com/loblaman996655/lobla.html#...">) redirects to a Google storage link instead of an Apple domain. Legitimate companies do not host critical account-related actions on third-party services like Google Storage.

6. Excessive Inline Styling and Obfuscation

The email contains overly complex and excessive inline CSS, such as numerous gradient styles and unnecessary hover effects (e.g., .divv:hover, .ligne:hover). These are often used by scammers to disguise malicious content and create a more "professional" appearance.

This quarter, we conducted a deeper analysis of the scams our customers receive in their email inboxes. From a collection of malicious emails that we analyzed, we assessed the type of scams using the AI scam type classifiers based on the email displayed to the customer.



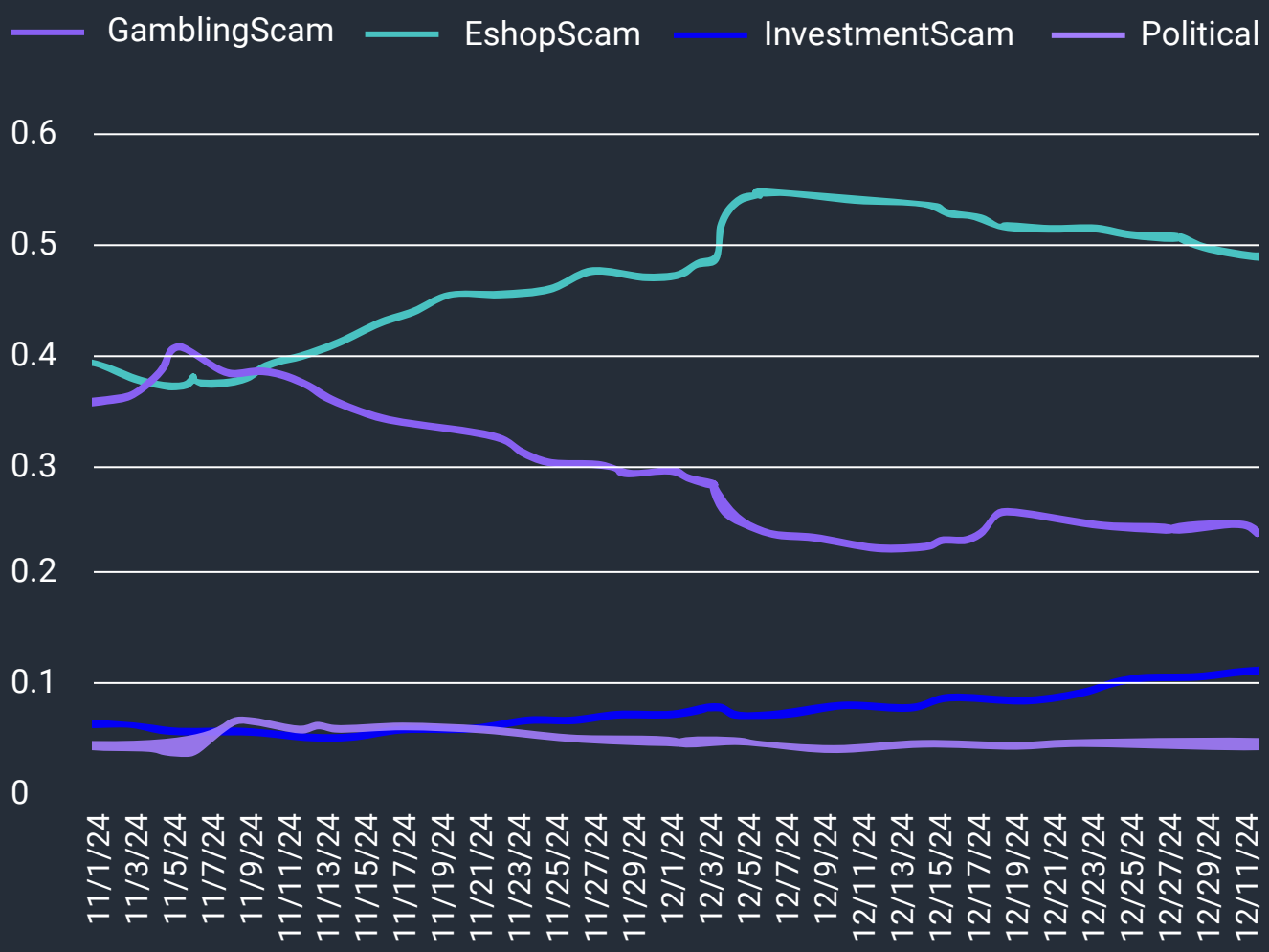
Types of scams in emails on Q4/2024

Interestingly, the most prevalent type of scam was the e-shop scam, where the attackers try to lure people to fake shopping websites. These sites either take payments and never deliver the goods or collect data from users to sell or exploit in other ways. E-shop scams accounted for 51% of all scam emails in Q4/2024.

The second most prevalent category was gambling scams, where attackers trick people into placing bets on fake gambling platforms but refuse to pay out winnings. The third most prevalent category was investment scams, where attackers advertise fake investments promising high returns or guaranteed profits in stocks, forex, property, cryptocurrencies and other assets. Finally, the fourth category was political scams, where attackers take advantage of campaigns and elections to scam people, for example by convincing them to contribute to fake campaigns.

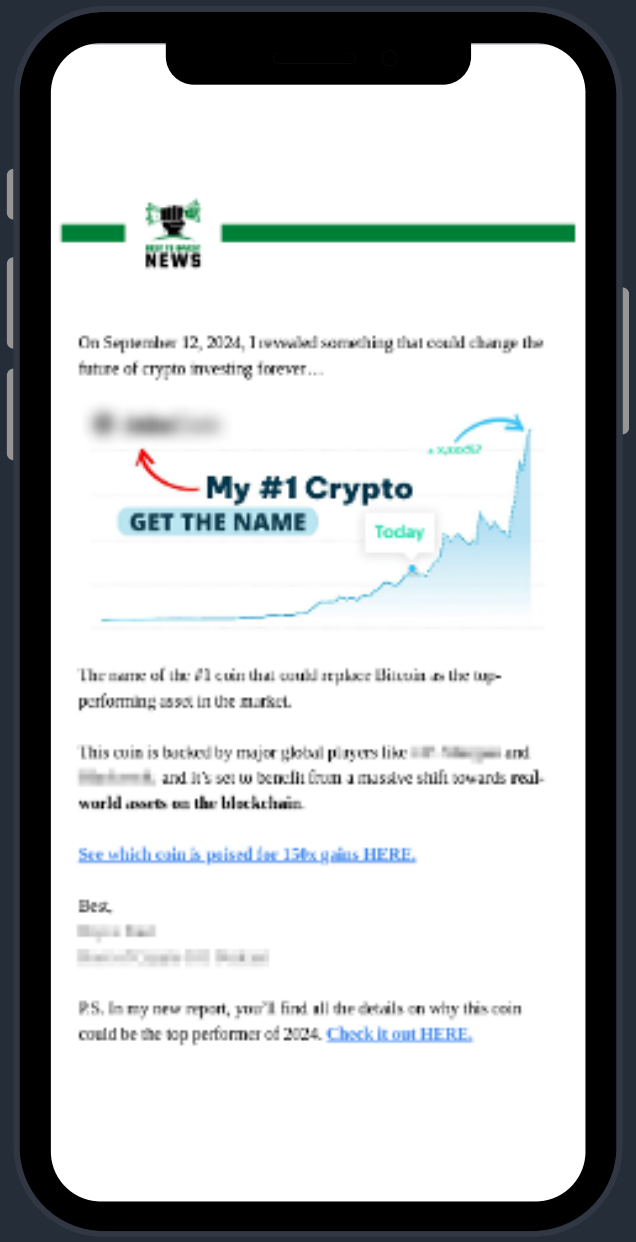
The statistics above represent the view for the whole quarter, however, towards the end of 2024, investment scams were on the rise and, in the last days of the year, there 15-25% of the daily analyzed samples were classified as investment scams.

Cumulative Relative Ratio of Email Scam Types Over Q4 2024



Cumulative relative ratio of email scam types in Q4/2024

A good example of an investment scam is displayed below. The scam in this case is luring people to click on the link to reveal the name of the cryptocurrency that is going to increase 150 times in the future. This is a common tactic used in scam emails, as the user can be redirected directly to a malicious website or asked to register and transfer funds that would never be retrieved.



Example of an investment scam seen in Q4/2024

Hidden Dangers of Fake E-Shops: Financial and Health Risks

Fake shop scams involve fraudsters creating imitation online stores that appear legitimate and trustworthy. These fake shops often mimic well-known brands or use professional-looking websites to deceive customers. Victims are lured into making purchases, believing they are buying genuine products. However, the goods never arrive after payment or are of inferior quality.

Fake e-shops, also known as scam shopping websites, pose significant consumer risks. A particularly alarming risk is to victim´s financial and physical health. Fake e-shops selling medications, supplements, or other health-related products may distribute unregulated or counterfeit drugs, which can be extremely dangerous. Additionally, falling victim to these scams often leads to financial losses and identity theft.

The largest category of fake e-shops consists of stores selling clothing and pharmaceuticals. In terms of medications, the most requested products are drugs for male erectile dysfunction, which require a prescription. Using these medications without consulting a doctor can lead to serious health complications. Moreover, the origin of these drugs is uncertain, and they may be faked substitutes with dangerous side effects.

The detected e-shops have been flagged as malicious due to several warning signs, such as the absence of a cookies consent popup, offering huge discounts, lack of clear contact information, and offering suspicious payment methods.

The payment gateways of fake e-shops are typically hosted on separate domains with valid certificates signed by untrustworthy certification authorities. Therefore, it isn't easy to immediately recognize that sensitive data is in danger since the certificate is valid from a technical perspective.

However, this ensures the victim's data is securely delivered directly to the attackers. Additionally, the attackers often enhance the legitimacy of secure data transfer by using logos of reputable security companies.

Victims typically end up on fraudulent websites by searching for specific medications, often prescription drugs, and encountering fake sites offering enticingly low prices among the search results. Another standard method to distribute fake e-shops is through advertisements on Facebook, YouTube, and Instagram, amongst other platforms. Finally, the third most frequent method is through unsolicited emails and spam.

Example of fraudulent payment gateways

In Q4/2024, we observed an increase in the activity of fake e-shops, which is an expected phenomenon during the holiday season as people are looking for attractive discounts and offers. The correlation between high-profile sales events, such as Black Friday and Christmas shopping, and the increase in scam incidents underscores the danger of online fraud during peak shopping seasons.

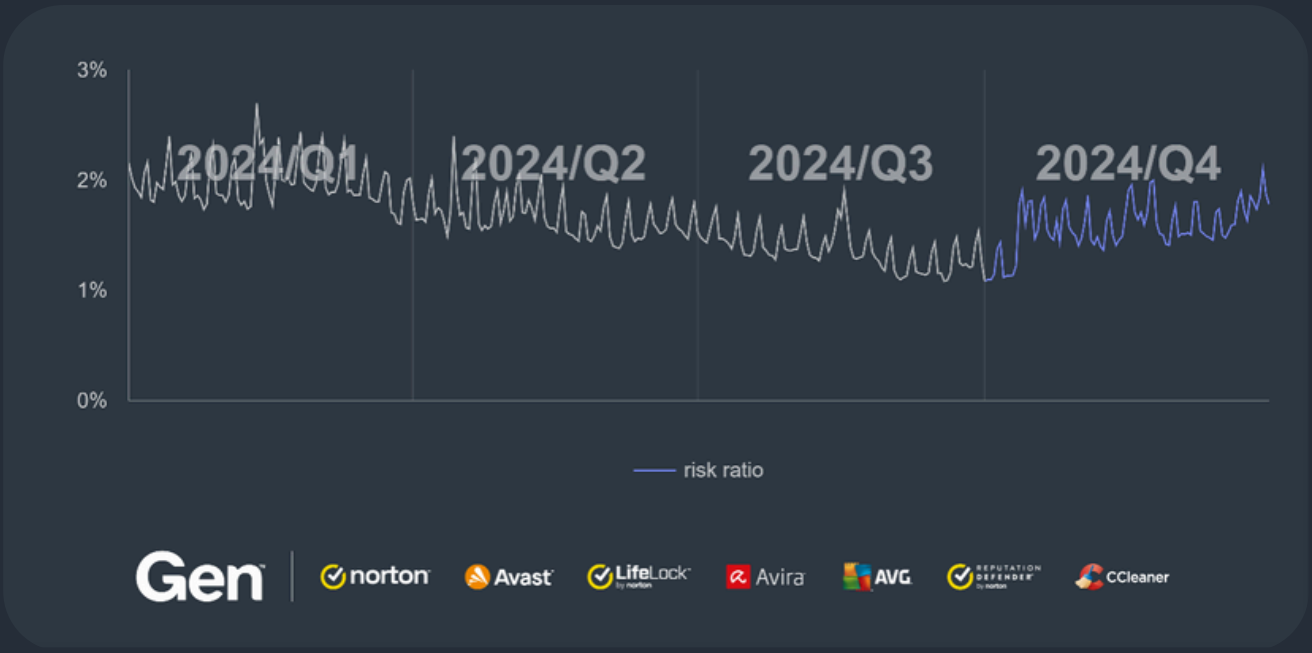
Increasing activity of fake e-shop scams in Q4/2024

The dangers of fake e-shops go beyond financial loss. These sites can compromise personal data, leading to identity theft, unauthorized transactions, and long-term damage to credit scores. Recognizing the signs of a fake e-shop and understanding the risks involved are crucial for safe online shopping.

Phishing:
A Year in ReviewFinancial and Health Risks

> *Phishing is a type of online scam where fraudsters attempt to obtain sensitive information including passwords or credit card details by posing as a trustworthy entity in an electronic communication, such as an email, text message, or instant message. The fraudulent message usually contains a link to a fake website that looks like the real one, where the victim is asked to enter their sensitive information.*

In Q4/2024, we protected 14% more users against phishing than in the previous quarter. Our data shows a diverse range of phishing activities, with some abused brands experiencing substantial increases in phishing attempts.

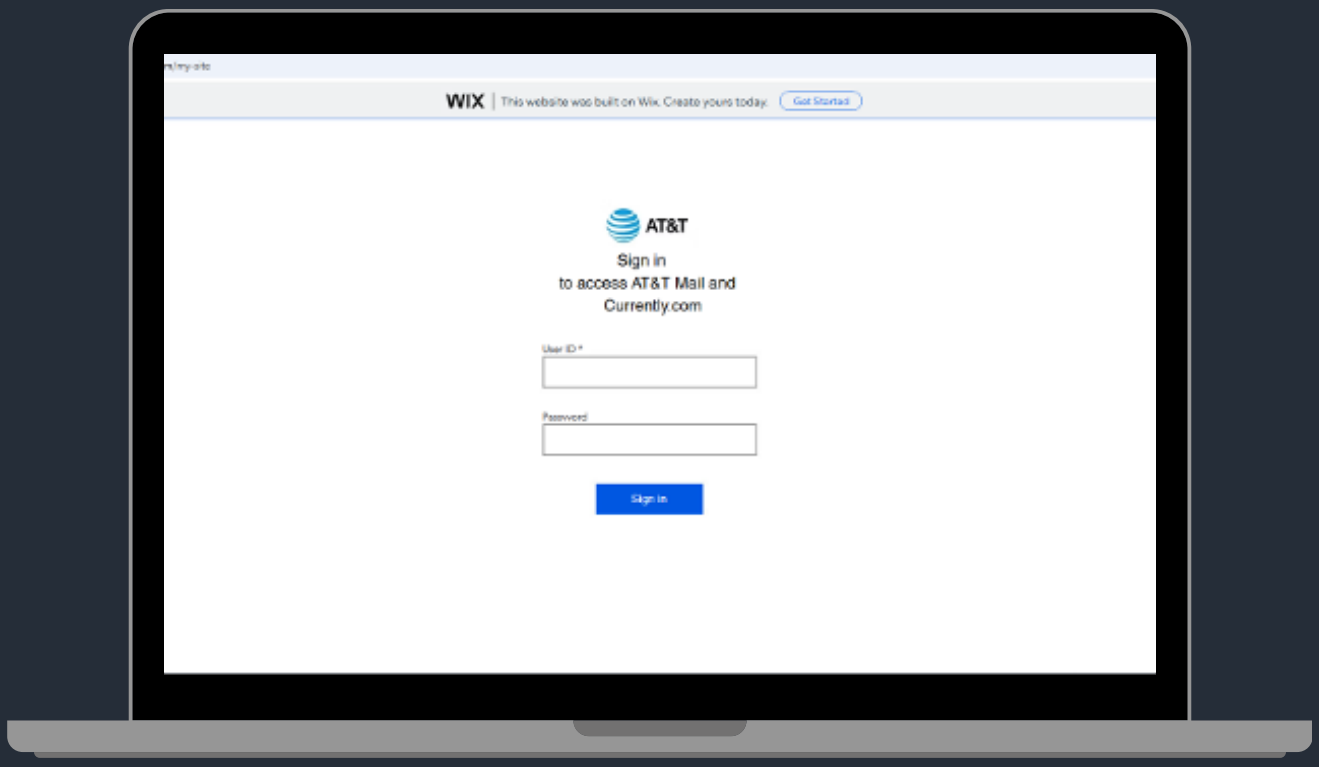


Phishing risk ratio for whole 2024

Let's start with phishing attempts targeting Amazon. We saw a dramatic increase, with a malware share of 2.42%, up by 509% from the previous quarter. This surge highlights the growing exploitation of Amazon's brand to lure unsuspecting users. Some of this increase could also be related to attackers trying to take advantage of discount shoppers, which tends to be higher towards the end of the year.

Despite a slight decrease of 1% in phishing activity for the brand, Microsoft remains a common target, with a malware share of 0.99%. This indicates a persistent threat level for users of Microsoft services.

Phishing attempts targeting Facebook increased by 36%, resulting in a malware share of 0.68%.



Example of phishing page hosted on WIS site

Financial institutions continue to be prime targets, with phishing attempts particularly for Chase increasing by 295%, leading to a malware share of 0.52%.

The most notable increase in brands imitated for phishing purposes was observed with Wix, which saw an astounding 2840% rise in phishing activity, resulting in a malware share of 0.39%. This spike indicates a new focus on exploiting website-building platforms. We observed similar behavior last year with Weebly, but this time, Wix is the primary target.

Alexej Savčin, Malware Analyst
Branislav Bošanský, Scientist
Martin Chlumecký, Malware Research
Matěj Krčma, Malware Analyst
Nikola Groverová, Data Scientist

Mobile-Related Threats

Mobile threats continues their evolution in Q4/2024 with several new strains and updates to existing ones. MobiDash adware made a resurgence fueled by a new Facebook campaign, distributing the ad-ridden threat to users worldwide by hiding in when installed and displaying out-of-context ads.

New bankers join the fray, with DroidBot utilizing its RAT capabilities to go after banking details and cryptowallets, targeting several EU countries. The newcomer ToxicPanda also made its mark, disguised as Visa, dating apps and Chrome. With its ability to disable system monitoring used by banking apps, it can act on behalf of the user to initiate payments. Lastly, the NGate banker mentioned in the previous report was spotted in new countries, utilizing the same NFC relay technique to siphon money away from users.

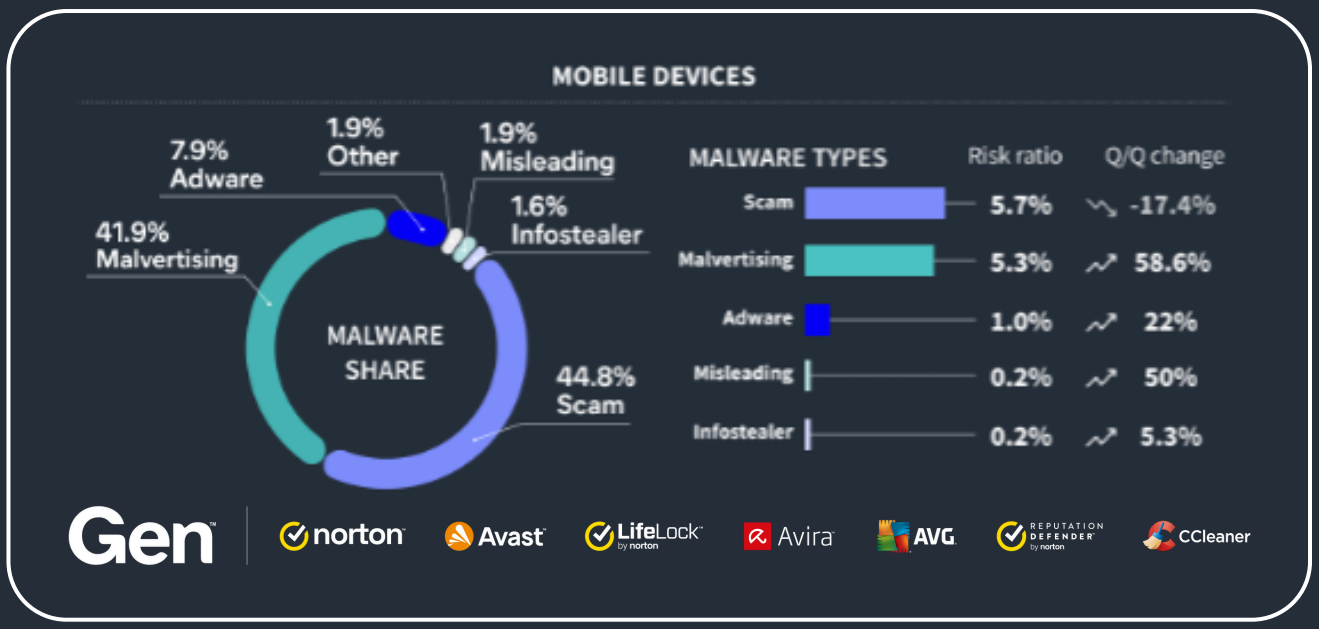
In the Spyware sphere, we saw a new strain sneak onto the Amazon app store, a rather novel distribution method. With its ability to record the screen and spy on victim's SMS messages, it posed a threat until its prompt removal by Amazon. SpyLoans continue to be a persistent threat to users worldwide, harvesting private and personal information that is later used to extort victims. Several law enforcement agencies have made inroads in tackling this nefarious threat.

Web Threat Data within the Mobile Landscape

Most blocked attacks on mobile devices in Q4/2024 were web-based, mirroring the previous quarter. Consumers are much more likely to encounter phishing websites, scams, malvertising and other web threats on their mobile devices than ever before. These threats can come in a variety of formats such as private messages, SMS and emails but also redirects on less reputable sites, unwanted pop ups and through other avenues.

In contrast to these types of mobile scams, traditional on-device malware requires a more complex infection vector where the consumer must also install the malware. For proper functionality of most mobile malware, permissions need to be granted by the consumer first, which again lowers the chances of malicious activity being triggered.

Hence, blocking web-threat based attacks is beneficial for the security of mobile devices, as malware actors often use them as an entry point to get the payload onto the mobile device of their victims.



Mobile threat landscape in Q4/2024

Norton Genie: Scam Trends and Insights from Q4/2024

Norton Genie, Gen's AI-powered scam detection tool, has proven to be an invaluable resource in identifying and categorizing the latest scam trends. This section focuses on the insights gathered during Q4/2024, comparing them with data from earlier periods to provide a clearer picture of how scammers are adapting their tactics.

Norton Genie keeps gaining popularity globally, with more than a million downloads. As its used base grows, it continues to detect an increasing variety of threats, reflecting the ever-expanding landscape of scams.

Norton Genie keeps gaining popularity globally, with more than a million downloads. As its used base grows, it continues to detect an increasing variety of threats, reflecting the ever-expanding landscape of scams.

pe of scams.

Key Scam Categories in Q4 2024

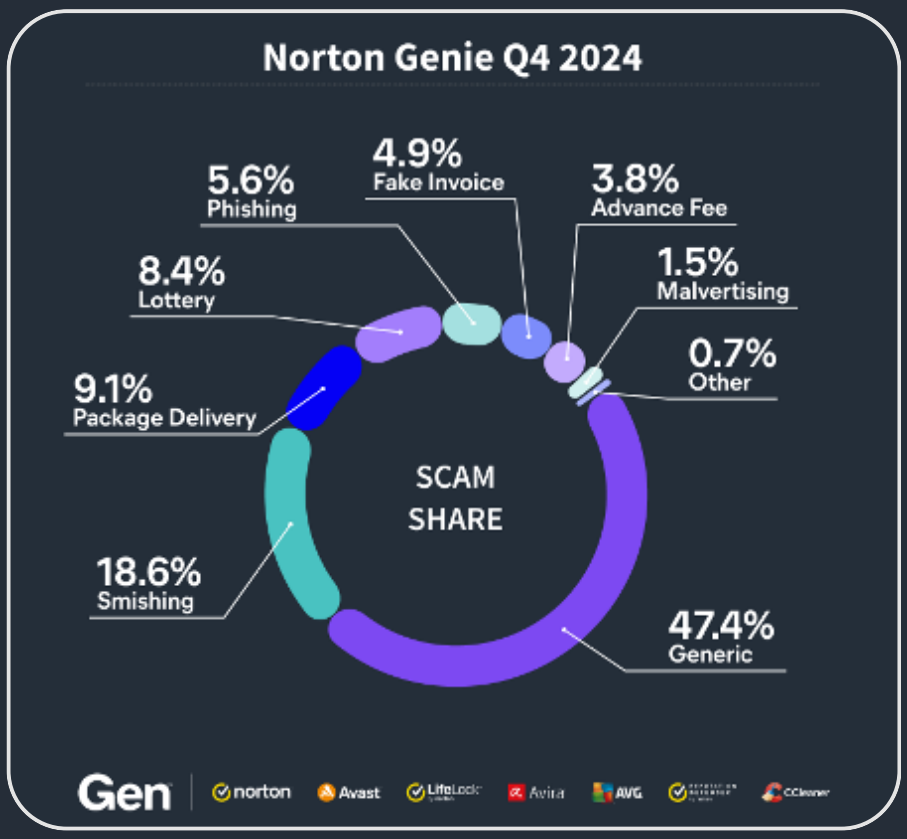
During Q4 2024, Norton Genie identified a wide range of scams, categorized as follows:

Category	Q4 2024 (%)	Q3 2024 (%)
Generic Scam	47.39%	33.80%
Smishing	18.61%	16.50%
Package Delivery Scam	9.12%	9.60%
Lottery Scam	8.43%	12.00%
Phishing	5.64%	10.60%
Fake Invoice Scam	4.90%	7.70%
Advance Free Scam	3.83%	4.50%
Malvertising	1.46%	4.10%
E-ship Scam	0.61%	-
Account Suspension Scam	0.02%	-

The table above highlights significant shifts in scam activity during the quarter. Generic scams made up nearly half of all detected threats (47.39%), a sharp increase from 33.80% in the previous report. Smishing scams (18.61%) also rose slightly, continuing to exploit the ubiquity of SMS as a communication tool. Conversely, traditional scams like lottery and phishing saw notable declines, suggesting that cybercriminals are shifting toward more diverse methods.

Visualizing the Threat Landscape

The distribution of scam categories for Q4 2024 is shown in the chart below:



Share of scams detected by Norton Genie in Q4 2024

Key Observations and Trends

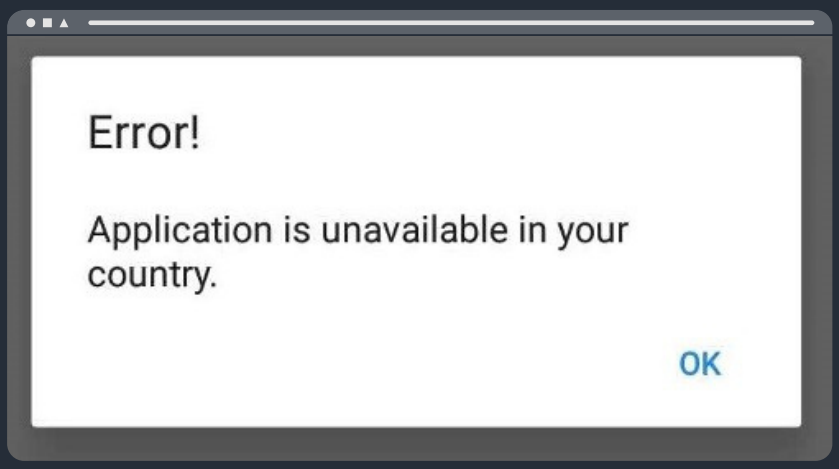
A significant rise in generic scams this quarter reflects the growing complexity of cyber threats that defy traditional categorization. These scams now account for nearly half of all threats detected (47.39%), showing the importance of adaptive, AI-driven tools like Norton Genie to address these challenges effectively.

Smishing, a form of SMS-based phishing, remains a significant threat, with its percentage rising slightly to 18.61%. This trend highlights the increasing use of mobile platforms by cybercriminals to deceive users.

Adware: Campaigning for growth

Adware threats on mobile phones refer to applications that display intrusive out-of-context adverts to users with the intent of gathering fraudulent advertising revenue. This malicious functionality is often delayed until sometime after installation and coupled with stealthy features such as hiding the adware app icon to prevent removal. Adware mimics popular apps such as games, camera filters and wallpaper apps, to name a few.

Mobile adware surged to new heights this quarter, with a 20% increase in protected users compared to the last quarter. We observed the usual adware culprits sneaking onto the PlayStore and spreading through malvertising and third-party app stores. New this quarter, several campaigns spreading MobiDash on Facebook, other social media and adult websites have contributed to the rise of adware this quarter. Generally disappearing once installed on a victim's device, adware rakes in fraudulent advertising revenue and often negatively impacts the user experience through intrusive advertising.

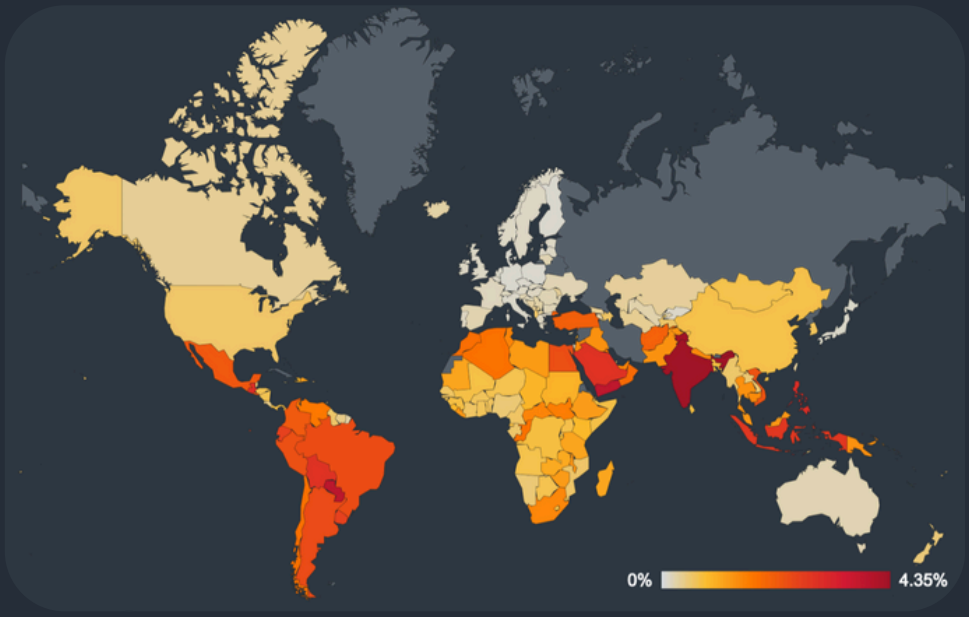


MobiDash displaying a false error message, hoping to trick the victim in leaving the app installed

HiddenAds dominated the adware sphere this quarter yet again. Once installed, this strain hides its icon and displays out-of-context device ads, much to the annoyance of its victims. HiddenAds were followed by MobiDash and FakeAdBlocker, often disguised as modded and repacked applications. Alongside the new Facebook and adult site campaigns, these strains relied on third party app stores and malvertising to spread to victims this quarter. They use various evasion techniques such as changing their icons to remain on the device and rake in fraudulent advertising revenue.

Global risk ratio of mobile adware in Q3/2024 and Q4/2024

While slower than last quarter, the growth in adware risk ratio and protected users is evident. HiddenAds and MobiDash are the main culprits, with the aforementioned campaigns bringing the threat to more victims.



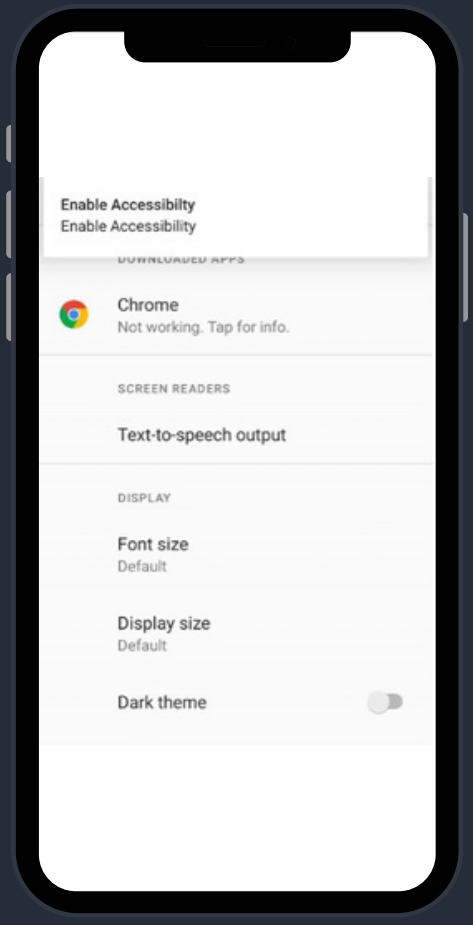
Global risk ratio of mobile adware in Q4/2024

Brazil, India, Argentina, US and Mexico have the most protected users of adware in Q4/2024. According to our telemetry, India, Paraguay and Yemen have the highest risk ratios this quarter, with India experiencing a 41% increase. The US, Brazil and Argentina experience an over 35% growth in adware risk ratio this quarter. Turkey's risk ratio has again gone down by 13%, while Egypt has gone up 15% compared to last quarter.

Bankers: More bank for your buck

Bankers are a sophisticated type of mobile malware that targets banking details, cryptocurrency wallets and instant payments with the intent of extracting money. Generally distributed through phishing messages or fake websites, Bankers can take over a victim's device by abusing the accessibility service. Once installed and enabled, they often monitor 2FA SMS messages and may display fake bank overlays to steal login information.

Bankers maintained their activity in Q4/2024, with some new strains coming in and a few older ones losing ground. We saw DroidBot banker with advanced RAT features being offered to threat actors as a Malware-as-a-service, targeting several EU countries. India becomes the target of a banking trojan that spreads through WhatsApp messages, claiming to be a utility company and requesting urgent payment. The ToxicPanda banker came into the fray, targeting Italy and Portugal while taking over victims' devices and stealing images and crypto wallet keys. Finally, NGate banker was caught stealing NFC tokens to be used for payments or withdrawals across Europe, with new hits in Slovakia, Hungary, and Poland.



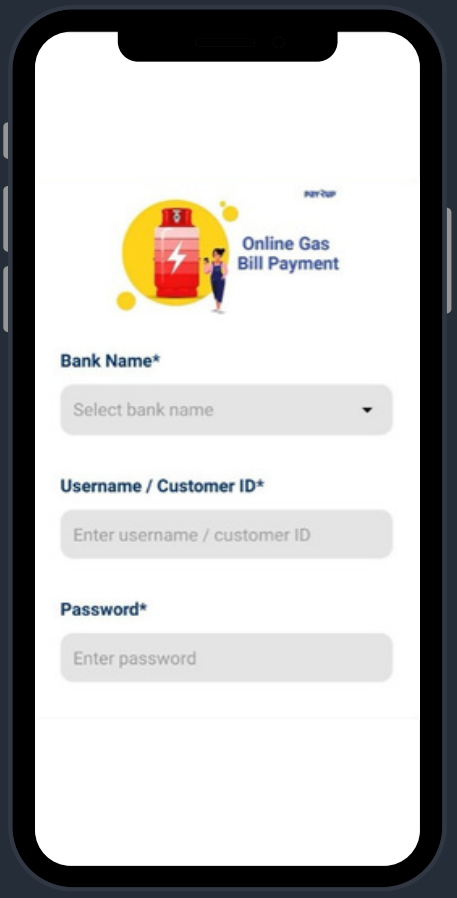
DroidBot asking for Accessibility Service permissions with a persistent notification coming from the top bar

Coper continues to lead the banker strains in terms of protected users, jumping by 19% this quarter. It is followed by the BankBot banker, which saw a staggering 236% increase in protected users compared to last quarter, owing to a new push from its creators. They are followed by Ermac and Cerberus, where no new developments mean they have mostly maintained their numbers this quarter.

DroidBot is a new banker focused on on-device-fraud through RAT capabilities with active development of new features. This threat targets the UK, Italy, Spain, Portugal, France, and Germany, with plans for a Latin America expansion down the line based on strings in its code. The creators are providing DroidBot through a Malware-as-a-Service with indications of up to 17 threat actors using the banker to steal banking credentials from victims.

As is the case with most bankers, it relies heavily on abusing the Accessibility Service. Once permissions are given to the banker, it can intercept SMS messages, key log the device and display bank phishing web pages to its victim. It can also take screenshots of the device screen periodically and even simulate user interaction through remote control, tapping buttons and controlling applications. The banker appears to be in active development, with functions such as root checks, further obfuscation and multi-stage unpacking in the works. We are likely to see the next iterations in the coming months.

A new banking trojan has recently been targeting Indian users through WhatsApp messages pretending to be utility or gas companies. Victims were threatened with losing service and advised to download an application to settle outstanding bills. Once downloaded, the banker requested various permissions such as SMS access in order to intercept 2FA messages, then prompted victims to enter their bank card details to settle the fake outstanding bills.



Banker pretending to be a gas bill payment application with intent to steal bank card details

The threat actors behind this banker used Supabase, an open-source database service used as an alternative to Firebase, to extract the banking details from victims' devices. Unfortunately, they left the instance unsecured, allowing access to thousands of stolen victim credentials. This highlights the potential severe negative impact bankers and the associated loss of stolen data can have on its victims.

ToxicPanda joined the banker field with account takeover features mainly targeting users in Italy and Portugal. Disguised as Chrome, Visa and dating apps among others, it aims to infiltrate victims' devices. Once installed, it requests the usual permissions to initiate its malicious activity. Through using the Accessibility service, it grants itself further permissions and begins its on-device-fraud activity, attempting to conduct payments on behalf of the victim. Interestingly, it attempts to disable common system behavior monitoring used by bank applications in order to mask its activity. It also collects images from the device, potentially leaking further sensitive information.

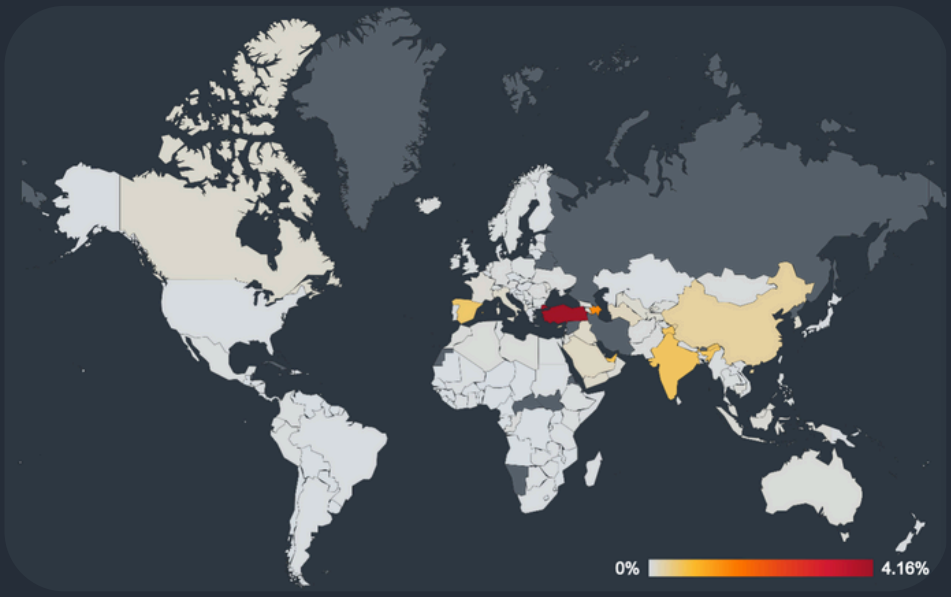
The actors behind ToxicPanda are able to remotely control the banker through a variety of commands, enabling them to record the screen and perform various operations on behalf of the victim. It may also download further payloads or attempt to extract wallet keys from crypto wallet applications. The group behind this new strain are likely based in China, as their C2 and code indicate a Chinese speaking developer. New iterations of this banker are to be expected soon.

ToxicPanda C2 login page, likely indicating a China-based developer is behind the banker

The NGate banker mentioned in the last quarterly report appears to be doing the rounds again in new countries, albeit in smaller numbers. Targeting victims in Slovakia, Poland and Hungary, the banker is distributed through phishing pages pretending the be the target bank. Using PWAs (Progressive Web Apps) with the appearance of the target's bank, victims are tricked into downloading the NGate banker payload. Once downloaded, the victim's device is used as an NFC relay. The victim is prompted to tap their card to their phone, effectively allowing the threat actors to withdraw money from ATMs or use the stolen NFC token for payments. The nature of the money theft is fairly unusual in the banker sphere due to the required physical presence near an ATM or card terminal. It is likely we will see this novel technique be used in the wild and potentially by other banker strains in the future.

Banker evolutions this quarter were not as dynamic as in previous quarters, but the numbers of protected users and risk ratio have remained consistent overall. Coper continues its rise with staggering numbers, owing to a new push from its creators. Strains such as MoqHao that were targeting Korea and Japan continue to do so, but with less effect as we see a 20% decrease in protected users.

Global risk ratio of mobile bankers in Q3/2024-Q4/2024



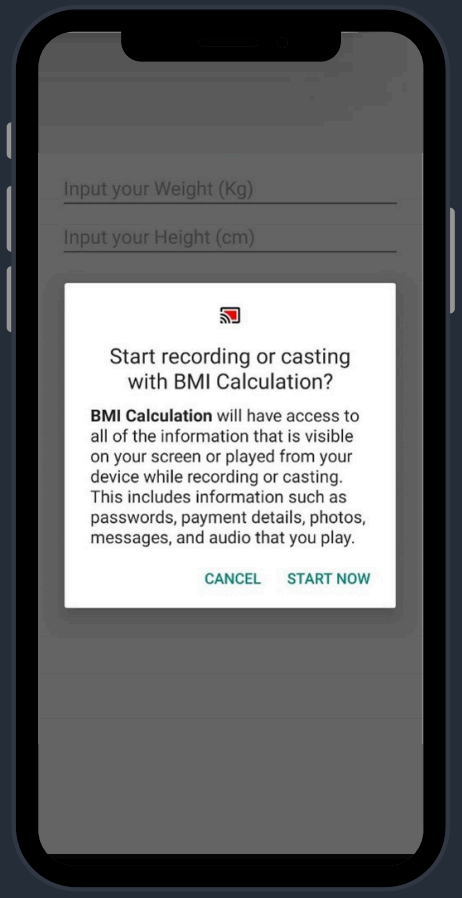
Global risk ratio for mobile bankers in Q4/2024

Turkey, Azerbaijan, UAE, Spain and India have the highest risk ratios for mobile bankers this quarter. Our telemetry shows an 83% increase in risk ratio coming from Spain, while Turkey mostly maintains its already high risk ratio and numbers of protected users. Italy also sees an 83% rise in risk ratio, owing to the new strains such as ToxicPanda and DroidBot that target the country.

Spyware maintained its activity in Q4/2024, with a 6% increase in protected users compared to the previous quarter. In terms of new spyware, the Amazon app store was used as a distribution platform for a new spyware disguised as a BMI calculator. Meanwhile SpyLoans continued to plague victims worldwide, stealing personal information for blackmail purposes. This has not gone unnoticed by law enforcement, as we see several large raids on call centers running these malicious apps.

SpyMax maintained its top place in the spyware category with unchanged numbers of protected users. It continues to spread through various fake applications on third party app stores and through malvertising. Malicious WhatsApp mods are trailing close behind, with a 24% increase in protected users. Mods for WhatsApp are popular, and threat actors are keen to get in on the fun, stealing user conversations and enabling further malicious activity on the device. We also see a staggering 268% increase in SpyLoan protected users this quarter, due to its continued spread on the PlayStore worldwide.

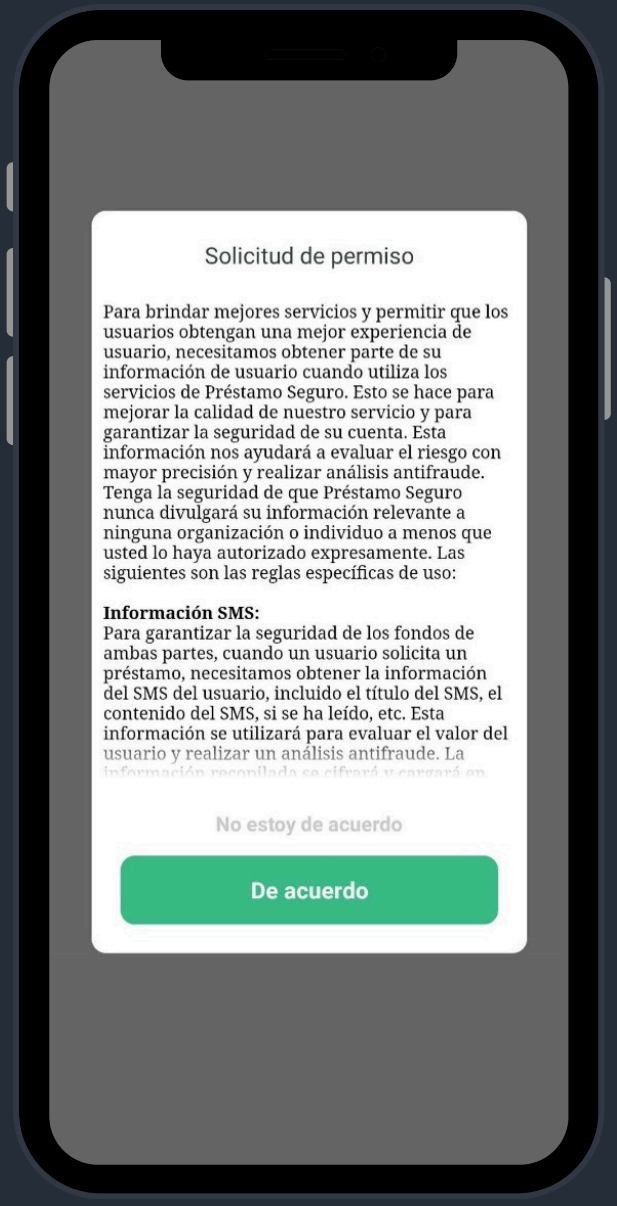
An emerging spyware strain has used a rather novel distribution method this quarter, utilizing the Amazon app store to target its victims. Disguised as a body mass index (BMI) calculator, the app requests to record the screen once a BMI calculation was initiated. While the app records the screen, the developers forgot to properly implement the code that would send the recording mp4 file to a C2. The spyware also collects all SMS messages and a list of installed apps on the device, these would be sent away correctly.



BMI Calculation requesting to start screen recording, despite being unable to send the recording file to its C2

While the PlayStore is normally the preferred app store of malware authors as it allows them to they can reach the biggest audience there, the rising number of official Android app stores leads to a more distributed approach.

SpyLoans have been a persistent threat targeting victims worldwide for several years now, going after private and personal information that is often used for blackmail. Historically, SpyLoans have been most active in India, Mexico, Brazil and Vietnam. Mostly using the PlayStore as a distribution method, operators of these shady loan apps are not registered with financial regulators and thus are not subject to any oversight. SpyLoans are often distributed through wide marketing campaigns promising quick money but with high interest rates and predatory repayment scheduling. Once installed, the malicious apps request access to SMS messages, photos and images on the phone as well as contact lists and call logs. In some cases, the SpyLoan apps will request access to the device's camera and microphone, potentially enabling further spying on the victim. The extortion and threats usually come within a few weeks, with the actors using the acquired personal information to threaten the victim unless payments are promptly made. Reviews on the PlayStore highlight the amount of harm caused by these practices, with threats of sensitive photos being released to entire contact lists or even threats of physical violence in some cases.



SpyLoan makes a request to access personal information which includes SMS, contacts, location, and others

★☆☆☆☆ April 15, 2024

The pay day says 1 day and they start charging you 1 day before, wth threatening calls and messages, also threatening to killing me or my contacts... Google take a look at this and validate the entity.... A complete scam and life threating.

107 people found this review helpful

★☆☆☆☆ March 22, 2024

They are sending P O R N to my contacts before the due date is tomorrow. They are so rude and not acceptable.

30 people found this review helpful

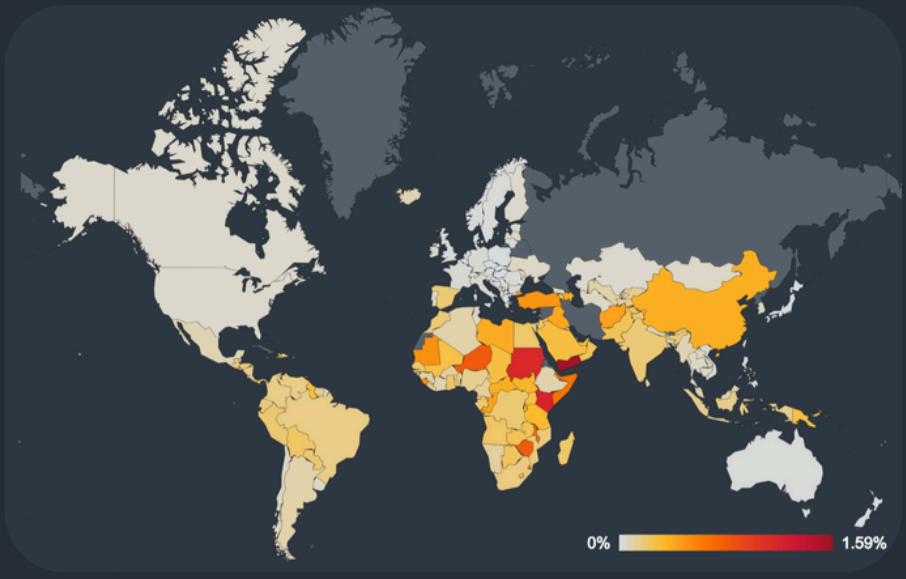
Victim reviews from the PlayStore, showcasing the threats and extortion they have been subjected to by the SpyLoan operators

SpyLoans have not gone unnoticed and numerous countries have gone after the actors behind these nefarious apps. A fake call center in Peru was shut down and the main actors arrested after scamming over seven thousand victims.

Global risk ratio of mobile spyware from Q1/2024 to Q4/2024

Chilean police have shut down a similar call center and arrested 25 people, with over two thousand victims losing their money. It is evident that SpyLoans are a persistent threat in countries where bank loans are more difficult to attain, causing severe financial and personal harm to victims.

The graph shows a substantial growth in spyware risk ratio throughout 2024. Threats such as SpyMax, malicious WhatsApp mods and SpyLoans have significantly increased their prevalence this year, through using the PlayStore and third party app stores as well as malvertising and push notifications to spread.



Global risk ratio for mobile spyware in Q4/2024

Yemen and Kenya have the highest risk ratio of spyware this quarter, while Brazil, India, Turkey, Spain, and the US have the highest numbers of protected users in Q4/2024. Brazil experienced a 23% growth in risk ratio this quarter while Spain had a staggering 137% increase this quarter.

Jakub Vávra, Malware Analyst
Michalis Pachilakis, Research Engineer

Acknowledgments and Credits

Malware researchers

Adolf Středa
Alexej Savčin
Branislav Bošanský
Branislav Kramár
David Álvarez
David Jursa
Igor Morgenstern
Jakub Křoustek
Jakub Vávra
Jan Rubín
Ladislav Zezula
Luigino Camastra
Luis Corrons
Martin Chlumecký
Matěj Krčma
Michal Salát
Michalis Pachilakis
Nikola Groverová
Ondřej Mokoš
Siggi Stefnisson

Communications

Aneta Šeráková
Ashlynn Rosenberg
Brittany Posey
Jenna Torluemke
Nyrmah J. Reina

Data analysis

Filip Husák
Lukáš Zobal
Nikola Groverová
Patik Holop
Pavol Plaskoň

Brand design

Alisha Robinson
Youan Lin