Avast Q2/2023 Threat Report

decoded.avast.io/threatresearch/avast-q2-2023-threat-report/

August 10, 2023

by Threat Research TeamAugust 10, 202353 min read

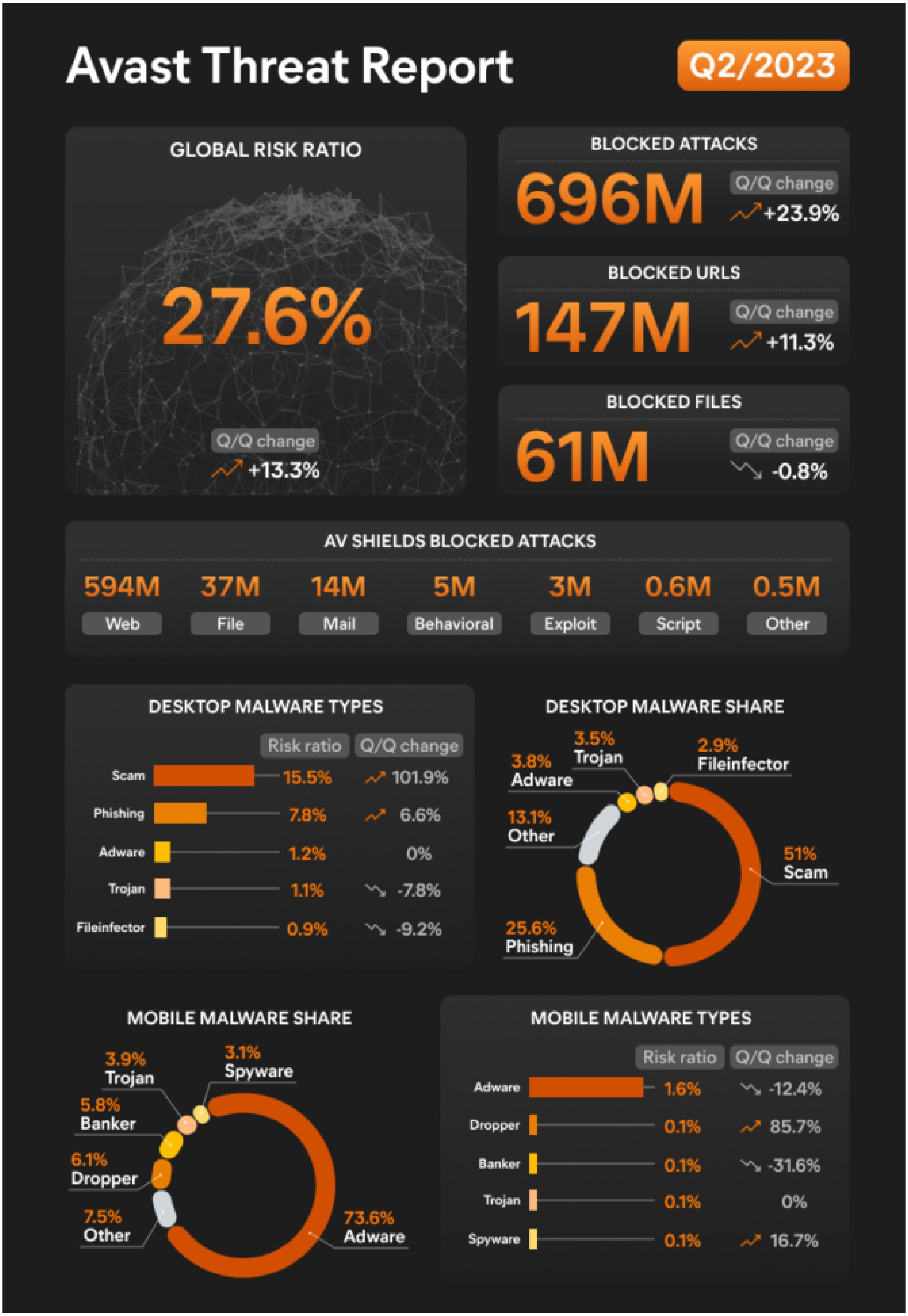
Unveiling the Dominance of Scams Amidst a 24% Surge in Blocked Attacks

Foreword

This quarter has been nothing short of extraordinary, with cyber-threat activity reaching its highest point in the past three years. We take this opportunity to offer you insights into the challenges we encountered in safeguarding our users against all these malicious threats.

In Q2/2023, our detection telemetry revealed a significant increase in overall cyber-threat risk. The risk ratio, reflecting the proportion of users protected from cyber threats out of all our protected users, rose by 13% quarter-on-quarter, reaching a concerning 27.6%. Moreover, the volume of unique blocked attacks surged by 24% over the same period, resulting in an average of close to 700 million unique blocked attacks each month.

During the quarter, we observed a notable shift in threat trends. While traditional consumer-focused cyber threats saw a slight decline, there was a dramatic surge in social engineering and web-related threats, such as scams, phishing, and malvertising. These threats accounted for more than 75% of our overall detections on desktops during the quarter, with scams alone contributing to 51% of the total detections.



Avast Threat Report

Q2/2023

GLOBAL RISK RATIO

27.6%

Q/Q change ↗ +13.3%

BLOCKED ATTACKS

696M

Q/Q change ↗ +23.9%

BLOCKED URLS

147M

Q/Q change ↗ +11.3%

BLOCKED FILES

61M

Q/Q change ↘ -0.8%

AV SHIELDS BLOCKED ATTACKS

594M	37M	14M	5M	3M	0.6M	0.5M
Web	File	Mail	Behavioral	Exploit	Script	Other

DESKTOP MALWARE TYPES

	Risk ratio	Q/Q change
Scam	15.5%	↗ 101.9%
Phishing	7.8%	↗ 6.6%
Adware	1.2%	0%
Trojan	1.1%	↘ -7.8%
Fileinfector	0.9%	↘ -9.2%

DESKTOP MALWARE SHARE

3.8% Adware

3.5% Trojan

2.9% Fileinfector

13.1% Other

51% Scam

25.6% Phishing

MOBILE MALWARE SHARE

3.9% Trojan

3.1% Spyware

5.8% Banker

6.1% Dropper

7.5% Other

73.6% Adware

MOBILE MALWARE TYPES

	Risk ratio	Q/Q change
Adware	1.6%	↘ -12.4%
Dropper	0.1%	↗ 85.7%
Banker	0.1%	↘ -31.6%
Trojan	0.1%	0%
Spyware	0.1%	↗ 16.7%

The prevalence of malvertising and malicious browser push notifications have also witnessed a dramatic increase, along with the proliferation of dating scams and extortion emails. More detailed information on these emerging threats can be found in the subsequent sections of this report.

While adware exhibited a slight decline in prevalence, it continues to persist across desktop, mobile, and browser platforms. One notable example is the HiddenAds campaign, which resurfaced on the Google Play Store and amassed tens of millions of downloads during its reign.

Another noteworthy observation was the discovery of the Mustang Panda APT group's attempt to infiltrate and infect TP-Link routers through compromised firmware. We also closely monitored the progress of the DDosia project, witnessing participants of this threat group targeting the Wagner Group infrastructure in response of its ephemeral rebellion in Russia.

Malicious coinminers, while experiencing a slight decline, posed unique challenges for its authors due to the shift from proof-of-work to proof-of-stake schema that recently happened in many cryptocurrencies. And some of the malware authors struggled to adapt, leading to the observed decrease in coinminer prevalence during this quarter. Our researchers also discovered HotRat in the wild, a .NET reimplementation of AsyncRat, featuring numerous new commands and features.

In addition, I am pleased to highlight another significant achievement by our researchers. Avast's discovery of CVE-2023-29336, a local privilege escalation vulnerability targeting win32k in the Windows kernel, led to a prompt patch in the May Patch Tuesday security update. While we shared a proof-of-concept exploit with Microsoft, we have responsibly withheld public disclosure of technical details to prioritize user safety.

However, ransomware remains an ongoing concern. Despite a slight decline in prevalence, ransomware authors persist in targeting victims, relying increasingly on targeted attacks and exploits to penetrate company networks. Notably, successful attacks on widely used software, such as PaperCut and MOVEit, underscore the evolving tactics of ransomware operators, who more than ever experiment with encryption-less extortion techniques and doxing.

On a positive note, we are pleased to share that our efforts have led to the development of a free decryption tool for Akira Ransomware. This tool has already assisted numerous victims of ransomware attacks in restoring their files and businesses, further solidifying our commitment to providing solutions and assistance to those in need.

Thank you for reading and placing your trust in Avast. Stay safe and secure.

Jakub Křoustek, Malware Research Director

Methodology

This report is structured into two 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.

In this report, we also slightly redefined the "Information Stealers" malware category. Moving forward, this category will encompass the following malware types: banking trojans, keylogger, password stealers (also known as pws), spyware, clipper, cryptostealer, exfilware, stalkerware, and webskimming. We also recalculated the related statistics so that we can provide you with the correct comparisons with the previous quarters.

Featured Story: The Rise of Scams

Scams, much like the many forms of deception and trickery that preceded them, have always been an inherent part of the human experience. In a digital era where information is largely exchanged through the Internet, these acts of deceit have found a fertile ground to evolve and proliferate, posing a significant threat to online safety.

Scams have transitioned from the physical to the digital world with alarming ease, leveraging the anonymity and expansive reach provided by the Internet. Today's scams employ a wide array of sophisticated tactics that range from financial and charity scams to online dating scams and deceptive advertising. The mechanisms may vary, but the end goal remains the same – to deceive unsuspecting individuals into revealing sensitive information or parting with their hard-earned money.

Furthermore, a related threat type, Phishing, accounted for another 25% of all threats. Phishing attempts often masquerade as legitimate requests for information, typically from a well-known and trusted entity such as a bank or a government agency. They prey on human instincts of trust and urgency, compelling victims to divulge confidential information or engage in financial transactions under false pretenses.

The rapid evolution of technology has led cybercriminals to adapt and innovate. They have harnessed AI tools to craft nearly flawless imitations of legitimate communication, making it increasingly difficult for individuals to differentiate between what is real and what isn't. Furthermore, the adoption of smishing – or phishing through SMS – has capitalized on the high open rates and inherent trust individuals place in text messages.

The data from Q2/2023 signifies a shift in the cybersecurity landscape. Threat actors are opting for the psychological manipulation afforded by scams and phishing rather than the technical exploits found in traditional malware attacks. As a result, our defense must adapt, focusing not just on improving technological measures but also on building awareness and promoting skepticism toward unsolicited communication.

In March we uncovered a new Instagram scam using fake SHEIN gift cards as lure. During Q2, we have found that the scammers are widening their operations, covering more countries such as Israel. They have also evolved and moved on from fake SHEIN gift cards to a maybe more appealing iPhone 14 targeting users in Mexico and Spain, such as the example below.

The outcome remains the same: victims never receive the promised price; instead, they find themselves subscribed to an unfamiliar service they have no knowledge of.

During these past three months, we have documented other scams as well. Avast Threat Labs identified a new data extortion scam targeting companies via email, seemingly from a ransomware or data extortion cyber gang. The emails, addressed to employees by their full names, claim a security breach has occurred, with a significant amount of company information stolen, including employee records and personal data. Senders purport to be from ransomware groups like "Silent Ransom" or "Lockffit." The emails press employees to notify their managers about the situation, threatening to sell the stolen data if ignored, and remind the recipients about the regulatory penalties of data breaches.

However, these communications appear to be more scare tactics than actual extortion campaigns following a data breach. It's an effort to intimidate decision-makers into paying to prevent further consequences like having their data sold or facing potential regulatory fines. There's no offered proof of the breach other than possession of the recipient's email and name. Avast has captured identical scam messages targeting different organizations, merely changing details like the recipient's name, the contact email, the supposed amount of stolen data, and even the alleged cybercriminal group. This modus operandi points to semi-automated attacks using a list of targets, akin to sextortion tactics.

In fact, this quarter a new sextortion campaign was uncovered by Avast. Sextortion scams are email-based cyberattacks where the scammers claim to have taken control of your system, often saying they have recorded your activities through your device's cameras and demanding payment to keep your privacy intact. The scammers capitalize on the victim's fear and embarrassment, hoping for quick payment to avoid potential exposure.

One of the nastiest scams we have detected is this disturbing crowdfunding scheme exploiting public generosity. The scam involves a series of emotionally charged video ads, narrating the story of a cancer-stricken child named "Semion," soliciting urgent financial aid for his treatment. These videos, primarily in Russian with multilingual subtitles, have been shared on platforms like YouTube and Instagram, eliciting significant monetary donations from empathetic viewers directed towards a donation page offering multiple payment methods.

Amidst these rising threats, it is essential to remember the fundamental rule of the Internet: trust, but verify. The shift towards a more scam-dominant threat landscape emphasizes the importance of digital literacy and security awareness for consumers.

In conclusion, the surge in scams and phishing incidents during Q2/2023 underscores a shifting threat landscape that demands adaptable, well-informed, and proactive cybersecurity measures. The cornerstone of these measures must be comprehensive education and awareness initiatives designed to empower users in recognizing and effectively responding to these deceptive and damaging attacks.

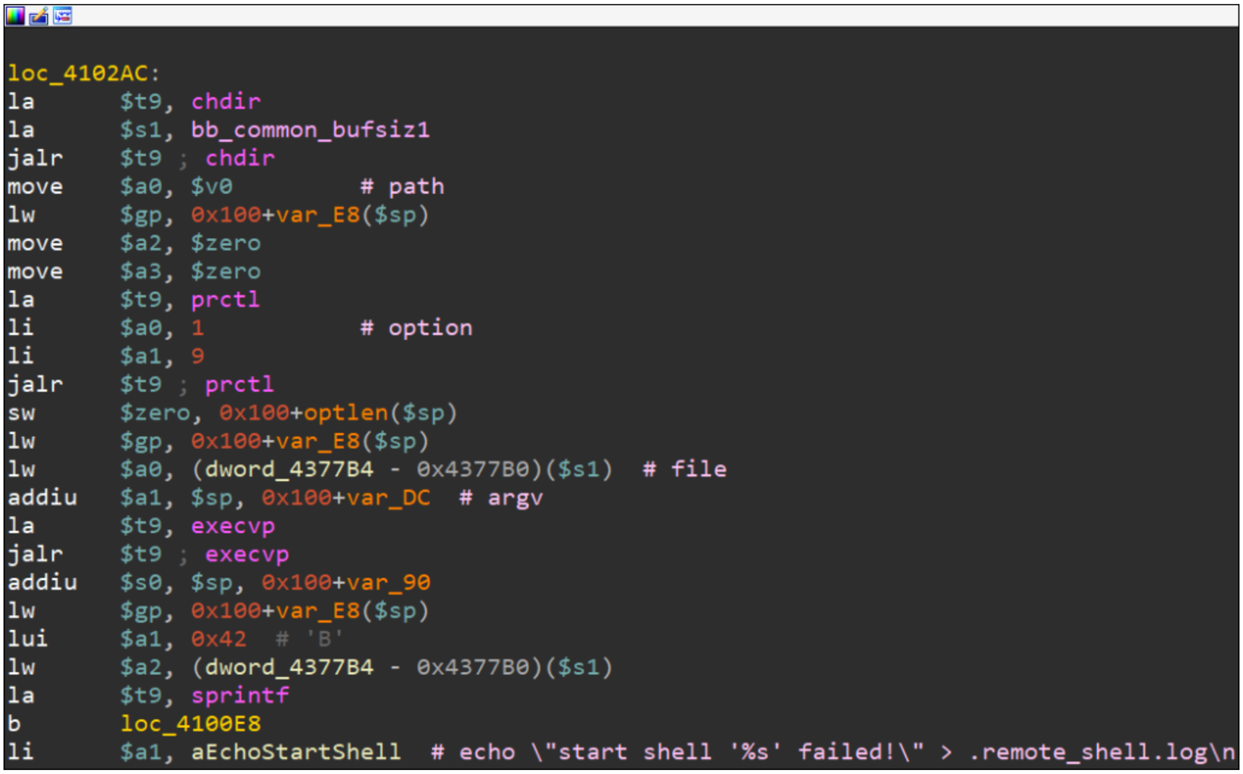
Luis Corrons, Security Evangelist

Desktop-Related Threats

Advanced Persistent Threats (APTs)

An Advanced Persistent Threat (APT) is a type of cyberattack that is carried out 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.

Avast researchers have been diligently monitoring the activities of the notorious hacking group Mustang Panda and their exfiltration server. During our investigation, a significant development emerged when the researchers discovered several new binaries on the server, one of which being a malicious firmware image that was customized for targeting TP-Link routers. This firmware image turned out to be laden with malevolent components, among them a particularly troublesome custom MIPS32 ELF implant.



```
loc_4102AC:
la      $t9, chdir
la      $s1, bb_common_bufsiz1
jalr    $t9 ; chdir
move    $a0, $v0         # path
lw      $gp, 0x100+var_E8($sp)
move    $a2, $zero
move    $a3, $zero
la      $t9, prctl
li      $a0, 1           # option
li      $a1, 9
jalr    $t9 ; prctl
sw      $zero, 0x100+optlen($sp)
lw      $gp, 0x100+var_E8($sp)
lw      $a0, (dword_4377B4 - 0x4377B0)($s1)  # file
addiu   $a1, $sp, 0x100+var_DC  # argv
la      $t9, execvp
jalr    $t9 ; execvp
addiu   $s0, $sp, 0x100+var_90
lw      $gp, 0x100+var_E8($sp)
lui     $a1, 0x42  # 'B'
lw      $a2, (dword_4377B4 - 0x4377B0)($s1)
la      $t9, sprintf
b       loc_4100E8
li      $a1, aEchoStartShell  # echo \"start shell '%s' failed!\" > .remote_shell.log\n
```

Remote commands execution functionality found in Mustang Panda's malicious firmware image

The implications of this custom implant are unsettling, as it affords the attacker three key functionalities. First, the attackers can execute arbitrary shell commands remotely on the infected router, granting them substantial control over the device from a distance. Secondly, the implant facilitates file transfer to and from the infected router, providing a means for the attackers to upload and download files which could lead to data theft or the dissemination of harmful payloads. Finally, the implant enables SOCKS protocol tunnelling, serving as a communication relay between different clients, further masking the attacker's identity and complicating their detection. The method used by the attacker to infect the router devices with the malevolent implant remains unknown. Overall, the threat group continues its operation in multiple countries including Hong Kong, Vietnam, Philippines continuously testing new techniques and malware. Simultaneously, they utilize well known tools such as Korplug and Cobalt Strike.

Lazarus, another infamous group notorious for their involvement in numerous high-profile cyberattacks, has carried out a fresh social engineering campaign this quarter. Their targets are blockchain-related developers, enticed through deceptive job assessments as a means to introduce malware. This strategy aims to compromise developers, potentially leading to significant security breaches and data compromises.

The Gamaredon APT group is demonstrating persistence in pursuing their malicious objectives, with Ukrainian institutions remaining a primary focus of their cyber-espionage operations. The group has a history of launching sophisticated attacks against government entities, military organizations, and critical infrastructure within Ukraine. Their modus operandi involves using spear-phishing emails, malicious documents, and social engineering techniques.

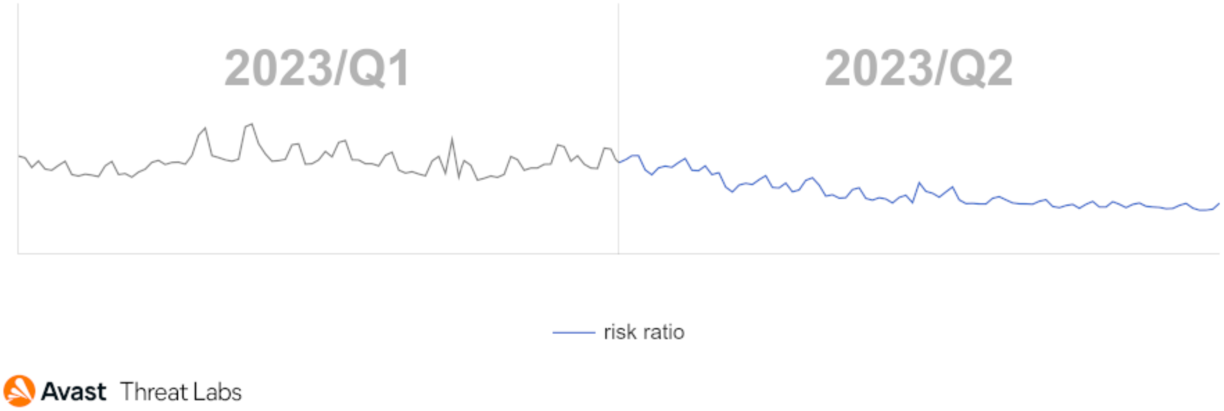
DoNot APT remains actively engaged in targeting the Pakistan government and military. We have identified a series of phishing emails containing LNK files to deliver the payload.

Luigino Camastra, Malware Researcher
Igor Morgenstern, Malware Researcher

Adware

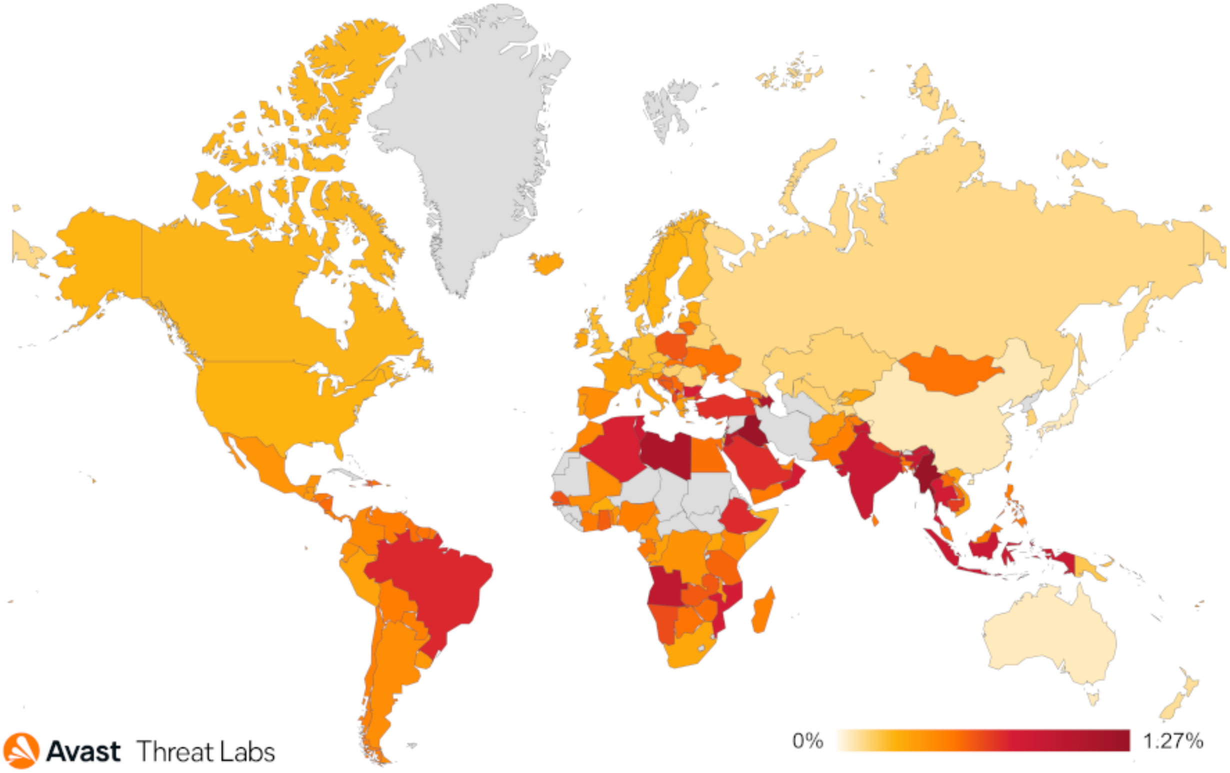
Adware is considered unwanted if installed without the user's consent, tracks browsing behavior, redirects web traffic, or collects personal information for malicious purposes such as identity theft.

Compared to last quarter, we have seen the beginning of a downward trend in desktop adware in Q2/2023, as the graph below illustrates. In the next quarter, we will see if this is a long-term trend or just a seasonal fluctuation since we did not notice any significant adware campaigns in this quarter.



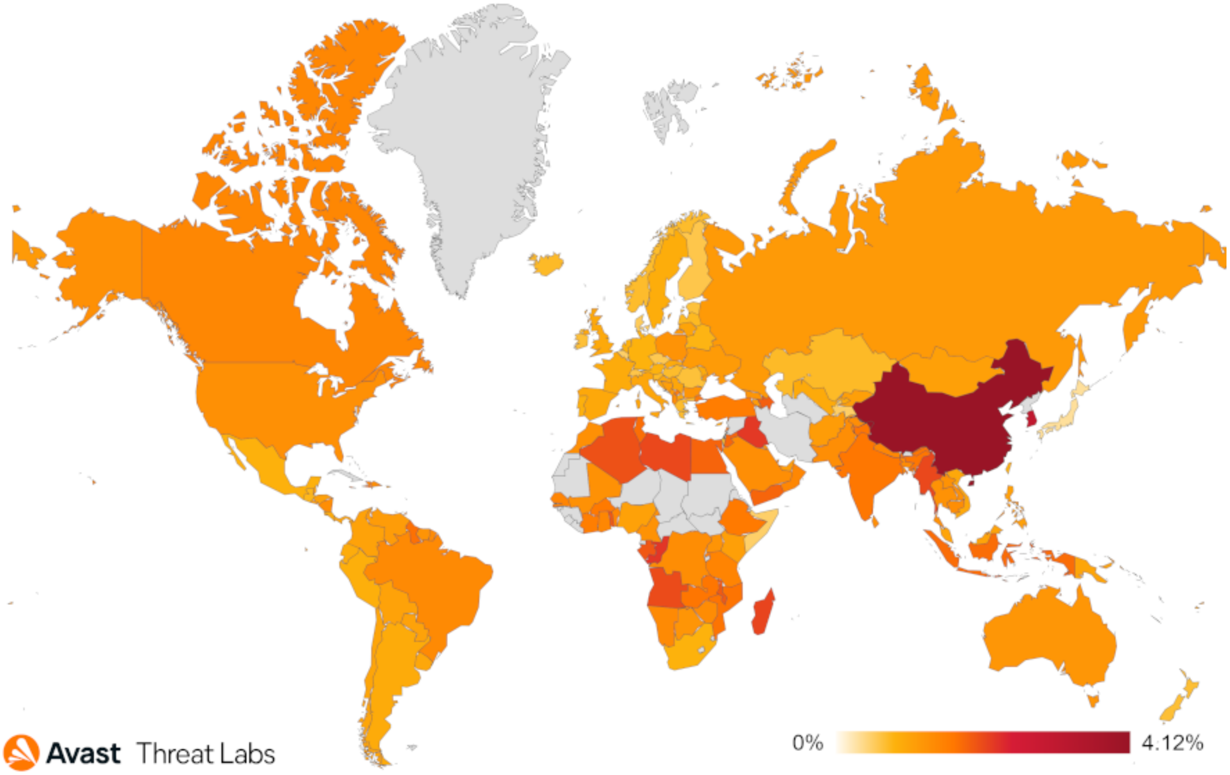
Global Avast risk ratio from desktop adware for Q1/2023 and Q2/2023

In the previous quarter, DealPly adware established itself as a leading force within the adware landscape with a 15% share. The map below shows that DealPly's risk ratio has increased globally by almost twice as much compared to Q1/2023.



Map showing global risk ratio for DealPly adware in Q2/2023

In contrast to the rise of DealPly, the risk of all adware strains is about half as much as Q1/2023. The significant increase in adware activity we observed in East Asia, namely Japan, Taiwan, and China, in Q1/2023 has stabilized with the overall average of Q2/2023. The complete risk ratio is illustrated in the map below.



Map showing the global risk ratio for Adware in Q2/2023

Adware Share

DealPly remains the undisputed market leader, holding a substantial 31% share. Smaller shares are allocated to other adware strains as follows:

- RelevantKnowledge (7%)
- BrowserAssistant (3%)
- Neoreklami (2%)

Nevertheless, lesser-known adware strains managed to capture a significant 32% market share in Q2/2023. The prevailing variant of these adware strains typically operates by intercepting user clicks on random hyperlinks and substituting them with redirects to advertising websites.

The following table provides a distribution of ad domains observed in the wild during the current and previous quarters. It is evident that ad domains are rotated dynamically each quarter to evade detection by ad blockers and other detection systems.

Q2/2023	Q1/2023
oovaufty[.]com (↑ 30%)	oovaufty[.]com (↑16%)
ptuvauthauxa[.]com (↑ 23%)	ptuvauthauxa[.]com (↓19%)
saumeechoa[.]com (↓ 15%)	saumeechoa[.]com (↑53%)
ninoglostoay[.]com (↑ 9%)	ninoglostoay[.]com (7%)
caumausa[.]com (5%)	—
applabzzeydoo[.]com (3%)	—
ad2upapp[.]com (↑ 2%)	ad2upapp[.]com (↓1%)

Representation of ad servers in the wild for Q2/2023 and Q1/2023

Adware tries to unobtrusively redirect users to websites that provide free software downloads or other products but also to dangerous content. In a separate section, we will overview the most common Web-based Adware in Q2/2023.

Martin Chlumecký, Malware Researcher

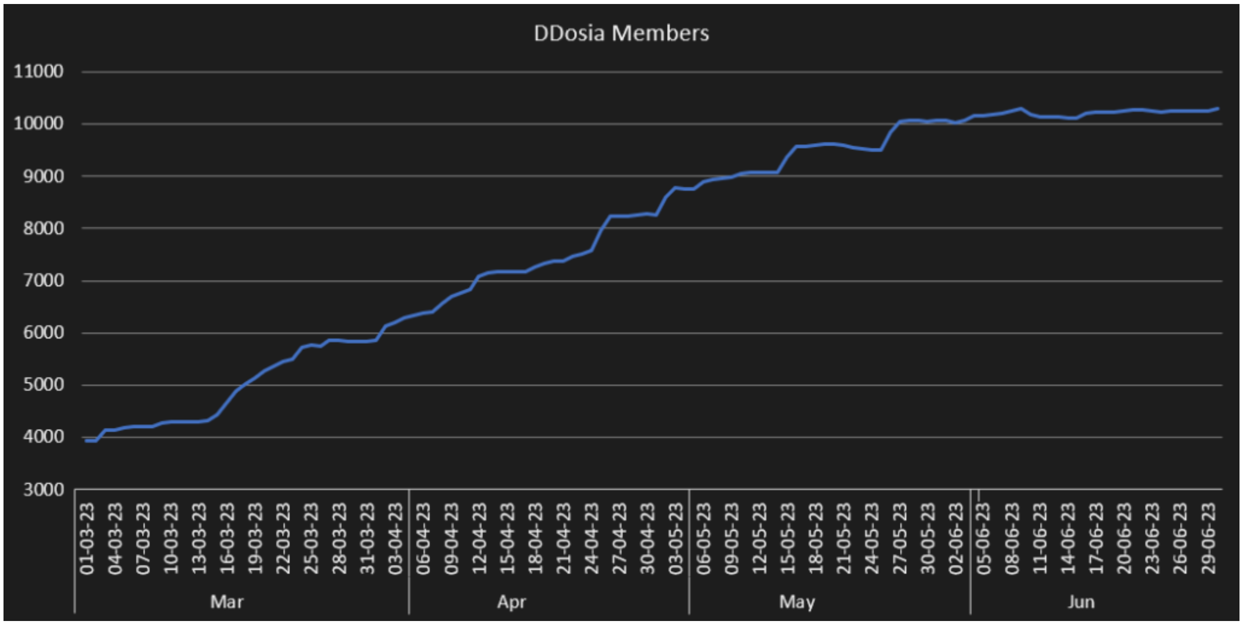
Bots

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.

We have continued to track the activities of notorious threat group NoName057(16), notably theirDDosia project. The release of our latest blogpost on the threat coincided with an update of DDosia's protocol. Just a day after the release, the protocol was updated to include encryption.

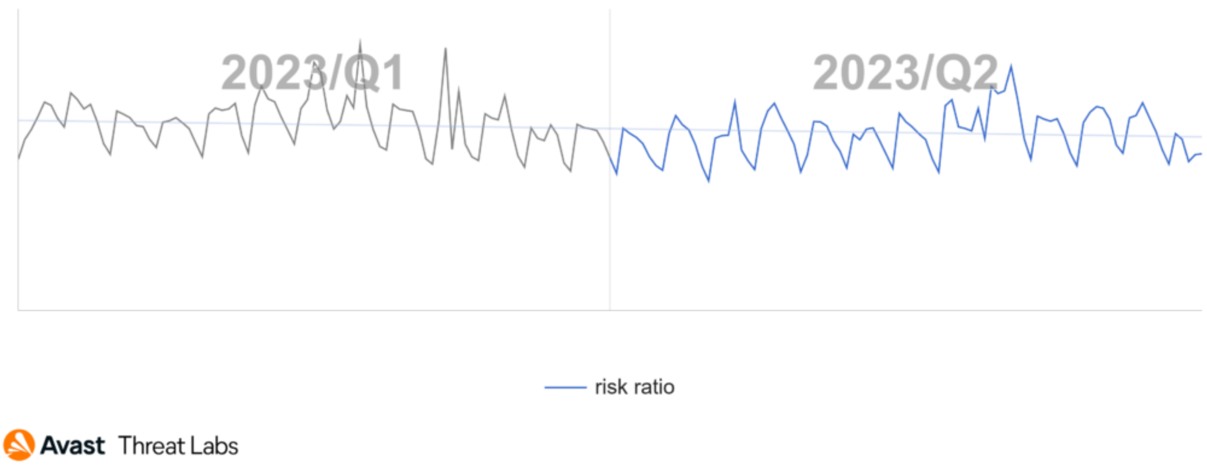
The most notable bot attack of Q2/2023 was the one following the Wagner Group rebellion. Just hours after the start of the rebellion, DDosia released a configuration targeting Wagner Group webpages which were up for almost a day. In contrast to usual operations, this attack wasn't announced on the project's Telegram channel. It is also worth noting that this attack was unsuccessful, and the targeted webpages were accessible throughout the DDoS attack without restrictions.

While it may seem unexpected for a Russian group to choose a Russian target, it seems to be well within their usual *modus operandi* which follows pro-government Russian interests. As for the group's development, it seems that the project's growth is slowly reaching its plateau with the current number of volunteers being around 11,500.



The size of DDosia community over last 4 months.

The overall botnet landscape to be rather stable, with a slight decline in risk ratio and no significant changes in the family distribution in comparison to the previous quarter. The only significant outlier is the MyKings family that has increased in activity by circa 20%.



Global risk ratio in Avast's user base regarding botnets in Q2/2023

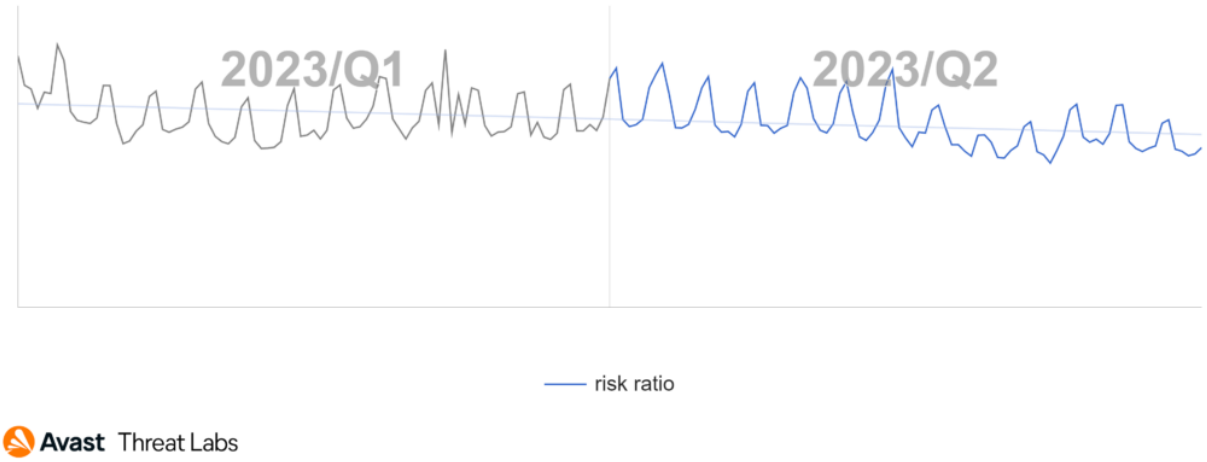
Adolf Středa, Malware Researcher

Coinminers

Coinminers are programs that use a device's hardware resources to verify cryptocurrency transactions and earn cryptocurrency as compensation. However, in the world of malware, coinminers silently hijack a victim's computer resources to generate cryptocurrency for an attacker. Regardless of whether a coinminer is legitimate or malware, it's important to follow our guidelines.

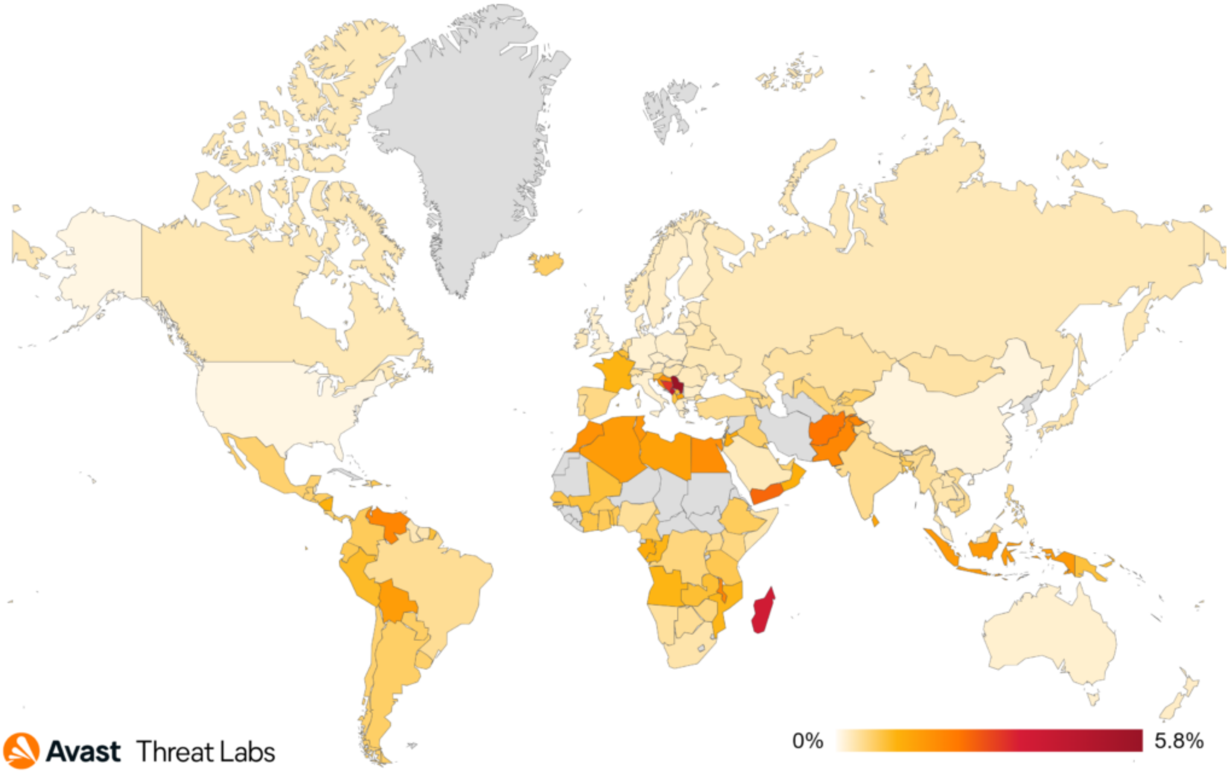
In the ever-evolving landscape of cryptocurrency mining, coinminers have been facing a continuous decline in their activity, a trend that has persisted over time. When compared to Q1/2023, we observed a 4% decrease in the risk ratio.

This sustained decline can be largely attributed to the growing adoption of proof-of-stake (PoS) protocols by various cryptocurrencies. PoS is considered a more energy-efficient and environmentally friendly alternative to the traditional proof-of-work (PoW) consensus mechanism used in coinmining.



Global risk ratio in Avast's user base in regard to coinminers in Q2/2023

In Q2/2023, users in Serbia faced the highest risk of encountering a coinminer once again, with a risk ratio of 5.80%. Following closely were Montenegro with 4.58%, Madagascar with 3.76%, and Bosnia and Herzegovina with a risk ratio of 3.17%.



Global risk ratio for coinminers in Q2/2023

Coinminer XMRig saw an increase in activity during Q2/2023, with its market share rising by 13% to reach 18.13%. Additionally, FakeKMSminer and VMiner became more prevalent, with their market shares increasing by 16% and 47% respectively, now holding 2.19% and 1.92% of the market each. Conversely, CoinBitMiner, CoinHelper, and NeoScrypt experienced declines of 7%, 13%, and 3% respectively, each holding roughly 1% of the market. Web miners also lost 2% of the market share, though they still dominate as the most prevalent form of coinmining, accounting for 65% of the market.

The most common coinminers in Q2/2023 were:

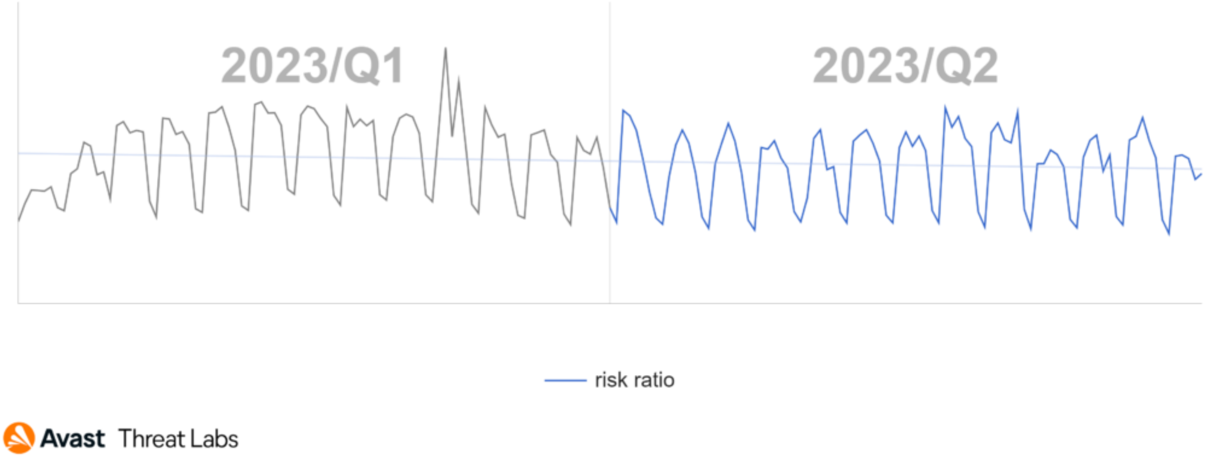
- Web miners (various strains)
- XMRig
- FakeKMSminer
- VMiner
- CoinBitMiner
- CoinHelper
- NeoScrypt

Jan Rubín, Malware Researcher

Information Stealers

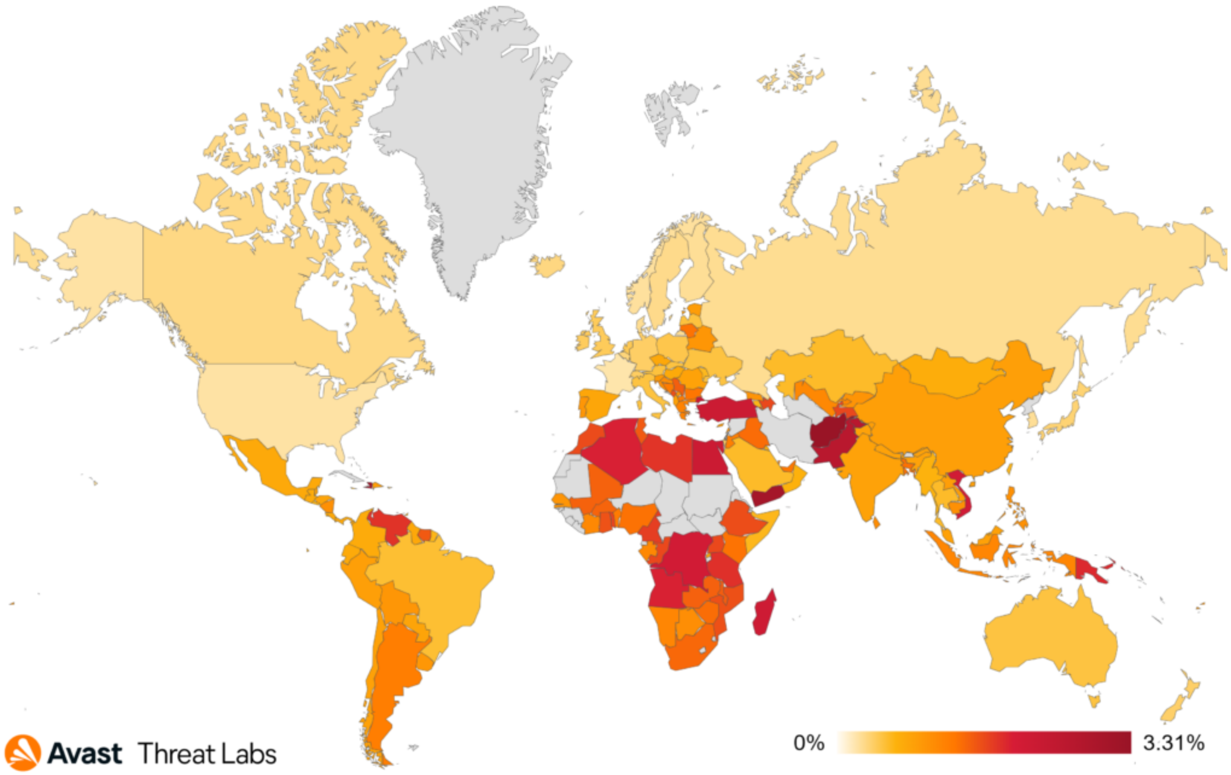
Information stealers are dedicated to stealing anything of value from the victim's device. Typically, they focus on stored credentials, cryptocurrencies, browser sessions/cookies, browser passwords and private documents.

During Q2/2023, information stealers experienced a 14% decrease in activity, mainly due to Raccoon Stealer and RedLine. These two saw their market shares drop by 31% and 36%, respectively.



Global risk ratio in Avast's user base in regard to information stealers in Q2/2023

Looking at the countries where we have more significant userbase, the highest risk of information stealer infections currently exists in Pakistan, Turkey, and Egypt, with risk ratios of 2.62%, 2.23%, and 2.22%, respectively. Surprisingly, during Q2/2023, there was a decrease in activity across almost every region, except for Switzerland (+7% risk ratio), Bulgaria (+2%), and Japan (+1%).



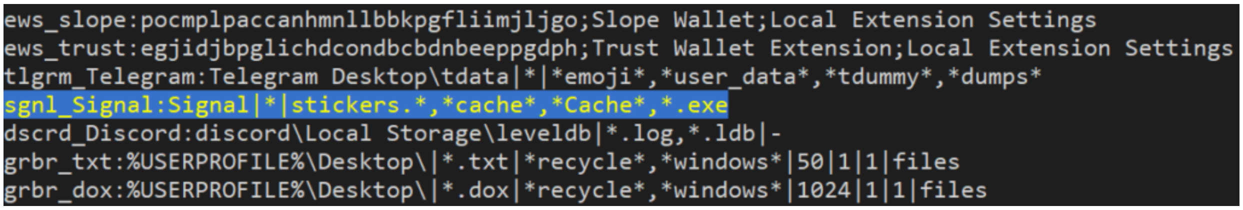
Map showing global risk ratio for information stealers in Q2/2023

Based on our data, AgentTesla holds the title of the most prevalent information stealer, with a market share of 27%. It experienced a noteworthy increase in activity during Q2/2023, boosting its market share by 26%. FormBook (11% market share), Fareit (5%), and Lokibot (5%) also saw their minor market shares rise. On the other hand, ViperSoftX maintained its levels with a slight 2% decrease in activity, now holding a 2.2% market share. As for Raccoon Stealer and RedLine, they currently hold market shares of 7% and 6%, respectively.

The most common information stealers in Q2/2023 were:

- AgentTesla
- FormBook
- Raccoon Stealer
- RedLine
- Fareit
- Lokibot
- ViperSoftX

Raccoon Stealer is constantly evolving. The malicious actors responsible for this threat have recently integrated Signal Desktop into their configuration, meaning they can now steal data from the popular communicator’s desktop clients, expanding their reach and potential impact on victims’ privacy and security.



```
ews_slope:pocmplpaccanhmnllbbkpgfliimjljgo;Slope Wallet;Local Extension Settings
ews_trust:egjidjbpglichdcondbcbdnbeeppgdph;Trust Wallet Extension;Local Extension Settings
tlgrm_Telegram:Telegram Desktop\tdata|*|*emoji*,*user_data*,*tdummy*,*dumps*
sgnl_Signal:Signal|*|stickers.*,*cache*,*Cache*,*.exe
dscrd_Discord:discord\Local Storage\leveldb|*.log,*.ldb|-
grbr_txt:%USERPROFILE%\Desktop\|*.txt|*recycle*,*windows*|50|1|1|files
grbr_dox:%USERPROFILE%\Desktop\|*.dox|*recycle*,*windows*|1024|1|1|files
```

Source: https://twitter.com/AvastThreatLabs/status/1648688808664215555

Additionally, new information stealers have entered the scene. One such stealer is Meduza Stealer used for data theft, compromising information such as login credentials, browsing history, bookmarks, crypto wallets, and more. Another stealer is Mystic Stealer that steals various information from infected systems, including computer details, user geolocation, web browser data, and cryptocurrency wallet information.

Clippers – another type of information stealer – are malware designed for clipboard hijacking and manipulation, usually focusing on cryptocurrency theft. They operate by monitoring the victim's clipboard for copied wallet addresses. When a clipper detects a cryptocurrency address being copied, the malicious code discreetly swaps it with the attacker's address. As a result, unsuspecting victims end up sending their digital assets to the attacker's wallet instead of the intended recipient, leading to financial losses.

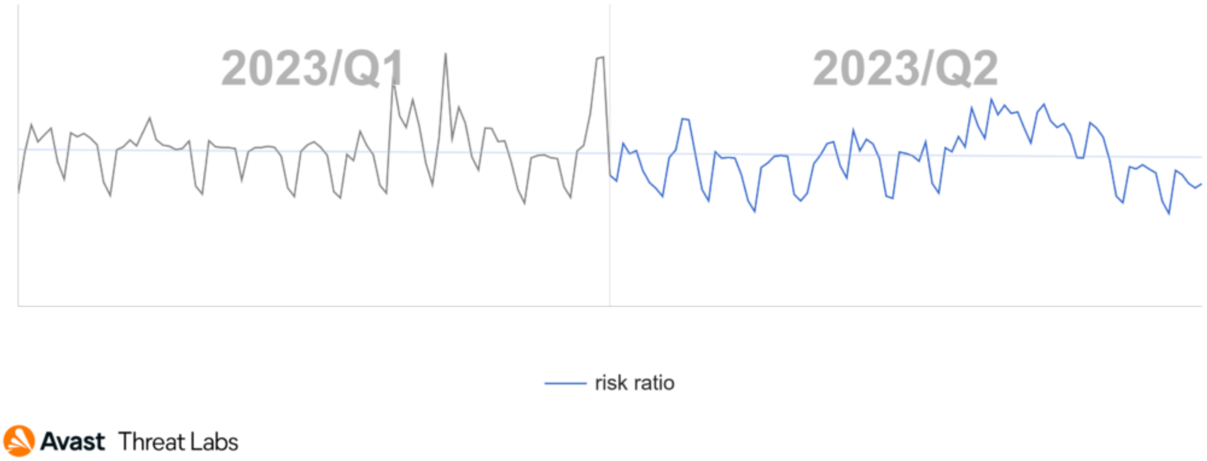
Laplas Clipper is one of the clippers that has gained popularity during Q2/2023. According to our data, it increased its market share by 224% compared to the previous quarter, now holding 1.49% of the entire information stealers market share.

Jan Rubín, Malware Researcher

Ransomware

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. In order to decrypt the files, attackers demand money, "ransom", hence the term ransomware.

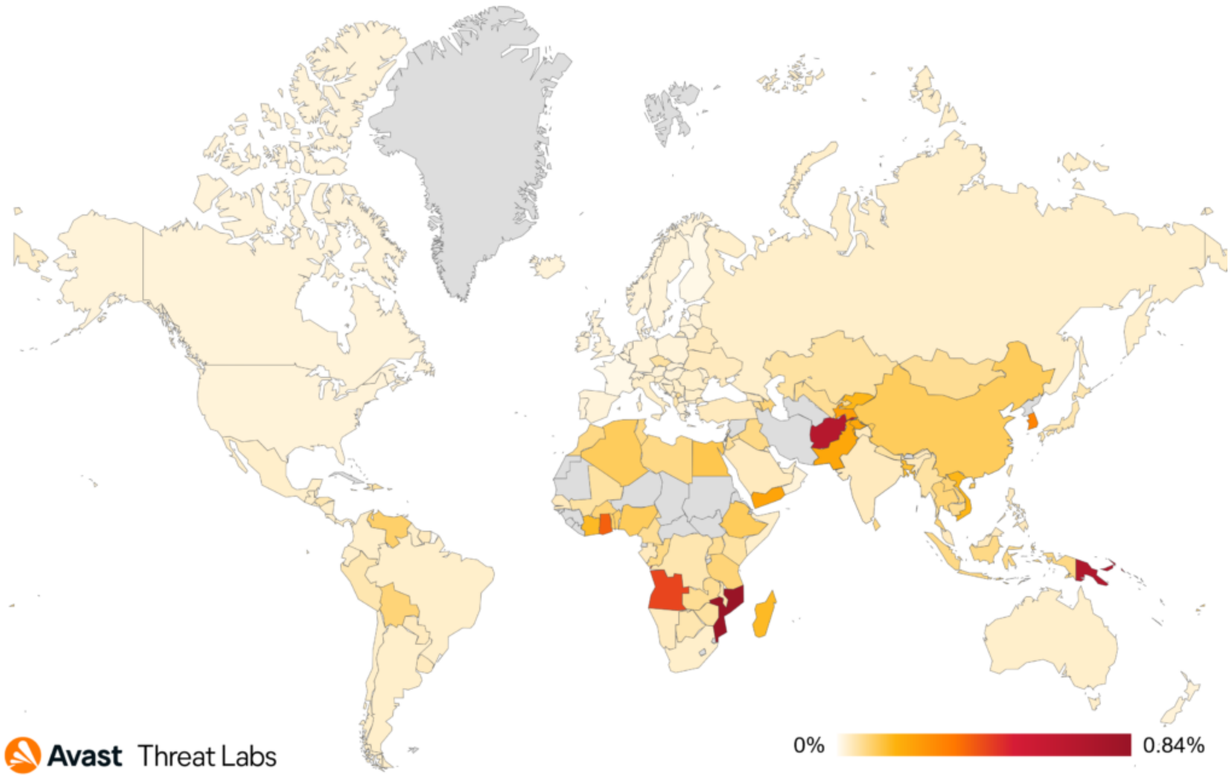
The overall risk ratio in ransomware declined slightly in Q2/2023 compared to the previous quarter:



Ransomware spreading in 2023

In Q2, countries with the highest prevalence of ransomware threats were:

1. Mozambique
2. Papua New Guinea
3. Afghanistan
4. Angola
5. Ghana
6. Republic of Korea



Map showing global risk ratio for ransomware in Q2/2023

The most prevalent ransomware strain in our userbase for the quarter were:

1. WannaCry
2. STOP
3. Magniber
4. GlobeImposter
5. Hidden Tear
6. Target Company
7. LockBit

Vulnerabilities on the Rise

A number of software vulnerabilities were used during the ransomware attacks in Q2/2023. Those included vulnerabilities in a widely used 3rd party software or leveraging of a vulnerable driver.

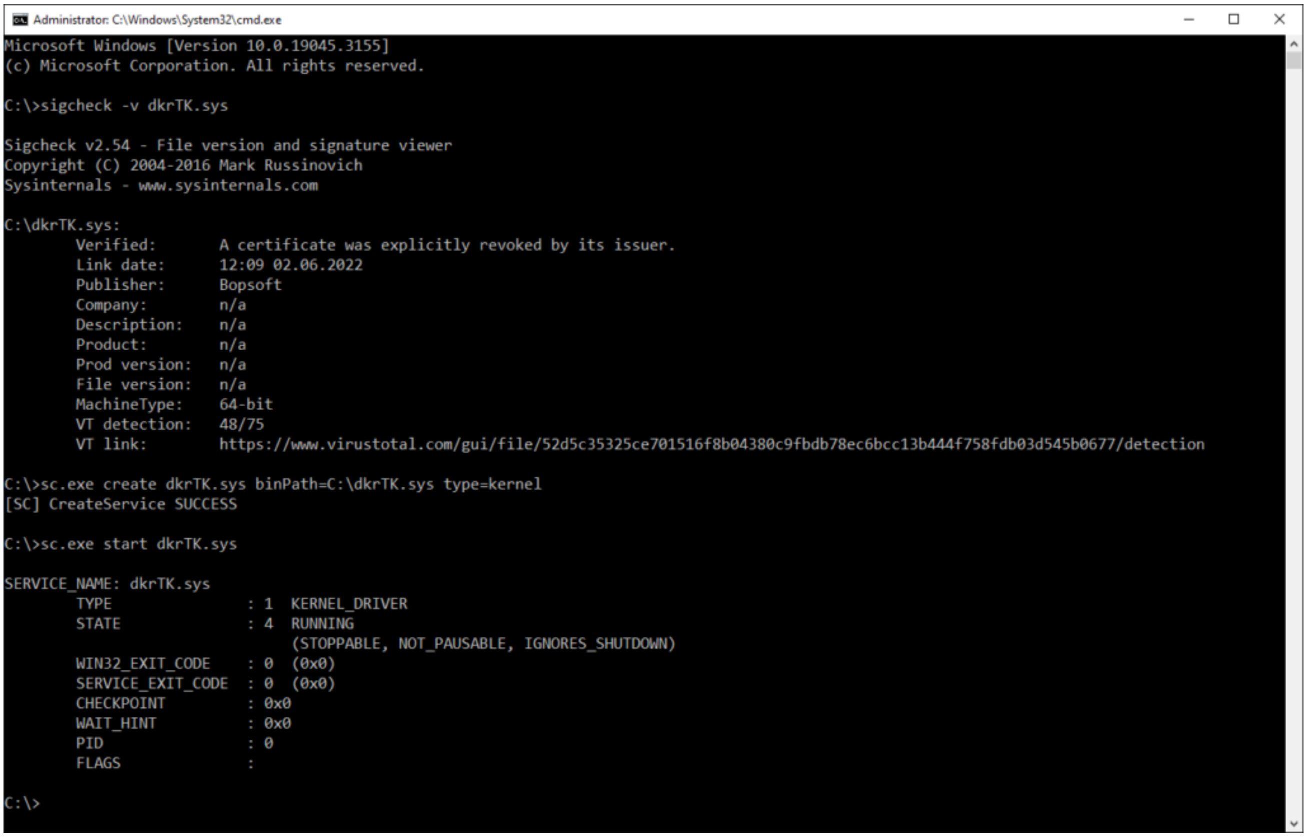
The most havoc in the ransomware world was caused by the CVE-2023-34362 vulnerability in the Progress MOVEit Transfer software. Unpatched versions of the MOVEit Transfer suffer from an SQL-injection vulnerability that allowed for unauthorized access to the MOVEit database as stated by the security advisory from Progress. Progress has since issued a patch to fix the vulnerability.

Another software vulnerability that was abused by threat actors to gain unprivileged access to the companies was in PaperCut, a print management software. As explained in the security advisory, there is a remote code execution (RCE) vulnerability, allowing to run a code on the PaperCut server without authentication. This vulnerability was abused by multiple ransomware gangs, such as Cl0p, LockBit and Bl00dy.

Papercut has since fixed these vulnerabilities. Users running PaperCut MF and PaperCut NG versions lower than 20.1.7, 21.2.11, and 22.0.9 should update their systems immediately to close this attack surface.

Additionally, the BlackCat ransomware was observed to be using a malicious driver to terminate running security software. A driver is a software component that runs in the very core of an operating system (in the kernel). As such, it needs to run with the highest permissions that are available in the operating system.

The Windows operating system protects its eco-system by only allowing drivers that are signed by a trusted certificate. But there is a catch: the driver used by the BlackCat ransomware is signed by a stolen, valid certificate. Such driver, even if the certificate was revoked, can still be loaded by Windows 10 even with the latest updates:



```
Microsoft Windows [Version 10.0.19045.3155]
(c) Microsoft Corporation. All rights reserved.

C:\>sigcheck -v dkrTK.sys

Sigcheck v2.54 - File version and signature viewer
Copyright (C) 2004-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\dkrTK.sys:
        Verified:       A certificate was explicitly revoked by its issuer.
        Link date:      12:09 02.06.2022
        Publisher:      Bopsoft
        Company:        n/a
        Description:    n/a
        Product:        n/a
        Prod version:   n/a
        File version:   n/a
        MachineType:    64-bit
        VT detection:   48/75
        VT link:        https://www.virustotal.com/gui/file/52d5c35325ce701516f8b04380c9fbdb78ec6bcc13b444f758fdb03d545b0677/detection

C:\>sc.exe create dkrTK.sys binPath=C:\dkrTK.sys type=kernel
[SC] CreateService SUCCESS

C:\>sc.exe start dkrTK.sys

SERVICE_NAME: dkrTK.sys
        TYPE               : 1  KERNEL_DRIVER
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
        PID                : 0
        FLAGS              :

C:\>
```

Akira Ransomware

Akira is a strain of ransomware that emerged in March 2023. This ransomware is written in the modern C++, which promises an elevated level of compatibility across multiple operating systems. It is no surprise that a Linux version appeared soon after the initial launch. Apart from replacing MS CryptoAPI (which is Windows-specific) by Crypto++ (which is multi-platform), the code remained mostly unchanged, including the exclusion list that has no meaning on Linux operating system. The list is as follows:

- winnt
- temp
- thumb
- $Recycle.Bin
- $RECYCLE.BIN
- System Volume Information
- Boot
- Windows
- Trend Micro

Avast discovered a flaw in the cryptography schema of Akira and published a decryptor that can help victims recover their data. However, Akira authors reacted swiftly and released an updated version of their encryptor that is no longer decryptable. Newer versions of the Akira ransomware use different extension for encrypted files; the Avast decryptor can only decrypt files that have the **.akira** extension. Nonetheless, many of the victims of the original version were able to recover their data and restore their businesses with the help of the Avast decryption tool.

New trend: Encryption-less ransomware

Encrypting user files is not a simple task. A typical computer may have gigabytes of potentially large data files – movies, music, ISO images, virtual machines. Those files' encryption takes a lot of CPU work and raises red flags for security solutions.

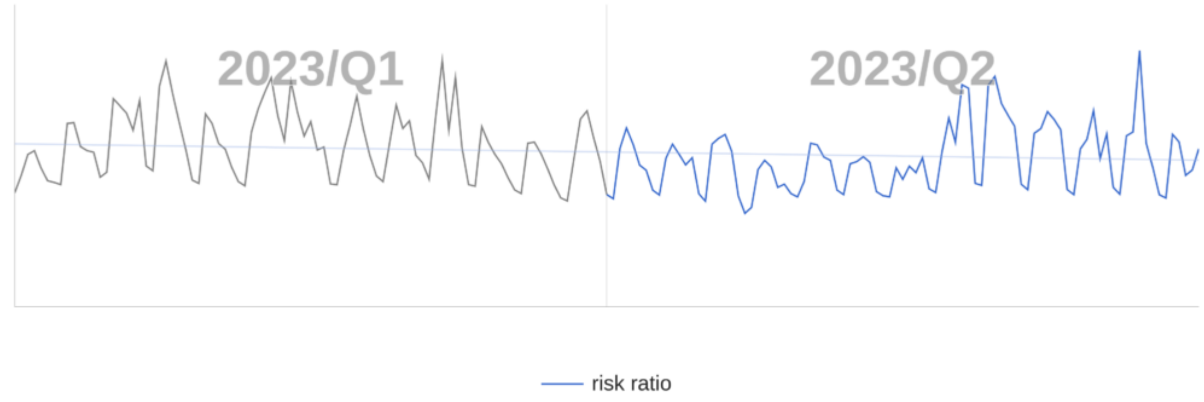
To help bypass these security solutions, a new trend was observed by ZScaler researchers – encryption-less ransomware. Instead of data encryption, such ransomware focuses on pure data extortion. Attackers then threaten to publish the data, which can severely damage the victim's reputation or expose their intellectual properties.

*Ladislav Zezula, Malware Researche*r
Jakub Křoustek, Malware Research Director

Remote Access Trojans (RATs)

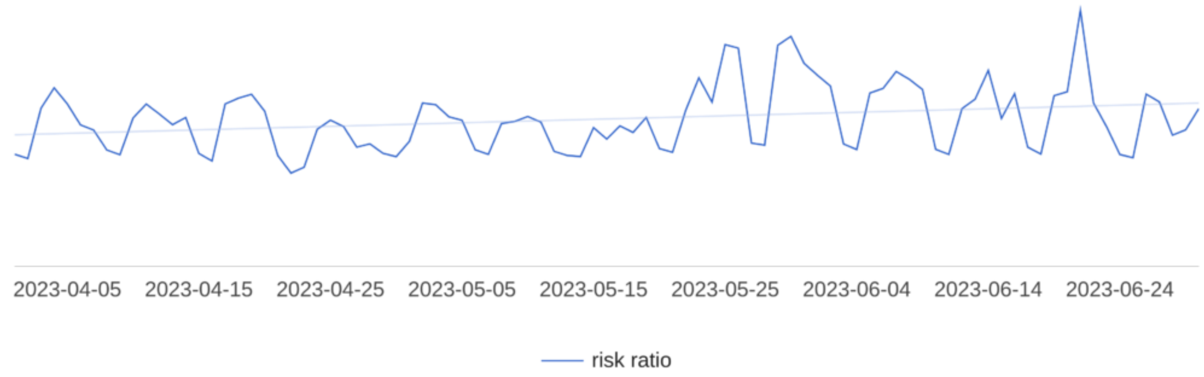
A Remote Access Trojan (RAT) is a type of malicious software that allows unauthorized individuals to gain remote control over a victim's computer or device. RATs are typically spread through social engineering techniques, such as phishing emails or infected file downloads. Once installed, RATs grant 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.

In Q2/2023, Remcos continued to increase its share of attacks among other RATs. We saw the largest increase In Europe, Canada, South Africa, Vietnam and Indonesia where it gained a little over 30 %, while in the rest of the world its share slightly declined. In overall Remcos gained 22% compared to Q1/2023. The overall risk ratio of RATs slightly decreased compared to Q1/2023, however, looking solely at numbers for this quarter the trend seems to be going up with April being the calmest month.



Avast Threat Labs

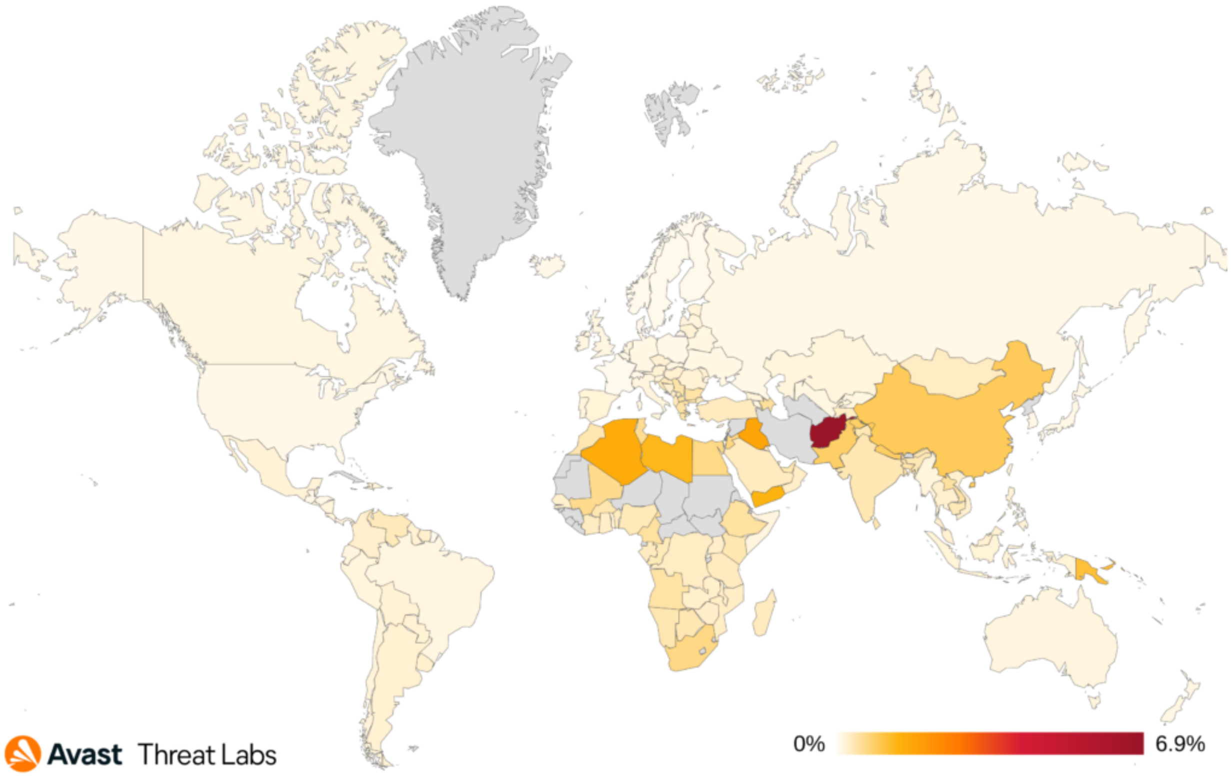
Global risk ratio in Avast's user base regarding RATs in Q2/2023 compared to Q1/2023



Avast Threat Labs

Global risk ratio in Avast's user base regarding RATs in Q2/2023

Countries with the highest risk ratio for RATs are Afghanistan, Iraq, and Algeria with the most prevalent threats being HWorm and njRAT. The countries with the highest increase in risk ratio are Bulgaria, Belgium and Serbia due to the activity of Remcos as mentioned above.



Map showing global risk ratio for information stealers in Q2/2023

Another strain with considerable market share gain of 25% is Warzone which was mostly active in Greece, Bulgaria, Serbia and Croatia. Conversely, NetWire saw a drop of 60%, which is the largest decrease of all RAT Avast tracks. This may be related to the takedowns and arrests of cyber groups which happened in Q1/2023.

The most prevalent remote access trojan strains in the Avast userbase are:

- HWorm
- Remcos
- njRAT
- Warzone
- AsyncRat
- QuasarRAT
- NanoCore
- Gh0stCringe
- DarkComet
- LimeRAT

We have published a blog post detailing the workings and infection vector of HotRat. HotRat is a reimplementation of AsyncRat in .NET. This new rewritten version adds multiple new commands which are focused mostly on stealing data from victim machines. HotRat is being spread through pirated software such as products by Adobe and Microsoft, video games, and premium system and development tools like IObit Driver Booster, VMware Workstation or Revo Uninstaller Pro.

Researchers from Avira also discovered a new RAT named ValleyFall which can log keyboard input, gather information from the victim's system, download and execute other executables and more. According to their data, the United States is the most affected country.

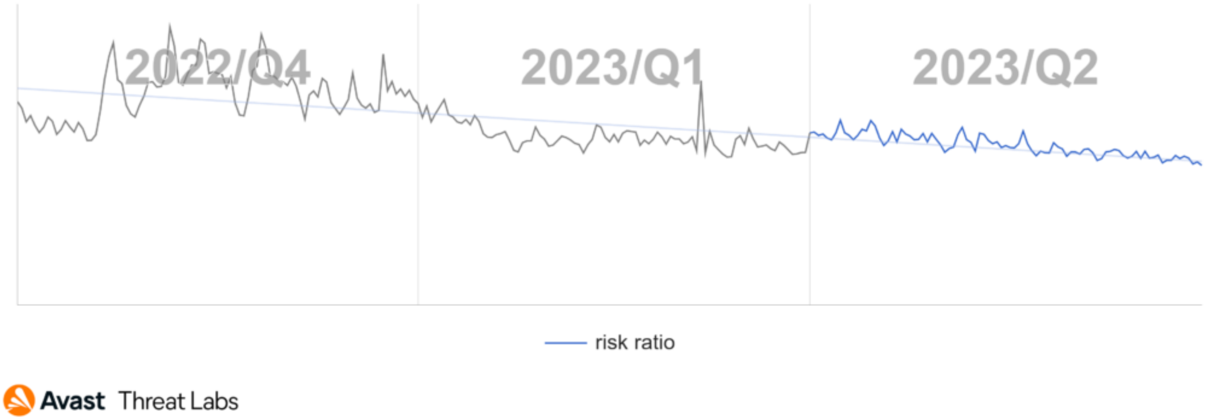
GobRAT is another RAT written in the programming language Go, capable of infecting Linux routers as reported by JPCERT/CC. It supports multiple architectures (ARM, MIPS, x86, x86-64). GobRAT has 22 commands available among them using reverse shell connection, running SOCKS5 proxy, attempting to log in to services running on other machines (sshd, Telnet, Redis, MYSQL, PostgreSQL) or carrying out DDOS attacks.

Ondřej Mokoš, Malware Researcher

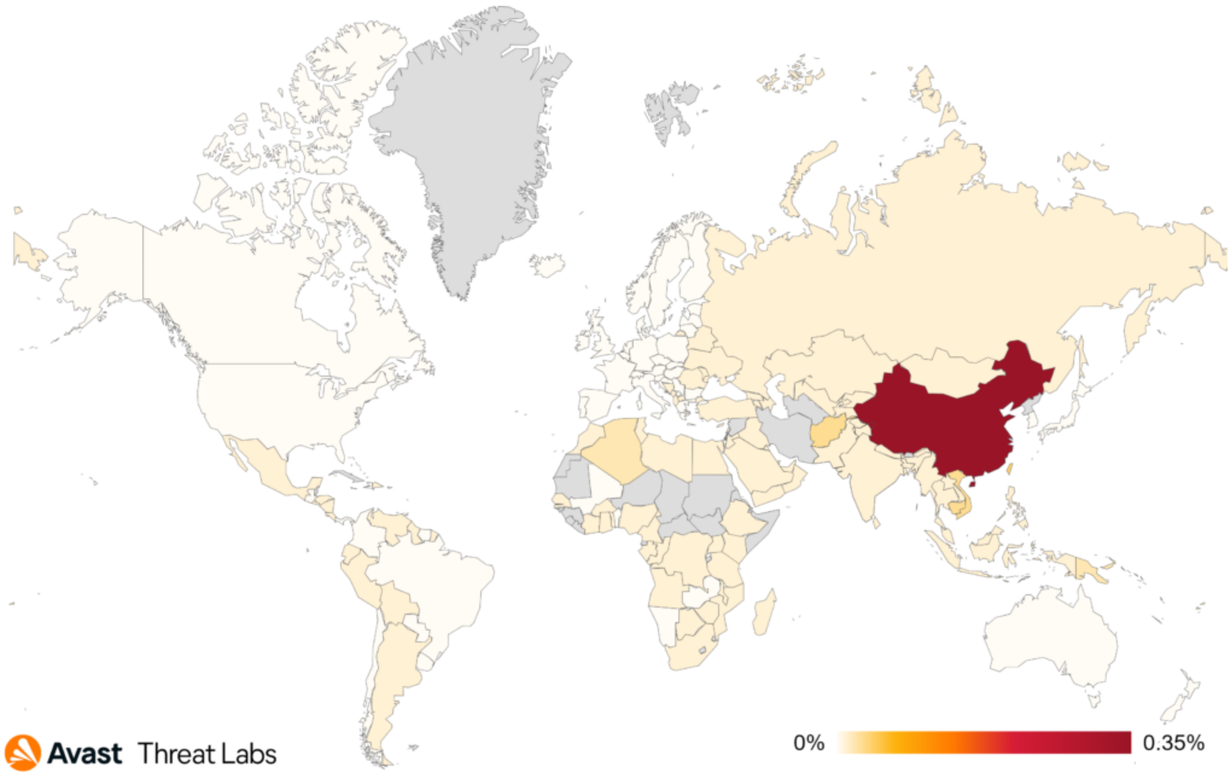
Rootkits

Rootkits are malicious software specifically designed to gain unauthorized access to a system and obtain high-level privileges. Rootkits can operate at the kernel layer of a system, which grants them deep access and control including the ability to modify critical kernel structures. This could enable other malware to manipulate system behavior and evade detection.

As reported in Q1/2023, we observed a downward trend in rootkits beginning in Q4/2022. If we compare the previous and the current quarter, we continue to see a decline, with the rate slightly tapering off. The next quarter should show whether the downward trend of rootkits is long term. The chart below shows the rootkit activity for the previous three quarters.



Rootkit risk ratio in Q4/2022 – Q2/2023

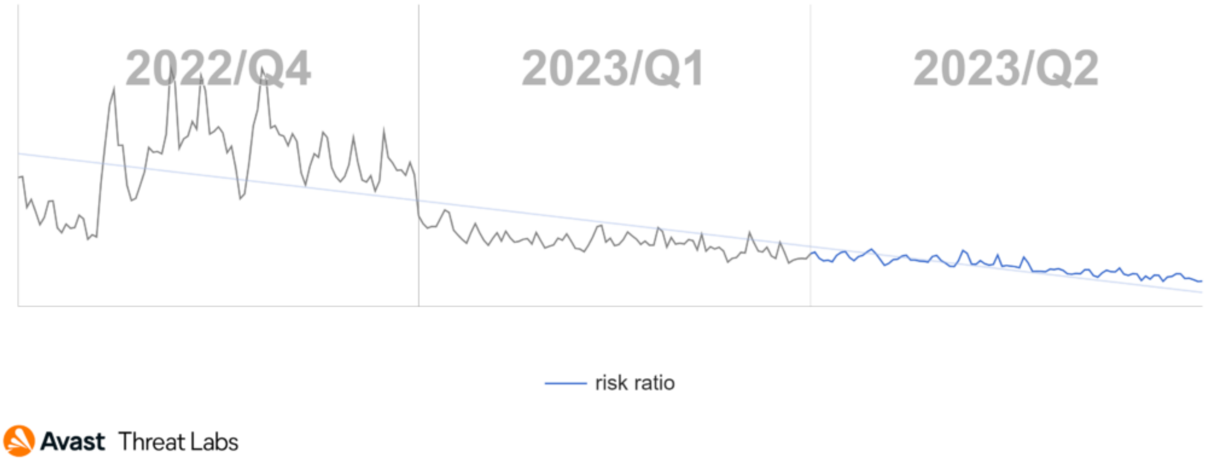


Global risk ratio for rootkits in Q2/2023

When considering the risk ratio on a country-by-country basis, China continues to hold the top position in terms of the magnitude of rootkit activities.

For the first time, we monitored the downtrend trend of the R77RK rootkit activity, which dominated the landscape for nearly 5 quarters. In Q2/2023, the R77RK market share is only 18% whereas the share was 40% on average for the previous year. In addition, the last R77RK release was on June 6, 2023, but was only a minor bug fix.

In Q1/2023, we noted a reduction in R77RK releases, which probably caused the drop in the prevalence of the R77RK activities in the wild. We therefore expect a gradual decrease in the activities of this rootkit in the next quarter based on the graph below, which shows a downward trend in activities from Q1/2023.



R77Rootkit risk ratio in Q4/2022 – Q2/2023

The market share also includes approximately 25% of rootkits of unspecified strains which are used as kernel proxies for various activities with higher system privileges such as killing processes, modifying network communication, etc.

Below you can see the complete list of clearly identified Windows rootkit strains, along with their corresponding market shares:

- Cerbu (7%)
- Alureon (7%)
- Perkesh (6%)
- ZeroAccess (3%)

The market share for clearly identified rootkit strains is the same as the previous Q1/2023 quarter.

In terms of Linux operating systems, we continue efficiently discovering and tracking new Linux Kernel rootkits, for instance, we were first detecting *Chicken* or NetHid. We saw an increase in rootkits using magic packets, for instance NetHid handles a UDP magic packet for executing a malicious user-mode application.

As you already know from the Syslogk rootkit, we are tracking threat actors in the development stage allowing us to early detect advanced threats but also PoCs and tools that they use during development (e.g. kernel modules for testing).

Martin Chlumecký, Malware Researcher
David Álvarez, Malware Analyst

Vulnerabilities and Exploits

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.

The May Patch Tuesday security update contained a patch for CVE-2023-29336, a local privilege escalation vulnerability discovered by Avast researchers in the wild. This is a kernel exploit that targets a vulnerability in win32k, a subsystem providing graphics functionality in the Windows kernel. We shared a proof-of-concept exploit with Microsoft along with our vulnerability report, but we did not make any technical details about this vulnerability public. However, fellow researchers from Numen Cyber analyzed the patch and published a great write-up and a proof-of-concept exploit.

While the win32k subsystem has always been a frequent target of exploits, there are some encouraging signs that indicate this subsystem might be getting more secure. First of all, Microsoft developed a number of win32k-specific exploit mitigations and security improvements over the years. Many of these aimed to eliminate kernel address leaks and break known exploitation primitives. A less-known security improvement is that Microsoft turned many raw pointers into smart pointers. This effectively made the CVE-2023-29336 use-after-free condition not exploitable on Windows 11, as well as on the latest builds of Windows 10. Furthermore, browsers such as Chromium adopted a mitigation sometimes known as “win32k lockdown“, which reduces the browser sandbox attack surface and makes win32k exploits impossible for sandbox escape exploits. Last but not least, a small part of win32k got recently reimplemented in Rust. Since Rust is designed to be a memory-safe language, this should significantly reduce the number of memory corruption vulnerabilities in the reimplemented code.

In our Q1/2023 threat report, we wrote about the Nokoyawa and Magniber ransomware groups using zero-day exploits to deploy ransomware. Q2/2023 continued this concerning trend, with the most notable event being the Cl0p ransomware group exploiting CVE-2023-34362, a remote code execution vulnerability in the MOVEit Transfer web application. This data theft-only attack hit an astounding number of organizations worldwide, with many of them getting their stolen data published on the Cl0p leak site.

In June, Kaspersky reported it was impacted by an APT attacker exploiting iOS devices, dubbing the attack Operation Triangulation. The exploits were delivered through an iMessage attachment in a zero-click manner. Kaspersky managed to recover three vulnerabilities: CVE-2023-32434, CVE-2023-32435, and CVE-2023-38606. The former two got patched by Apple in June and the third one was patched on July 24. As Eugene Kaspersky discussed in a blog, discovering such attacks is currently extremely hard due to the lack of visibility resulting from the closed nature of iOS.

On top of these three CVEs in early July, Apple released a rapid security fix for a remote code execution vulnerability CVE-2023-37450 in WebKit, the browser engine powering the Safari browser. The vulnerability was reported by an anonymous researcher and might have been actively exploited. Apple later mentioned that the fix might affect the display of certain pages. Redhat's support portal suggests that the vulnerability is related to processing of WebAssembly code. It is important to note that other apps using WebKit might be also affected by this vulnerability.

Just after the end of Q2/2023, US CISA and the FBI published a joint advisory regarding a serious espionage attack by Chinese APT group Storm-0558 which was able to access tens of Outlook enterprise accounts. The attackers were able to obtain inactive MSA consumer signing key which they used to forge Azure AD access tokens. While the MSA key had been expired since 2021, the system still accepted the tokens signed by it. Researchers from Wiz later speculated, that the key also was trusted to sign OpenID tokens which are used for other Microsoft services such as Teams, SharePoint and OneDrive. Microsoft revoked the compromised key which mitigated the issue.

There was a lot of activity surrounding vulnerabilities and exploits in Q2/2023 and at the beginning of Q3/2023. While some would say that there were many more reported vulnerabilities or with higher impact, it seems to be only a professional bias as we were not able to gather hard data that would show a general surge.

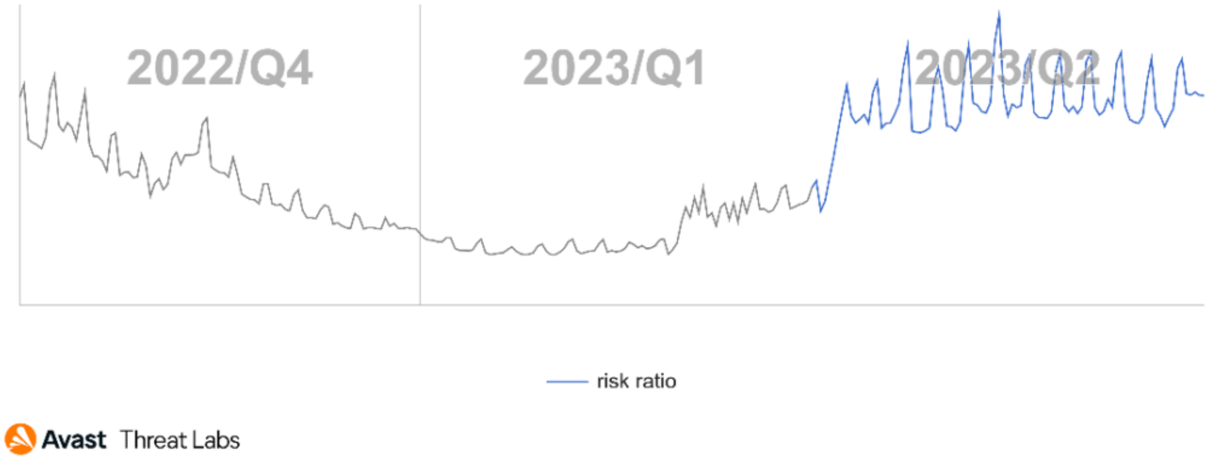
Jan Vojtěšek, Malware Reseracher
Michal Salát, Threat Intelligence Director

Web Threats

Scams

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

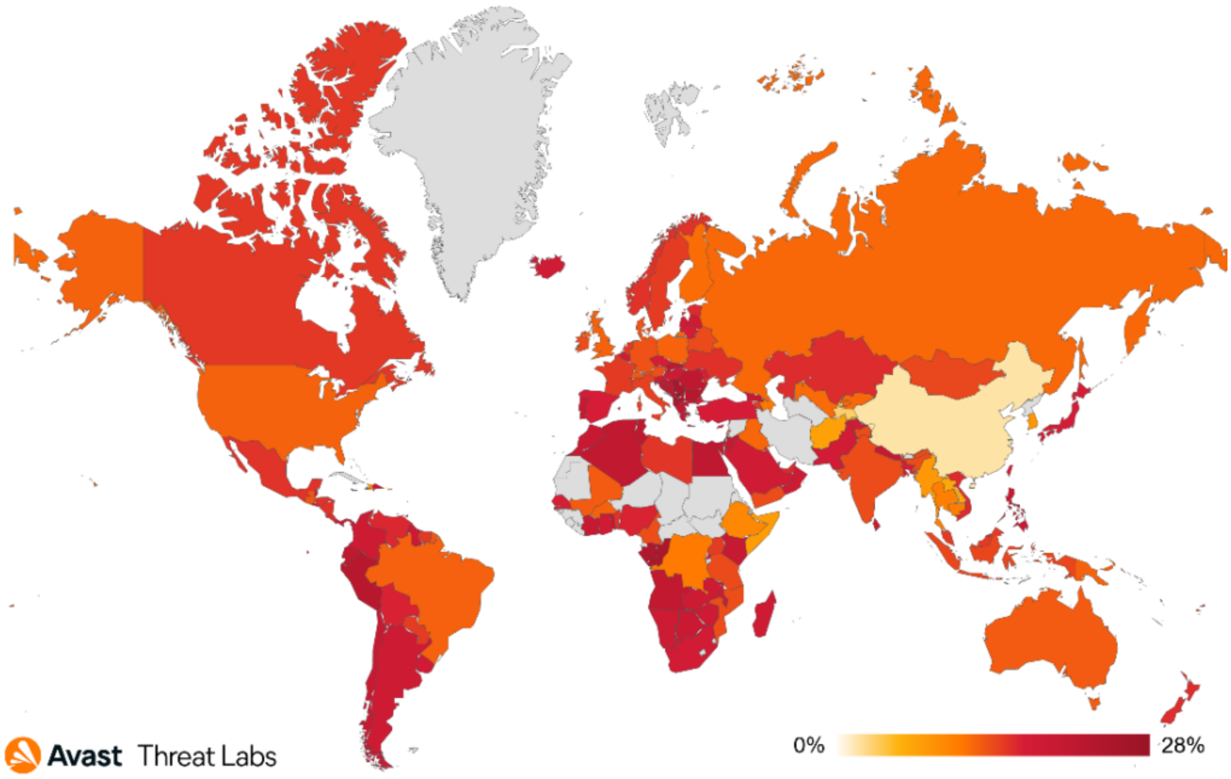
The Q1/2023 Threat Report shared that scams were the most prevalent threat type with a significant overall risk ratio of 7.7% and a 33% share among the other malware types. In Q2/2023, the situation has further escalated, and the risk ration has more than doubled as demonstrated in the following chart.



Scam risk ratio over the last three quarters

Our telemetry saw a massive surge in scam attacks which began in April and lasted the duration of the quarter. Attackers have focused mostly on malvertising and malicious browser push notifications as a delivery mechanism for these scams – those are described below. As a result – **scam attacks now form more than a half of all the blocked attacks in the Avast userbase**.

When we focus on targets of these attacks, we can see that scammers are not picky and target users across the world:



Global risk ratio for scam in Q2/2023

The countries most at risk of the scam attacks were Kosovo, Serbia, Bulgaria, and Slovakia. Furthermore, we've monitored one of the largest increases in scam risks in Vietnam (more than threefold), Argentina (+117%), Spain (+112%), France (+97%), Brazil (+95%), Mexico (+87%), Czech Republic (+81%), and in UK (+78%).

The second most prevalent subtype after malvertising was dating scams (AKA romance scam), which also increased significantly quarter over quarter.

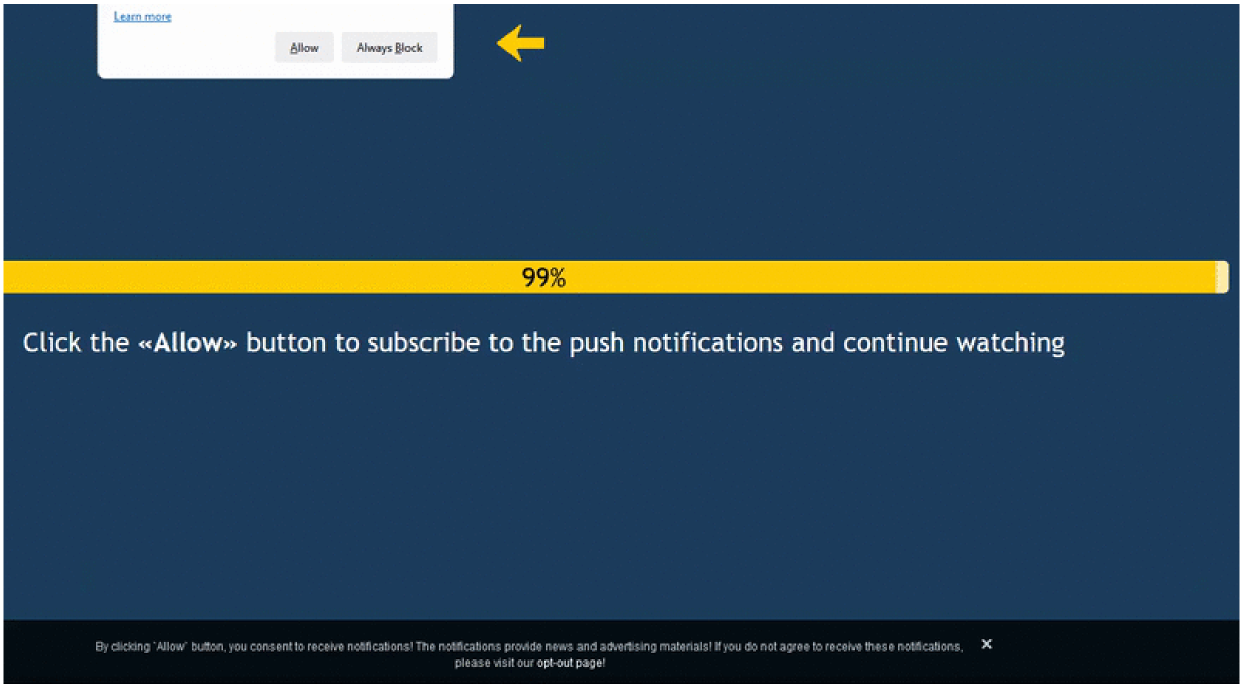
Technical support scams followed in terms of overall prevalence but actually decreased slightly in Q2/2023 compared to the previous quarter.

Finally, though not as prevalent as the other scam types, the extortion email scams had the most dramatic boost in Q2/2023 with a severalfold increase. We warned consumers of these emails in April 2023 and expect to see more of these types of threats in the future.

Malicious Browser Push Notifications

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.

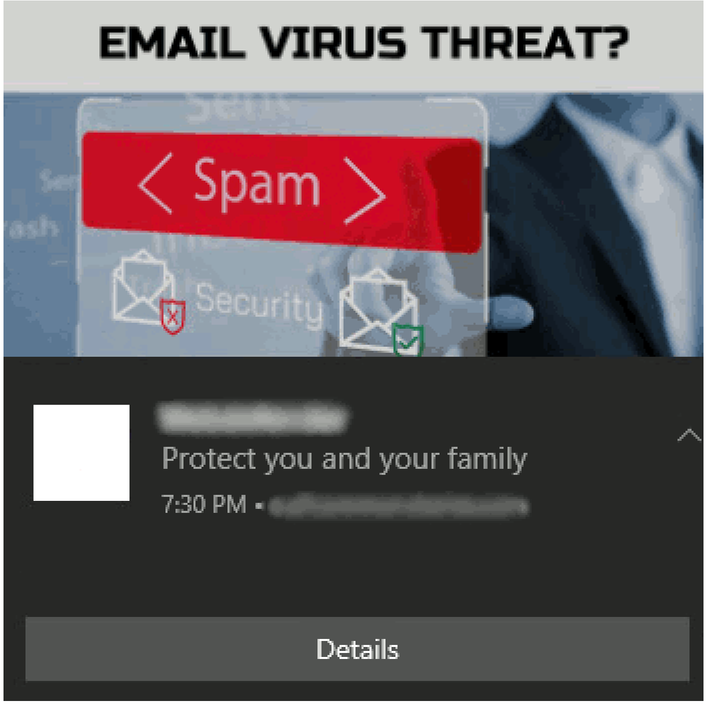
A trendy tactic of scam and adware authors is exploiting "push notifications" on web browsers. The user is forced to enable notifications in order to continue to the desired page – sometimes, a simple miss-click. The result is that the user is then redirected to various scam sites or bombarded with notifications for various offers and services that lure the user into clicking, for example popups that say the user's computer is infected, enticing dating sites or incredible "deals" on products.



Click the «Allow» button to subscribe to the push notifications and continue watching

By clicking 'Allow' button, you consent to receive notifications! The notifications provide news and advertising materials! If you do not agree to receive these notifications, please visit our opt-out page!

Example of a malicious browser push notification blocked by Avast in Q2/2023



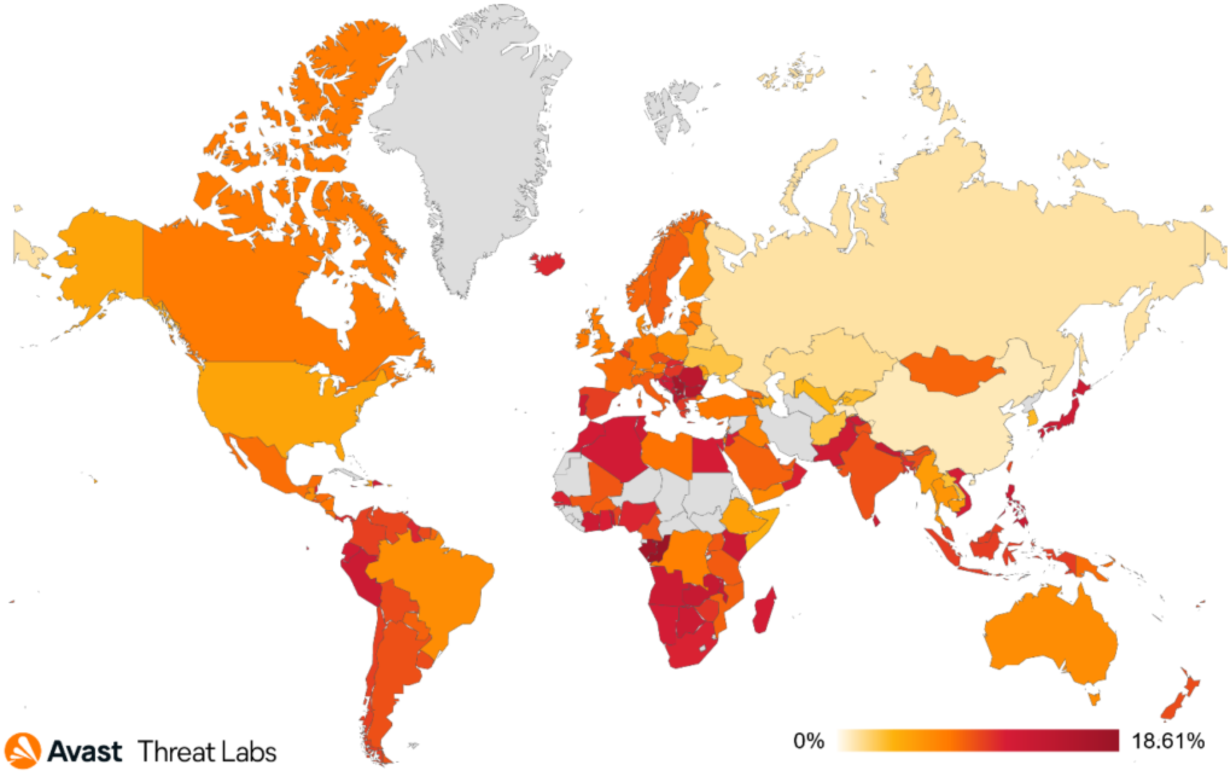
[redacted]

Protect you and your family

7:30 PM • [redacted]

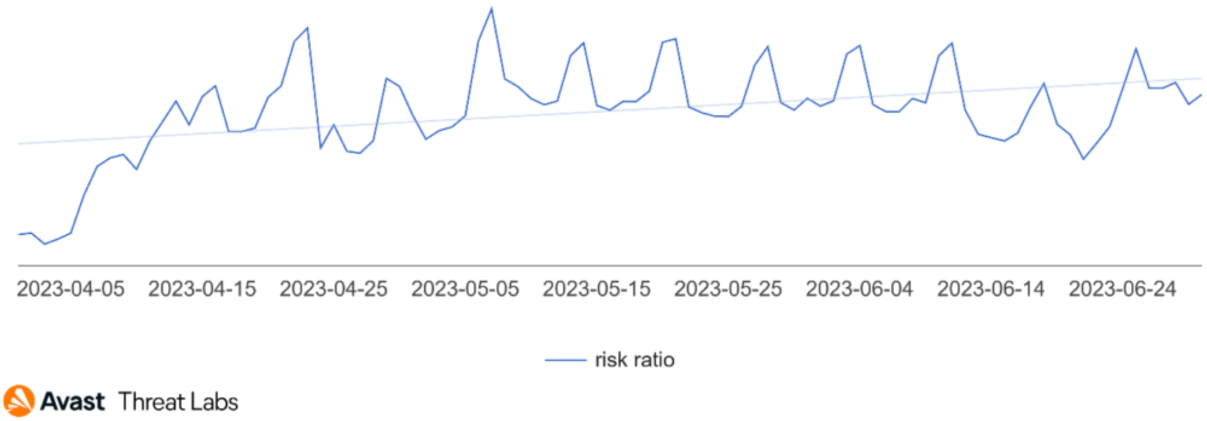
Another example of a malicious browser push notification blocked by Avast in Q2/2023

As previously mentioned, malicious push notifications were very prevalent in Q2/2023. The risk ratio was extremely high in African countries, such as Congo (18% risk ratio), as well as Japan (12%), Slovakia (11%), Spain (10%), and India (9%).



Risk ratio for malicious browser push notifications in Q2/2023

Based on our detection telemetry, this particular wave of attacks started in the middle of April and lasted through the entire quarter.



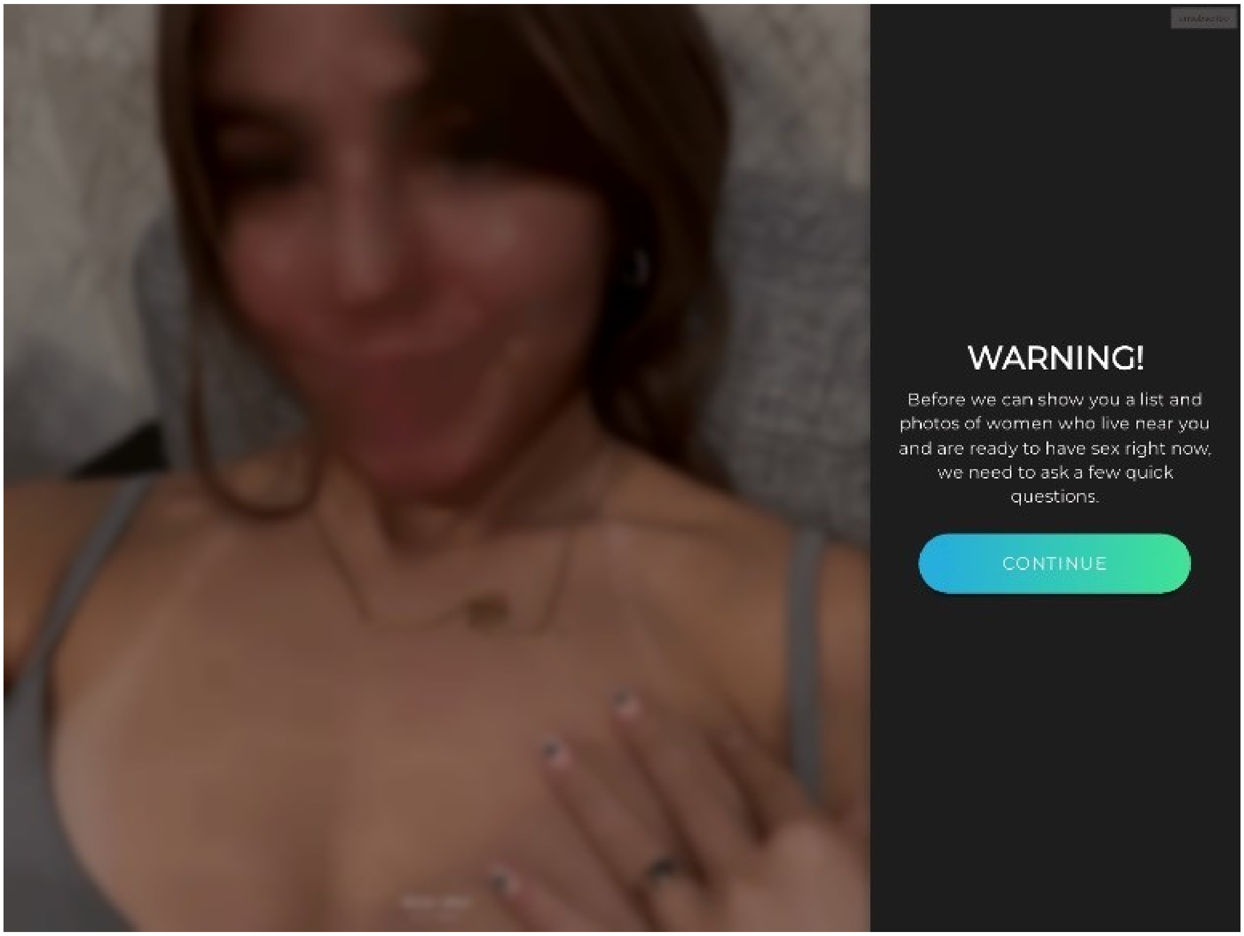
Risk ratio for malicious browser push notifications in Q2/2023

Dating Scams

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.

There was a concerning and substantial rise in dating scams in Q2/2023 compared to the previous quarter. The surge is evident with a 39% increase, posing a significant threat to individuals seeking romantic connections online.

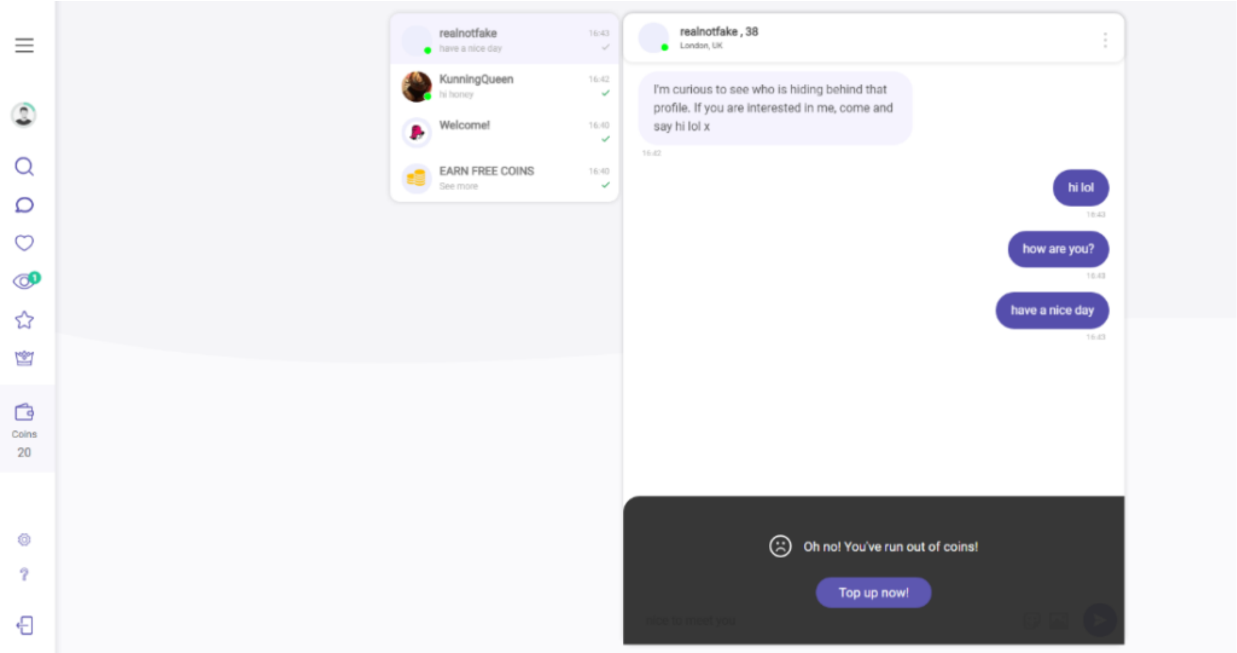
In Q2/2023, we observed yet another variation of this scam, as attackers employed various methods of initial infection including deceptive emails, push notifications, and misleading advertisements. Once targeted, victims were redirected to seemingly legitimate dating sites populated with fake bot profiles. When individuals attempted to engage in conversation with these profiles, they were coerced into paying for a subscription, falling prey to the scam.



WARNING!

Before we can show you a list and photos of women who live near you and are ready to have sex right now, we need to ask a few quick questions.

Example of a dating scam lure site blocked in Q2/2023



realnotfake 16:43
have a nice day

KunningQueen 16:42
hi honey

Welcome! 16:40

EARN FREE COINS 16:40
See more

realnotfake , 38
London, UK

I'm curious to see who is hiding behind that profile. If you are interested in me, come and say hi lol x
16:42

hi lol
16:43

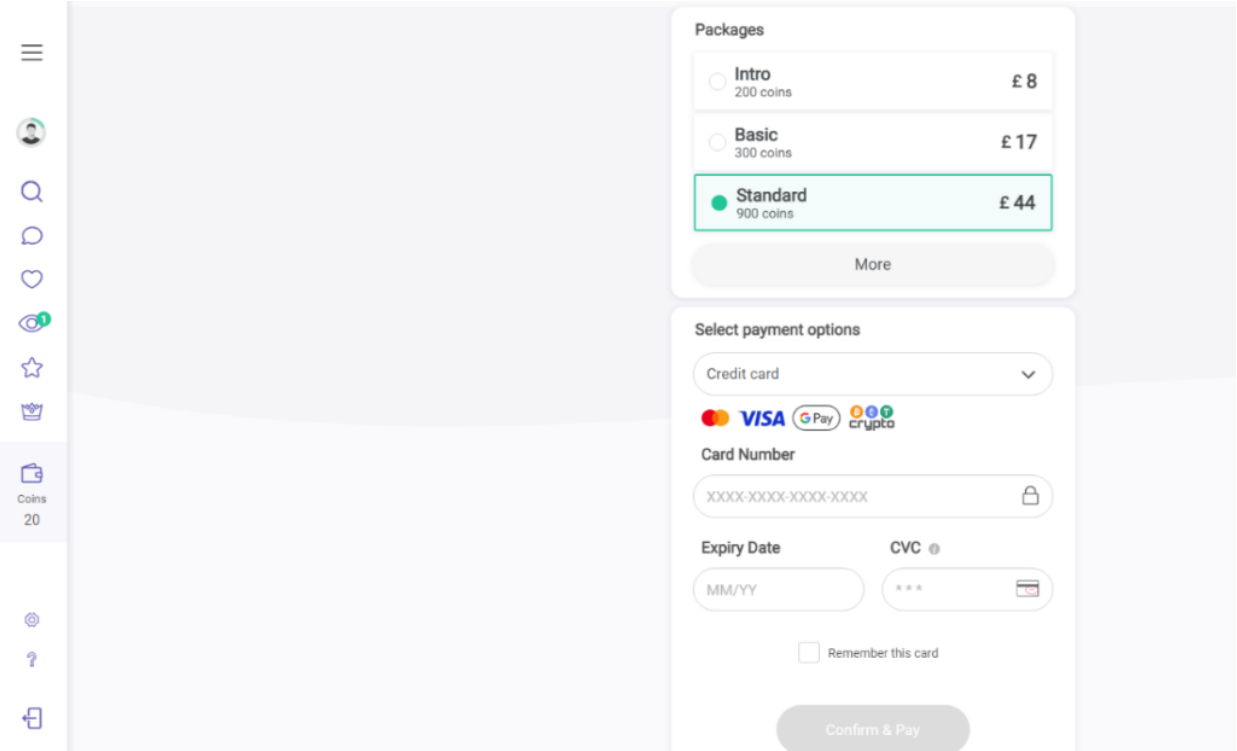
how are you?
16:43

have a nice day
16:43

Oh no! You've run out of coins!

Top up now!

Example of a dating scam blocked in Q2/2023



Packages

○ Intro 200 coins	£ 8
○ Basic 300 coins	£ 17
● Standard 900 coins	£ 44

More

Select payment options

Credit card

Card Number

XXXX-XXXX-XXXX-XXXX

Expiry Date

MM/YY

CVC

* * *

□ Remember this card

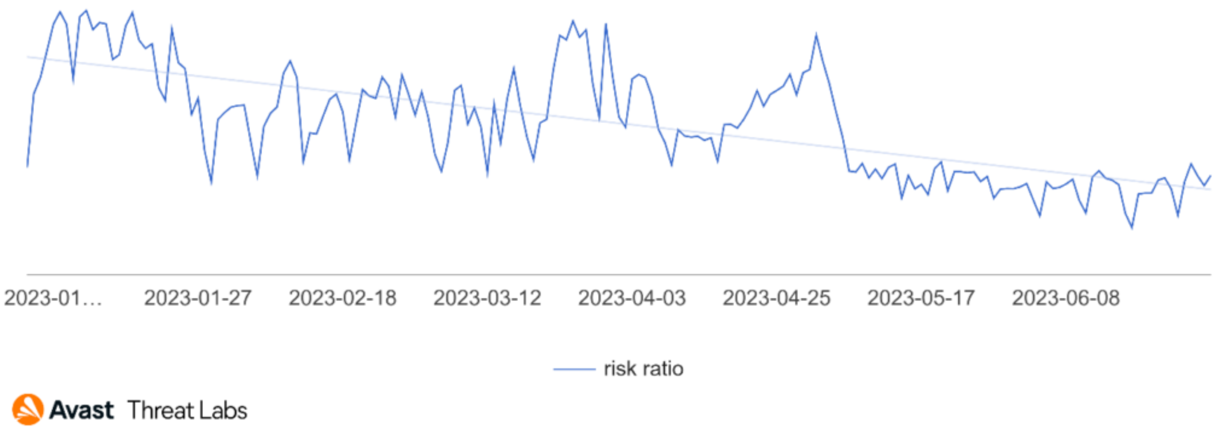
Confirm & Pay

Example of a dating scam blocked in Q2/2023

Tech Support Scams

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.*

Luckily, one scam type was not on a rise in Q2/2023 – the technical support scam (TSS). The graph below demonstrates a notable decrease in TSS activity during this period compared to Q1/2023. This decline began at the end of April.



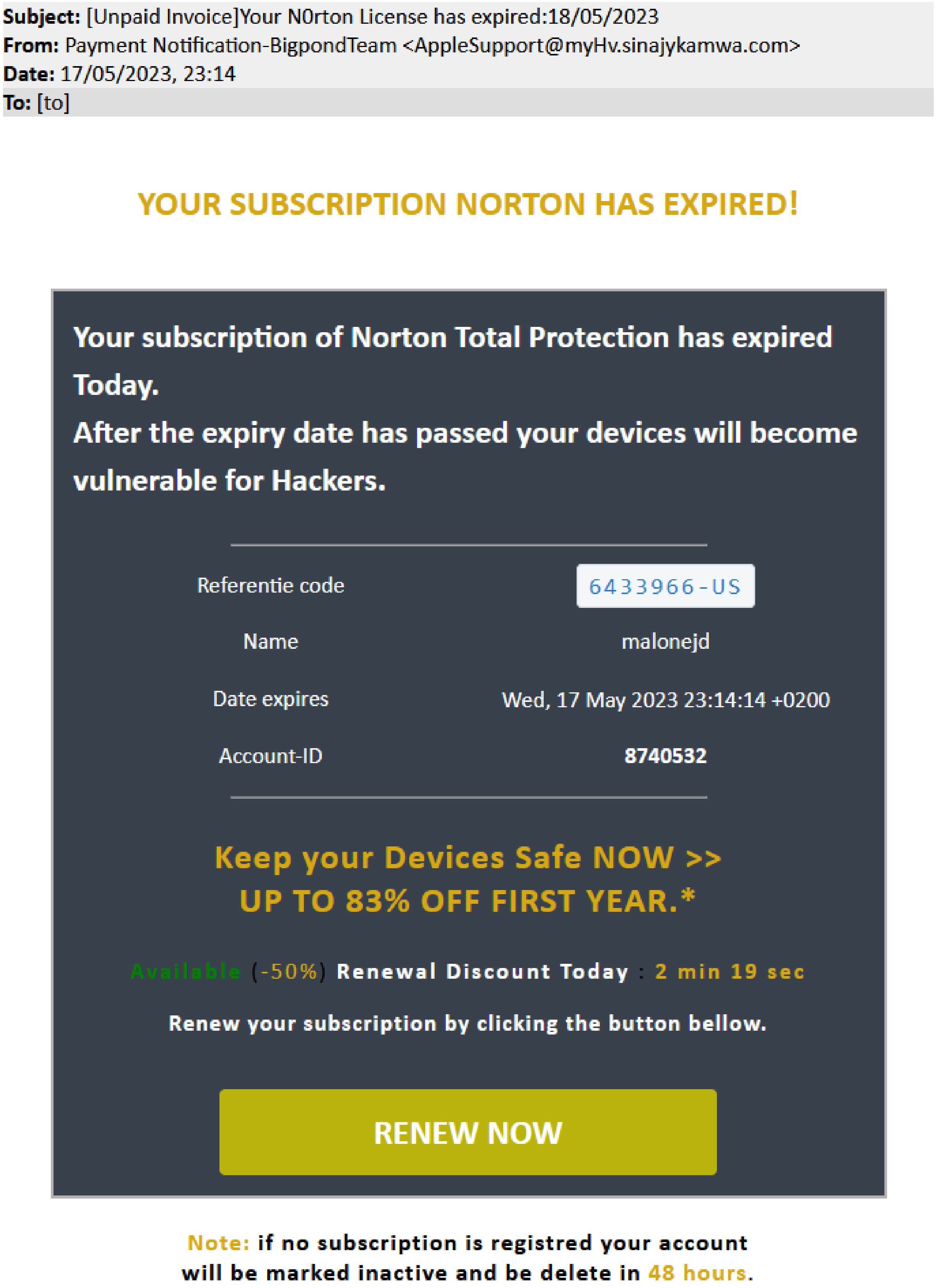
Technical support scams in Q1/2023-Q2/2023

Analyzing the data for Q2/2023, Japan emerges as the most active country with a TSS risk ratio of 3.63%, closely followed by Germany at 3.23%. The next top-performing countries are Canada with 2.60% and the USA with 2.51%, while Switzerland secures its place in the top five with a risk ratio of 2.18%.

Refund and Invoice Scams

Invoice scams involve fraudsters sending false bills or invoices for goods or services that were never ordered or received. Scammers rely on invoices looking legitimate, often using company logos or other branding to trick unsuspecting victims into making payments. These scams can be especially effective when targeted at businesses, as employees may assume that a colleague made the purchase or simply overlook the details of the invoice. It's important to carefully review all invoices and bills before making any payments and to verify the legitimacy of the sender if there are any suspicions of fraud.

In the digital world we live in, scam emails trying to trick us with fake invoices are becoming more common than ever. The people behind these scams are cunning – they play on our fears of forgetting to pay a bill, they use time pressure and talk about expired deadlines to make us panic, and they even tempt us with discounts to make the deal seem better. So, what's the best way to avoid falling into this trap? Keep the lines of communication open with your accounting department.



Subject: [Unpaid Invoice]Your N0rton License has expired:18/05/2023
From: Payment Notification-BigpondTeam <AppleSupport@myHv.sinajykamwa.com>
Date: 17/05/2023, 23:14
To: [to]

YOUR SUBSCRIPTION NORTON HAS EXPIRED!

Your subscription of Norton Total Protection has expired Today.
After the expiry date has passed your devices will become vulnerable for Hackers.

Referentie code	6433966-US
Name	malonejd
Date expires	Wed, 17 May 2023 23:14:14 +0200
Account-ID	**8740532**

Keep your Devices Safe NOW >>
UP TO 83% OFF FIRST YEAR.*

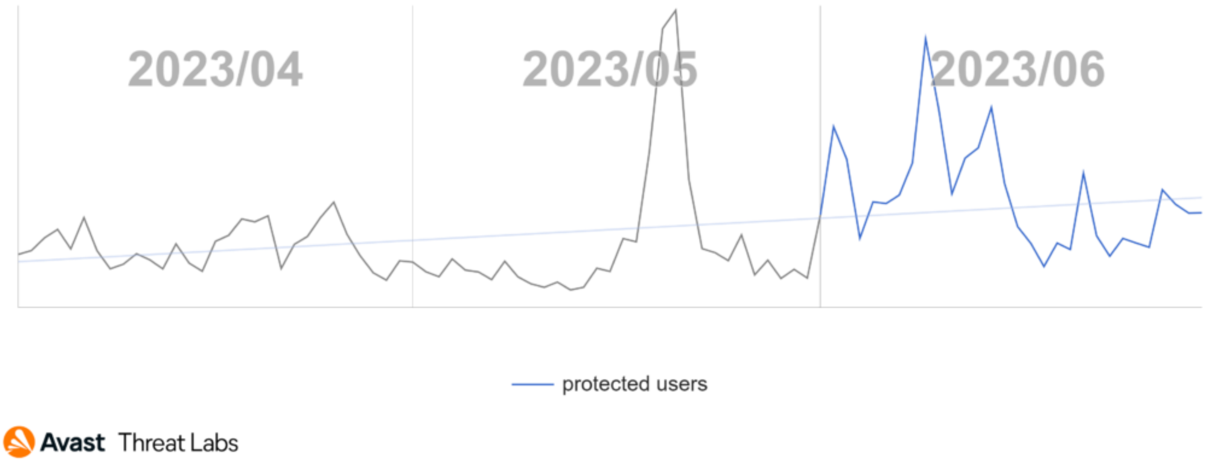
Available (-50%) **Renewal Discount Today** : **2 min 19 sec**

Renew your subscription by clicking the button bellow.

Note: if no subscription is registred your account will be marked inactive and be delete in 48 hours.

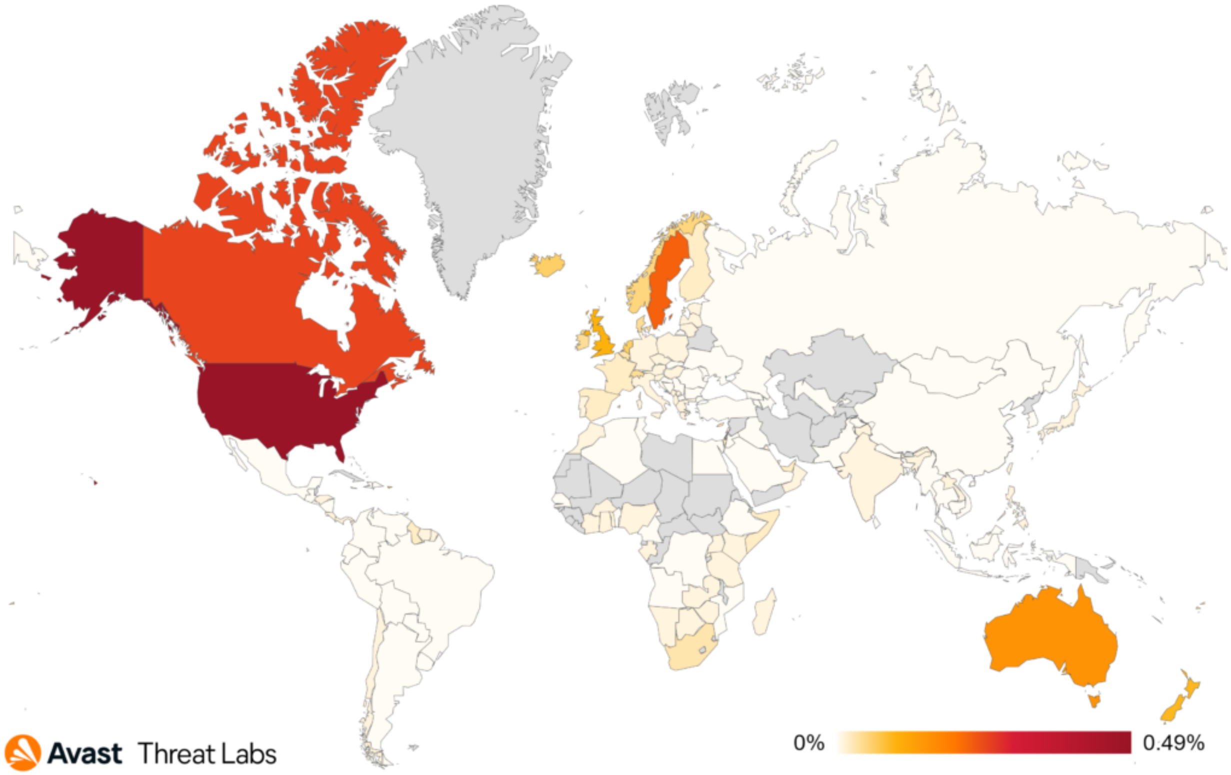
Example of an invoice scam – May 2023

Throughout Q2/2023, we observed a growing trend in the risk ratio of this threat type, with a notable peak in May.



Invoice Scams in Q2/2023

Looking at the map, we see that refund and invoice scams are mainly prevalent in the US and Australia, indicating a high level of activity in these regions. In contrast, Europe shows less activity.

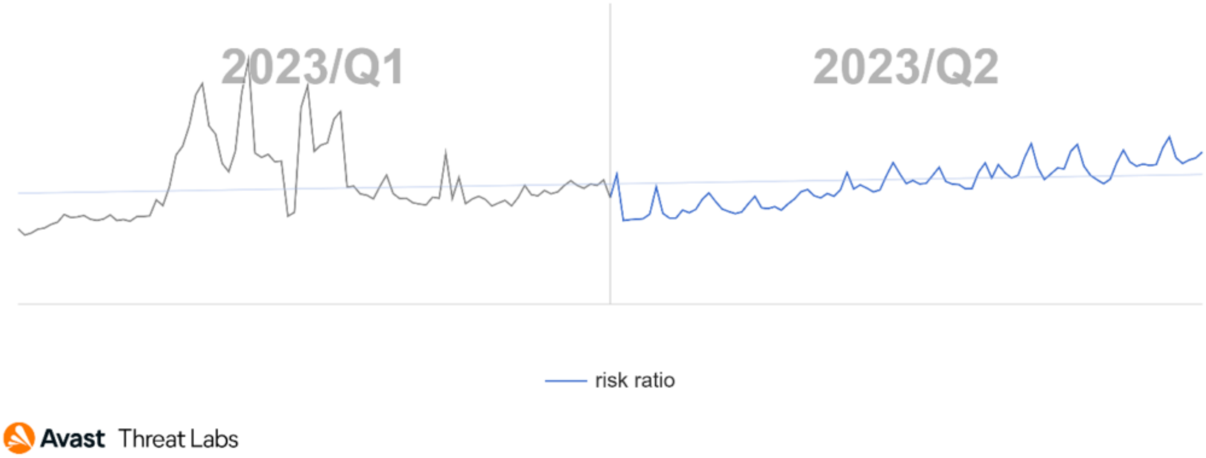


Global risk ratio for invoice scams in Q2/2023

Phishing

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 Q2/2023, we observed a more stable, growing, trend in phishing compared to the previous quarter, with no drastic fluctuations. However, it is evident that activity has started to pick up again after experiencing a minor dip in April; this indicates the potential for an upward trajectory in the coming months.



Phishing spreading in 2023

Cybercriminals continuously refine their tactics and find new ways to exploit users. Vigilance and awareness are crucial to staying protected in the ever-evolving threat landscape. The increase in phishing incidents and the prevalence of smishing attacks serve as a reminder for consumers to be cautious of and skeptical about unsolicited messages and requests for personal information.

Additionally, it's noting that Google's recent introduction of the ".zip" top-level domain (TLD) has led to an increase in domain registrations which can exploit strong similarities to a very popular archive file type. This development presents new challenges for organizations and cybersecurity professionals, emphasizing the need for continued vigilance and proactive cybersecurity measures.

In conclusion, while the current quarter shows relative stability, the ever-present threat of cyber-attacks necessitates ongoing diligence and preparedness in safeguarding our digital presence.

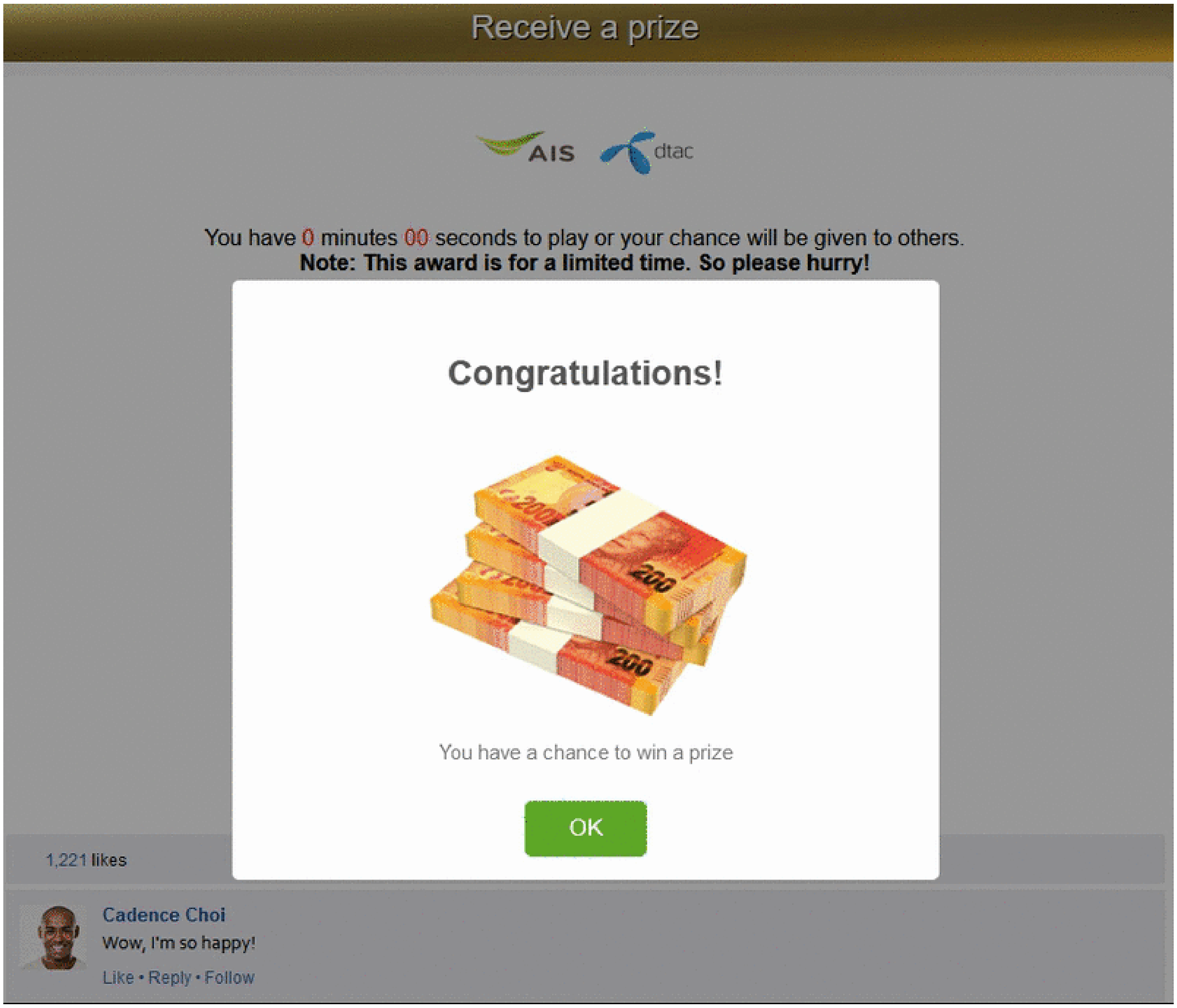
Web-based Adware

Web-based adware refers to malicious software or web pages that display unwanted advertisements in the form of pop-ups, banners, or redirects to third-party websites. Web-based adware can slow web browsing, potentially compromising user privacy and security.

During Q2/2023, web-based adware continued to be widespread, featuring several noteworthy examples. Throughout this period, three primary adware types emerged as dominant – we will introduce each within this section.

Fake Win

One of the most popular ad types are “winning pages” with various winning prices. Adware authors often misuse the names of well-known brands to lure their victims. The modus operandi is always similar: the user spins the virtual roulette or clicks on some wheel of fortune. The first attempt is always unsuccessful, and the next attempt informs users about the win. However, the condition for the payment of the prize is registration and entering personal data, often including credit card data. The appearance of credibility is added by a chat on the same page, which declares that the processing of the information worked as expected.



Receive a prize

You have 0 minutes 00 seconds to play or your chance will be given to others.
Note: This award is for a limited time. So please hurry!

Congratulations!

You have a chance to win a prize

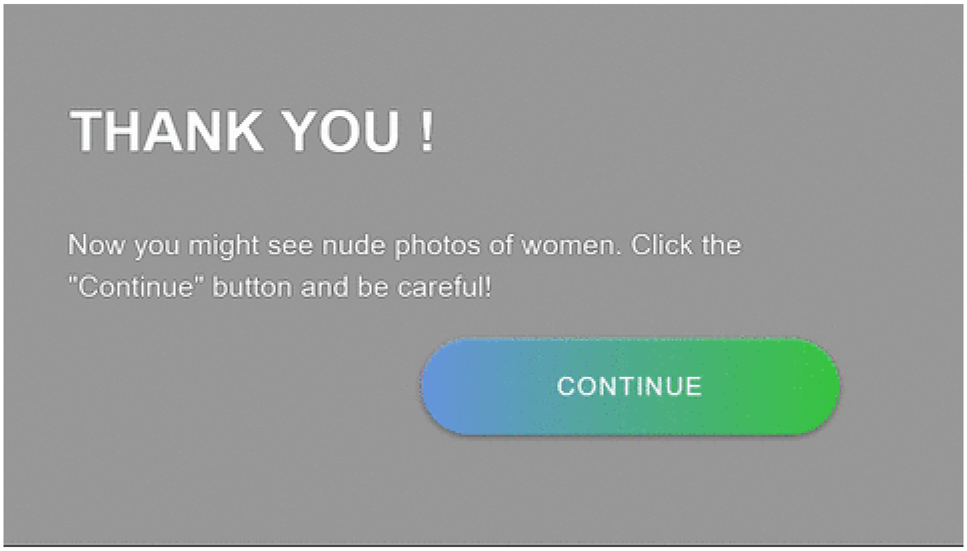
Cadence Choi
Wow, I'm so happy!

An example of a Fake win adware blocked by Avast in Q2/2023

Adult Content

One of the most significant forms of adware revolves around enticing users with adult content. Particularly prevalent within this category are adult chat rooms, which try to compel users to access an app or website where they can register and “enjoy flirting”. Victims ultimately end up on a website where most profiles are fake or even dangerous since attackers can use social engineering to extort money from users under the pretext of sending photos, paying travel expenses, etc.

As shown in the animation below, even if the user indicates they are below the required legal age, they are still redirected to a site with adult content, which is always suspicious.



THANK YOU !

Now you might see nude photos of women. Click the "Continue" button and be careful!

An example of an adult-content adware blocked by Avast in Q2/2023

Movies for "free"

Web-based adware also hides under the promise of watching popular movies for free. The animation below shows that a hunting page plays a few seconds of intro and then asks for a click and registration, which usually leads to a page with some adware.

An example of a Fake free movie adware blocked by Avast in Q2/2023

Alexej Savčin, Malware Analyst
Martin Chlumecký, Malware Researcher
Branislav Kramár, Malware Analyst
Matěj Krčma, Malware Analyst
Bohumír Fajt, Malware Analysis Team Lead
Jakub Křoustek, Malware Research Director

Mobile-Related Threats

This quarter, we have witnessed several interesting developments in the mobile threat ecosystem. Notably, a spyware kit has surfaced on GitHub, adding to a series of spyware kits that have become publicly accessible in recent months. Furthermore, there are indications of another spyware being utilized for state surveillance, boasting extensive access to victims' personal information.

In an interesting incident, a seemingly benign screen recorder in the Play Store turned malicious after an update delivered a spyware RAT. This technique of delayed malware delivery through updates was also used to drop banker malware under the guise of an AI text reader update.

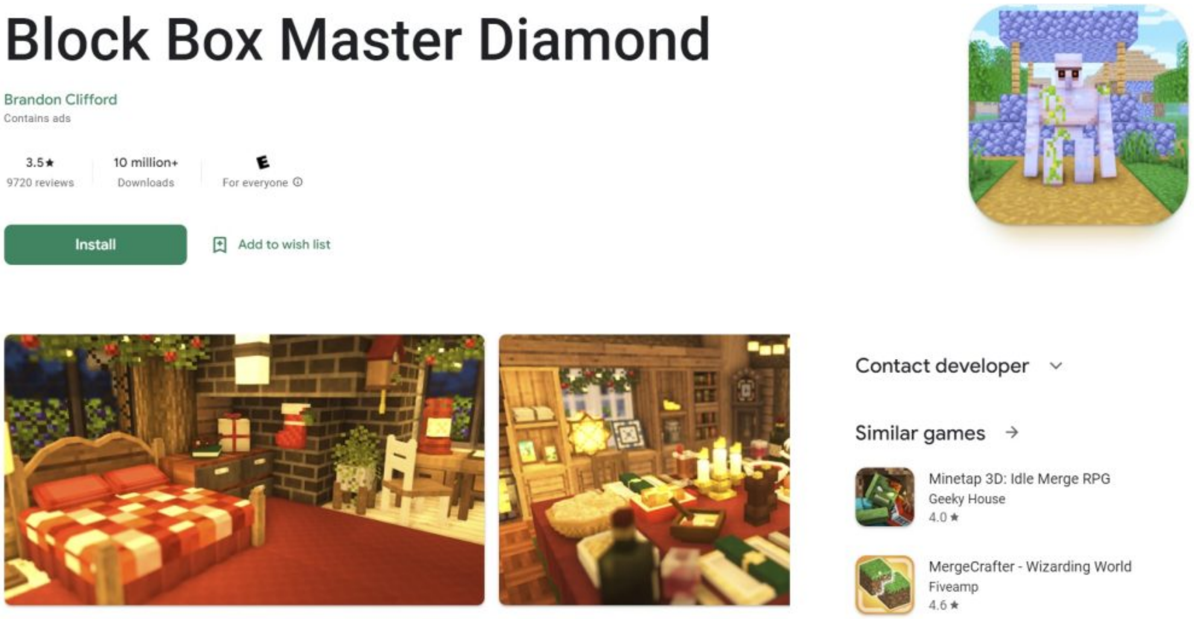
Finally, we observed a worrying trend of mobile loan applications with intrusive permissions using personal information to blackmail victims.

Adware at the top again

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

Mobile users had to contend with adware as the most prevalent threat in Q2/2023. Adware serves intrusive advertisements to the devices of its victims, raking in fraudulent advertising revenue. Hiding its presence is a core component in maintaining its ability to generate this revenue, hence adware generally hides its icon or otherwise masquerades itself.

HiddenAds were the main strain of adware targeting users this quarter, closely followed by MobiDash and FakeAdBlockers. MobiDash continued its climb in popularity from last quarter with a 19% increase in targeted users, surpassing FakeAdBlockers which are down by 66%. All three strains have a similar modus operandi: displaying out-of-context full screen adverts to their victims while hiding their presence on the device. These are generally delivered through third-party app stores, pop-up messages on less reputable sites and malicious advertisements. Once installed, it may prove difficult to uninstall the apps due to their stealthy features.



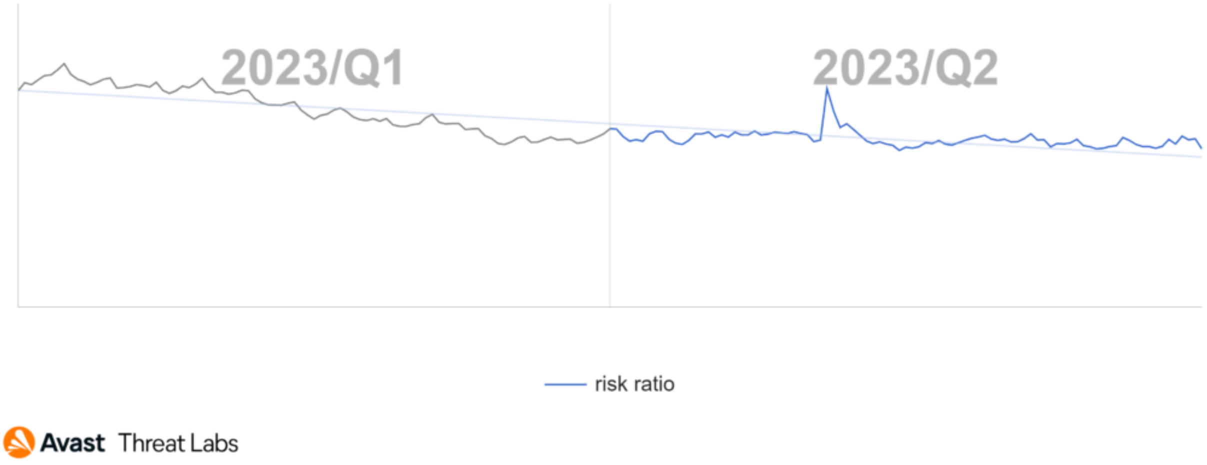
Block Box Master Diamond

Brandon Clifford
Contains ads

A repacked HiddenAds Minecraft clone app as seen on Play Store prior to its removal

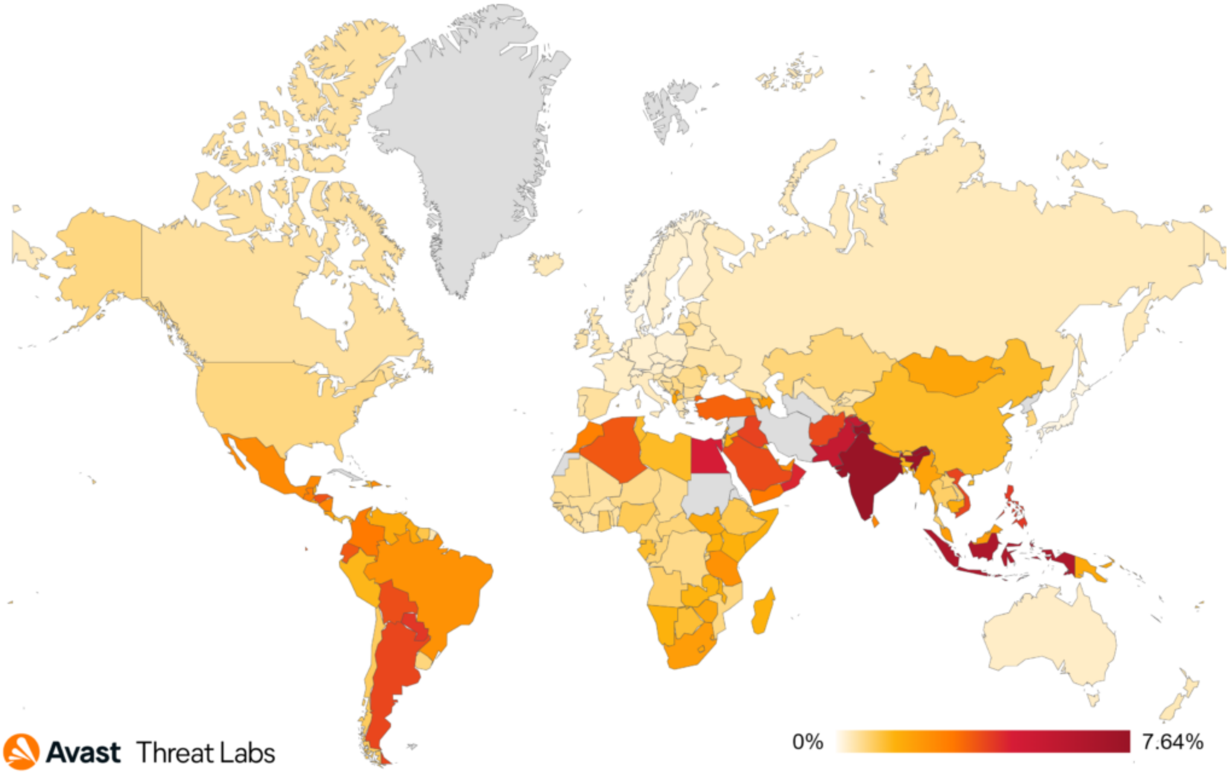
Of note is another HiddenAds campaign discovered on the Play Store that garnered tens of millions of downloads during its reign. This strain focused on abusing advertising SDKs to fake displaying adverts to users to gather revenue. Victims were able to play the Minecraft clone game while these malicious actions were going on in the background, without their knowledge.

Threat actors continue to find new ways to sneak HiddenAds onto the Play Store, either through further obfuscation of malicious features or introducing said features in later updates.



Global risk ratio of mobile adware in Q1/2023-Q2/2023

We see a decrease in adware targeted users compared to last quarter, which can likely be attributed to the sharp fall in FakeAdBlocker hits. This is balanced by the new HiddenAds campaign that snuck onto the Play Store this quarter.



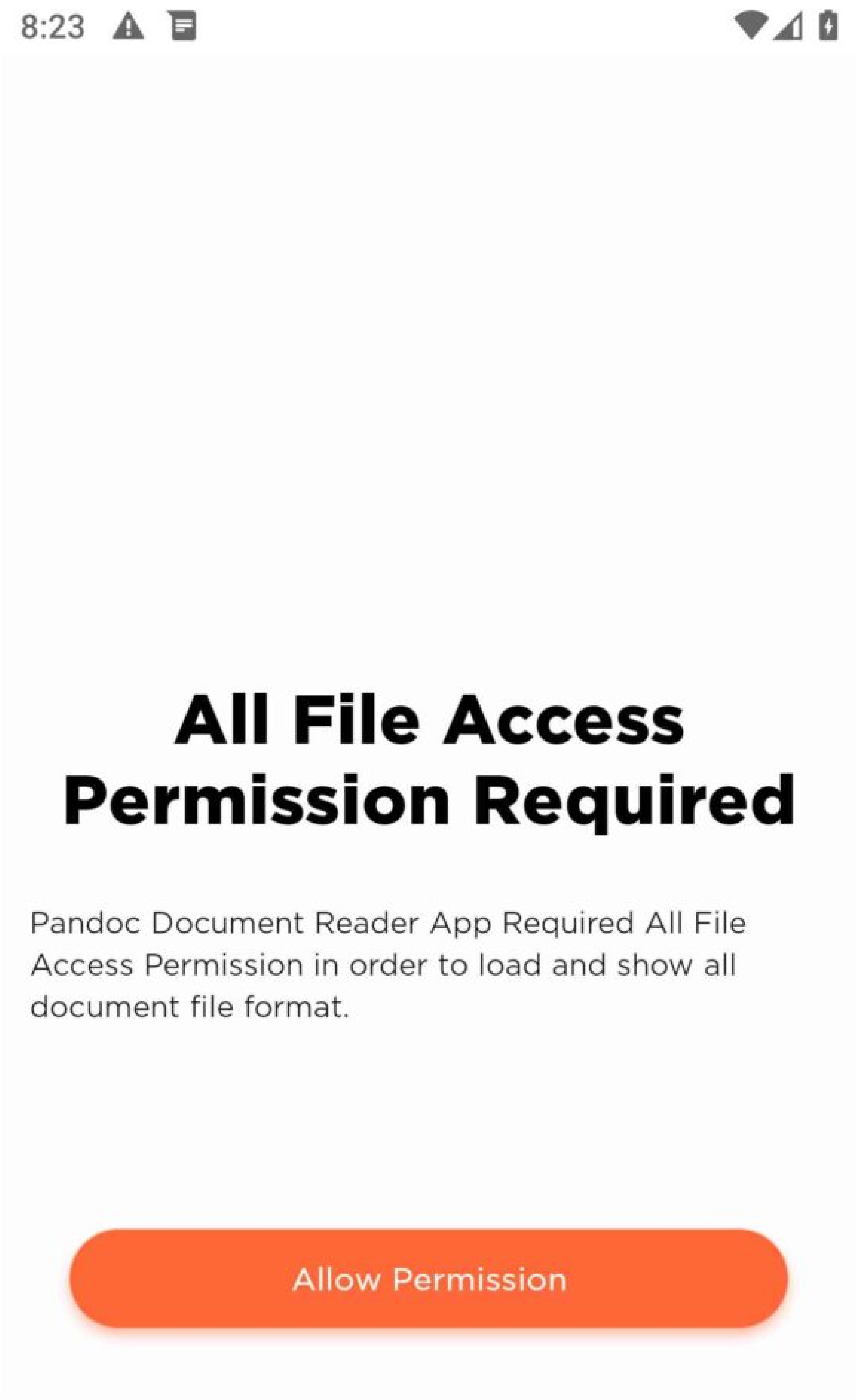
Global risk ratio for mobile adware in Q2/2023

Brazil, India and Argentina keep their top spots this quarter with the most affected users. This remains unchanged despite the decrease in overall users affected by adware and Brazil having 26% less affected users in Q2/2023. India, Indonesia and Pakistan have the highest risk ratio, meaning users are most likely to encounter adware in these countries.

New Banker strains added to the fray

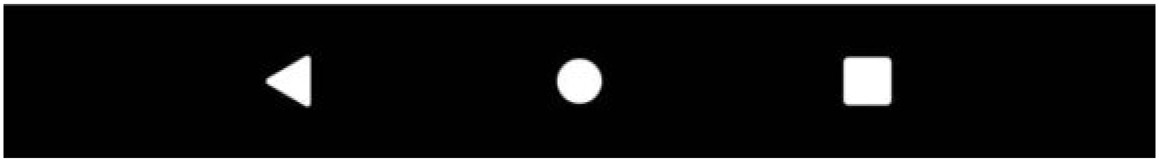
Bankers are a sophisticated type of mobile malware that targets banking details, cryptocurrency wallets, and instant payments with the intent of extracting money. Generally distributed through phishing messages or fake websites, Bankers can take over a victim's device by abusing the accessibility service.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

This quarter brings with it continuations of established banker strains as well as some new strains that make use of established techniques with a few twists. A continuing trend, the overall prevalence of bankers is on the decline as observed over the last few quarters, even with new strains popping up every quarter. Cerberus/Alien maintains its top spot in our telemetry despite losing a significant 50% of its prevalence. Coper has moved up to 2nd place surpassing Hydra, another banker strain that lost over 50% of its victim base.



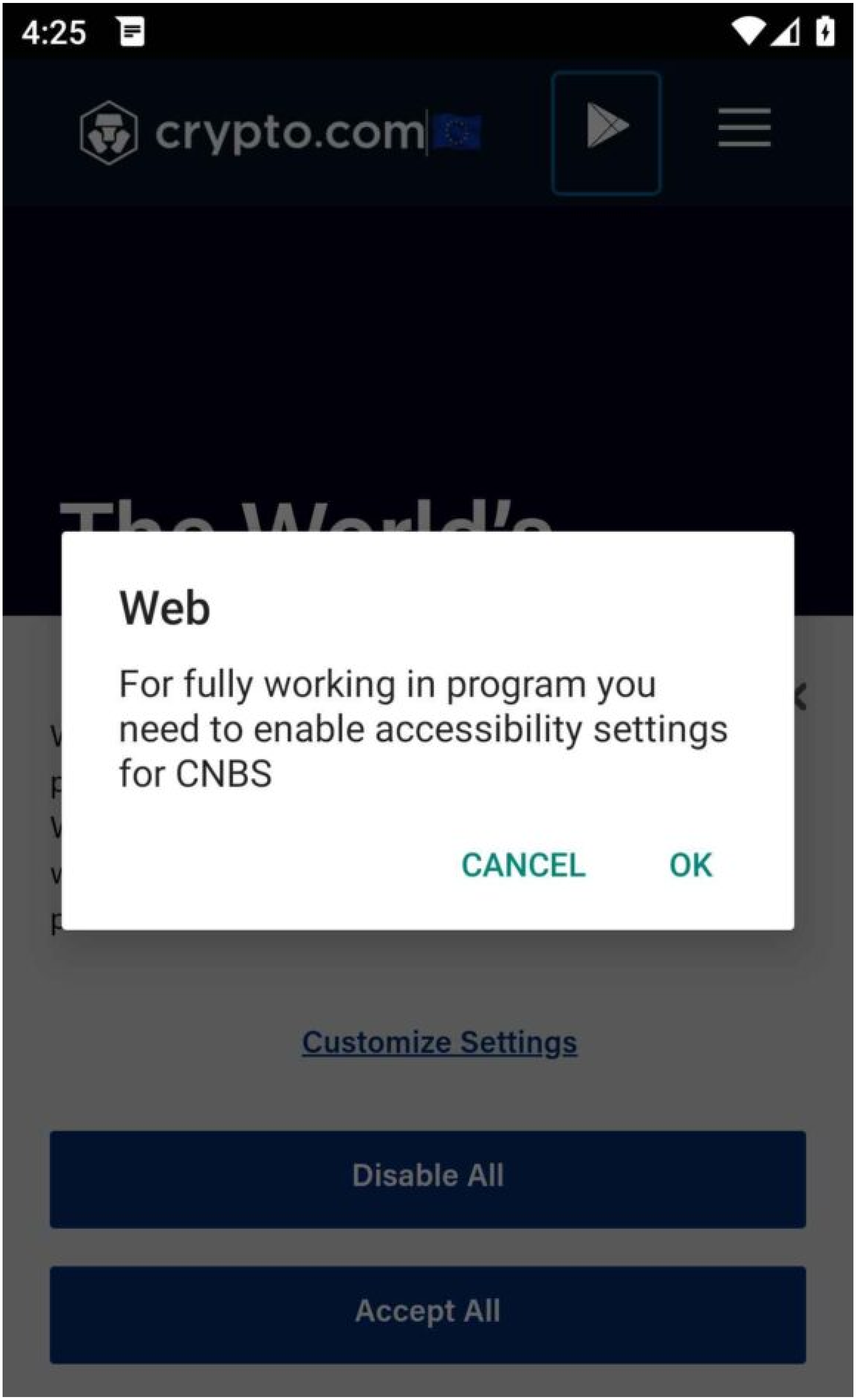
All File Access Permission Required

Pandoc Document Reader App Required All File Access Permission in order to load and show all document file format.



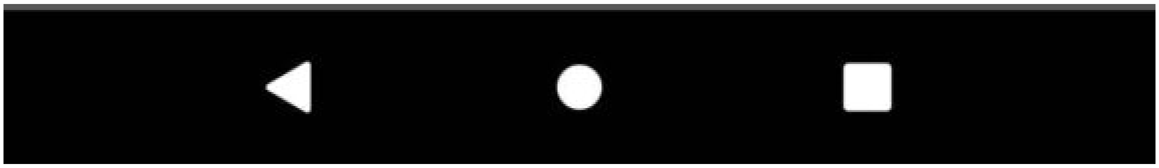
Fake PDF editor app requesting file access permission, preparing the stage for the Anatsa banker delivery

Of note is a new dropper campaign on the Play Store which delivered the Anatsa banker. The US, UK, Germany and other European countries were the main targets of fake PDF reader applications that were used as droppers over the course of a few months. Initially benign, these apps were later updated to activate malicious components that delivered the banker in the form of an AI text reader ‘update’. With the ability to target and exfiltrate login information from over 600 financial institution apps, Anatsa also features full device takeover that allows it to perform transactions on behalf of the victim.



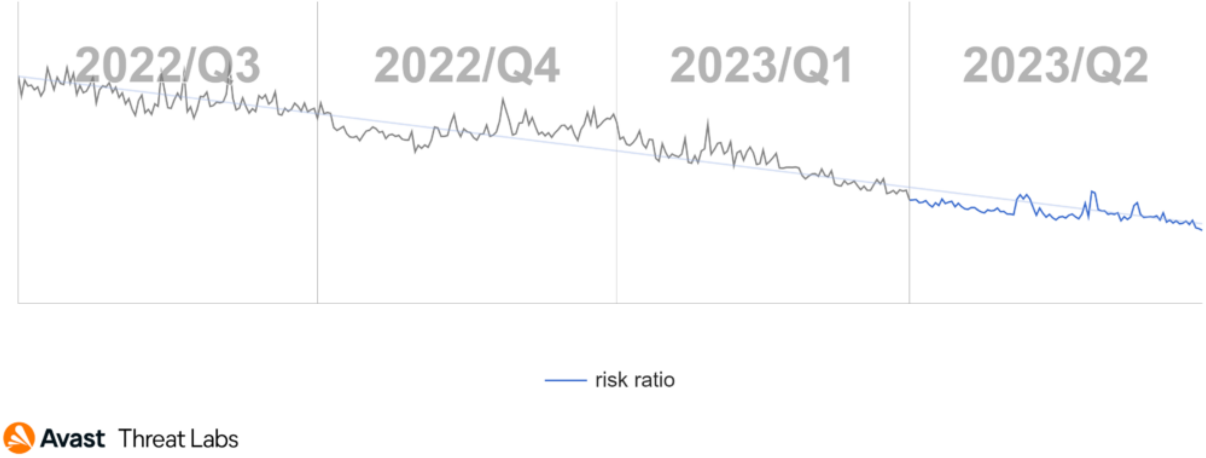
Web

For fully working in program you need to enable accessibility settings for CNBS



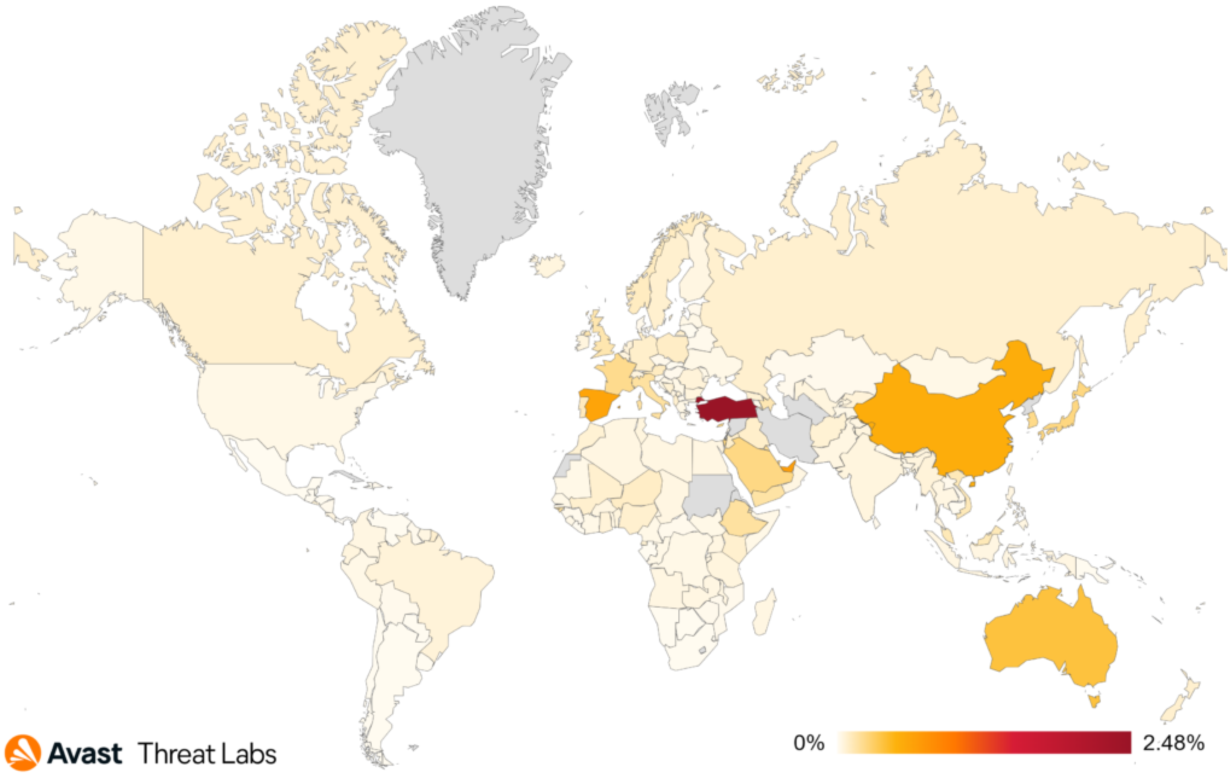
Chameleon banker masquerading as the Crypto.com app requesting Accessibility permissions to initiate its malicious activity

Another recent addition to the banker ecosphere is the Chameleon banker. Distributed through compromised websites and Discord servers, it appears to mainly target Poland and Australia. Disguised as ChatGPT, Bitcoin and Chrome among others, it uses keylogging and phishing HTML injection to steal credentials from its victims. Interestingly, it also features the ability to exfiltrate cookies when a victim attempts to access the popular Coinbase crypto exchange website, likely attempting to hijack the session to perform transactions on the victim’s behalf. Finally, the banker can detect uninstallation efforts by the victim and deletes itself if it anticipates the user getting suspicious about the banker app.



Global risk ratio of mobile bankers in Q3/2022-Q2/2023

We continue to observe a steady decline in the banker risk ratio in our telemetry for the last few quarters. This is despite new strains appearing in the banker ecosphere. It is likely that threat actors behind bankers are more focused on specific countries with more elaborate methods of banker delivery as well as tailored fake bank login pages.



Global risk ratio for mobile bankers in Q2/2023

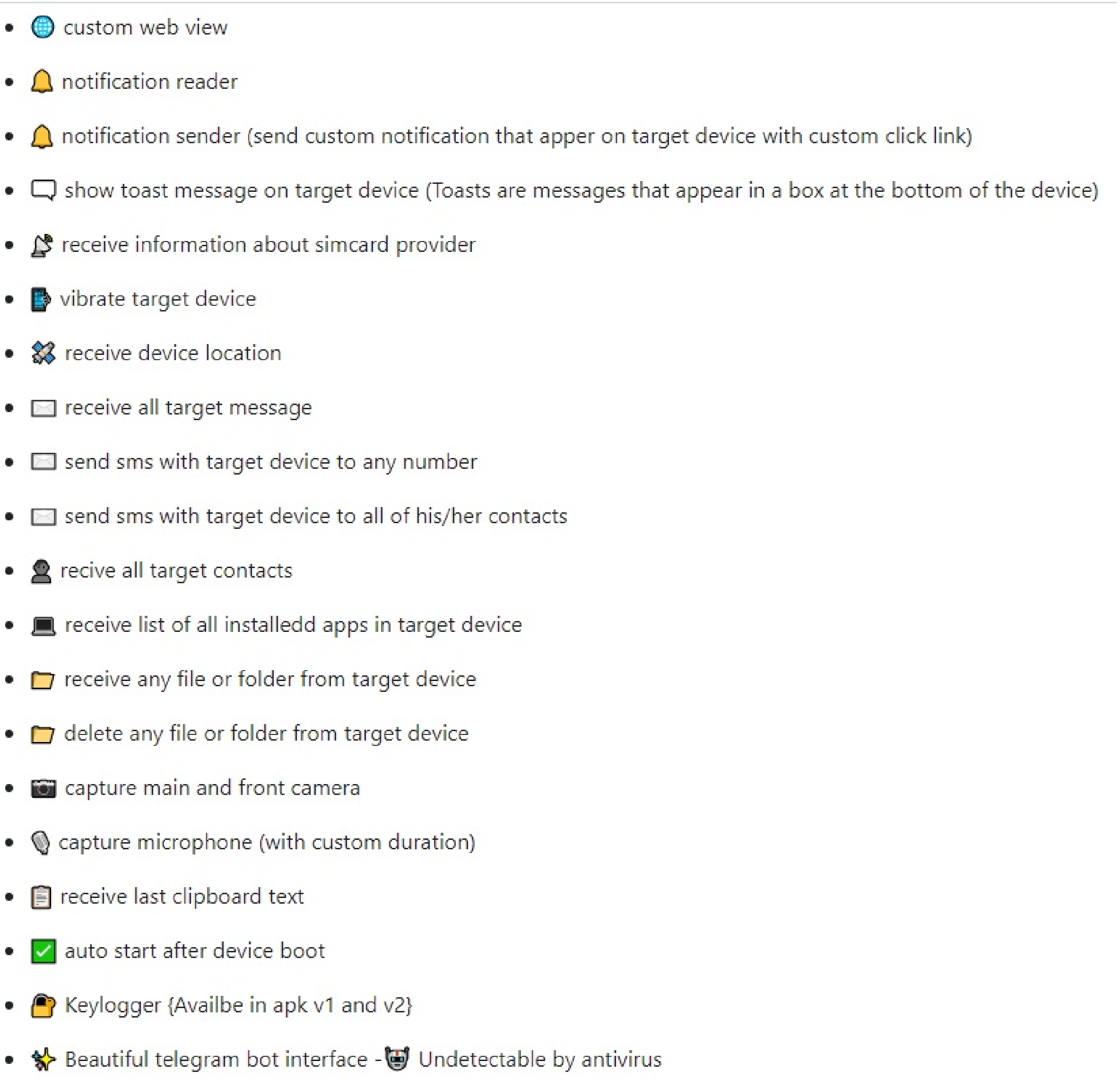
Turkey holds its top place from last quarter with the most protected users and highest risk ratio while Spain, France, Brazil and Italy follow closely behind. We do observe a focus on EU countries and Australia through the newly discovered strains in the past few quarters.

Spyware evolution & SpyLoans

Spyware is used to spy on 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 becoming more prevalent and is used to target individuals with 0-day exploits.

This quarter has witnessed a notable surge in the prevalence of spyware, with Spymax once again taking the lead. The landscape is further enriched by several new additions, including BouldSpy, which potentially has affiliations with state surveillance, an SDK titled SpinOK that features potential spyware functionalities, and DogeRAT, a spyware kit made accessible on GitHub.

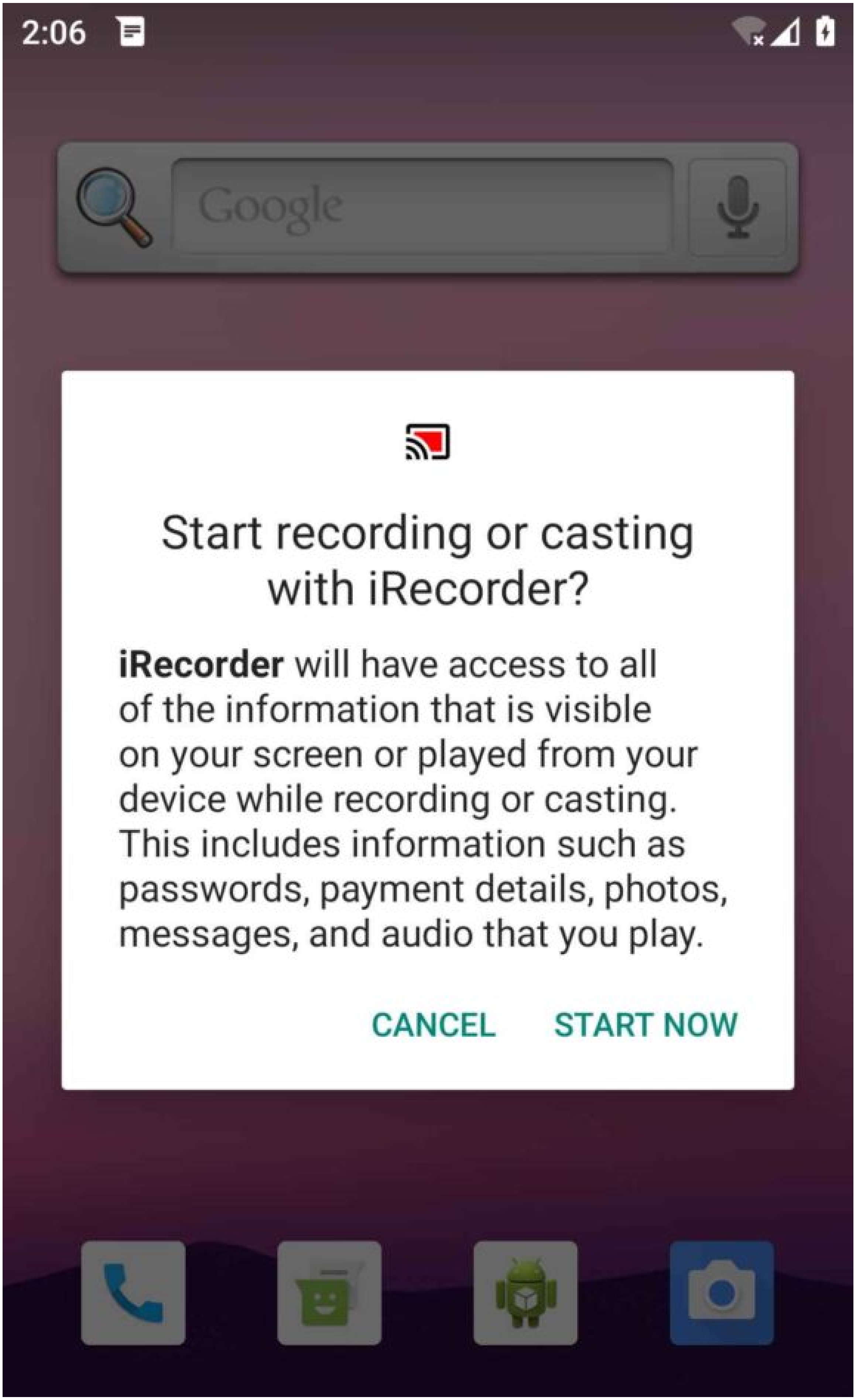
Alongside these new entries we observe an increased prevalence in SpyLoans, loan applications that extract personal information with intent to blackmail victims for money.



- 🌐 custom web view
- 🔔 notification reader
- 🔔 notification sender (send custom notification that apper on target device with custom click link)
- 🗨 show toast message on target device (Toasts are messages that appear in a box at the bottom of the device)
- 📡 receive information about simcard provider
- 📳 vibrate target device
- 🛰 receive device location
- ✉ receive all target message
- ✉ send sms with target device to any number
- ✉ send sms with target device to all of his/her contacts
- 👤 recive all target contacts
- 💻 receive list of all installedd apps in target device
- 📁 receive any file or folder from target device
- 📁 delete any file or folder from target device
- 📷 capture main and front camera
- 🎤 capture microphone (with custom duration)
- 📋 receive last clipboard text
- ✅ auto start after device boot
- 🔓 Keylogger {Availbe in apk v1 and v2}
- ✨ Beautiful telegram bot interface - 🤖 Undetectable by antivirus

DogeRAT's promised features listed on its GitHub page

Spymax remains the top spyware despite a slight decrease in its risk ratio this quarter. It continues to be used to extract personal information such as SMS messages, contact lists, location and more. DogeRAT, a spyware kit available on GitHub, appears to have taken inspiration from Spymax as we note similarities in its code and functionality. A novel addition is the employment of a Telegram panel for spyware control and execution of various functions, notably encompassing microphone and camera capture. Dissemination occurs through SMS messages guiding users to download the application.



Start recording or casting with iRecorder?

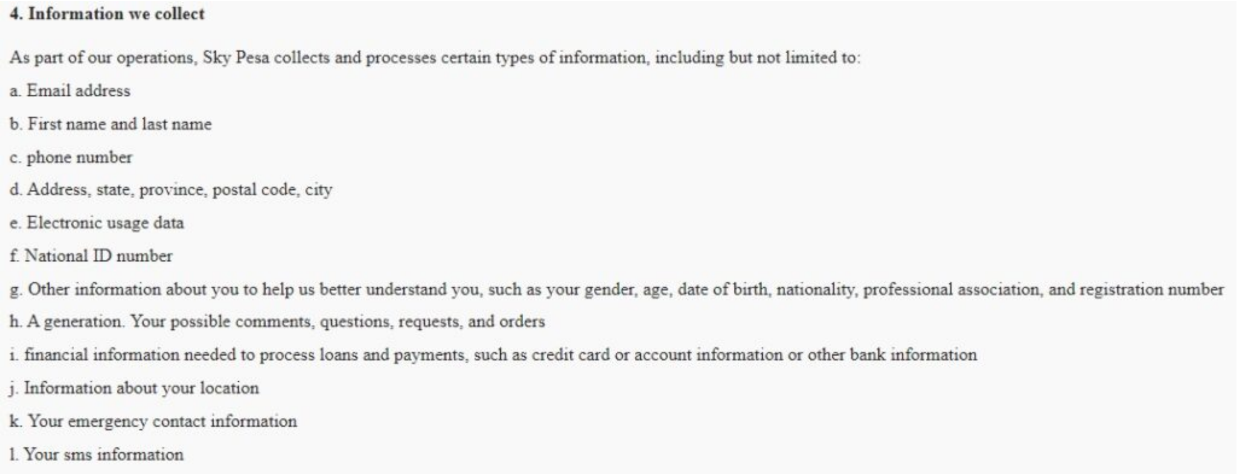
iRecorder will have access to all of the information that is visible on your screen or played from your device while recording or casting. This includes information such as passwords, payment details, photos, messages, and audio that you play.

A benign request that can be mis-used by AhRAT with a later malicious update

Spyware managed to sneak onto the Play Store this quarter when a screen recorder app turned malicious with a delayed update bringing AhRAT spyware with it. A tactic observed several times in recent years, users who installed the previously clean version of the app would automatically update to the malicious version without their knowledge. AhRAT's C2 communication indicates it should be able to perform a variety of spying functions such as SMS extraction, location tracking, screen recording and others. However, it appears that it was only capable of extracting files from the device and recording with the device microphone. We speculate that future versions may have introduced further features, but the app was detected and removed from the Play Store before that could happen.

Another Play Store campaign of note is the SpinOK spyware capable SDK that was present in highly prevalent applications. This spyware can gather file lists, telemetry from device data sensors and in some cases copy the clipboard contents and exfiltrate these to a remote server. Some applications were removed from the Play Store while others were allowed to stay after they removed the spyware SDK.

An interesting strain called BouldSpy was discovered by Lookout, with possible links to Iranian state police. Labelled as a possible botnet, it also contains CryCrypt ransomware capability, although it appears this remains unused, potentially saved for future use. Often masking as the official Android phone app, it can record voice calls from popular messenger applications such as WhatsApp, Viber and others. It uses the Accessibility service to hide its presence and masquerade as an official app, even mimicking its look and functionality. Meanwhile, it extracts SMS messages, browser history, photos and more in the background.



4. Information we collect

As part of our operations, Sky Pesa collects and processes certain types of information, including but not limited to:

a. Email address

b. First name and last name

c. phone number

d. Address, state, province, postal code, city

e. Electronic usage data

f. National ID number

g. Other information about you to help us better understand you, such as your gender, age, date of birth, nationality, professional association, and registration number

h. A generation. Your possible comments, questions, requests, and orders

i. financial information needed to process loans and payments, such as credit card or account information or other bank information

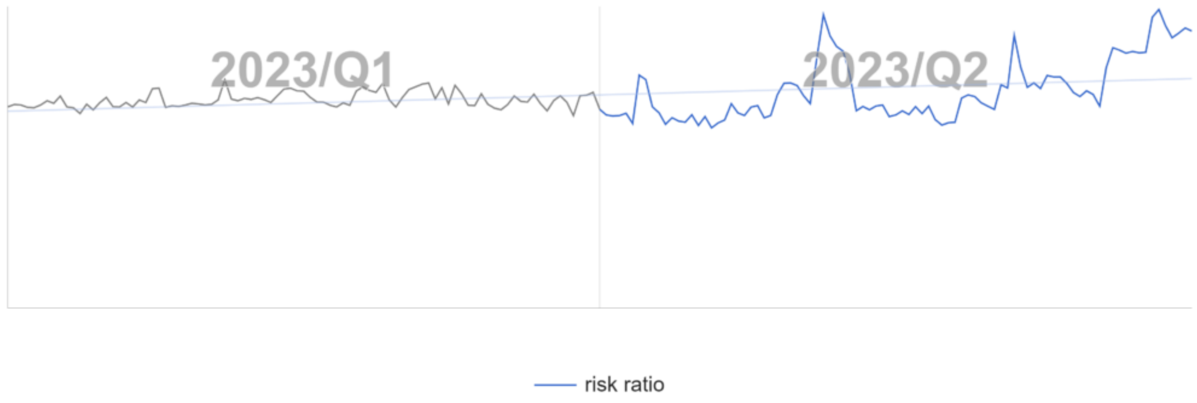
j. Information about your location

k. Your emergency contact information

l. Your sms information

Invasive information collection under the guise of enabling loan processing as often stated in ToS of spy loan applications

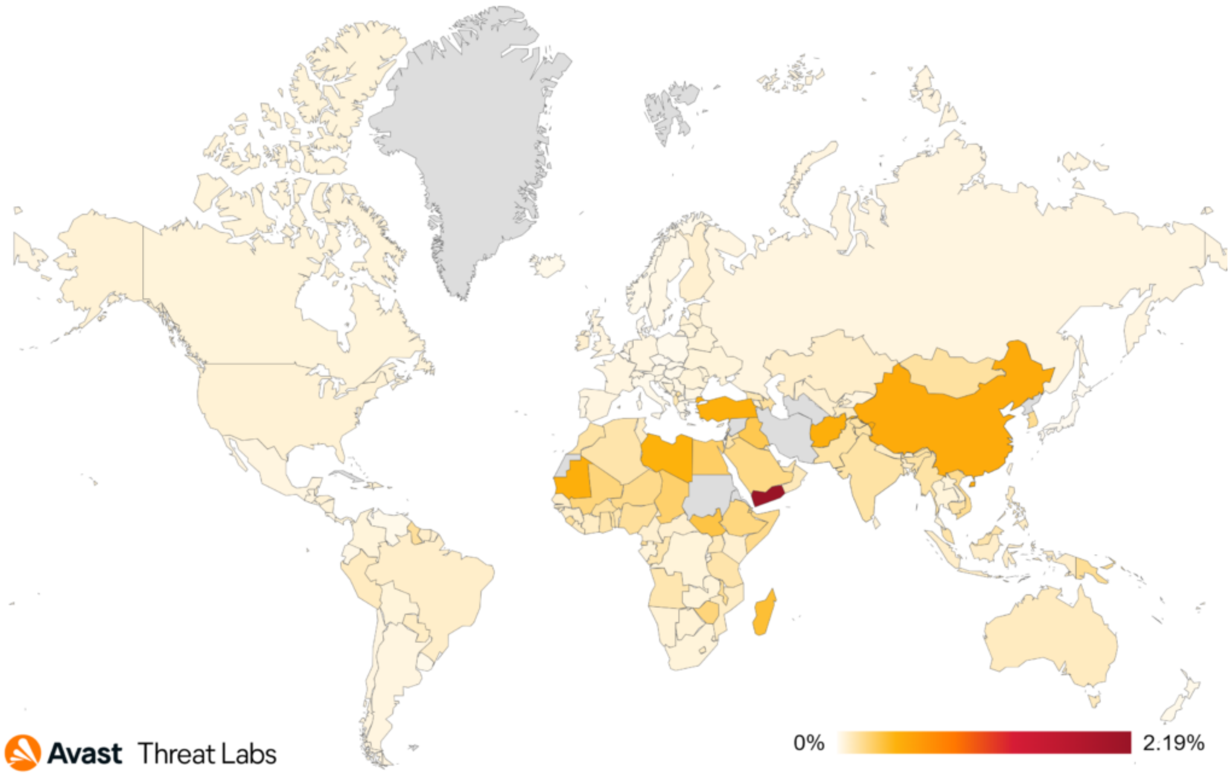
A worrying trend that has been ongoing for several quarters now is the prevalence of loan applications that promise fast cash distributed through the Play Store. Previously reported on by Zimperium, these loan applications request invasive permissions under the guise of a credit check or loan security. Once the user allows these permissions, the spy loan apps extract sensitive information such as messages, contact lists, photos or browsing history. These are then used to blackmail victims, oftentimes even if they pay the agreed loan repayments. Unfortunately, this trend is gaining popularity with blackmail loan apps appearing to focus on regions with limited bank loan access such as South America or Asia. Users are advised to avoid mobile loan applications that are not from a trusted financial institution.



Avast Threat Labs

Global risk ratio of mobile spyware in Q1/2023 and Q2/2023

We see a slight uptick in the risk ratio of spyware this quarter, likely attributable to the high number of new strains entering the market. Freely available strains on GitHub such as DogeRAT can also contribute to the increased spread of spyware.



Global risk ratio for mobile spyware in Q2/2023

Brazil has the highest number of protected users, followed by India, Turkey and the US. Users in Yemen continue to be at higher risk of encountering mobile malware when compared to the rest of the world.

Jakub Vávra, Malware Analyst

Acknowledgements / Credits

Malware researchers

Adolf Středa
Alexej Savčin
Bohumír Fajt
Branislav Kramár
David Álvarez
Igor Morgenstern
Jakub Křoustek
Jakub Vávra
Jan Rubín
Jan Vojtěšek
Ladislav Zezula
Luigino Camastra
Luis Corrons
Martin Chlumecký

Matěj Krčma
Michal Salát
Ondřej Mokoš

Data analysts

Pavol Plaskoň
Filip Husák
Lukáš Zobal

Communications

Brittany Posey
Emma McGowan
Marina Ziegler

Tagged asdesktop, malware, mobile, report, risk, threats
Share:XFacebook