Trend Research

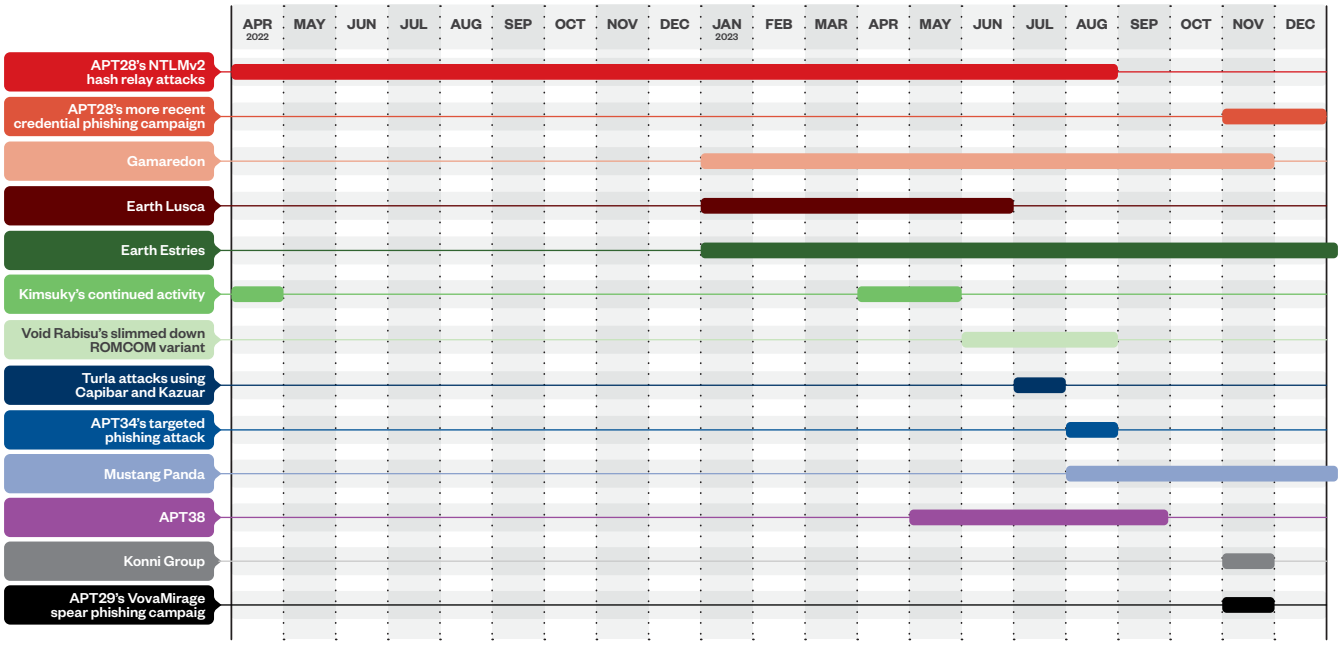
TREND MICRO

CALIBRATING EXPANSION

2023 ANNUAL CYBERSECURITY REPORT


03
APT CAMPAIGNS
07
RANSOMWARE THREATS
13
CLOUD AND ENTERPRISE THREATS
16
MITRE ATT&CK DETECTIONS
20
THREAT LANDSCAPE

APT CAMPAIGNS



APT28's NTLMv2 hash relay attacks

April 2022 – August 2023

- Targets:
  - Organizations involved in a wide range of fields, but primarily in foreign affairs, energy, defense, and transportation
- Possibly an attempt to brute-force its way into target networks
- Exploited CVE-2023-23397 that was patched in March 2023, at which point APT28 used more elaborate methods that involved scripts hosted on Mockbin sent to targets

APT28's more recent credential phishing campaign

November – December 2023

- Targets:
  - Various government organizations in Europe
- Shares similarities to the earlier hash relay campaign in technical indicators, such as sharing the same computer name used to send out spear-phishing emails and to craft LNK files.

Gamaredon

January – November 2023

- Targets:
  - Government organizations in Ukraine
- Gamaredon continues its activity with attacks using Remote Template Injection and self-extracting executable files
- The timeline of increased activity of the investigated sample suggests the campaign was launched to intensify espionage activities

Earth Estries

January 2023 – present

- Targets:
  - Government organizations and technology industries in the Philippines, Taiwan, Malaysia, South Africa, Germany, and the USA.
- They use multiple backdoors and hacking tools, as well as PowerShell downgrade attacks to avoid detection
- They use public services such as Github, Gmail, AnonFiles, and File.io to exhance and transfer commands and stolen data
- Earth Estries is known to deploy cyberespionage campaigns.

Earth Lusca

January – June 2023

- Targets:
  - Government departments involved in foreign affairs, technology, and telecommunications in countries in Southeast Asia, Central Asia, and the Balkans, with scattered attacks on Latin American and African countries
- The decrypted payload is a Linux-targeted backdoor, a new variant named SprySOCKS
- Targets the public-facing servers of its victims

Kimsuky's continued activity

April 2022, and April – May 2023

- Targets:
  - Individuals working in fields related to the Democratic People's Republic of Korea
  - Possibly organizations related to military, diplomacy, and unifications, and Korean-language support groups, based on Kimsuky's previous campaign history
- Delivered as an email file
- Likely aimed to gather information on geopolitical events, diplomatic strategies, and activities impacting the target's interests
- Could also be launched to gather armament-related information and for cryptocurrency-related attacks

Void Rabisu's slimmed down ROMCOM variant

June – August 2023

- Targets:
  - Military personnel and political leaders in Europe
- Exploited the then zero-day vulnerability CVE-2023-36884
- Primarily known for cyberespionage activities targeting governments and military with financial motivations

APT34's targeted phishing attack

August 2023

- Targets:
  - Possibly organizations inside the Kingdom of Saudi Arabia
- The malicious document in the phishing scam dropped a new malware designed for espionage, capable of identifyiung the machine, reading and uploading files from the machine, and downloading another file or malware.
- APT34 is known for its cyberespionage activities targeting government agencies, organizations involved in critical infrastructure, and telecommunications in the Middle East.

Turla attacks using Capibar and Kazuar

July 2023

- Targets:
  - Diplomatic and military organizations in Ukraine
- In this phishing campaign, the Capibar malware was used for intelligence gathering, while the Kazuar malware was used for credential theft.
- Turla has been active since 2014, and is known for its cyberespionage activities.

Mustang Panda

August 2023 – present

- Targets:
  - Government organizations in the Philippines, and other related organizations
- Utilized components of legitimate software commonly used in Southeast Asia for DLL sideloading
- Possibly launched for information gathering purposes
- Samples contain strings that suggest the possibility of attacking Myanmar government officials

APT38

May – September 2023

Targets:
- Cryptocurrency-related organization, investment firms, and banks

Detected in a sample used by BlueNoroff, which is associated with APT38. The sample was later reported by SentinelOne as used in the later stages of SwiftLoader and indicated in a connection between KandyKorn and SwiftLoader

Likely financially motivated and launched to acquire foreign currency to fund armaments and espionage

Konni Group

November 2023

Targets:
- Companies within the Republic of Korea

Associated with OSMIUM, Opal Sleet, SectorA07, TA406, and Kimsuky

According to our analysis, the campaign's malicious zip file contains an LNK file, that when executed drops html and VBScript to fetch additional payloads, possibly pointing to APT37.

Possibly launched as additional means of acquiring foreign currency

APT29's VovaMirage spear phishing campaign

November 2023

Targets:
- Embassies and diplomatic entities in European countries, particularly Azerbaijan, Greece, Romania, and Italy

Exploited WinRAR vulnerability CVE-2023-38831 in a spear phishing campaign

Likely launched to gather information on strategic activities involving the respective country targets

RANSOMWARE THREATS

What to Watch Out For

The following tactics were observed in 2023 and could possibly be seen in the coming year as ransomware activities grow more sophisticated.

There is a continued increase in the use of remote encryption

- Observed in Akira, BlackCat, BlackMatter, LockBit, and Royal
- Attackers actively map drives to encrypt on the affected endpoint instead of doing lateral movement. This could be a leap in tactics to reduce their footprint in attacks to avoid detection.

Ransomware groups are also maximizing the convenience of intermittent encryption

- Observed in NoEscape, Ransomware Play, BlackBasta, Agenda, and BlackCat
- Attackers encrypt chunks of data instead of encrypting all data in one go; this process speeds up encryption while still rendering the affected data useless to the victim, and also makes for a more complicated decryption process.

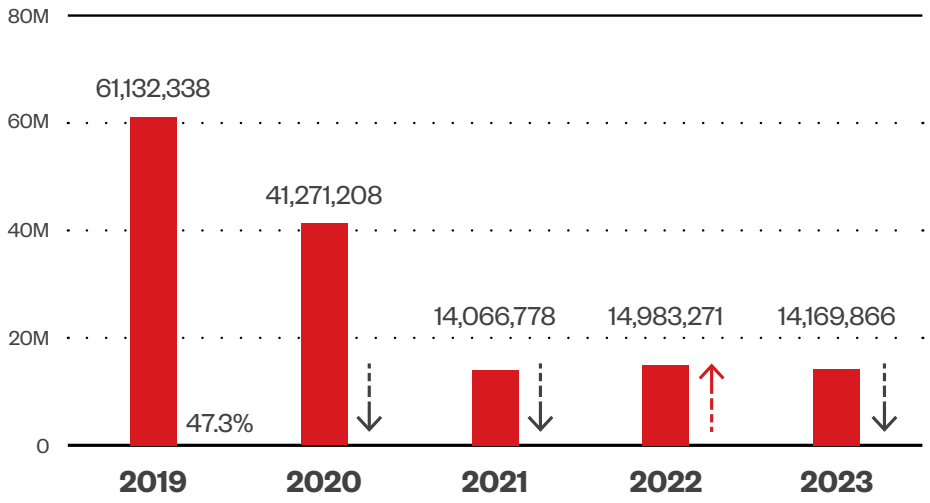
Endpoint Detection and Response (EDR) bypass using unmonitored virtual machines (VM)

- Observed in Akira and BlackCat
- Attackers bypass EDR by creating unmonitored VMs to navigate, map and encrypt files within the Windows Hyper-V hypervisor systems and attached VMs.

Multi-ransomware attacks

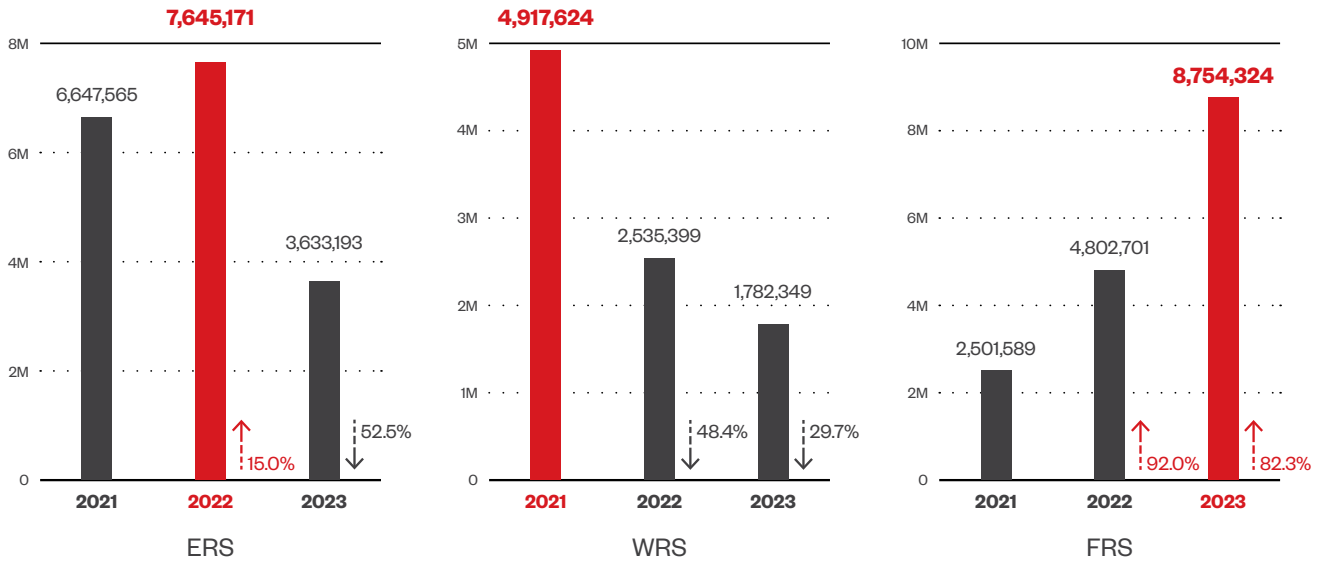
- The initial attacker sells its access to other ransomware groups to launch multiple attacks with a combination of malware, data theft, and wiper tools to maximize manipulation and pressure against the victims.

Total Ransomware Detections

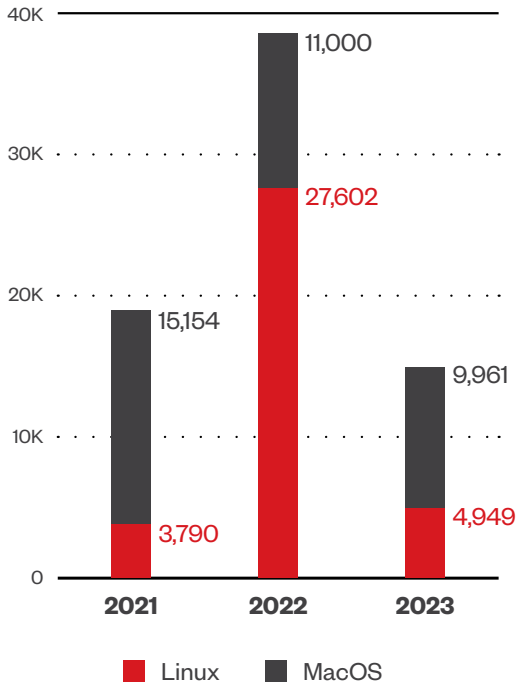


There has been a general downward trend in ransomware detections, with detections from 2021 to 2023 averaging less than half of the recorded detections in 2020; however, this should not be misconstrued as a cue for security operations centers and decision-makers to lower their guards. Historically, ransomware attacks were launched in "bulk," such as spam campaigns with malicious links, but attacks that focus on quantity can more easily be blocked, as shown in our ransomware ERS and WRS data in the following figure. These figures show a general downward trend consistent with the total ransomware detections.

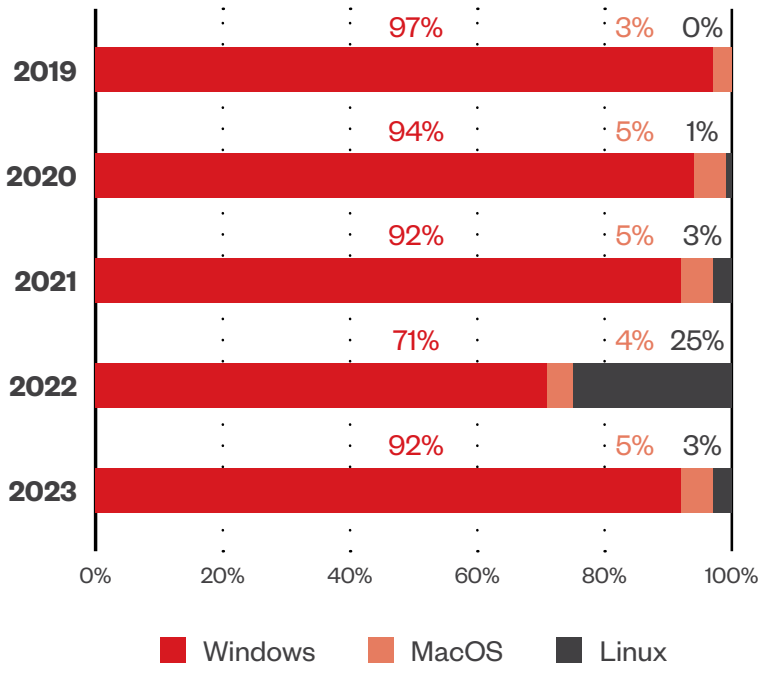
However, a continued increase in FRS detections could suggest that attackers are using more effective ways to evade preliminary detection by focusing on arrival and defense evasion techniques such as Living-Off-The-Land Binaries and Scripts (LOLBINs/LOLBAs), Bring Your Own Vulnerable Driver (BYOVD), zero-day exploits, and AV termination. We detect and identify ransomware payloads as malicious at endpoint as the ways they get into systems become more complex. This pattern is also observed in SPN data for overall threats blocked.



Operating Systems Affected by Ransomware



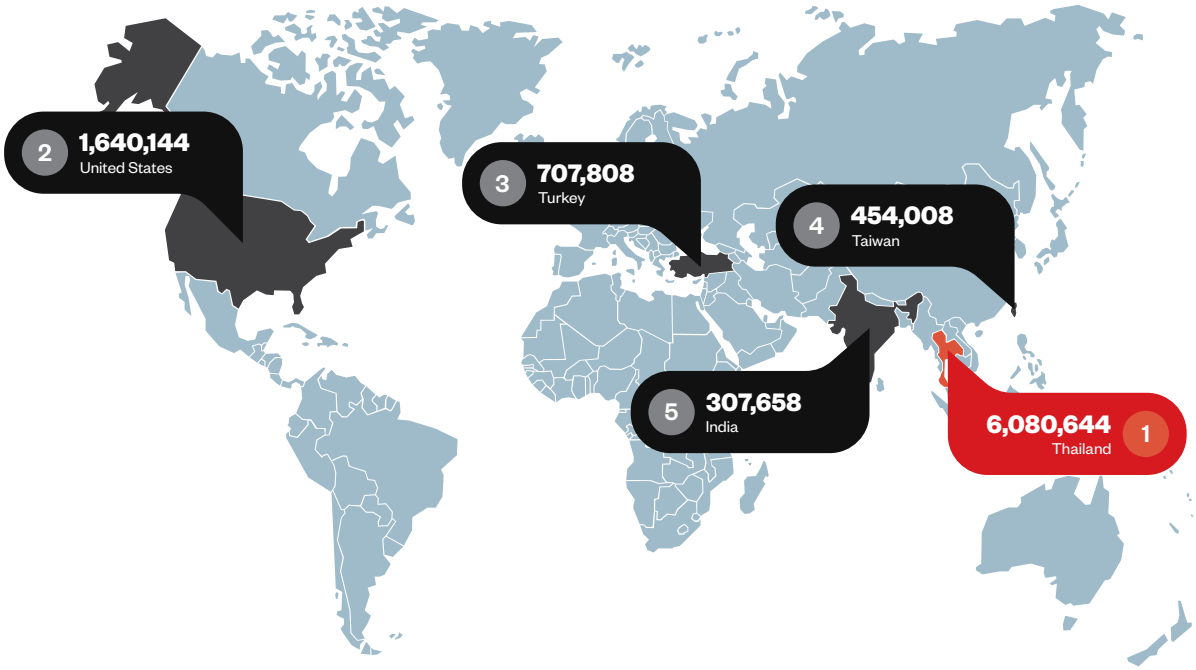
Based on data from our midyear report, customer detections on Linux-targeted ransomware attacks from the first half of 2023 continues to overshadow MacOS attacks. This is consistent with data gathered from 2022, which was an exceptional year for Linux-based malware detections, making up 25% of our telemetry; previously, Linux-targeted attacks only made up two to three percent of the OS ratio. It should be noted that Windows continues to take the bulk of our ransomware detections, with the only significant decrease in 2022.

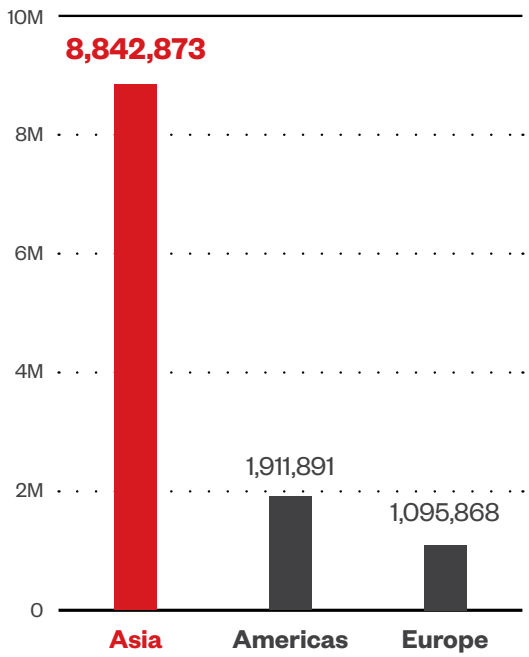


However, as our data for 2023 was completed, MacOS ransomware attacks came out higher with 9,961 detections, while Linux detections were finalized at 4,949. This could suggest that Linux-targeted attacks are stabilizing after the influx of novel Linux variants in 2022 to early 2023, but it could also be influenced by the overall decrease in ransomware activity.

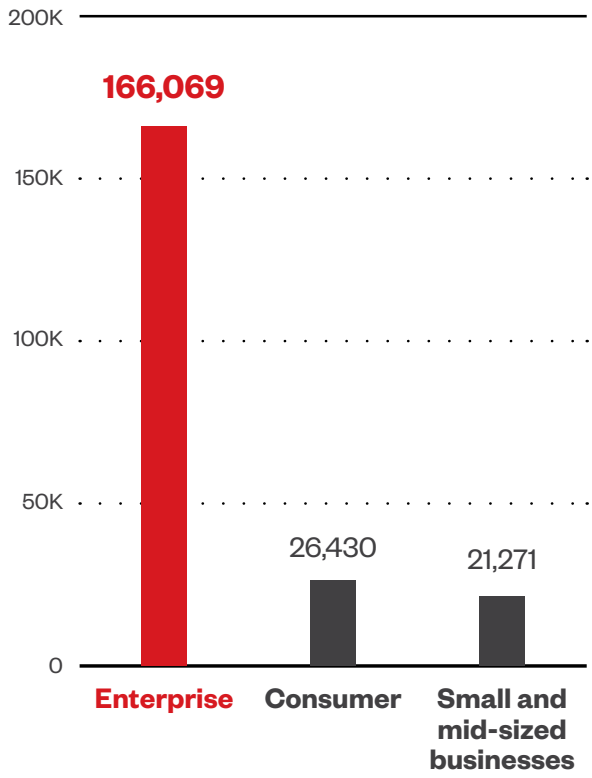
Top Countries and Regions by Detected Ransomware Attacks

Thailand made up 68% of ransomware detections in Asia.





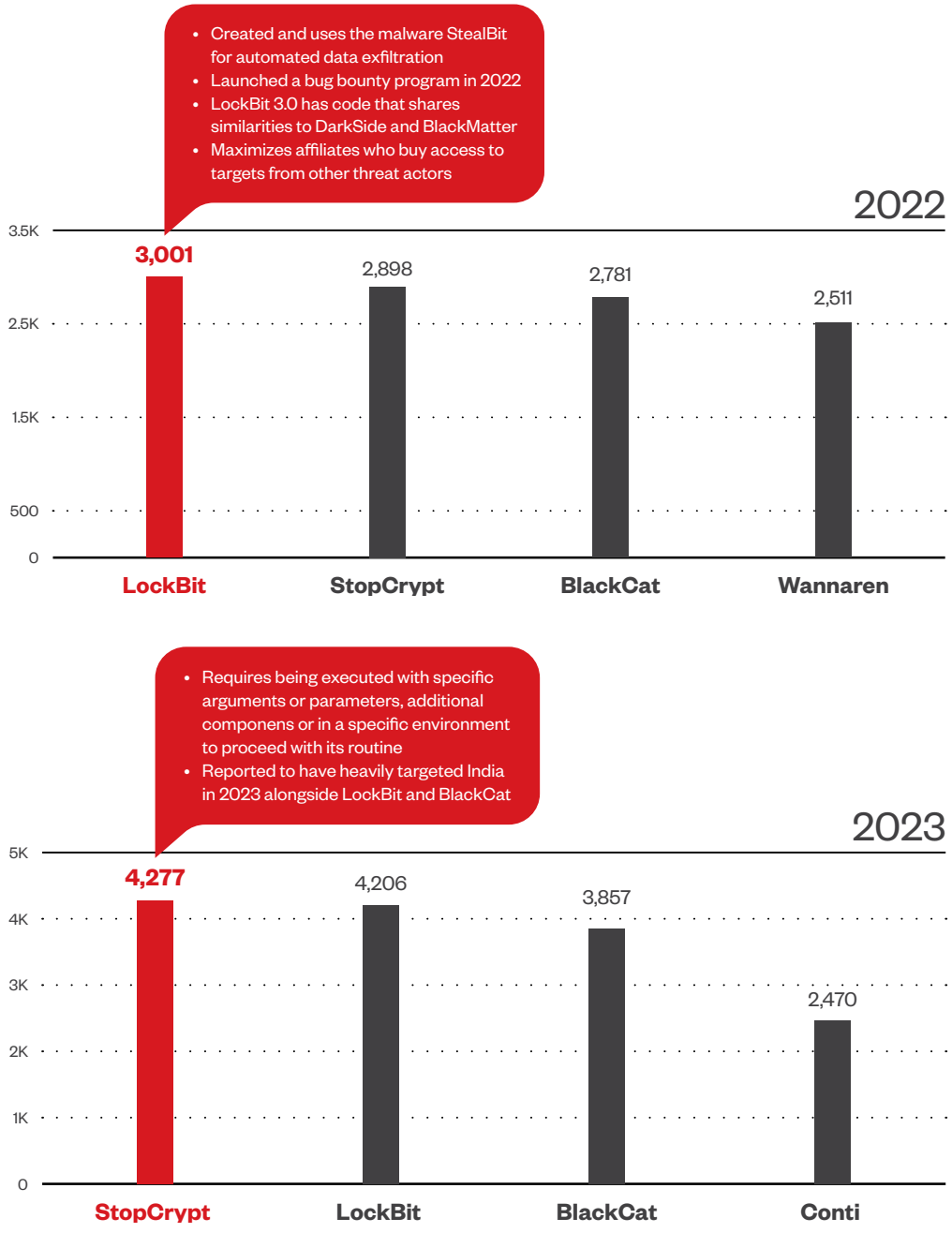
Top Industries and Segments by Detected Ransomware Attacks



Industry rankings and segment breakdowns based on unique detection counts at the endpoint shows that enterprises are the primary targets, with significant interest in the banking sector in 2023.

Top Ransomware Families

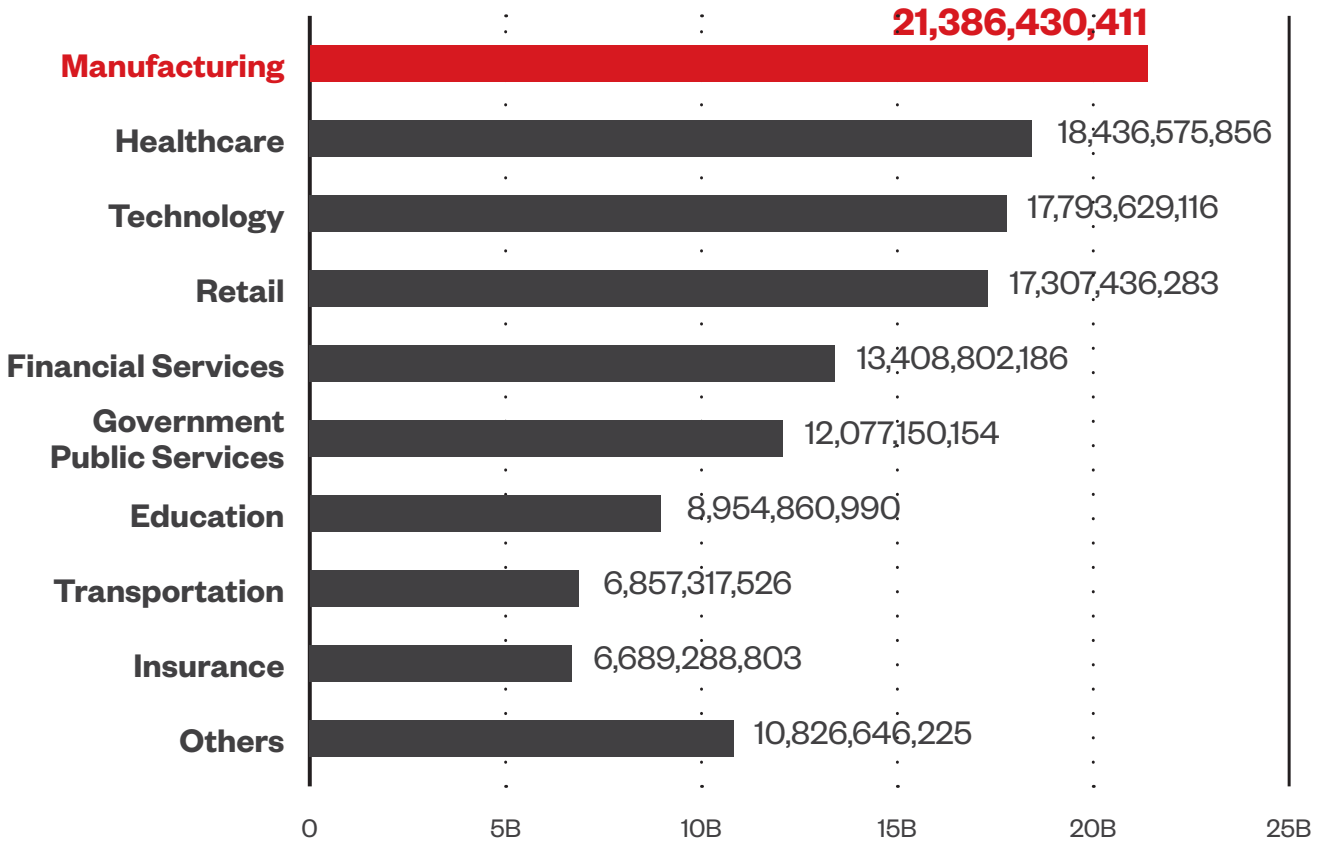
StopCrypt and LockBit maintain the top spots in terms of most prolific ransomware families for 2023 as it did in the previous year, but the former overtook the latter by a narrow margin this year. Note that this data does not include legacy ransomware families.



CLOUD AND ENTERPRISE THREATS

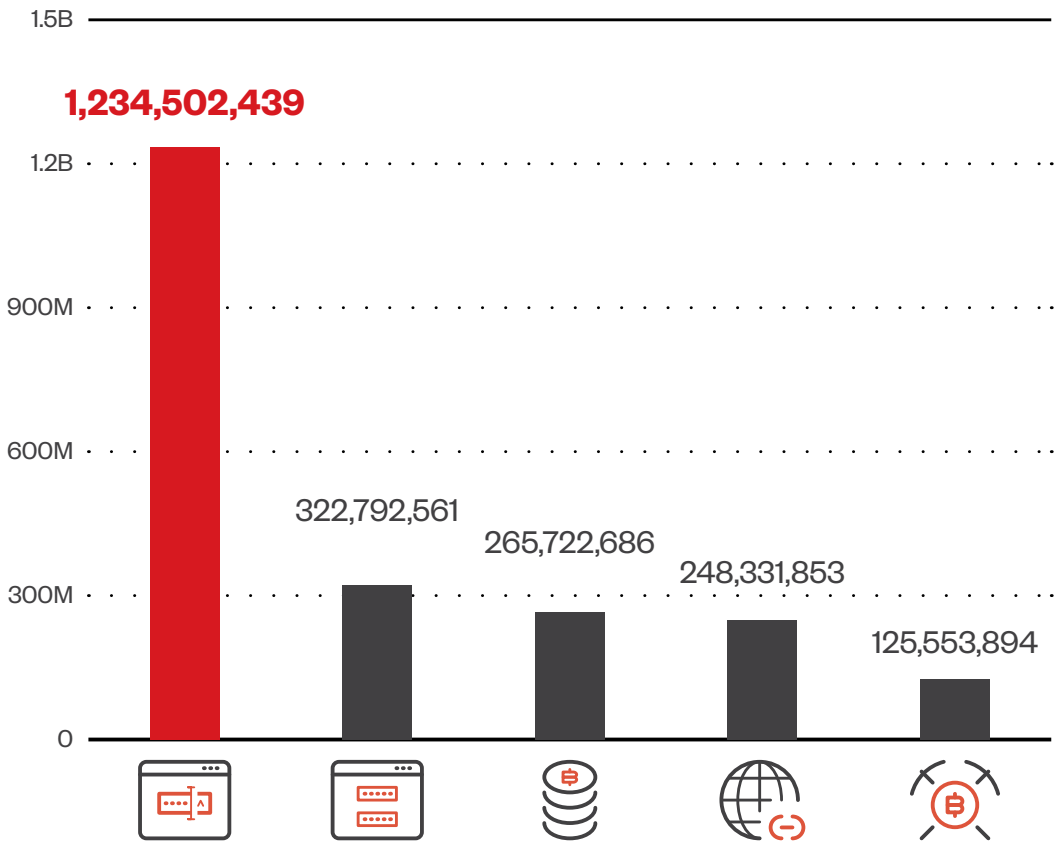
Risk Events

Top Industries by Risk Events (ASRM)



Home Network Security Top Events

With hybrid work now established as part of business operations, we looked at our Home Network Security telemetry to see what specific events cybercriminals particularly favor to use and what devices they target to maximize the larger attack surface created by remote and home workspaces.



Brute-Force Login

- Might be RDP via port 3389, FTP via port 21, or SSH via port 22 to repeatedly attempt to log in to target hosts using a dictionary of common usernames and passwords

TELNET Default Password Login -6

- Detects when a user within the network uses the default password to log in

MISC Bitcoin/Litecoin/Dogecoin Mining Activity -1

- Related to information disclosure and possibly to Bitcoin/Litecoin/Dogecoin Mining Activity

WEB HTTP Invalid Content-Length -2

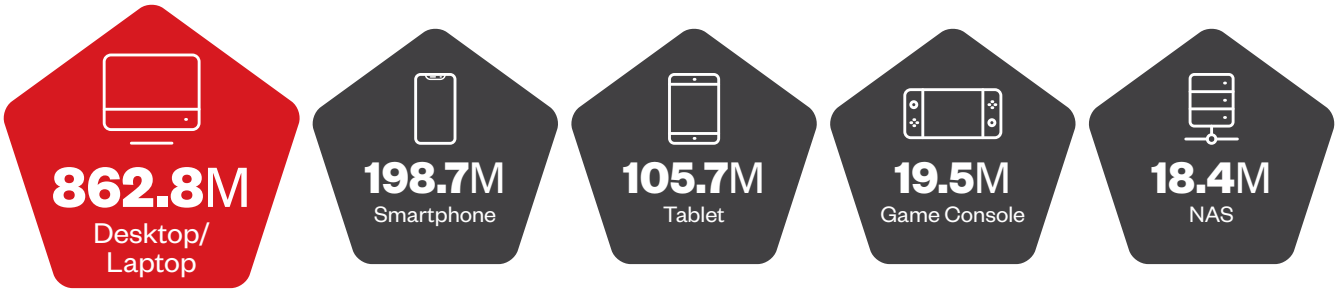
- Caused by an error in processing HTTP packets containing negative Content-Length header field values that result in a heap buffer overflow

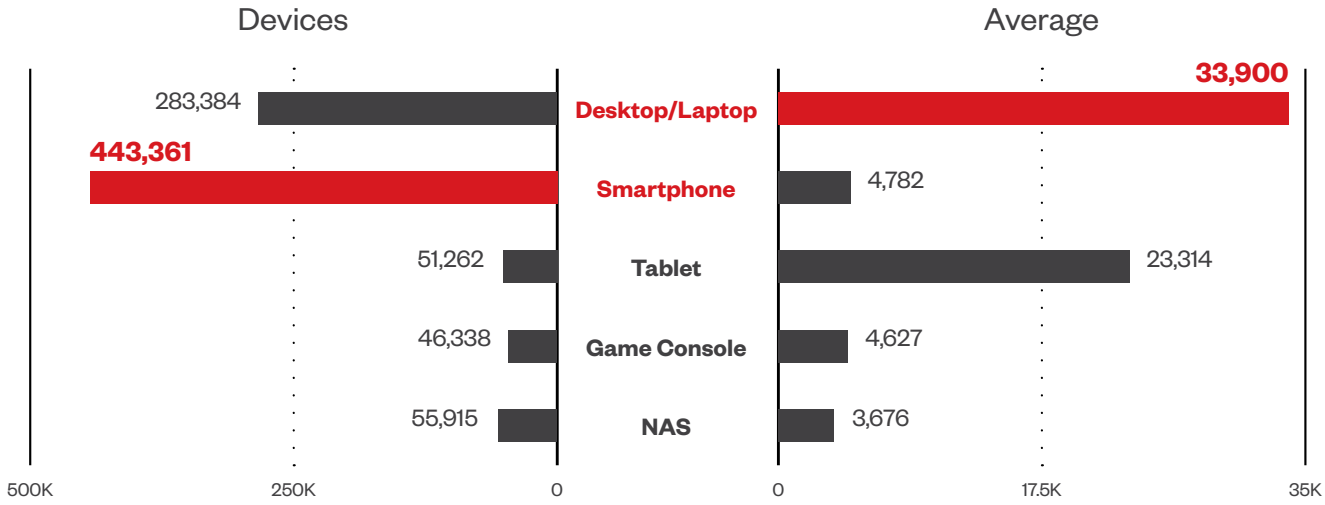
MISC Cryptocurrency Monero Mining Activity -1

- Possible Monero (XMR) cryptocurrency mining activity

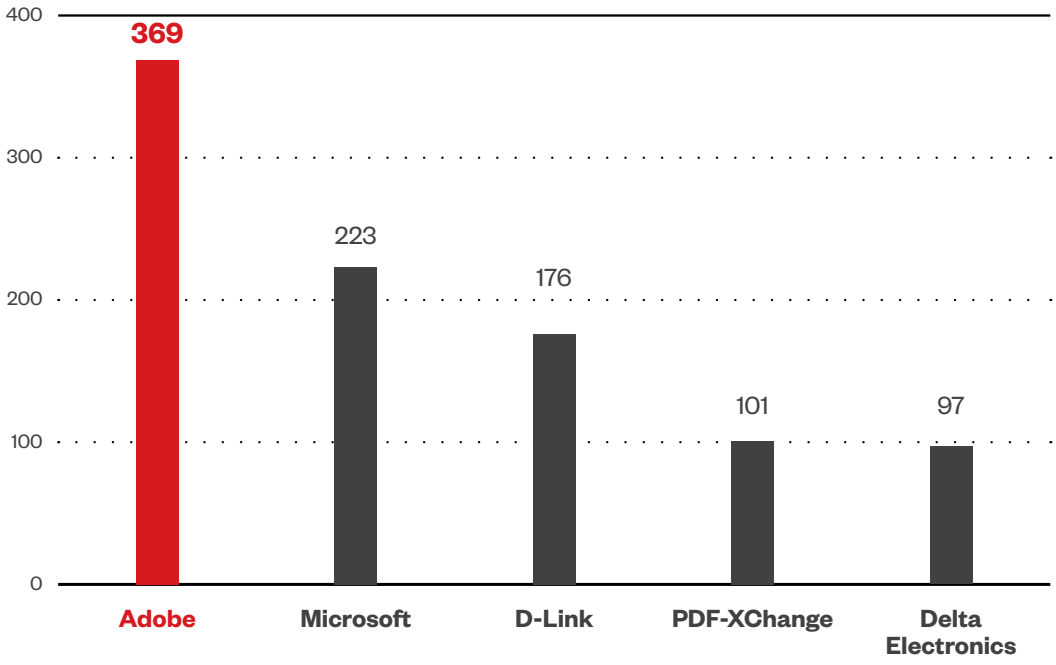
Home Network Security Top Affected Device Types

Desktops and laptops recorded the most inbound attack detections based on our Home Network Security telemetry data.





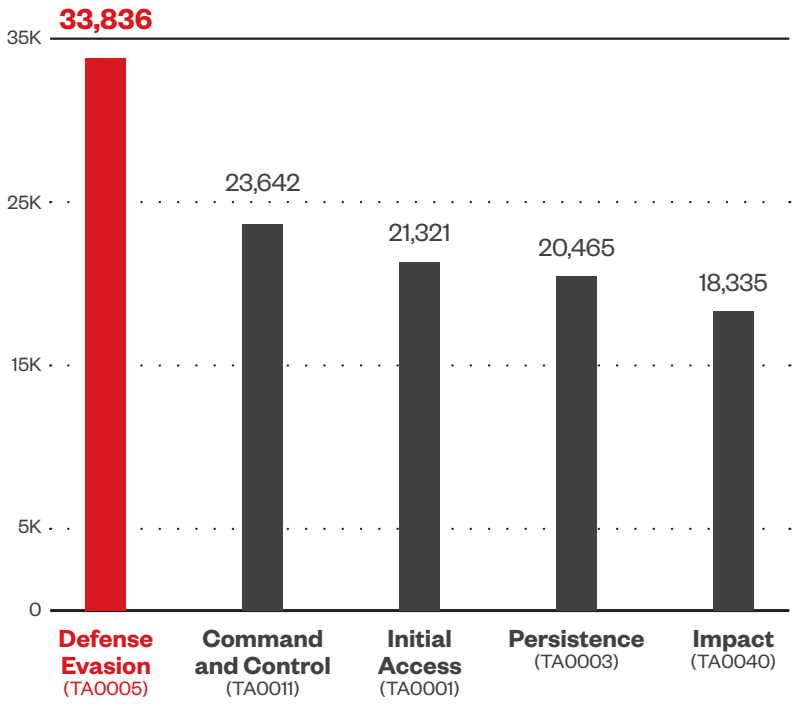
Vulnerability by Vendor



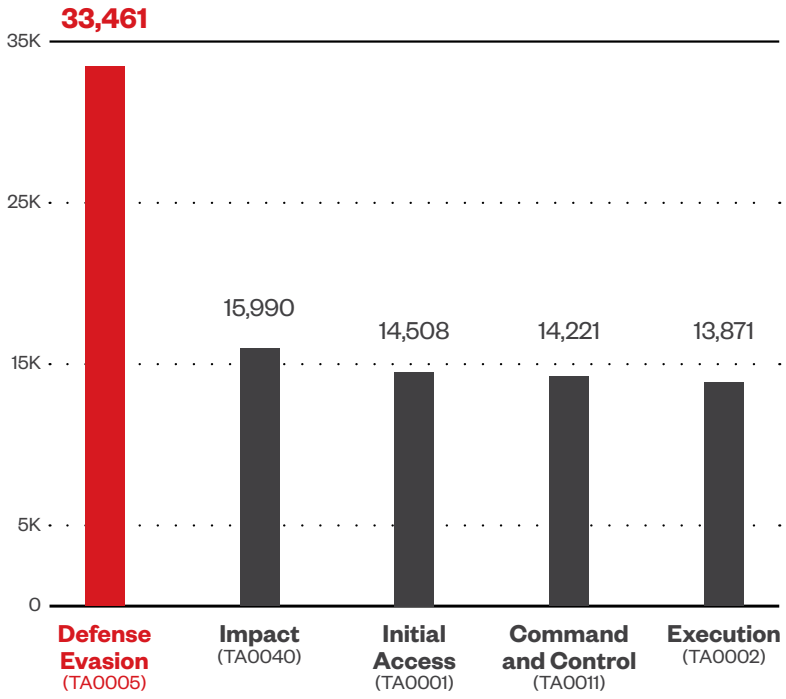
MITRE ATT&CK DETECTIONS

Top 5 Tactics Detected (Overall)

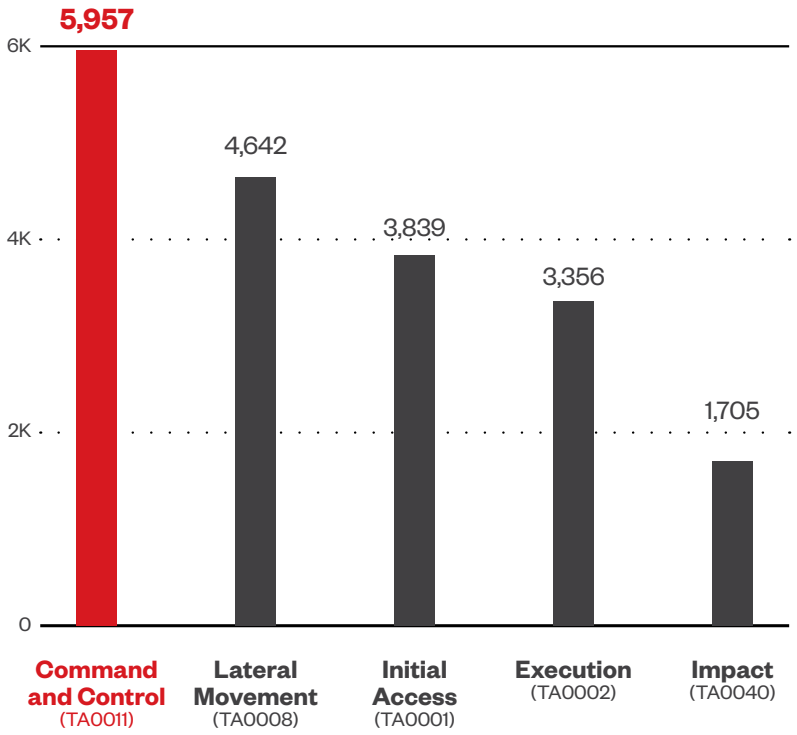
Dodging security tools, communication and control of compromised systems, and gaining a foothold within victim's systems and networks are the most used TTPs (overall, endpoints, network, and email)



Top Tactics, Techniques, and Procedures (TTPs) Endpoint



Top TTPs Network

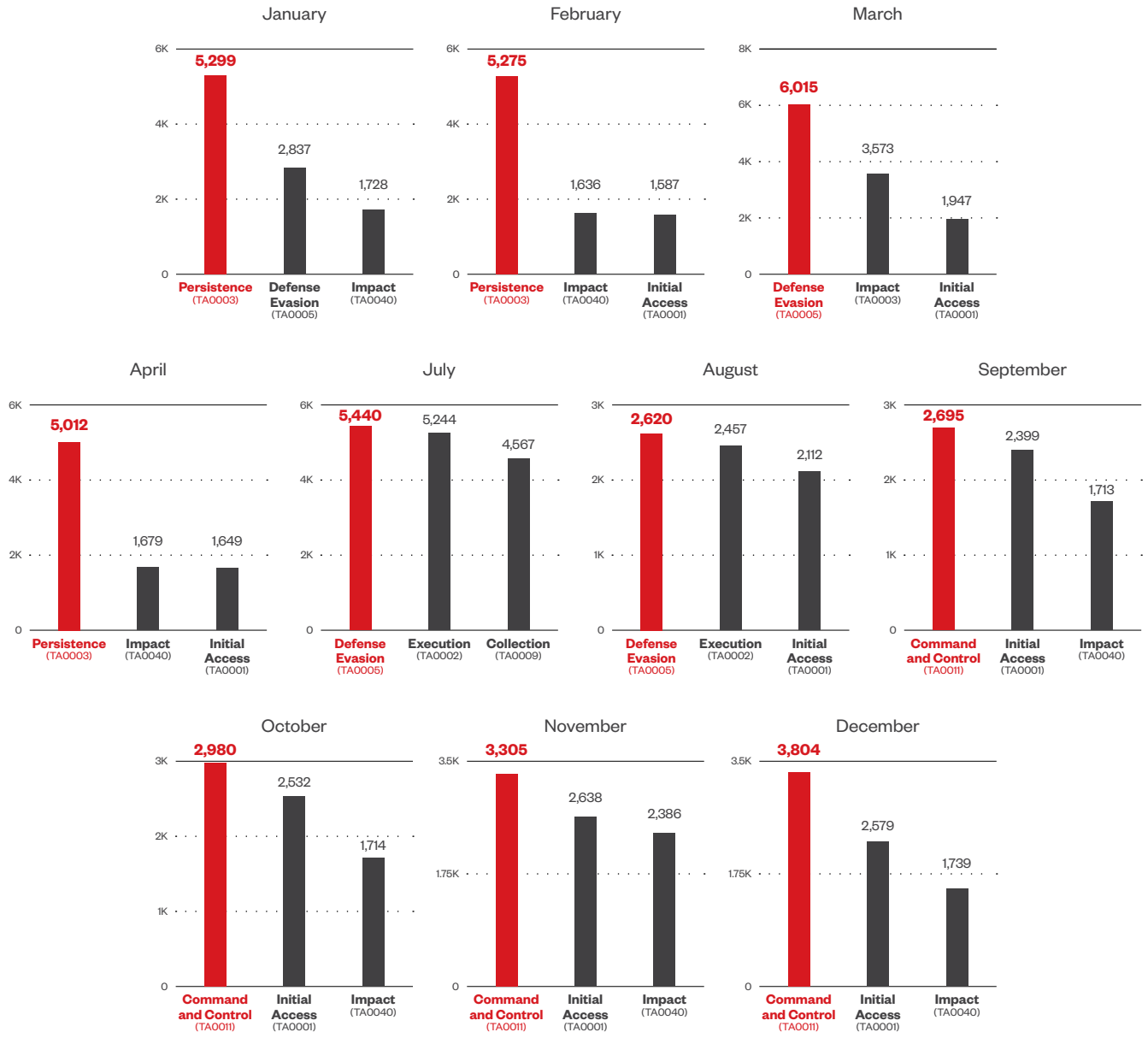


TTPs Overall Trend by Detections

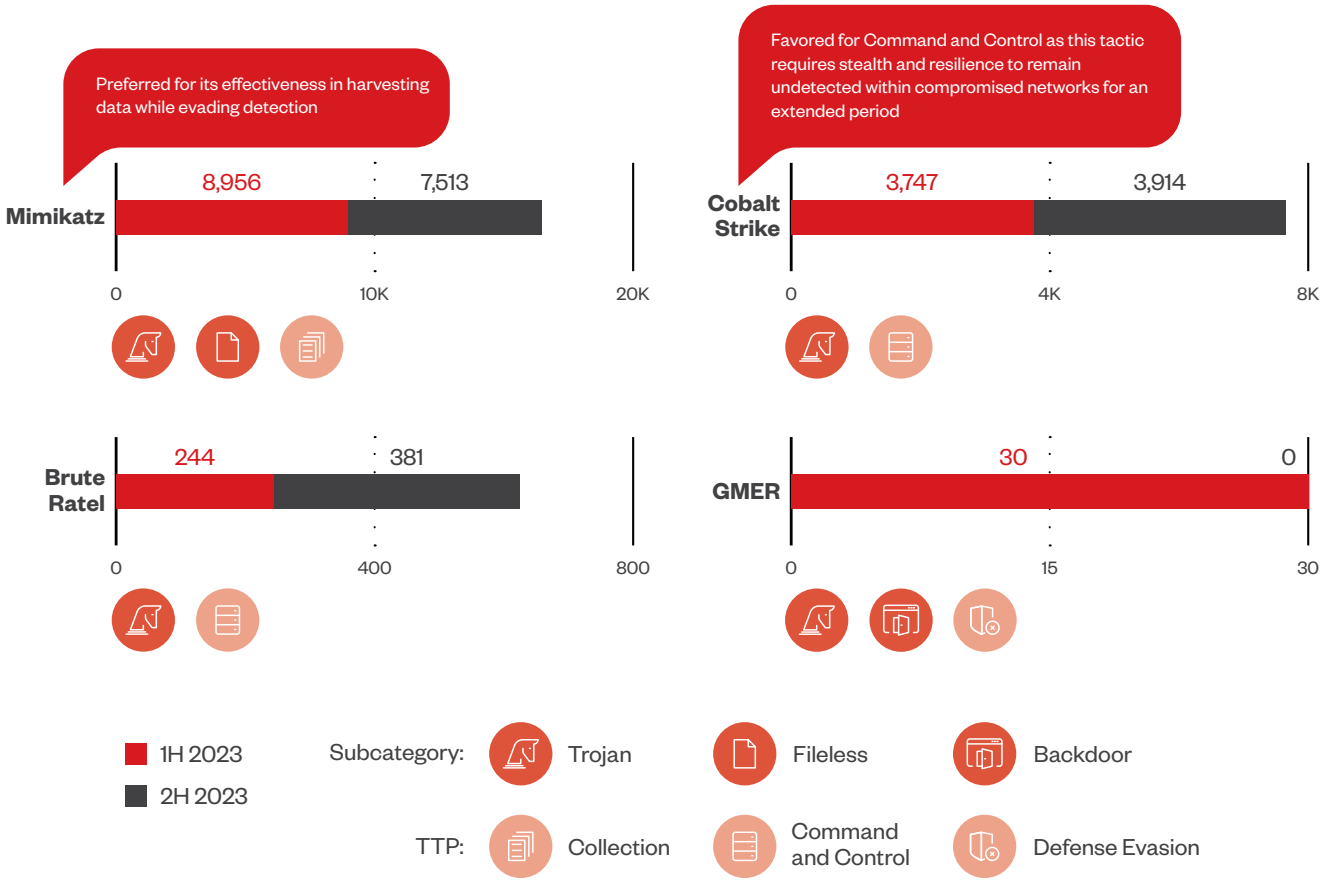
Command and Control showed a gradual increase from September to December, while Defense Evasion peaked in March and July before declining in customer detections in subsequent months. Execution entered the top three TTPs detected in July and August, while Impact showed no clear trend despite a spike in November.

Persistence only entered the top three in the first quarter of the year but was in a downward trend before dipping below the top three. Despite fluctuations, Initial Access maintains a moderate number of detections, since it is the primary goal of threat actors to gain a foothold in target victim systems and networks.

Note that the monthly detections do not show data for May and June due to a system error experienced during that period.



Living-Off-The-Land Tactics



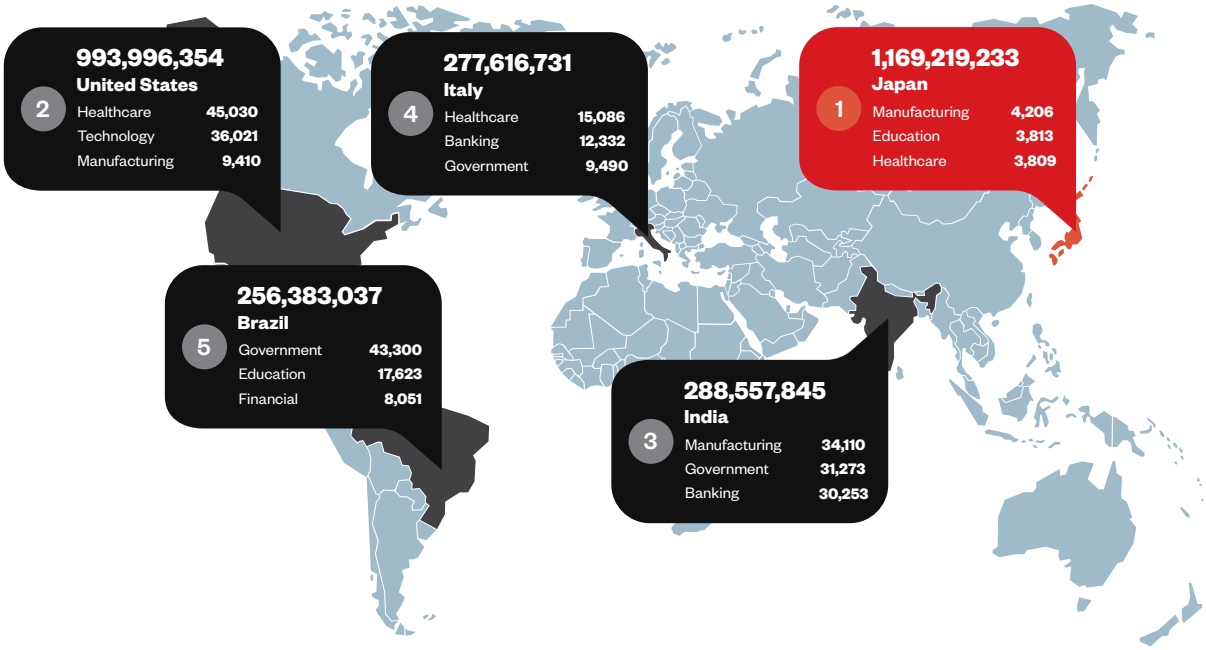
There is no clear trend in the detections, though Mimikatz and Cobalt Strike continue to be the preferred legitimate tools to abuse to aid criminal activity. It can be assumed that threat actors prefer to use well-known tools instead of exploring novel ones, a logical behavior that is commonly observed as it guarantees more likelihood of success with less effort.

THREAT LANDSCAPE

Malware Detection

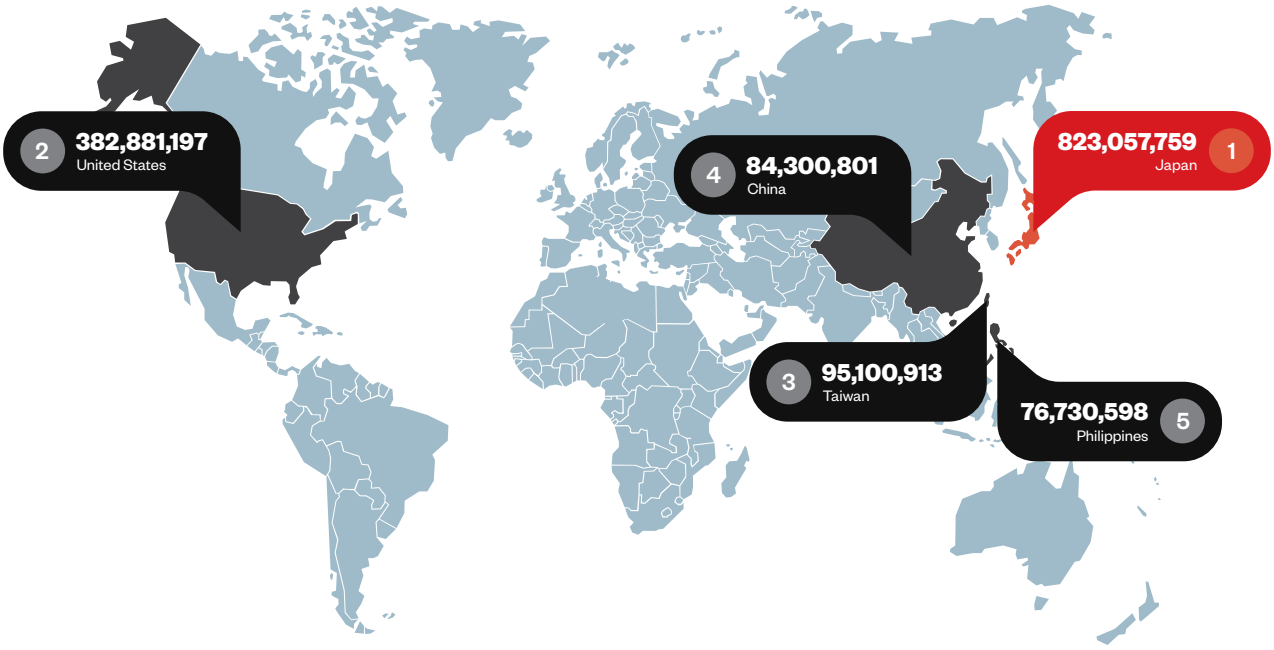
Countries With the Most Malware Detections

and the corresponding top industries targeted for each



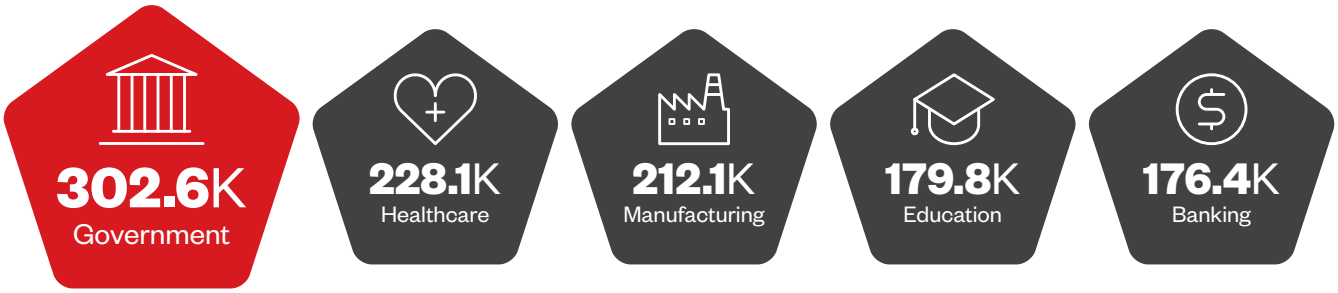
Note that industry data counts are limited to customers who have elected to provide details pertaining to the business sectors in which they belong. Total malware detection counts include customers who did not provide any information on their industries.

Top Countries Accessing Malicious URLs



Top Industries Affected by Malware Campaigns

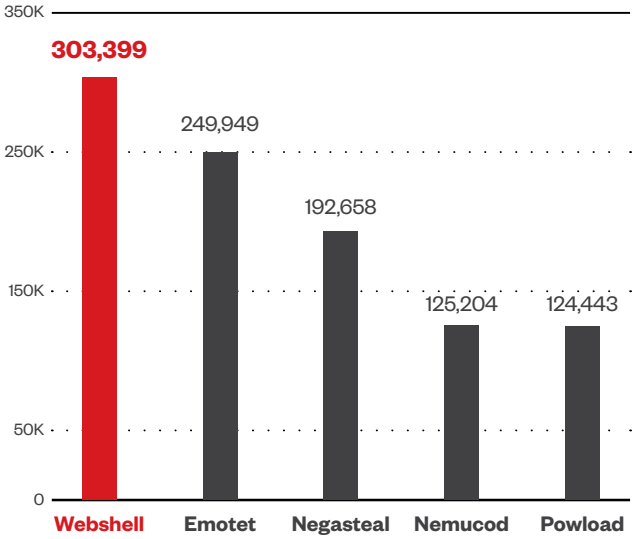
From the aggregate average of our Smart Protection Network (SPN) data, malware campaigns targeted government organizations the most with 302,555 detections.

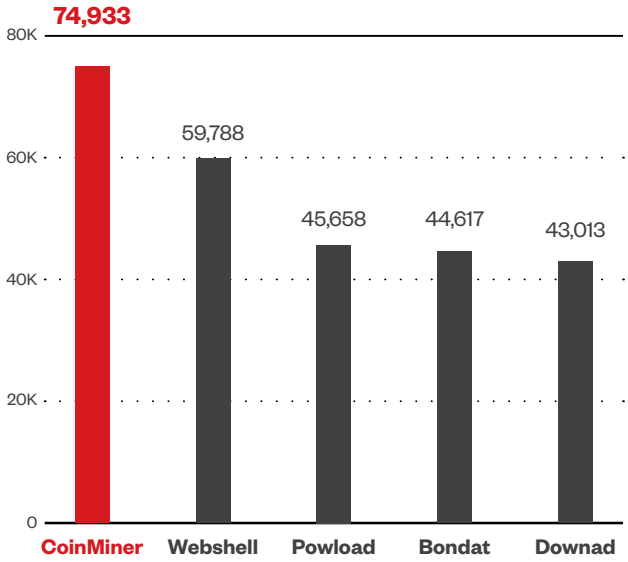


Top Malware Families

A cryptocurrency mining malware surpassed prolific names in 2023.

Personal data remains the most valuable commodity in underground criminal communities; cryptocurrency wallets and crypto-related data are the most actionable data that can be stolen by malicious actors, equivalent to cash that can immediately be spent without traceability.





Cryptocurrency mining malware CoinMiner takes the lead over notorious Webshell

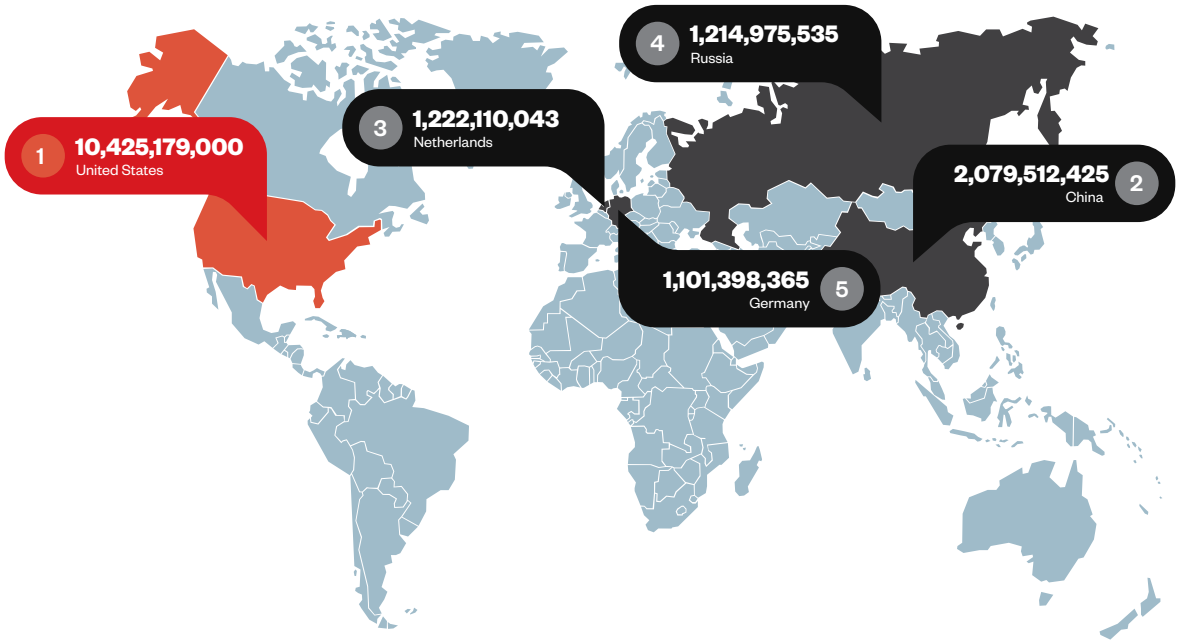
- Last reported exploit: Oracle WebLogic Server vulnerabilities (CVE-2020-14882)
- Reported to have been deployed by malicious Python Package Index packages targeting Linux
- Uses the victim system's central processing unit (CPU) and/or graphical processing unit (GPU) resources to mine cryptocurrency
- The following can be observed during the infection:
  - High CPU utilization either with powershell.exe or schtasks.exe
  - Monero.Cryptocurrency.Miner app detection from the network
  - Execution source can be identified during service installation
  - WMI powershell scripts on the DC server

Despite being overtaken, Webshell remains a go-to for threat actors

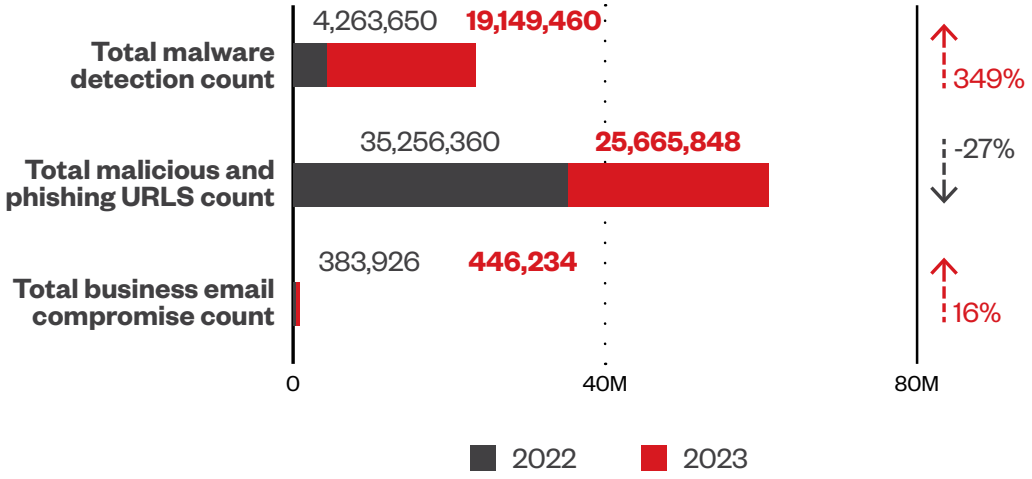
- Exploits vulnerabilities in internet-facing web servers

Email Threats

Top Countries by Detection

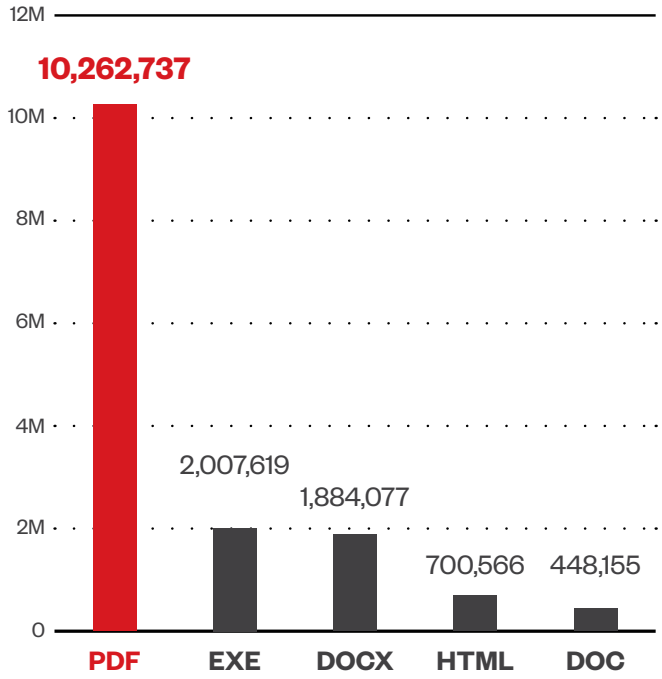


High-Risk Email Threats

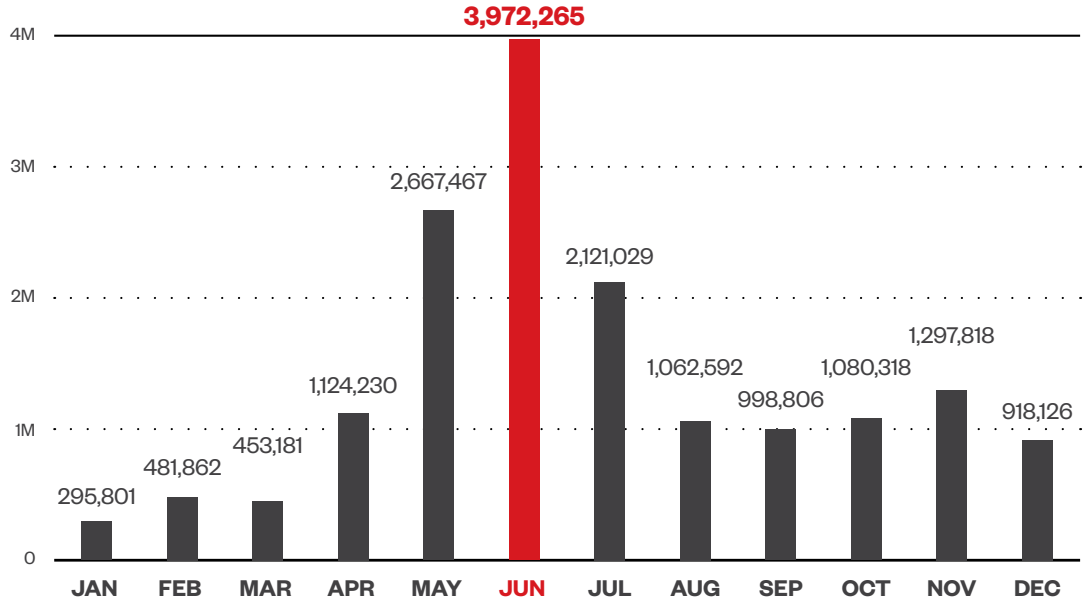


While there is a decrease in malicious and phishing URL detections from 2022 to 2023, the increase in malware detection count and BEC count suggests the change in the threat landscape that finds attackers making use of more sophisticated ways to avoid detection. In this case, instead of focusing on malicious and phishing URLs to randomly victimize users, BEC schemes suggest more targeted operations, while a closer look at our malware detection count includes phishing links embedded within the attachments. This is consistent with patterns observed in our SPN data on threats blocked from 2021 to 2023, where detections that rely on attribution of URLs (WRS) and emails (ERS) show a decrease, while endpoint detections that directly identify malicious files have consistently increased.

Top 5 Spam Attachments

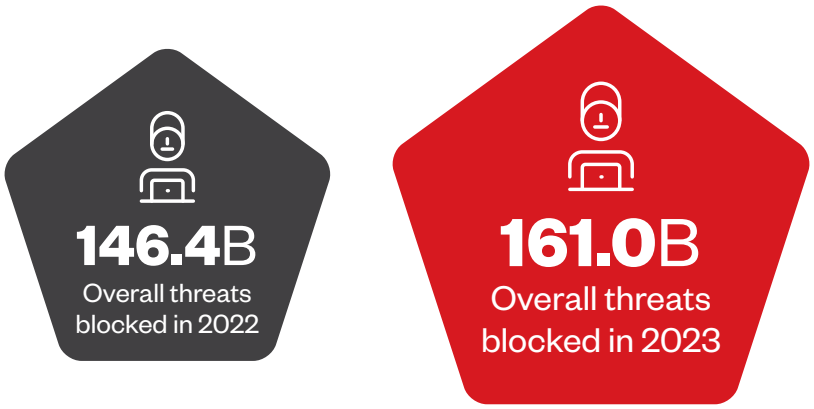


Spam attachments per month of 2023

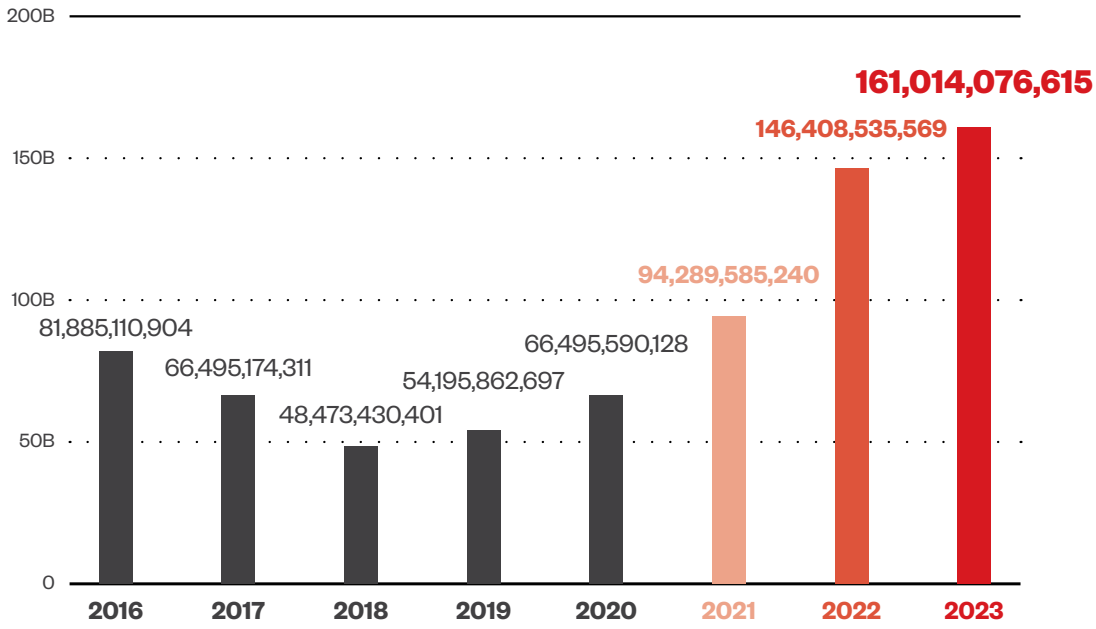


There is a general increasing trend for the first half of the year, where malicious spam attachment detections peaked in June. This is followed by fluctuations in the second half of the year, that eventually decline until December. Despite more cunning ways to lure victims into clicking malicious links, spam campaigns remain a go-to for cybercriminals.

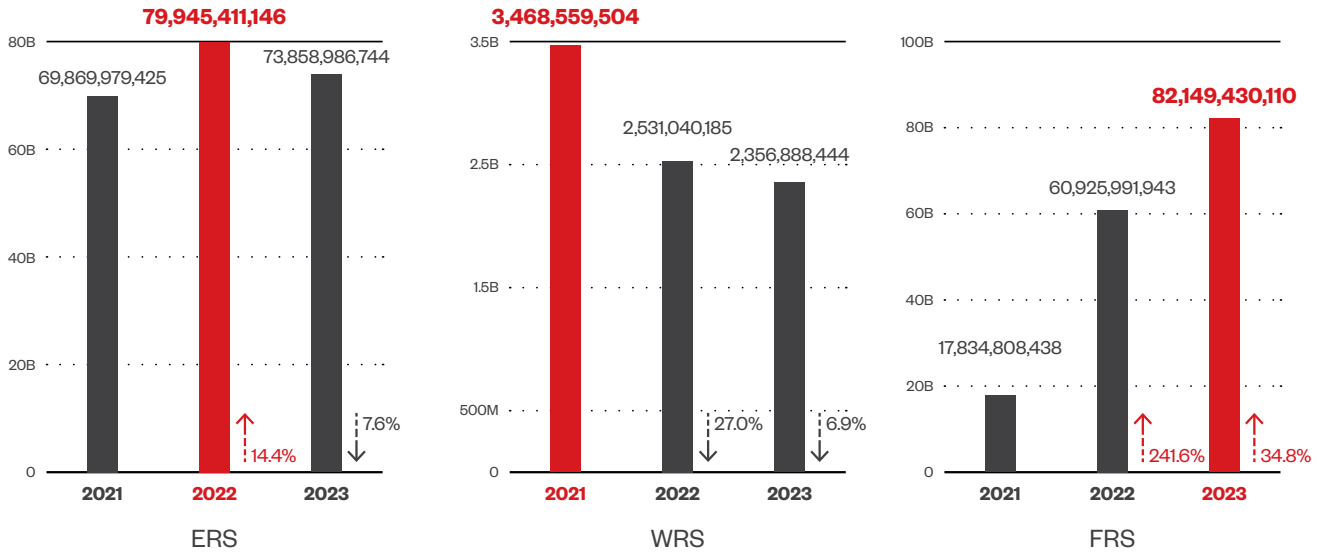
Threats Blocked



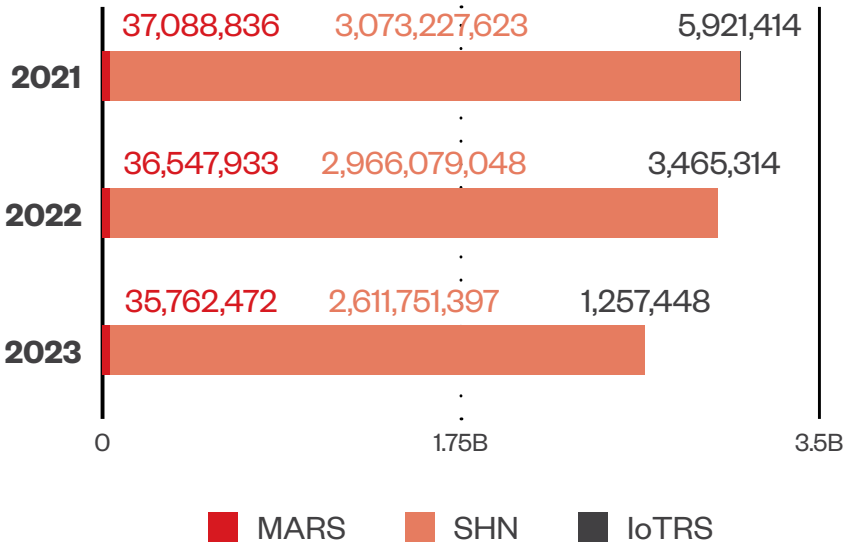
The total number of threats blocked based on our SPN reached a record high in 2023, 10% higher from the previous year. It also continues the dramatic climb of threats blocked that began to be recorded in 2021, the first year that surpassed the previous peak of 82 billion in 2016. This coincided with the pandemic, strongly suggesting its role in driving the upswing.



Despite the overall threats blocked peaking in 2023, there is a fluctuating and downward trend in threats blocked under our Email Reputation Service (ERS) and Web Reputation Service (WRS), indicating that threats in these areas are being better managed or are less frequent. However, there is a continuous increase in threats blocked under our File Reputation Service (FRS).

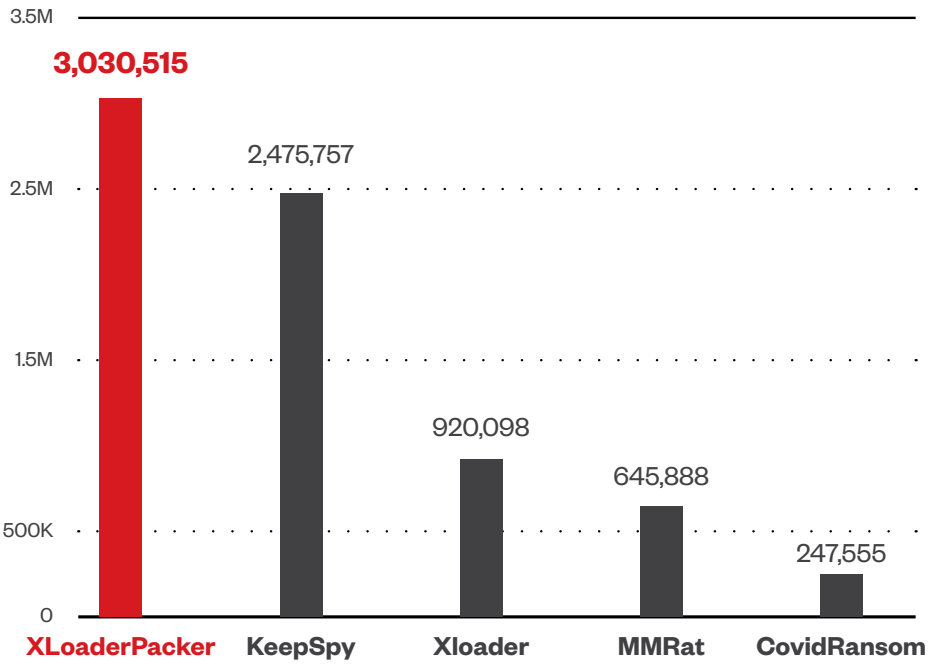


This could be indicative of the changing threat landscape where it can be assumed that threat actors are now opting for quality over quantity: Instead of launching attacks on a wider range of users and relying on victims clicking on malicious links in websites and emails, more sophisticated attacks are launched using specificity to trick a narrower field of high-profile victims. This also allows them to bypass early detection layers like network and email filters. It could be speculated that this contributed to the continuous increase in malicious file detections that are detected at endpoints.



There is also a continuous decrease in threats blocked under our Mobile Application Reputation Service (MARS), Smart Home Network (SHN), and Internet of Things Reputation Service (IoTRS), suggesting that cybercriminals are choosing their targets carefully rather than randomly. It remains crucial to protect all layers of the attack surface, and SOCs should realize that understanding the attackers' targeting strategies is important for effective defense.

Android Malware Families

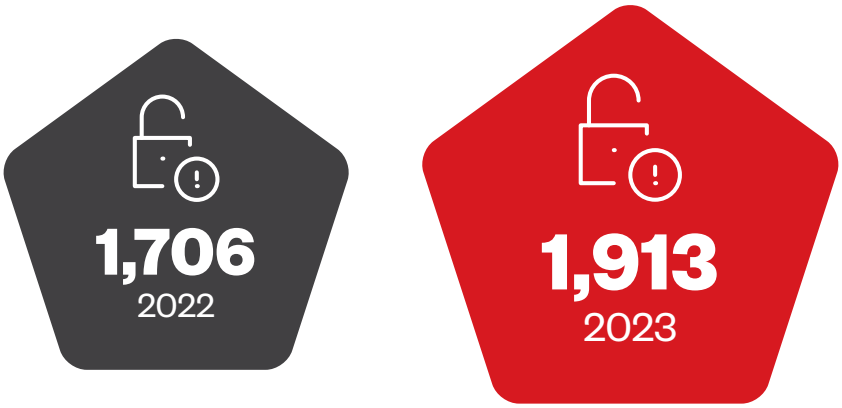


- XLoaderPacker is a spyware that can be manually installed by a user. It poses as an Android app using different app names, and, once installed can monitor incoming and outgoing calls, and lock the screen of the affected system.
- KeepSpy is sideloaded through a TianySpy malware delivered via smishing messages. It also poses as an Android app using different app names, and, once installed, can collect banking credentials and Wi-Fi settings.

Vulnerabilities

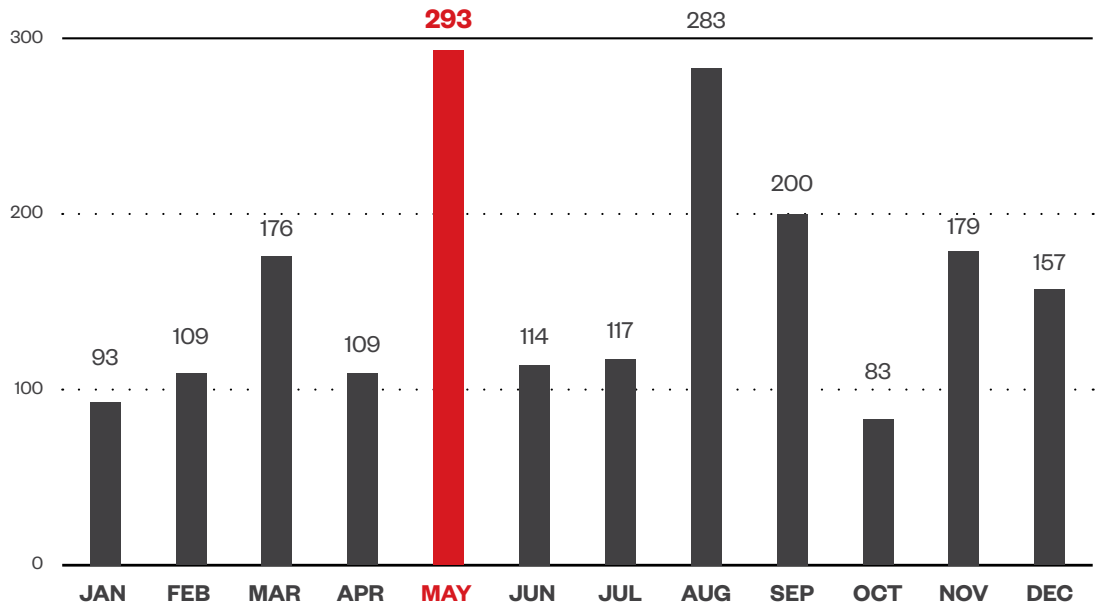
Total Vulnerabilities

(Number of published Zero-Day Initiative (ZDI) vulnerability advisories)

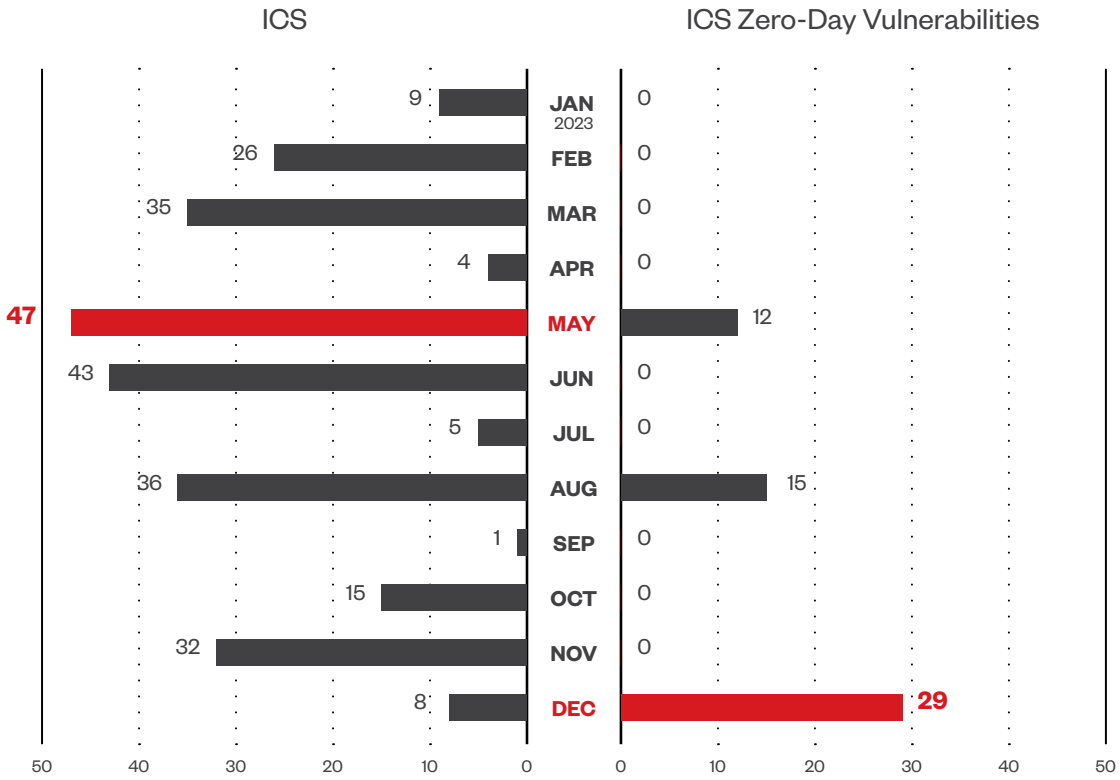


Zero-Day Exploits (ZDI) Advisories

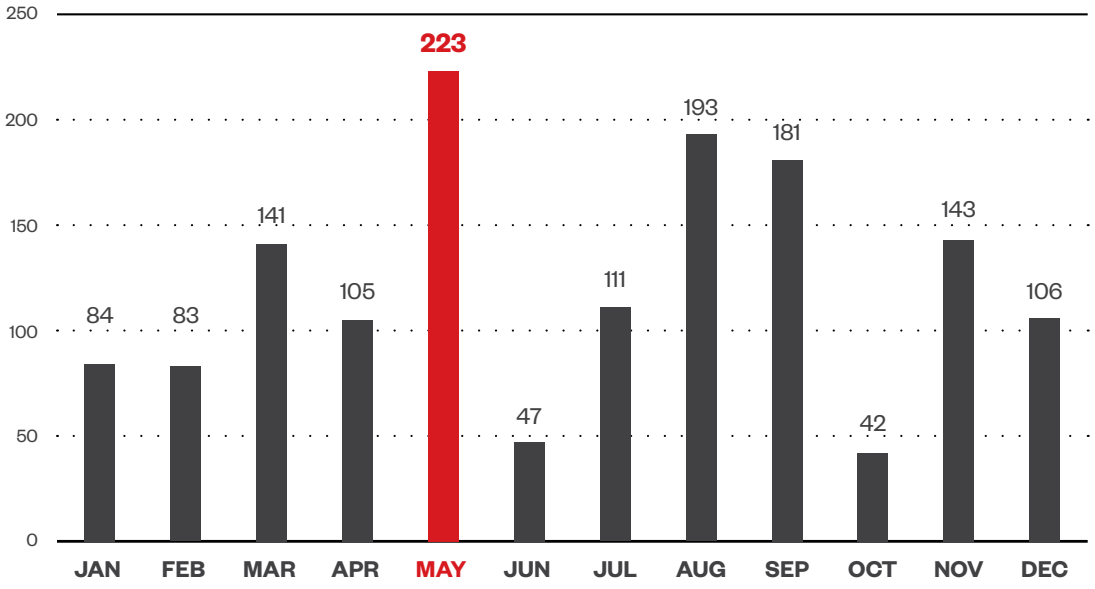
The first quarter of 2023 starts with relatively low zero-day advisories, with a significant increase by the end of the quarter in March. The second quarter fluctuates and peaks in May, while the third quarter stabilizes at a relatively high level of activity. The last quarter dips to the year's lowest number of zero-day advisories in October, picks back up again in November, but shows a slight downturn in the last month indicating a possible decrease in threat actor activity as the year ended.



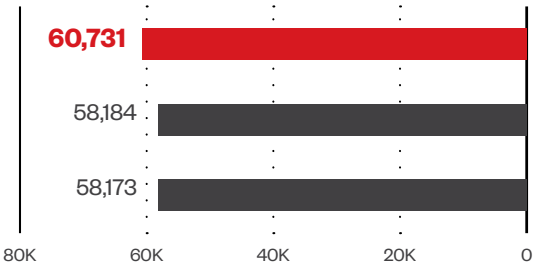
ZDI Industrial Control System and Zero-Day Vulnerabilities



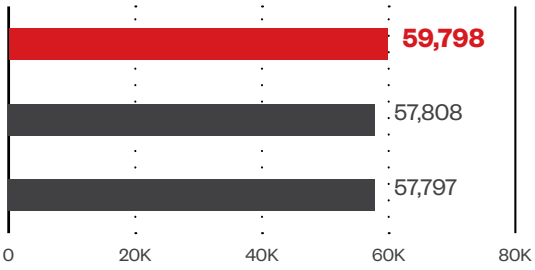
Non-ICS and N-Day Vulnerabilities



Riskiest CVEs by customer count



3 riskiest unpatched CVEs



CVE-2023-2488 (Windows SmartScreen Security Feature Bypass Vulnerability)

- CVSS base score: 4.4 medium

CVE-2023-21823 (Windows Graphics Component Remote Code Execution Vulnerability)

- CVSS base score: 7.8 high

CVE-2023-23376 (Windows Common File Log System Driver Elevation of Privilege Vulnerability)

- CVSS base score: 7.8 high

Risk Events

Top 2 Risk Events Detected

The top two risk events detected via our attack surface risk management (ASRM) involve risky cloud applications and accessing risky websites.

82,976,277,500

Risky Cloud App Access

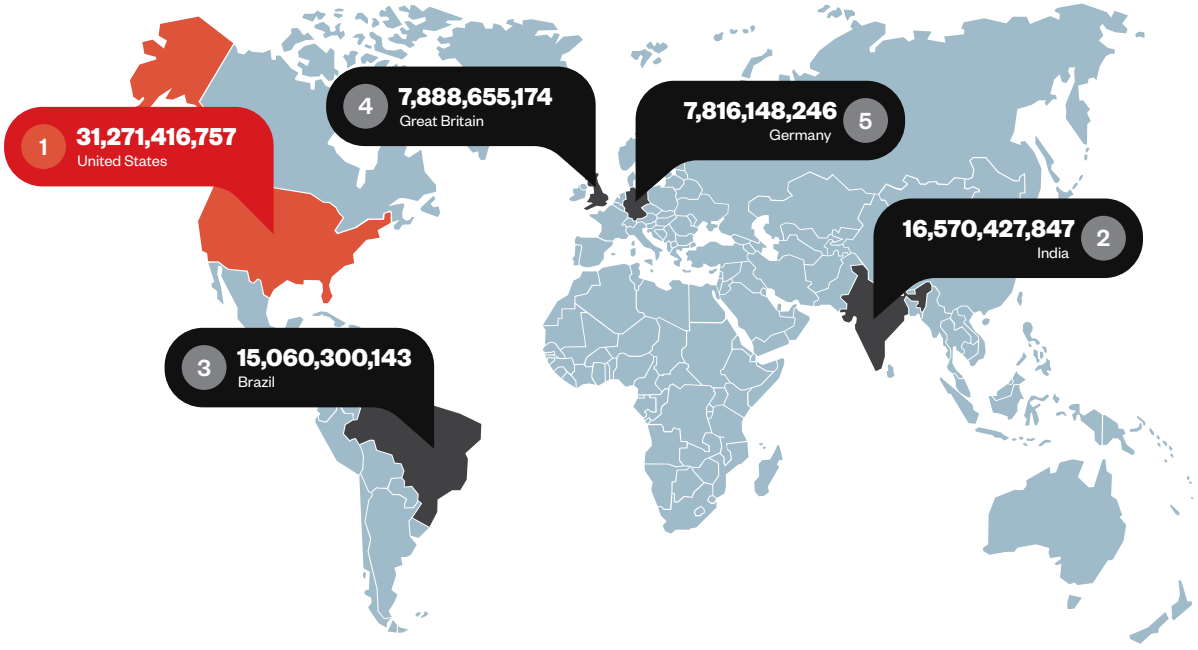
18,819,067,819

Risky Website Access Detected

- SOCs are recommended diligence in monitoring cloud applications accessed by their networks, especially as more organizations are integrating cloud environments in their operations.
- Security teams should also conduct training to equip end-users with the knowledge to identify and avoid accessing risky websites and links; human negligence remains the weakest link in cybersecurity.

Top Countries with Risk Events Detected

The United States of America recorded the most risk events at over 31.2 billion detections, almost doubling the number of the country with the second most risk events, India at 16.5 billion detections.



Recommendations for Lowering Risk

Apply the latest patch or upgrade your operating system or application version.

Apply prevention rules from Trend Micro products to protect vulnerabilities from being exploited.

Optimize weak settings in current environment.

Avoid accessing the reported risky app or make the app a sanction one

Disable accounts with weak passwords or reset them with strong ones. Enable the Account Lockout Policy in your Active Directory.

Restrict user account usage on affected device and verify and resolve the at-risk device's high-risk events.

CALIBRATING EXPANSION

2023 ANNUAL CYBERSECURITY REPORT

Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, our unified cybersecurity platform protects over 500,000 organizations and millions of individuals across clouds, networks, devices, and endpoints.

The Trend Micro One unified cybersecurity platform delivers advanced threat defense techniques, extended detection and response (XDR), and integration across the IT ecosystem, including AWS, Microsoft, and Google, enabling organizations to better understand, communicate, and mitigate cyber risk.

Trend Micro's global threat research team delivers unparalleled intelligence and insights that power our cybersecurity platform and help protect organizations around the world from 100s of millions of threats daily.

We have 7,000 employees across 65 countries, singularly focused on security and passionate about making the world a safer and better place.

Trend Micro enables organizations to simplify and secure their connected world.

TrendMicro.com