

Gen™



Q1/2025 Threat Report

Gen Protects Millions of People as Breached Personal Information, Phishing Reports, Fake Browser Update Scams and Scam-Yourself Attacks Are on the Rise



- 03 Foreword**
- 06 Threat Landscape Highlights**
- 17 Featured Stories: Deception, Innovation and Exploited Trust**
- 34 In Closing**
- 35 Acknowledgments**

Table of Contents

Foreword

With this issue of the Gen Threat Report, we are introducing a more streamlined format, making it easier to digest and focusing more on key highlights, trends and emerging threats rather than attempting to catalog every detail. The Threat Landscape Highlights section will capture notable trends and evolving threat dynamics, and Featured Stories will now dive deeper into specific investigations.

The threat landscape in Q1/2025 might look surprising to some. At first glance, the decline in the total number of blocked attacks compared to the previous quarter might seem like a welcome reduction in activity. However, this drop is not solely seasonal or due to reduced attacker activity. More importantly, this decrease highlights a deeper evolution in tactics: broad 'spray and pray' campaigns are giving way to more tailored, deceptive and persistent attacks. The threats that did emerge this quarter are more focused, strategic and reflect the growing sophistication of attackers.

Q1/2025 uncovered: Gen Threat Labs reveals latest trends

Financial threats

- **3.8M** stolen in deep-fake led CryptoCore campaign
- Rise in banking trojan activity
- Surge in fraud alerts

Data-stealing threats

- Spike of **+186%** in breached records
- Increase in infostealer malware
- Emergence of AI-built ransomware

Scam threats

- Over **+4M** users protected from Scam-Yourself Attacks
- **17x** increase in fake software updates
- Rise in AI personas pushing scams

Financial threats showed new levels of innovation. The CryptoCore group executed one of its most refined campaigns to date, blending deepfake videos of public figures, compromised YouTube accounts and professionally cloned websites. This most recent campaign resulted in an estimated \$3.8 million in illicit profits over 2,200 transactions (although the real number is likely far higher). Mobile financial threats also escalated. The Crocodilus banking trojan, most active in Spain and Turkey, abused accessibility features to overlay fake login pages and steal crypto wallet credentials. Meanwhile, our LifeLock insights showed rising levels of credit and transaction alerts, indicating both increased monitoring activity and more frequent fraud attempts targeting users' financial footprints.

Data-stealing threats also continued to rise across multiple categories based on our telemetry. The number of data breach events — meaning instances where a company or platform was breached — increased by more than 36% quarter over quarter, while the total number of breached records — or personal data such as email, passwords, credit card numbers, etc. — surged by more than 186%. While large-scale service breaches made headlines, attackers were also using direct compromise of user data through infostealers such as Lumma Stealer (which has since been successfully taken down through a [collaboration between Europol and Microsoft](#)). Furthermore, phishing continued to play a growing role in data compromise — we documented how adversaries are abusing low-code form-building platforms to host phishing campaigns on legitimate infrastructure, making detection and takedown significantly harder. Lastly, ransomware remained a high-risk threat, building over the last three quarters. The majority of cases continued to be driven by the usual suspect, Magniber, but new strains, such as FunkSec, also emerged. FunkSec, in particular, had been allegedly partially generated using AI and large language models (LLMs).

Scam threats were marked by significant diversification and reach. We protected more than 4 million people from Scam-Yourself Attacks, a category that now spans platforms and operating systems. FakeCaptcha, once confined to Windows, expanded to macOS and began distributing the infamous infostealer AMOS (Atomic Stealer) under the guise of phishing protection. Touché.

Moreover, social media remained a key vector for scams, with compromised Facebook and YouTube accounts used for both distribution and monetization. Attackers combined AI-generated personas, hired influencers and platform-native ad systems to lend legitimacy to fraudulent campaigns. In parallel, Fake Update attacks, another type of Scam-Yourself Attack in which people are asked to update their device or programs but are instead guided to infect their devices, targeted European users causing an unprecedented growth of 17 times of the risk exposure compared to last quarter.

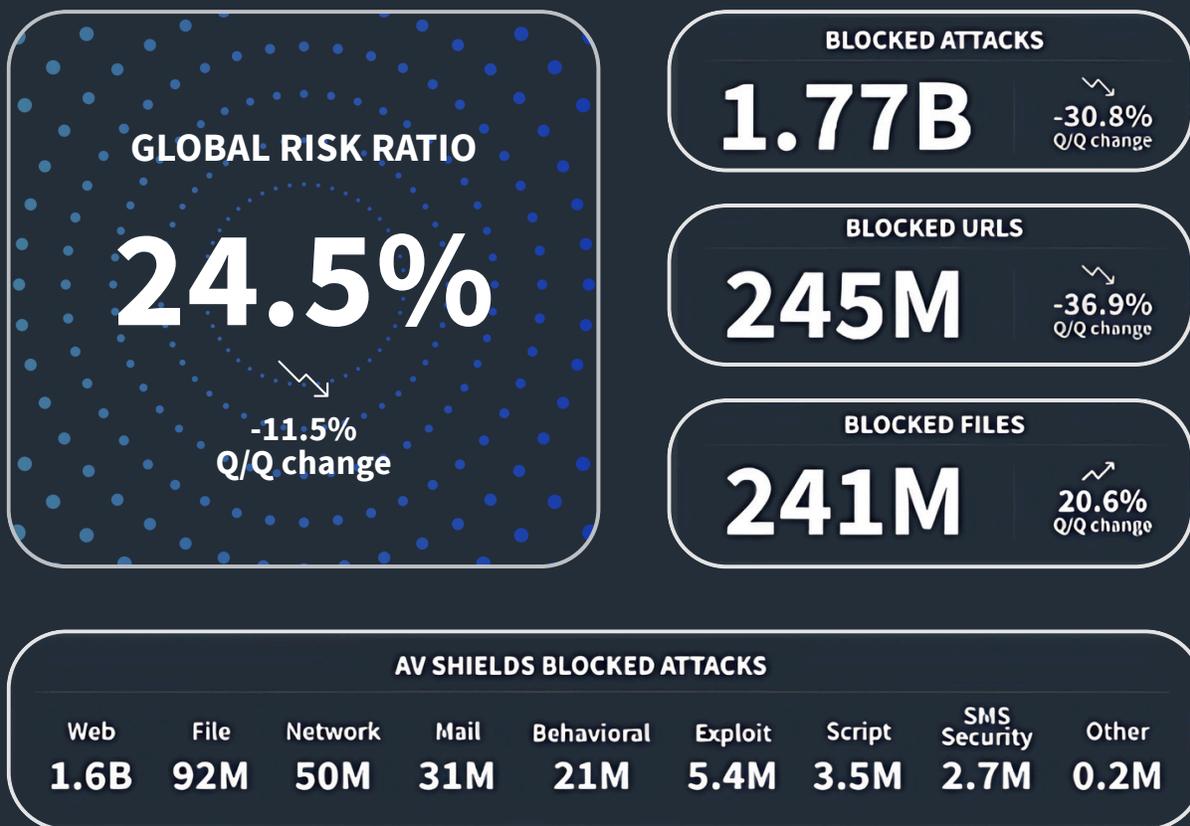
We hope you find the Q1/2025 Gen Threat Report engaging and informative and the new format easy to digest. Thank you for reading.

Jakub Křoustek, Threat Research Director

Threat Landscape Highlights: Q1/2025

While the list of the most prevalent threat type remains the same or nearly similar throughout the years, the threat landscape continuously evolves through the ways in which threat actors work to achieve their malicious ambitions. How the landscape shifts is inevitably affected by our digital activities, from the use of social media to online shopping and learning to recent events affecting the security of our digital lives, such as data breaches.

In this section, we aim to provide insight into emerging threats, new techniques and trends and interesting changes in the otherwise expected behavior of the global threat landscape.



BREACH PROTECTION

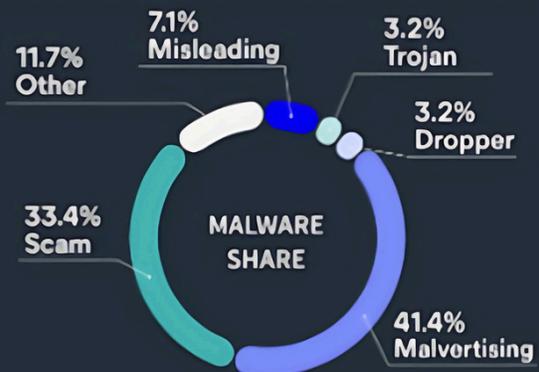
Metric	Value	Q/Q change
Breached records	12.9M	↗ 186.3%
Breached user e-mails	0.5M	↗ 102.9%
Breach events	1172	↗ 36.1%

IDENTITY PROTECTION

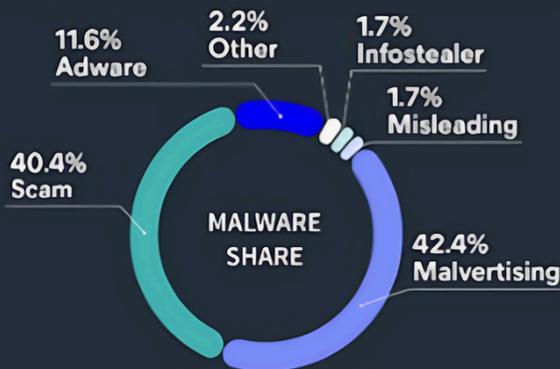
Metric	Value	Q/Q change
Number of alerts	31M	↗ 1.4%
Number of alerted users	5M	↗ 3.7%

DESKTOP DEVICES

MALWARE TYPES	Risk ratio	Q/Q change
Malvertising	14.6%	↘ -15.5%
Scam	11.8%	↘ -16.7%
Misleading	2.5%	↘ -8.9%
Trojan	1.1%	↗ 5.0%
Dropper	1.1%	↘ -38.7%



MOBILE DEVICES

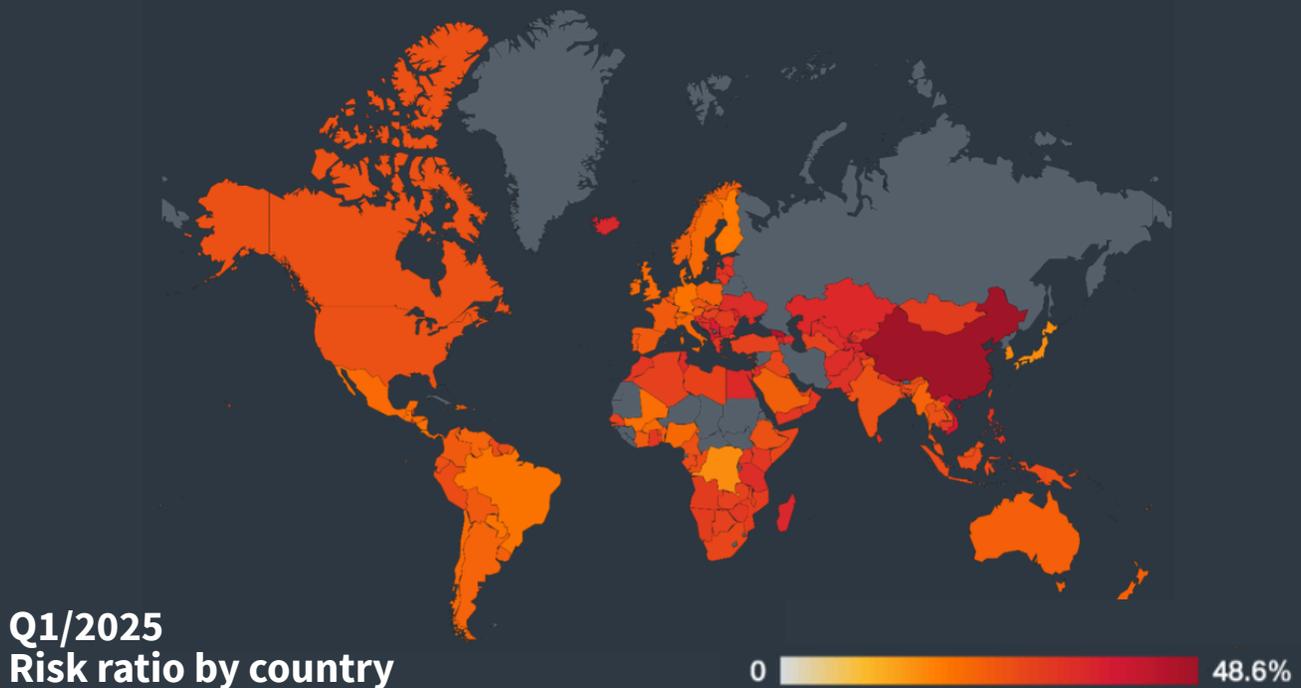


MALWARE TYPES	Risk ratio	Q/Q change
Malvertising	4.3%	↘ -18.7%
Scam	4.1%	↘ -27.4%
Adware	1.2%	↗ 18.6%
Infostealer	0.2%	↘ -16.6%
Misleading	0.2%	↘ -28.3%

Global Risk Snapshot

Global risk ratio: 24.53%

Cyber risk remained high in Q1/2025, with a global average risk ratio of 24.53%, consistent with the heightened levels observed in late 2024. However, exposure remained highly uneven across regions.



The highest threat activity concentrated in parts of **Asia and Eastern Europe**. **China** topped the list with a risk ratio of 48.60%, followed by **Georgia (44.51%)** and **Vietnam (39.06%)**. These figures reflect a mix of aggressive targeting, insufficient defensive infrastructure and high digital engagement.

In contrast, major economies like **Japan (16.12%)**, **Germany (20.11%)** and **France (24.93%)** reported significantly lower risk ratios, while **Scandinavian countries** like **Finland (19.36%)**, **Sweden (22.14%)** and **Norway (23.96%)** continued to show resilience against attacks thanks to mature cybersecurity practices.

South America remained a region of interest, with **Brazil (20.14%)** and **Argentina (23.24%)** experiencing spikes in mobile-specific threats. Meanwhile, countries with limited digital infrastructure — such as **Haiti (18.44%)** or the **Democratic Republic of Congo (16.24%)** — saw reduced exposure simply due to lower internet penetration.

Countries most at risk

1. China	48.60%	6. North Macedonia	37.68%
2. Georgia	44.51%	7. Tajikistan	36.88%
3. Vietnam	39.06%	8. Moldova	36.64%
4. Serbia	37.85%	9. Iceland	36.02%
5. Albania	37.72%	10. Armenia	35.75%

Personal Data at Stake: Data Breaches & Information Stealers

Personal data is like digital gold to criminals, and risks to digital identities continue to increase. Based on our telemetry, data breach events — instances where a company or platform was breached — rose 36.12% quarter-over-quarter. Breached records increased by 186.26%, with breached user emails alone up 102.93%. More than 1.19 million records were reported with high or critical severity, meaning that the breached records also included plaintext passwords, potentially giving cybercriminals the figurative keys to over a million of people's personal accounts.

Large-scale data breaches are no longer rare. Notable digital-identity events in Q1/2025 included:

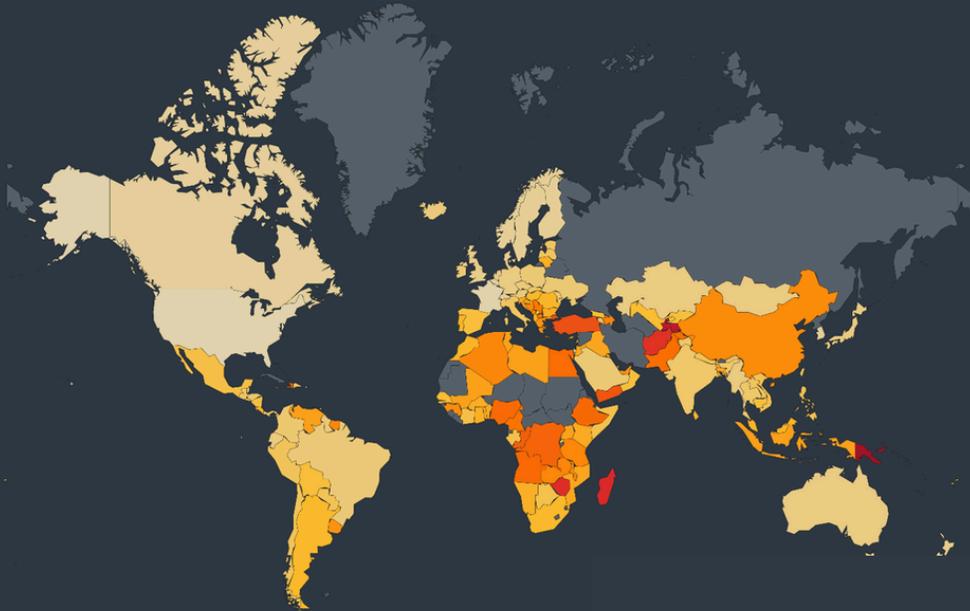
- **USOSGM:** Exposed full names and addresses of U.S. shoppers.
- **ALIEN TXTBASE:** Huge collection of stolen user credentials published on Telegram channel — 493 million unique website and email address pairs, affecting 284 million unique email addresses.

One of the protective measures we provide for our users is alerting them when a significant breach happens and their personal data is exposed or possibly affected by a recent data leak. These alerts give our customers the opportunity to responsibly react and secure their personal data in advance of fraudulent activity by attackers. In Q1/2025, alerted users increased too with notable spikes in:

- **Credit Alerts:** +13.83%. These alerts are related to new accounts, credit inquiries, changes in credit profiles, etc., and they notify users of potential fraud attempts or suspicious activity in real time.
- **Criminal Record Alerts:** +11.98%. These are related to users' identity appearing in legal or criminal records, including court cases, judgments, and sex offender notifications. These alerts inform users of potential misuse of their identity or unauthorized legal associations.
- **Transaction Alerts:** +3.04%. Transaction alerts track financial transactions across users' bank accounts, credit cards, and investment accounts. These notifications highlight unusual charges, threshold limits were exceeded, or payday loan applications.

Data stealing efforts via information stealers also rose in Q1/2025, with a 8.24% increase in risk ratio, again driven by the [Lumma Stealer](#) which:

- saw a +59.4% increase in malware prevalence, now at 19.51%, now at 19.51%
- harvested credentials, crypto wallets, 2FA tokens
- delivered via phishing, GitHub abuse, and Scam-Yourself attacks



Q1/2025

Global risk ratio for information stealers

0%  4.03%

Other prominent infostealers by their malware share were:

- FormBook (12.47%)
- AgentTesla (10.99%)
- Ramnit, MassLogger, Fareit, SnakeKeylogger, Lokibot

The regions most impacted by information stealers were Turkey, Egypt, Indonesia and Argentina.

Scams & Social Media Exploits

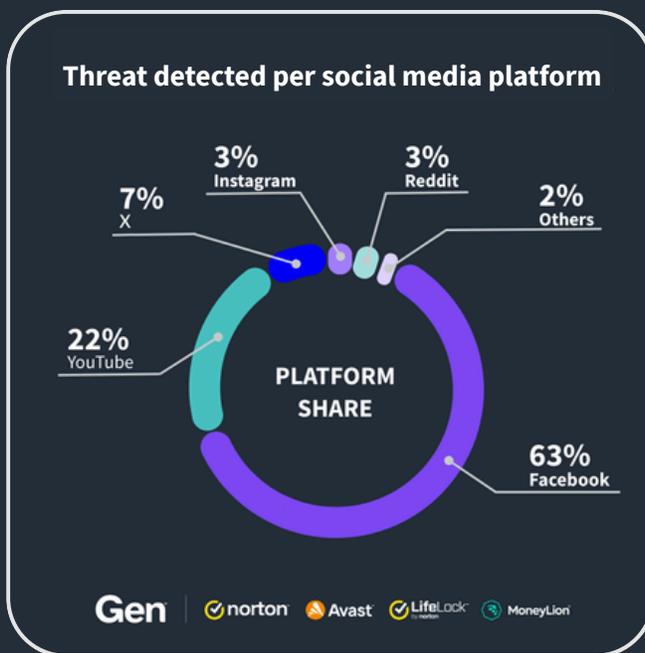
Scams continue to evolve as one of the most widespread and adaptable cyber threats, exploiting both traditional and modern delivery channels. In Q1/2025, we observed scammers leveraging everything from [malvertising](#) (malicious advertising) to social media platforms and push notifications to reach potential victims. This broad attack surface was amplified by the wealth of user data available online, enabling highly targeted and convincing scams. Bellow, we highlighted some of the key trends and tactics shaping the scam landscape this quarter:

- **Malicious push notifications** delivering scams increased 10.26% in the risk ratio for Germany, followed by Norway (+24.85%) and Denmark (+22.42%).
- **Financial scams** increased 500% in Lebanon, 223% in Moldova, 112% in Portugal and tens of percents also in Slovakia, Serbia, Estonia and Slovenia.

Social media also remained a favored delivery mechanism for scams and other related threat types. In Q1/2025, 63% of social-media-related threats were observed on Facebook, followed by YouTube with 22% platform share.

Platforms like Reddit and Instagram remained a relevant threat, while X (formerly Twitter) held steady at 7%. LinkedIn, a business and employment-oriented social network, observed a rising trend with 26.23% increase of its share.

The types of threats found on each social media site varied due to user demographics and usage patterns, with malvertising continuing to top the threat types on social media 30% of the total share, followed by phishing (21.72%).

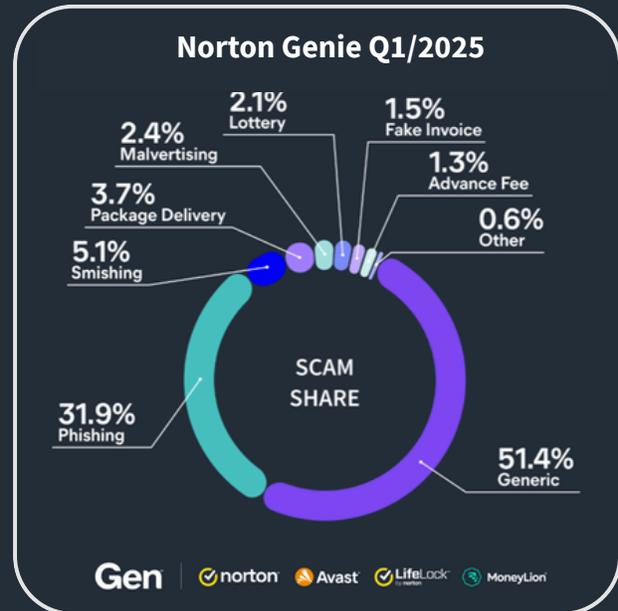


Attacks delivered through social media platform

Q1 Scam Trends Revealed by Norton Genie

Our Norton Genie scam detection tool shows the different type of scams reported by users:

- **Generic scams:** 51.4%
- **Phishing:** 31.9% with a massive 4x increase quarter-over-quarter
- **Malvertising:** 2.41%



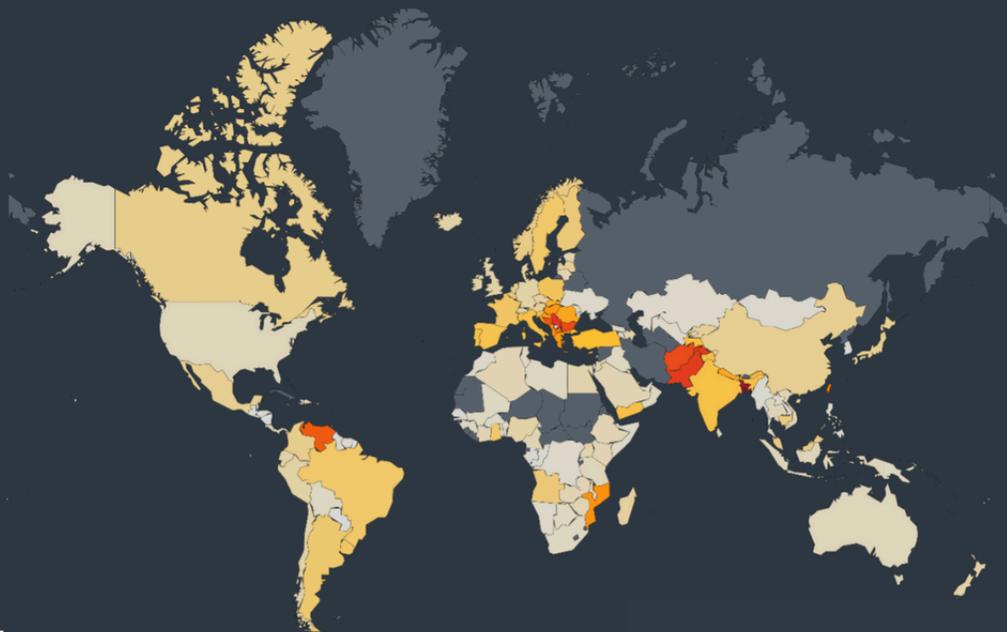
Category	Q1/2025 (%)	Q4/2024 (%)	Q/Q
Generic scam	51.40%	47.39%	8.64%
Phishing	31.91%	5.64%	465.80%
Smishing	5.05%	18.61%	-72.89%
Package delivery scam	3.70%	9.12%	-59.42%
Malvertising	2.41%	1.46%	65.27%
Lottery scam	2.14%	8.43%	-74.57%
Fake invoice scam	1.51%	4.90%	-69.19%
Advance fee scam	1.28%	3.83%	66.48%
E-shop scam	0.55%	0.61%	-10.53%

Scams detected by Norton Genie

Ransomware: A Changing Battlefield

The ransomware threat level remains elevated since Q4/2024. In Q1/2025:

- **Magniber** dominated (67% of ransomware cases and over 100,000 protected users)
- **WannaCry** and **Enigma** trailed far behind



Q1/2025
Global risk ratio for ransomware

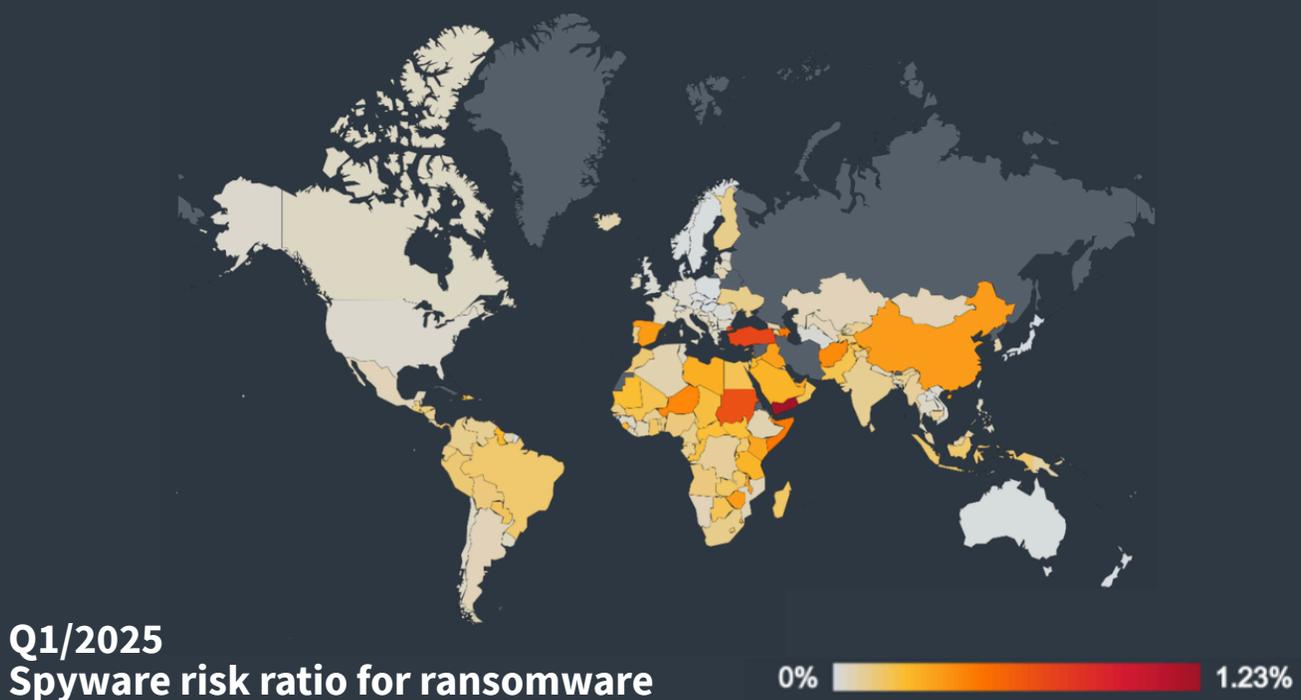
0%  1.35%

While the notable players maintain the largest share of ransomware threats, there is a new player on the ransomware scene, called **FunkSec**. Some of their tools were most likely generated by an LLM agent, a sign that AI tools are lowering the barrier for creating ransomware. This also applies to the [template source code](#), where comments are written in perfect English (as opposed to very basic English in other mediums).

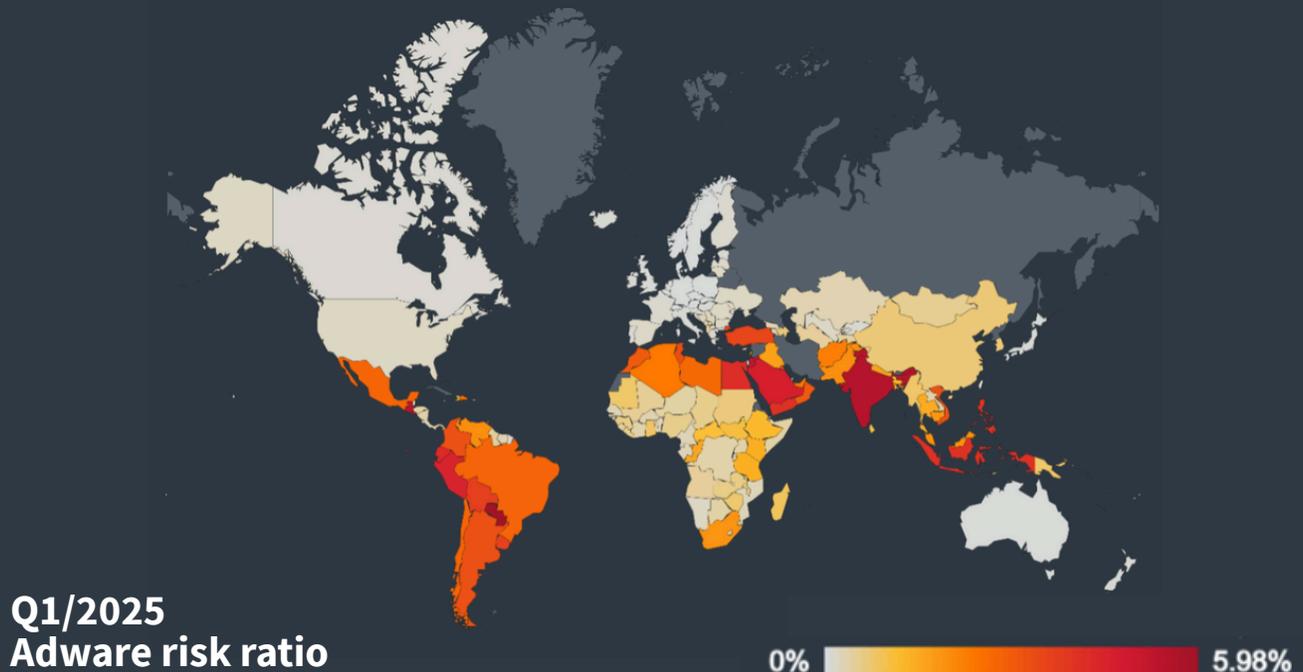
Based on a report from [Chainalysis](#), the total volume of ransom payments decreased year-over-year (YoY) by approximately 35%. There are a few reasons why the payments declined — companies have adapted to this type of cyber-threat and are understanding the need for cybersecurity while more frequently declining to pay ransomware gangs while law-enforcement agencies have increased pressure on ransomware infrastructure and crypto-mixers. The total amount paid in 2024 was \$813 million.

Mobile Threats on the Rise

Mobile threats surged in Q1/2025, with a 25% increase in protected users across adware and spyware categories. Adware, particularly strains like HiddenAds and MobiDash, dominated the mobile threat landscape, while older families like FakeAdBlockers faded from view. Brazil, India, Argentina and Mexico saw some of the largest country-specific spikes, with Mexico notably experiencing a 42% jump in protected monthly users.



The evolving nature of mobile adware and spyware suggests these threats will continue to escalate in the coming quarters, particularly as attackers experiment with new delivery methods and leverage regional campaigns to maximize impact.



Spyware, though growing more modestly (+6% protected users), revealed worrying trends with new or resurging strains like SpySolr, Tambir and SpyLend, targeting victims in Turkey and India with increasingly aggressive data theft and blackmail tactics. Spain stood out with a 96% spike in spyware risk, while Turkey followed closely behind at +84%.

Patrik Holop, Researcher
Luis Corrons, Security Evangelist
Ladislav Zezula, Malware Researcher
Jakub Vávra, Threat Operations Analyst
Jan Rubín, Malware Researcher
Alexej Savčín, Threat Analysis Engineering Manager
Lukáš Zobal, Research Engineering Manager

Featured Stories: Q1/2025 – Deception, Innovation and Exploited Trust

The first quarter of 2025 demonstrated that cybercriminals are not merely refining their methods, they're rewriting the playbook entirely. Our Featured Stories expose how threat actors employed groundbreaking technologies, hijacked trusted platforms and used highly personalized deception to trap victims more effectively than ever.

CryptoCore's manipulation of deepfake technology around President Donald Trump's 2025 inauguration illustrates how major media events can become powerful tools for financial fraud on a global scale.

In parallel, cybercriminals exploit legitimate online website builders, rapidly deploying convincing phishing pages designed to bypass traditional security measures and deceive users into handing over their most sensitive data.

We also explore the sophistication of Scam-Yourself Attacks, a disturbing trend where victims are deceived into willingly infecting their own devices. Attackers increasingly use realistic AI-generated personas, cleverly compromised social platforms and sophisticated cross-platform techniques to evade detection and persuade users to lower their defenses voluntarily.

Together, these featured stories paint a clear picture of a threat landscape driven by innovation, deception and an alarming exploitation of trust.

Hijacked Inauguration: How CryptoCore Used Deepfakes to Scam Millions

CryptoCore, the sophisticated cybercriminal group that exploits the popularity of cryptocurrencies, has perfected the art of deception. By combining deepfake technology, hijacked YouTube accounts and professionally designed websites, they transform media events into launchpads for sophisticated scam operations targeting cryptocurrency users. Their approach exploits trust, manipulates public attention and turns fabricated reality into a convincing trap. We broke down their methods further in our article about [CryptoCore](#).

In Q1/2025, CryptoCore found the perfect stage. As the 2025 inauguration of U.S. President Donald Trump captured global headlines, the group launched one of its most aggressive deepfake campaigns yet, targeting cryptocurrency enthusiasts caught in the media frenzy.

Our telemetry shows that during this period, CryptoCore's activity surged to over four times the typical baseline, reflecting the scale of the operation.

CryptoCore activity around the 2025 inauguration



CryptoCore significantly increased its activity on YouTube during the inauguration, hijacking more accounts and rebranding them to look like official accounts linked to Donald Trump. Deepfake technology was at the heart of the operation, creating realistic, fabricated videos featuring both Donald Trump and Elon Musk promoting fraudulent giveaway events.

The scam narrative remained consistent: leveraging the inauguration's media spotlight to push cryptocurrency investments schemes, promising participants the chance to double their profits. The videos were carefully crafted, often reusing authentic footage with manipulated lip-syncing and embedded QR codes that redirected viewers to sophisticated fake websites. These sites were highly professional in appearance, featuring interactive elements and images of Trump and Musk to enhance their credibility.



Original live stream footage repurposed by attackers, featuring a malicious QR code

In addition to the inauguration event, Donald Trump's meme coin, \$TRUMP, officially launched on January 18, 2025, just before Donald Trump's second inauguration. The coin quickly gained public attention, fueled by media coverage and the political spotlight.

Seizing the opportunity, CryptoCore created a wave of scam promotional content featuring deepfakes of Trump and other high-profile figures. The scam once again promised exclusive benefits and double profit, this time tied to investments in the \$TRUMP coin.

Beyond the inauguration, CryptoCore maintained a stable trend of distributing fake videos exploiting the likenesses of other cryptocurrency personalities such as Vitalik Buterin, Michael Saylor and Brad Garlinghouse. These deepfakes were spread across hijacked platforms, extending the reach of their scams far beyond the political event.

CryptoCore's operations in Q1/2025 resulted in estimated profits of \$3.8M across 2,200 transactions, based on analysis of cryptocurrency wallets identified on fraudulent sites. As this estimate only includes tracked wallets and visible activity, the actual profit is likely much higher.

CryptoCore's latest campaigns show how quickly attackers adapt, combining deepfake technology, hijacked trusted platforms, and media-driven moments to lure unsuspecting victims. Today's scams no longer rely on crude deception: they look polished, professional and dangerously convincing. It is crucial to stay vigilant and verify the authenticity of any cryptocurrency-related content, especially that tied to high-profile events or personalities, to avoid deception.

The Hidden Threat of Phishing Attacks Through Online Forms

Cybercriminals have always been on the lookout for simple, effective and low-cost ways to run phishing campaigns. While some invest in elaborate infrastructure—offering realistic phishing pages as part of paid “phishing-as-a-service” kits—others opt for a cheaper, faster approach: abusing legitimate website builders. These low-effort alternatives abuse legitimate tools with drag-and-drop interfaces, enabling anyone to create a website without needing coding skills. This approach allows for a quick, although limited, way to create phishing pages on legitimate hosting domains. Such pages have a higher chance of bypassing standard email filters, which is a significant threat to ordinary users. Therefore, phishing links are predominantly sent via email. The main tactic is to create a sense of urgency about a blocked account or service limitation requiring immediate action. Another type of email is informational, requesting the review of a document accessible online, but only after logging in.

Even though many of these websites can be spotted with a bit of scrutiny, they remain consistently present in the wild—and in some regions, increasingly so. They primarily mimic the login screens of major companies providing telecommunications, email and streaming services. Financial institutions and forms requiring payment information, social security numbers and other sensitive data are also common targets. Additionally, the phishing pages appear in various languages across all continents.

Attackers often abuse popular website builders, e.g., Weebly or Wix, hosted on trusted domains and infrastructure. These tools are frequently free, making their misuse very simple and anonymous. Phishing pages typically have a legitimate second-level domain, which does not raise suspicion with spam filters or antivirus software.

Additionally, attackers can choose arbitrary third-level domains, often using their names to evoke familiarity with the phished brand. A popular tactic is also typo squatting in the subdomain name, such as:

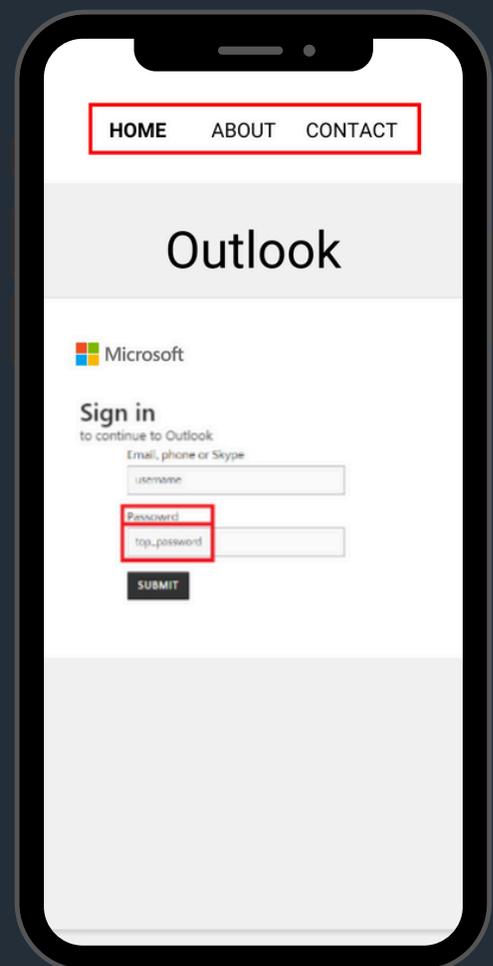
- updatefacebookmeta[.]weebly[.]com
- microsoftdocumentfile[.]weebly[.]com
- outlookauthenticationmicrosoft[.]weebly[.]com
- myfmsbank[.]weebly[.]com
- onlinedesk[.]wix.com

Beyond website builders, attackers increasingly abuse dynamic DNS (DDNS) services and subdomain providers like DuckDNS to host phishing sites. These services allow the creation of custom subdomains that mimic well-known brands, further enhancing the deception. By leveraging such flexible infrastructure, attackers can quickly scale campaigns without requiring extensive technical knowledge, expanding their reach and impact.

Some login pages are sophisticated and require greater attention to detect, especially if the legitimate login form is simple to copy. On the other hand, there are also many obviously fraudulent pages where, e.g., the entered password is not masked, the footer displays the logo of the abused platform or the header contains links leading to unrelated sites. In any case, the login page sitting on the website builder domain is a red flag indicating that something is wrong.

The figure illustrates an example of an obvious phishing page. Notice the suspicious menu items, including irrelevant options unrelated to the site's purpose. The page layout is also inconsistent and unprofessional, with mismatched fonts and awkward formatting. One of the most obvious red flags, though, is that passwords are displayed in plain text rather than masked—an immediate giveaway that the site is not legitimate.

Phishing attacks of this type are steadily increasing worldwide, with distinct spikes in specific regions.



Example of an obvious phishing page, showing common warning signs

Global risk ratio of phishing abusing online website builders Q1/2025



In the U.S., a significant campaign targeted AT&T and Xfinity customers in early 2025. Conversely, in Australia, we have observed a steadily increasing trend since February, relentlessly targeting Telstra email users.

AU risk ratio of phishing abusing online website builders

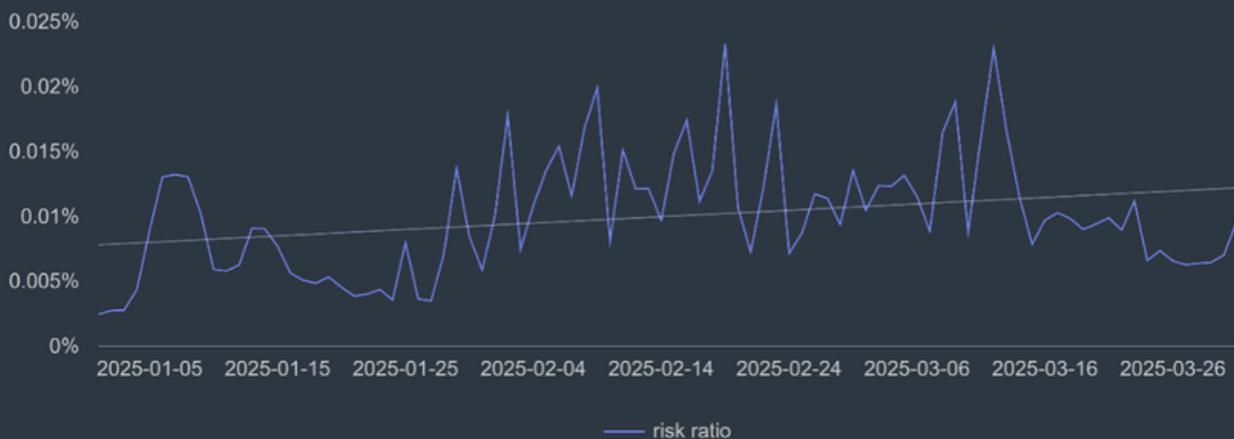


These regional waves reflect how attackers can easily localize their campaigns using publicly available tools, targeting specific providers, languages and users with minimal effort and maximum reach.

The technique remains widely used for a reason: it's fast, cheap and often effective. Even when phishing pages are poorly made, their trusted hosting domains give them an edge, making them harder to filter and easier to overlook.

Notably, Q1/2025 telemetry shows a rising number of phishing campaigns hosted on DDNS services and subdomain providers, adding to the already widespread abuse of site builders. While the overall phishing threat landscape remained relatively stable this quarter, these shifts in hosting methods point to an evolving playbook that emphasizes speed, flexibility and low operational costs.

Phishing via DDNS: Daily activity snapshot

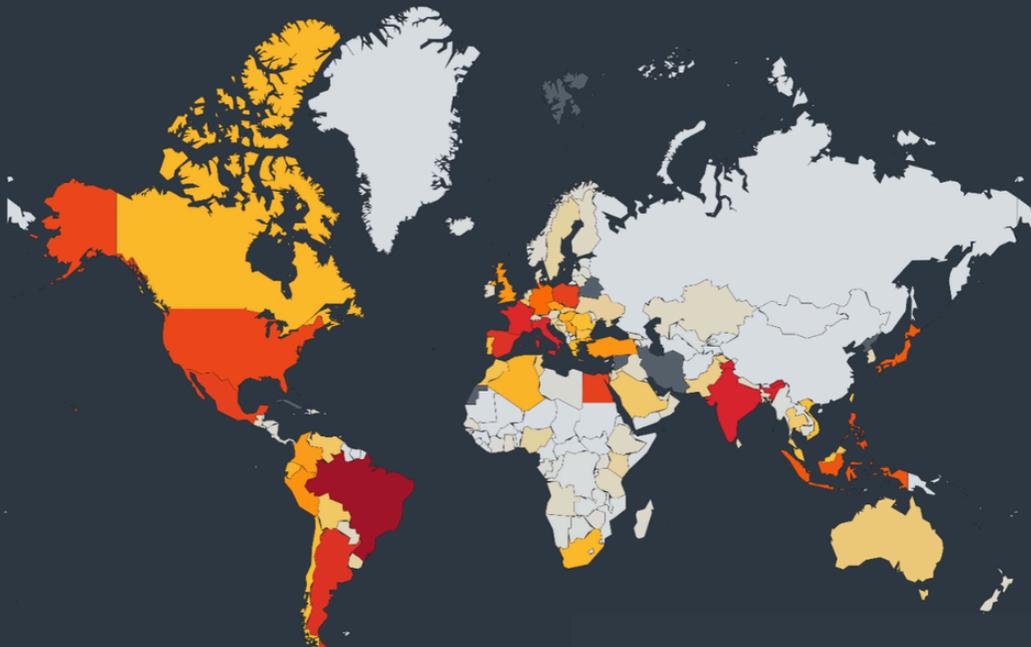


The Evolution of Scam-Yourself Attacks: Smarter, Sneakier and Cross-Platform

The most dangerous attacks aren't always the ones that sneak in unnoticed — they are often the ones that make you open the door yourself.

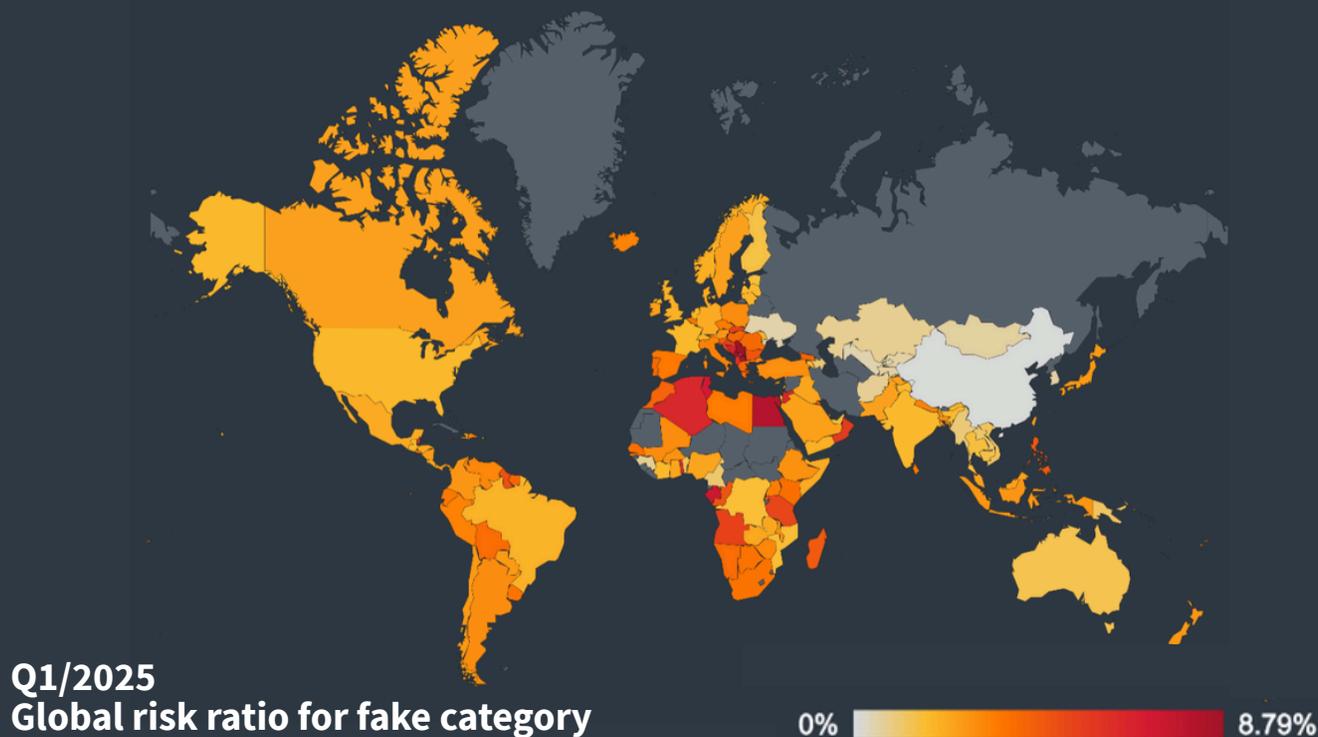
[Scam-Yourself Attacks](#) rely on well-crafted social engineering tactics, designed to trick users into infecting their own devices. The malicious steps don't hide in the background — they're laid out in front of the user, disguised as helpful instructions. It's [malware](#) you install *yourself* — and attackers are getting better at convincing you to do it.

In Q1/2025 alone, we protected more than 4 million people from Scam-Yourself Attacks like ClickFix and FakeCaptcha, some of the most widespread and persistent threats across the globe. While the overall “Fake” category, which includes Scam-Yourself Attacks, saw a slight decrease in global risk ratio by 8.96% this quarter, its impact remains massive, with persistent activity observed worldwide.



The widespread use of ClickFix and FakeCaptcha

0 230,297

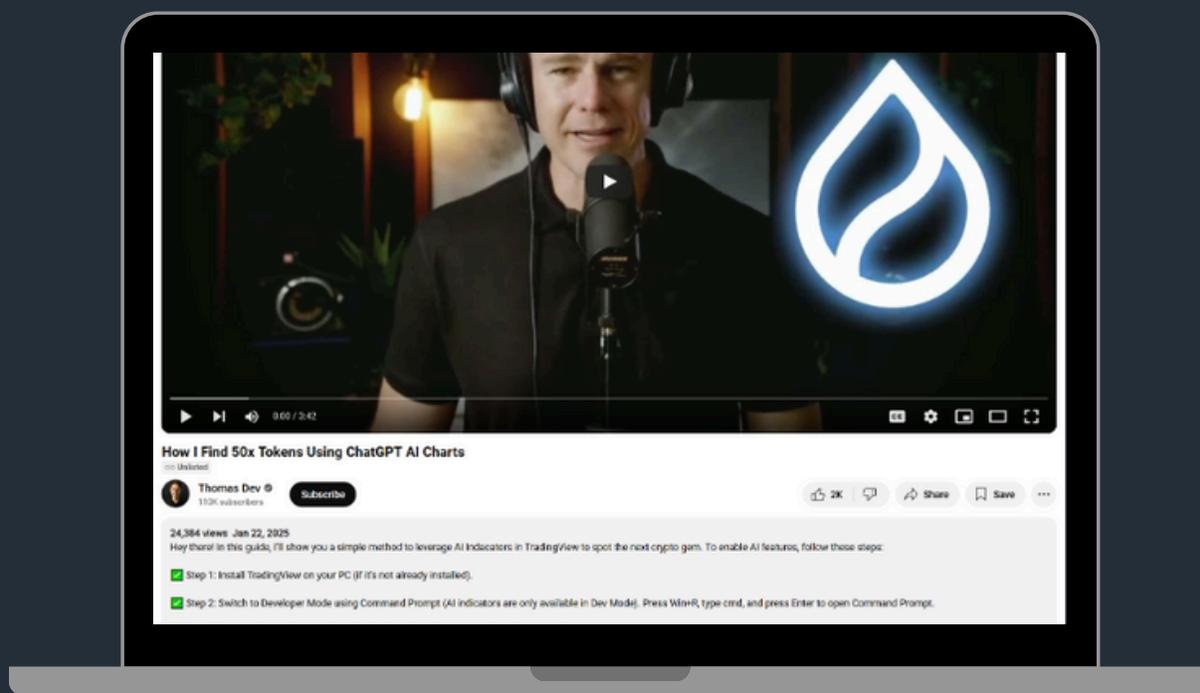


In Q1/2025 alone, we protected more than 4 million people from Scam-Yourself Attacks like ClickFix and FakeCaptcha, some of the most widespread and persistent threats across the globe. While the overall “Fake” category, which includes Scam-Yourself Attacks, saw a slight decrease in global risk ratio by 8.96% this quarter, its impact remains massive, with persistent activity observed worldwide.

AI Personas, Fake Finance Tools and the YouTube Trap

One of the most striking evolutions we observed this quarter is how attackers use AI-generated personas, deepfake influencers and hired actors to deliver Scam-Yourself campaigns, primarily through compromised YouTube accounts.

Meet Thomas Harris, also known as Thomas Roberts or Oscar Davies, among other names. He is very active on YouTube providing advice on how to easily make money using otherwise paid extensions for TradingView, like ChatGPT AI Charts (no matter if such an extension actually exists or not). Typically present as an unlisted video on a compromised YouTube account, "Thomas" verbally and visually explains how to proceed with the installation, effectively performing a Scam-Yourself Attack. The most shocking part is Thomas isn't real at all but is instead a rising star of an influencer who is completely deepfaked.



Screenshot of the AI-generated video hosted on YouTube verbally and visually explaining the steps the user should take, including the instructions in the description of the video

Usually, the video is unlisted and is not visible on the compromised YouTube channel where it is hosted, and it cannot be searched for on YouTube. In order for the user to reach the video, the attackers frequently use YouTube's advertising system, recommending the scam videos when it recognizes the user is interested in the related topic.

The attackers also use a lot of tricks to make the compromised accounts look as convincing as possible. To impersonate the original vendor, the attackers made some typical changes:

- Renaming the channel (arbitrary, perfectly mimicking the original channel)
- Renaming the @handle (must be unique, typo-squatting is typically used)
- Deleting all of the content of the previous owner
- Filling the channel with linked videos leading to the official channel the attackers are impersonating

Let us explain the last step more using the example below.

Linked videos are a feature of YouTube where the user can link videos from different channels and present them on their own channel. In the screenshot below, we can see a compromised YouTube channel. Because the videos in this case point to the official TradingView channel, they look very convincing and legitimate – that’s because they are legitimate — even though they don’t belong to this channel at all. The user would need to click on the individual videos and observe that they are actually hosted on a different channel to recognize they’re on not on the page of the company, account or vendor that they think they’re on.

For more details about this campaign, [read our blogpost](#).

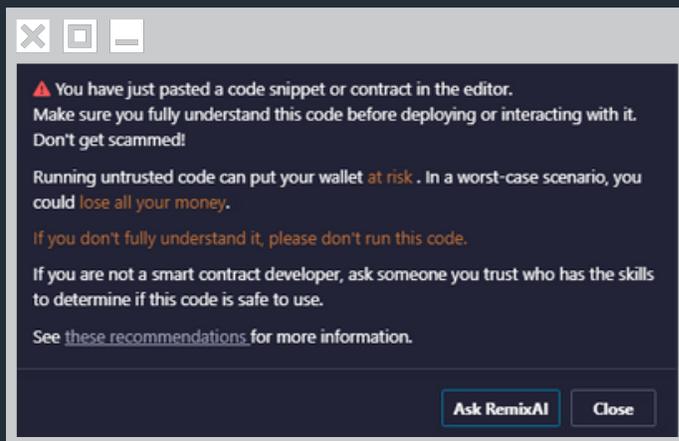
[Trading Bot Scam](#) is yet another type of AI impersonation campaign we observed during Q1/2025 (and beyond). In the 500+ videos so far, we observed more than 15 different personas, and we are still counting. Either completely AI-generated, deepfaked, or performed by hired actors, all these personas carry out the Trading Bot Scam.



Either completely AI-generated, deepfaked, or performed by hired actors, all these personas carry out the Trading Bot Scam

All of the personas shown above advise users on how to get rich, quickly and easily, by exploiting price differences in cryptocurrency on blockchains. To do so, users are instructed to copy and paste a smart contract code into an online Integrated Development Environment (IDE platform) to the cryptocurrency contract. When the user adds money into the contract, their money is sent to the attacker's wallet instead. This method takes Scam-Yourself Attacks to the next level, instead of simply tricking users into pasting malicious commands into their computer, it uses legitimate websites or tools to trick them into setting up a malicious smart contract on the blockchain.

The attacker usually hosts their own fake coding platform on a website with a slightly misspelled name. This way, they avoid the warnings and pop-up messages that real platforms show to protect users from copying dangerous code.



A warning typically displayed on the online IDE platforms for smart contracts when the user is copy & pasting the code

By self-hosting the IDE, the attackers are changing its implementation in such a way that these warnings are suppressed, making it a tradeoff between user noticing the typo-squatted domain and the warning dialogue.

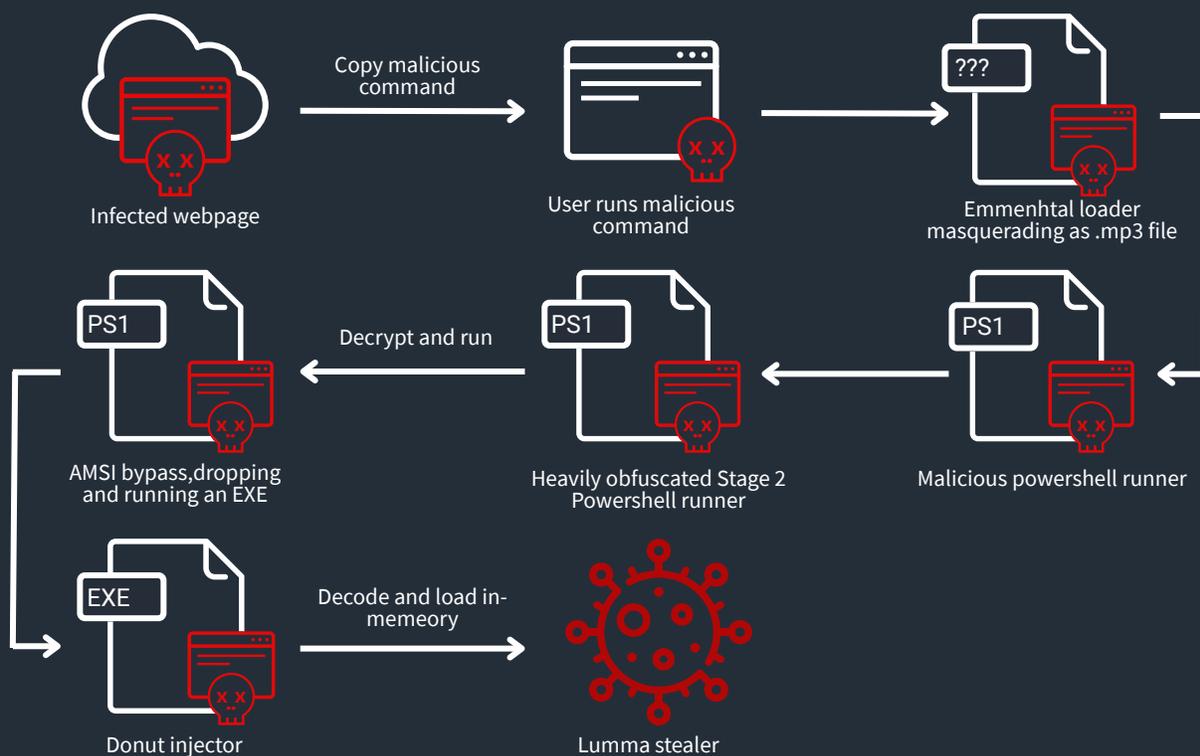
FakeCaptcha Gets Smarter (and More Cross-Platform)

ClickFix and FakeCaptcha continue to evolve. One new tactic involves [interactive image-based](#) CAPTCHAs mimicking the classical “select all the traffic lights” puzzle. However, after selecting the image (quite frankly any image for that matter), the user is once again redirected to the common set of malicious steps which result in infecting the user's device.

Another FakeCaptcha campaign [focused on countries in Asia](#), uses typo-squatted URLs trying to impersonate well-known brands like Pepsi, McDonalds and Coca-Cola. In campaigns like this, we can observe usage of variety of loaders —programs designed to secretly install malware on a victim’s device—, including the well-known Emmehntal loader. In some cases, the loader is cleverly hidden inside a polyglot MP3 file, which can be playable as normal audio but also contains malicious JavaScript. This hidden code is then run by a tool called mshta.exe to install Lumma Stealer malware.

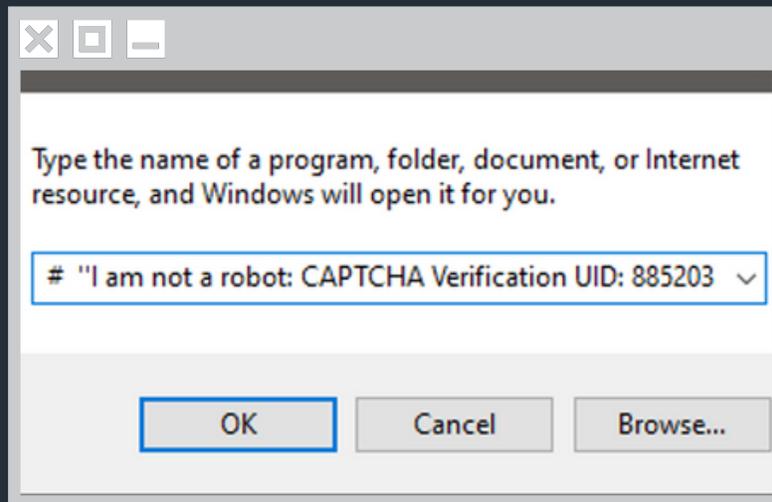
The attacker usually hosts their own fake coding platform on a website with a slightly misspelled name. This way, they avoid the warnings and pop-up messages that real platforms shows to protect users from copying dangerous code.

By self-hosting the IDE, the attackers are changing its implementation in such a way that these warnings are suppressed, making it a tradeoff between user noticing the typo-squatted domain and the warning dialogue.



Execution chain illustrating the flow from the FakeCaptcha infected website to the Lumma Stealer execution

In FakeCaptcha attacks, attackers hide malicious code by adding comments that make the command look harmless. This way, the user only sees the supposed verification message and the malicious command is hidden just before the comment, as can be seen below:



A harmless comment further misleading users into believe there is nothing wrong with the steps they are taking

In Q1/2025, we saw an [improvement of this technique](#). The attackers started to use Unicode characters in these comments in an attempt to avoid detection. Nothing really changed for the user, but under the hood, the byte representation varies significantly.

FakeCaptcha also [exploits the userinfo part of URLs](#) (credentials before the '@' symbol) in mshta.exe requests. This is done to obfuscate the URL, so it seems like a common google.com domain (see below) but in fact the request is made to the attacker's hosted website.

hxxp://google[.]com@hlp[.]macosfytie[.]com/check/microsoft[.]doc

mshta command for running malicious script from attacker's hosted website, attempting to disguise as a google.com domain

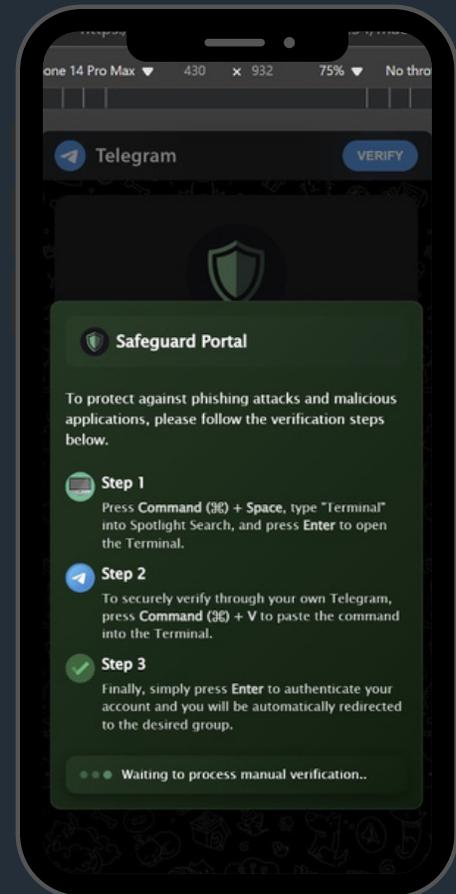
Additionally, FakeCaptcha is not just a Windows thing anymore. In early Q1/2025, this attack was [observed on macOS](#). With a promise of protection against phishing attacks, by following the steps, the campaign was distributing AMOS, an information stealer also known as Atomic Stealer.

In parallel, we also observed a considerable rise in Fake Update campaigns, where attackers trick victims into installing supposed browser updates (such as for Chrome or Opera) that actually deliver malware. These fake updates, designed to closely mimic legitimate prompts, caused a massive +1711% spike in global risk ratios during Q1. While situational, such campaigns can surge dramatically in short bursts before settling back into quieter periods. Notably, this particular wave hit countries like Belgium, Poland, Italy, New Zealand, Switzerland, Spain, the Netherlands, Germany and the United Kingdom especially hard.

Scam-Yourself Attacks also allow previously dead malware strains to shine again. During Q1/2025, we observed a resurrection of Wincir RAT/dropper, also known as Legion Loader, which rose to popularity in 2022 before quickly beginning its steady decline.

The attack starts with an unofficial third-party website for downloading software. This website is, however, hosted by the attacker and instead of a direct download, instructions on how to proceed are displayed to the user.

Note that the instructions aren't infecting the victims' devices directly. Instead, the installer is simply downloaded and conveniently displayed to the user in a traditional Explorer window. After the user double-clicks on it, or presses enter, they execute Wincir manually on their own.



FakeCaptcha on macOS spreading AMOS (source: <https://x.com/g0njxa/status/1884166667498054004>)

Looking ahead, we anticipate Scam-Yourself Attacks will continue evolving in sophistication and scope. The blending of AI-generated personas, cross-platform malware delivery (including macOS), and advanced social engineering techniques suggests that these attacks will remain one of the most adaptive and challenging threat categories in the quarters to come. Regional surges, like those seen in the Fake Update campaigns, are likely to reappear as attackers test new angles and exploit localized opportunities.

Martin Chlumecký, Malware Researcher

Jan Rubín, Malware Researcher

Luis Corrons, Security Evangelist

In Closing



The Gen Q1/2025 Threat Report revealed an evolving threat landscape where cybercriminals are becoming increasingly sophisticated, leveraging advanced technologies like AI, deepfakes and cross-platform scams to exploit trust and target their victims. These issues aren't just technological; they're deeply personal, affecting real people and real lives.

Key insights included a 186% surge in breached records, a growth in Fake Update Scams of 17 times the previous quarter's levels, and the rise of Scam-Yourself Attacks, which deceived millions of users into compromising their own systems. We saw new players on the ransomware scene, developing attacks created by AI that target businesses' bottom lines. Financial threats, like CryptoCore's deepfake-powered cryptocurrency scams, reaped millions in profits, while mobile threats took a deeply personal turn, targeting users' sensitive data through spyware and banking Trojans.

While the overall volume of cyberattacks has not significantly increased, this signals a shift from broad, indiscriminate strategies to more targeted, innovative, and persistent tactics.

Despite these challenges, there's hope. Awareness, proactive measures, and robust cybersecurity practices are critical in countering these threats. Together, we can build a digital future that's smarter, safer, and more resilient.

Stay protected. Stay alert. Stay ahead.

Visit our [Glossary](#) and [Taxonomy](#) for clear definitions and insights into how we classify today's cyberthreats.



Acknowledgments

Malware Research

Alexej Savčín
Jakub Křoustek
Jakub Vávra
Jan Rubín
Ladislav Zezula
Luis Corrons
Martin Chlumecký
Michal Salát
Michalis Pachilakis

Brand Design

Alisha Robinson
Youan Lin

Data Analysis

Filip Husák
Lukáš Zobal
Patrik Holop
Pavol Plaskoň

Communications

Aneta Šeráková
Ashlynn Rosenberg
Brittany Posey
Emily Lockwood
Emma Brownstein
Jenna Torluemke
Pavel Klimeš
Tereza Karbanová