CYBLE

Threat Landscape Report

2023-2024

Table of **Contents**

Executive **Summary**

At Cyble Research and Intelligence Labs, we pride ourselves on being one of the first to analyze, contextualize, and report on notable events in cyberspace across the surface, deep, and dark web. This report aims to summarize our observations for 2023 and contextualize them for our readers' consumption, providing insights, data points, and predictions for the year ahead.

2023 was an extremely volatile year in cyberspace, marked by several notable events, including 2 ongoing armed conflicts in the Middle East and Ukraine, the rise in the adoption of AI by cybercriminals, and high-profile cyberattacks targeting major entities, governments, and critical infrastructure around the world.

The cyber attacks we observed last year have been multi-faceted, be it the emergence of new cybercrime forums, the advent of novel malware and ransomware threats, changing and aggressive tactics of Hacktivism due to shifts in geopolitics dynamics, or state-sponsored cyberwars. Cyber security risks are mounting by the day, and governments and businesses should prepare to confront them in 2024.

In this annual threat landscape report, we have summarized our findings for 2023 basis sectoral and regional trends and listed our observations with regard to emerging patterns and tactics. Readers can also gain inisghts for the coming year basis our predictions.

Key **Takeaways**

- Multiple threat groups tried to establish new cybercrime forums to monetize the opportunity to fill the void created after the seizure of BreachForums.
- Over 7,000 cybercrime forum incidents were reported being actively involved in the sale of compromised data, unauthorized access, exploits, and multiple claims of data compromises by financially motivated threat actors and hacktivist groups.
- Ransomware threats doubled in 2023, with disruptions in threat groups and the emergence of new groups and attack vectors.
- The United States suffered the highest number of attacks from ransomware groups and other threat actors.
- Following the US, the Government, Law Enforcement Agencies (LEA), and Banking, Financial Services, and Insurance (BFSI) sectors in India were targeted the most.
- Hacktivism threats due to volatile geopolitical scenarios grew more intense and widespread.
- Zero-day exploits targeting - Citrix NetScaler ADC, PaperCut, F5 BIG-IP, MOVEit, Ivanti EPMM, and WinRAR - were observed to be actively weaponized on cybercrime forums as well.
- Threat actors have increasingly started adopting new languages for malware development, including Rust, Go, and Nim.
- Deception-based attacks have seen a notable increase through the use of SEO poisoning, malvertising, QR Codes, and open-source package supply chain attacks.
- Emerging threats appear through new attack vectors leveraging Python-based malware, PowerShell, and Android-centric malware.
- Multiple major world events have played a part in the brewing of a highly volatile threat landscape, offering a complex playground for Threat Actors to disguise their malicious activities.

Persistence in Underground Threat Activities –**An Evolution from 2023 towards 2024**

Threat activities on underground forums and marketplaces were followed by the preset of seizures and arrests by law enforcement agencies. On March 15, 2023, the Threat Actor (TA) and founder of the notorious cybercrime platform BreachForums at breached[.]vc, "**pompompurin**", was reportedly arrested.

Following the reports of arrests, the other administrator, **Baphomet**, announced the closure of BreachForums on their Telegram channel on March 21, 2023. Three months after shutting down, on June 23, 2023, the clearnet domains for BreachForums were seized by the Federal Bureau of Investigation (FBI).

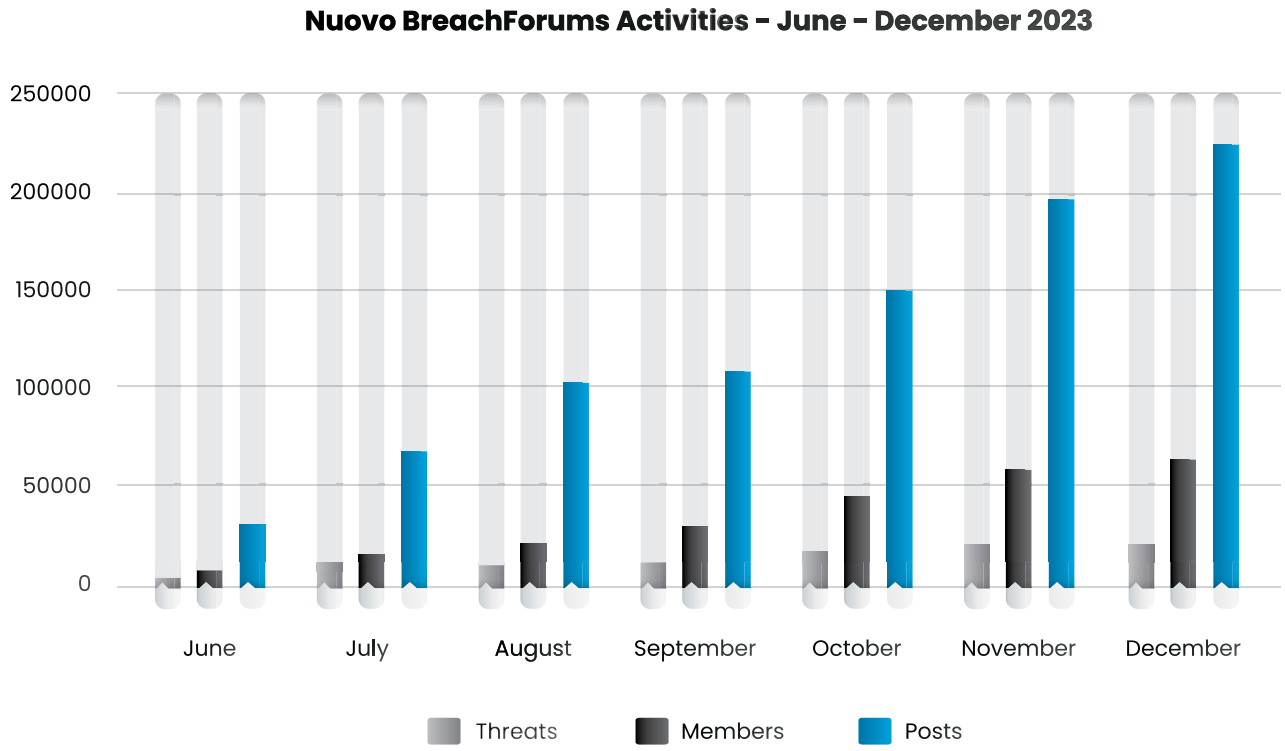
This closure once again gave threat actors and cybercriminals an impetus to establish their own cybercrime for-profit communities, like the previous RaidForums and BreachForums. Multiple cybercrime forums, including *PwnedForum, KKKSecForum, Ares, ExposedForums, Darkforums, OnniForums,* and *BlackForums,* were established by threat actors in an attempt to replace or continue the legacy of BreachForums.

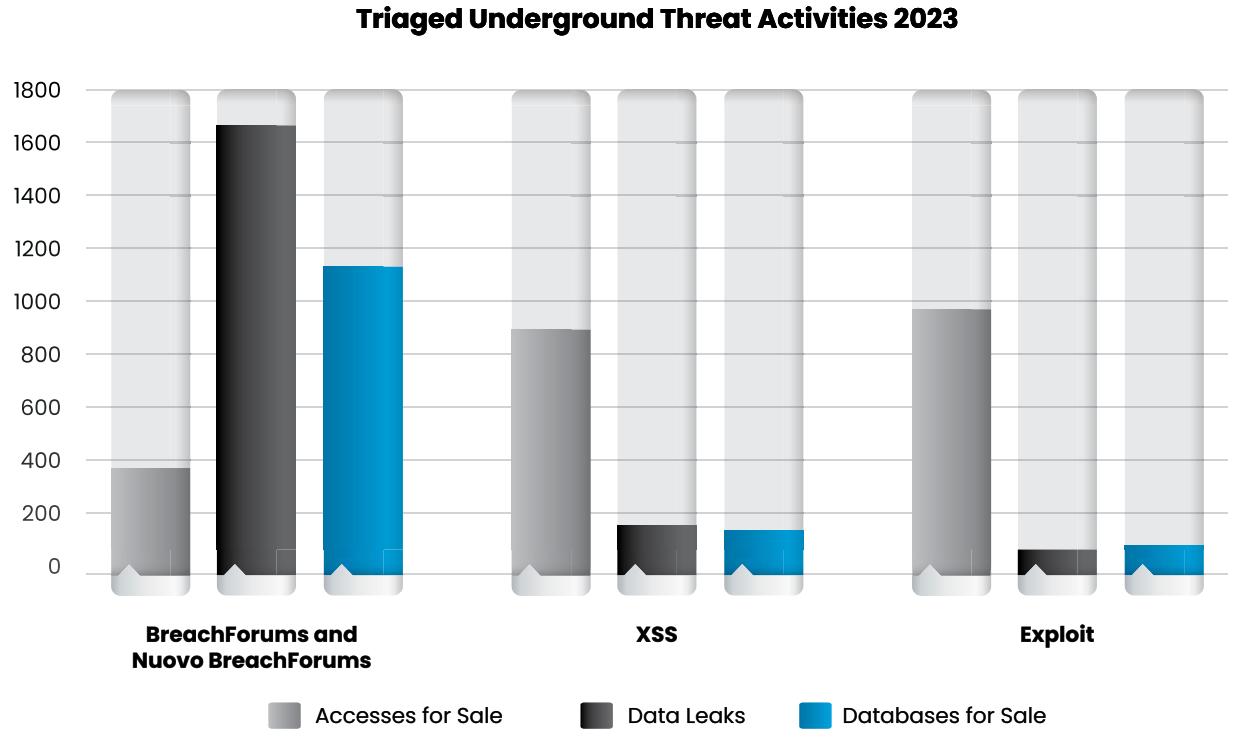
Due to the downfall of pompompurin's BreachForums, an exponential increase in the activities was observed on popular Russian-speaking forums, Exploit and XSS. On the other hand, a huge increase in re-circulation of compromised databases was observed on the Nulled, Sinisterly, and Cracked forums that were originally leaked on the seized forums.

On June 12, 2023, the threat actor group **ShinyHunters** launched "nuovo BreachForums" in an apparent collaboration with the administrator **Baphomet** of the now-defunct BreachForums. The appearance and layout design were kept identical to RaidForums and BreachForums to preserve their legacy.

During the first three months, nuovo BreachForums observed a gradual increase in the number of members joining the forum, with many of them distributing databases that were originally posted on the previous forums (RaidForums and old BreachForums). The group admins of these forums also leveraged tactics to orchestrate DDoS attacks on competing forums in order to gain dominance in the market.

In just a few months, the new forum established itself as a popular new channel for illicit activities. The forum members started posting new data containing leaked and stolen databases, documents, and compromised accounts. The forum currently has over 64k members and over 21k threads posted.





With a comprehensive picture of where these activities are being discussed with regard to cybercrime discussions and marketplaces for illicitly sourced information, we can now dive into the specific geographies and industries that the most prolific Threat Actors have targeted to gain this information over the past year to better understand their targeting priorities based on nations and sectors.

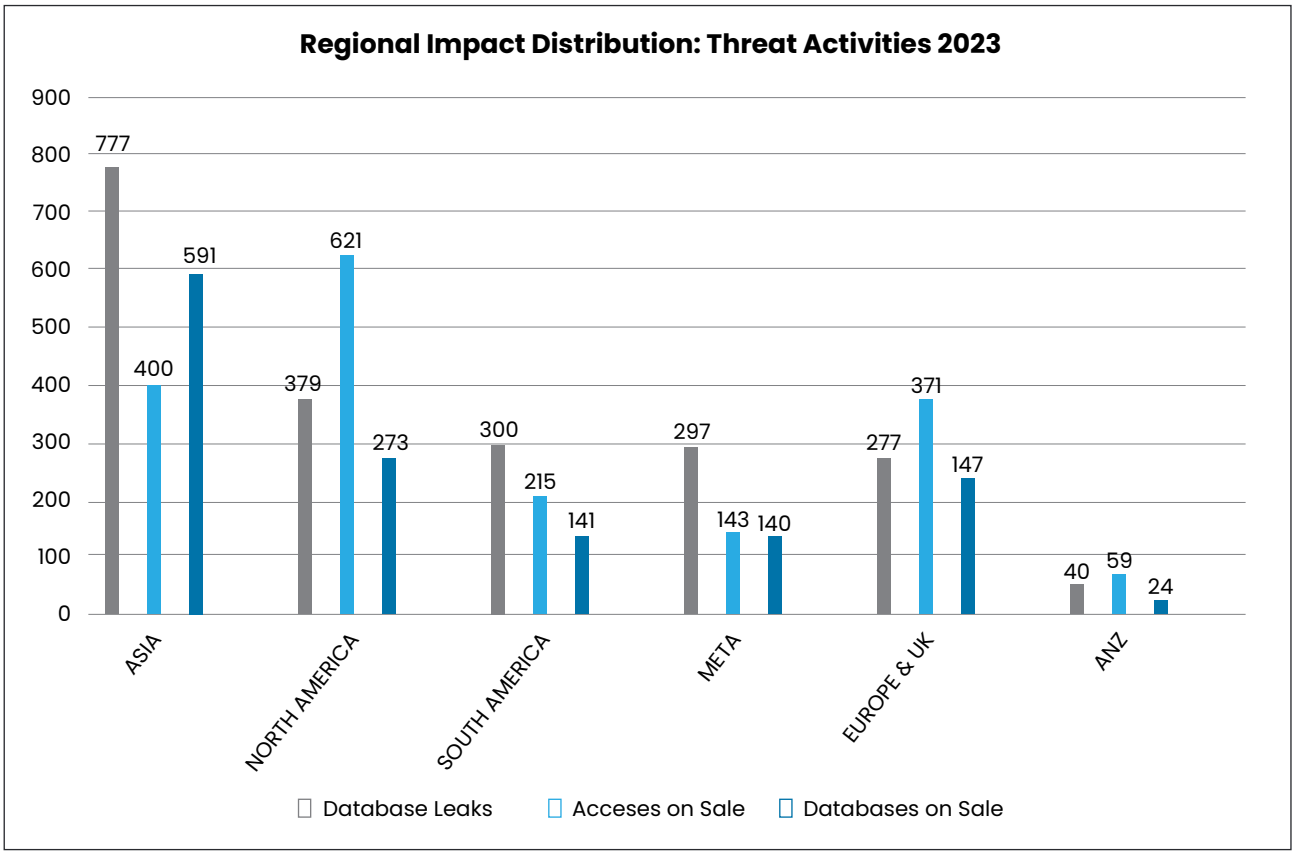
Threat **Activity Statistics**

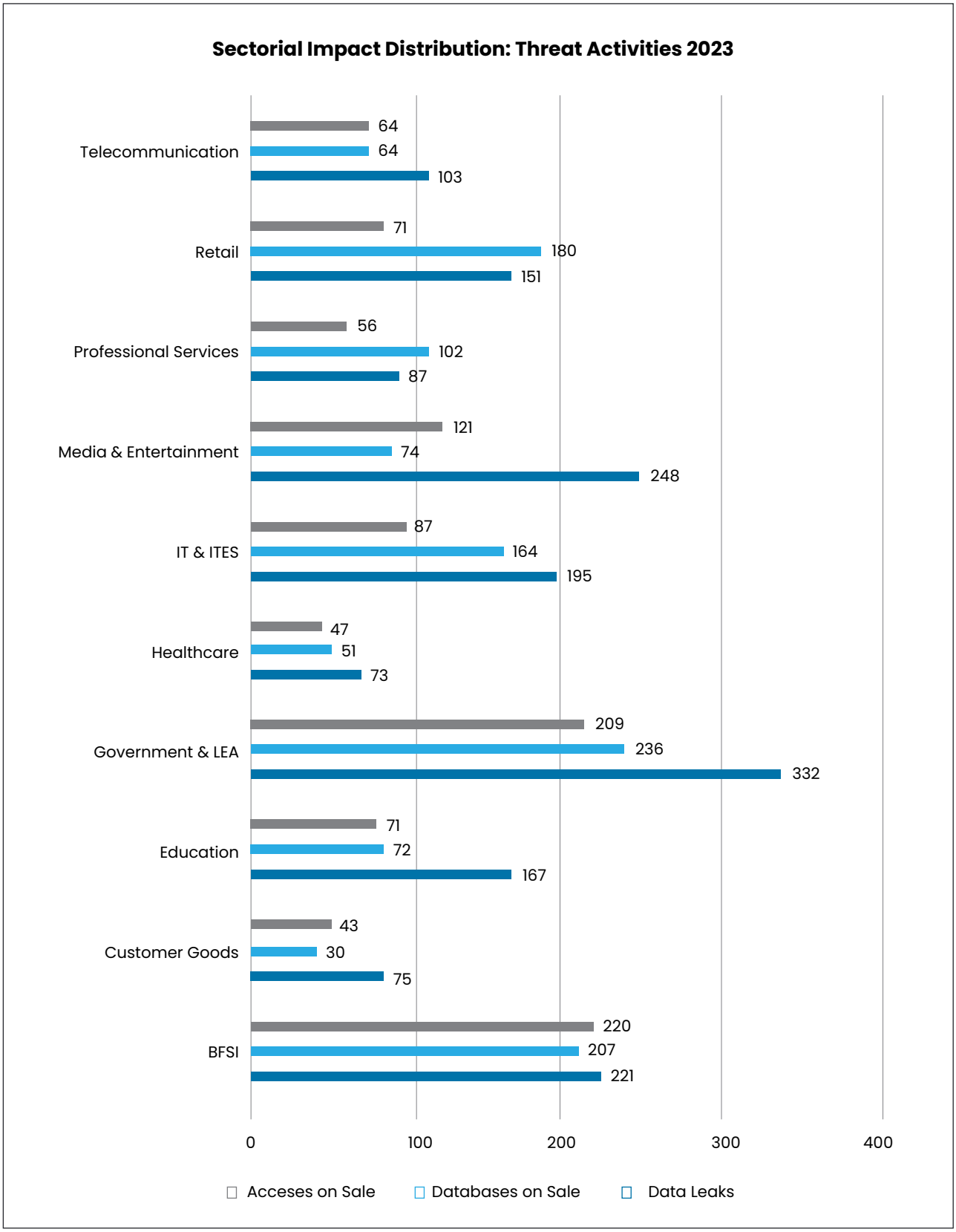
In 2023, CRIL (Cyble Research and Intelligence Labs) observed 7,219 incidents in cybercrime forums and channels that have impacted multiple organizations, including Critical Infrastructure, Government, and Law Enforcement Agencies.
Statistics revealed that 3,867 incidents were related to data breaches and compromised data put online for sale, and 2,355 incidents were related to the sale of unauthorized access on the forums. CRIL was able to determine that **Government, LEA, and BFSI were the most targeted sectors for 2023**.

Further statistical analysis into the most affected regions and countries in 2023 revealed 1,368 incidents of data breaches and leaks impacting organizations in Asia and 621 incidents related to the sale of unauthorized access impacting organizations in North America. In terms of country-wise targeting, the **United States and India were the most targeted countries** of all.

Cyber incidents in 2023 also uncovered multiple newly emerged threat actors on nuovo BreachForums, including **Ddarknotevil, cookiemonster,** and **g0d,** whose activities rose to prominence. TA **Leakbase** continued to compromise the data stolen from small or medium-sized businesses and leaked on their forum and telegram channel. **IntelBroker** and **threatbear** evolved to be the most impactful threat actors that targeted large corporations and monetized their stolen data.

While the overall incidents were slightly higher compared to 2022, we also observed that a few of the most active threat actors, such as **shadowhacker** and **Kelvinsecurity,** announced the end of their operations. **Kelvinsecurity** was reportedly arrested from Spain in December 2023.
As per the statistics that we observed, the most active Initial Access Brokers (IABs) were TA **Sqlety** on the Russian language cybercrime forum Exploit, followed by the TA **sandocan,** TA **stars4,** TA **Blackod,** TA **Darkbyte,** and TA **YYYXXX** on the cybercrime forum, XSS.





Now that we have a baseline for the most targeted regions and sectors let us take a look at the individuals and groups behind these illicit activities. In the following section, we will dive into specific Threat Actor profiles where we analyze them based on their activities, aliases and preferred targets based on sector and nations.

Notorious Threat **Actors of 2023**

Intelbroker

- Active Since: October 2022
- Alias: Nationalist, ATF
- Affiliation: CyberNiggers
- Forums: BreachForums, Nuovo BreachForums
- Activity: Access Broker/ Data Broker
- Targeted Sectors: BFSI, Telecommunication, Government & LEA, Consumer Goods, IT & ITES, Professional Services, Retail, Transportation & Logistics, Automotive, Food & Beverages, Healthcare, Hospitality, Aerospace & Defense, Education, Energy & Utilities
- Targeted Countries: Australia, Canada, France, India, Indonesia, Japan, Netherlands, Singapore, Spain, Sweden, Turkey, United Arab Emirates, United Kingdom, United States

threatbear

- Active Since: August 2022
- Forums: BreachForums, Nuovo BreachForums
- Activity: Access Broker/ Data Broker
- Targeted Sectors: Automotive, BFSI, Education, Food & Beverages, Government & LEA, Manufacturing, Professional Services, Technology, Telecommunication, Transportation & Logistics
- Targeted Countries: India, Japan, China, US, Singapore, South Korea, Nigeria, Paltestine, Malaysia, Germany, France, Spain, South Africa

Ddarknotevil

- Active Since: October 2023
- Forums: Nuovo BreachForums
- Activity: Access Broker/ Data Broker
- Targeted Sectors: Retail, Education, Media & Entertainment, BFSI, Government & LEA, IT & ITES, Consumer Goods, Healthcare, Organisation, Professional Services, Technology
- Targeted Countries: Saudi Arabia, France, Spain, US, India, Türkiye, Greece, Italy, Egypt, Netherlands, Angola, Brazil, Oman, UK, Israel

dawnofdevil

- Active Since: November 2023 - Present
- Forums: Nuovo BreachForums
- Activity: Access Broker/ Data Broker
- Targeted Sectors: Aerospace & Defense, BFSI, Government & LEA, Healthcare, IT & ITES, Media & Entertainment, Technology, Telecommunication
- Targted Countries: India, Mexico, Puerto Rico, Taiwan, Thailand, United States, Vietnam

Sanggiero

- Active Since: August 2022 - Present
- Forums: Exploit, Nuovo BreachForums
- Activity: Access Broker/ Data Broker
- Targeted Sectors: Transportation & Logistics, Media & Entertainment, Manufacturing, Hospitality, Food & Beverages, Education, BFSI, Retail, Professional Services
- Targeted Countries: India, United States

Big-Bro

- Active Since: December 2022 - Present
- Forums: Exploit
- Activity: Access Broker
- Targeted Sectors: Education, BFSI, Multiple, Media & Entertainment , Retail, Government & LEA, Transportation & Logistics, Energy & Utilities, IT & ITES
- Targeted Countries: United Arab Emirates, United States, Germany, Sweden, Netherlands, Ecuador, South Korea, Canada, Switzerland, Qatar, Brazil

budda12

- Active Since: October 2017 - Present
- Forum: Exploit
- Activity: Access Broker
- Targeted Sectors: Automotive, BFSI, Consumer Goods, Food & Beverages, Government & LEA, Healthcare, Hospitality, IT & ITES, Media & Entertainment , Pharmaceuticals & Biotechnology, Professional Services, Retail
- Targeted Countries: Indonesia, Malaysia, US, India, Chile, South Africa

Blackod

- Active Since: July 2023 - Present
- Forums: XSS
- Activity: Access Broker
- Targeted Sector: Aerospace & Defense, IT & ITES, BFSI, Media & Entertainment, Education, Telecommunication, Manufacturing, Professional Services, Technology
- Targeted Countries: US, France, Vietnam, India, Malaysia, Brazil, UK, Thailand

0xCee

- Active Since: December 2022
- Forums: Exploit
- Activity: Access Broker
- Targeted Sectors: BFSI, IT&ITES, Retail, Government&LEA
- Targeted Countries: Kenya, Qatar, UAE, Indonesia, India

With a comprehensive picture of where these activities are being discussed with regard to cybercrime discussions and marketplaces for illicitly sourced information, we can now dive into the specific geographies and industries that the most prolific Threat Actors have targeted to gain this information over the past year to better understand their targeting priorities based on nations and sectors.

Threat Actors to **Watch Out for in 2024**

Threat Actor	Summary	General Tactics, Techniques and Procedures (TTPs)
Blackod	TA Blackod joined the Russian cybercrime forum, XSS, in July 2023 and gained attention when they offered VPN access to a major technology company. The TA has now emerged as a prolific initial access broker and continues to operate privately to offer accesses in bulk.	• Leverages web-scanning tools to extract the IP addresses hosting the VPN service. • Developed scripts to launch brute-force attacks on the collected IPs from several remote machines.
dawnofdevil	TA dawnofdevil joined nuovo BreachForums in November 2023 and gained attention by offering databases and unauthorized access to an Indian banking organization. The TA targeted multiple Indian government entities along with a few private entities based in India, Thailand, Taiwan, and the United States.	• Utilizes the Metasploit framework to target organizations by leveraging open-source exploit scripts. • Sends phishing emails attached with documents embedded with macro-based exploit payloads as an attack vector for gaining an initial foothold in targeted networks. • Research suggests that the TA was collaborating with other threat actor groups and may opt for data extortion methods in 2024.
IntelBroker	TA IntelBroker joined BreachForums in October 2022. The TA claimed to be a founding developer of the alleged Endurance wiper-cum-ransomware. The TA initially targeted organizations in the United States. However, their threat activities expanded, impacting East Asia, Southeast Asia, Europe, and South American countries. The TA recently joined the CyberNiggers group and continues to be an active collaborator in compromising organizations.	• TA was seen extorting data and then demanding ransom after the successful deployment of the 'Endurance ransomware'. • Recently, the TA was observed to have resorted to target organizations that can lead to a diverse/supply-chain impact.
threatbear	TA threatbear was first observed on RaidForums selling databases stolen from various organizations. The TA has now emerged as a prolific data broker. Our research found that their historical activities share attribution to a notorious data seller, indicating that the TA has been active since 2021.	• Utilizes Sqlmap, an open-source tool, for discovering and exploiting SQL injection vulnerabilities in domains.
budda12	TA budda12 joined Exploit Forum in October 2017. The TA is known for their auction of initial accesses and has targeted multiple organizations in Indonesia, Malaysia, the United States, India, Chile, and South Africa.	• The TA has a positive reputation on the forum and is known for selling unauthorized accesses on the forum, typically related to Point of Sale (PoS) systems.

Ransomware is one of the most potent threats in cyberspace, with the last few years seeing ransomware attacks compromise a wide range of victims, from individuals to organizations and, in extreme cases, even entire governments and their various entities. In the sections that follow, we take a closer look at the state of Ransomware in 2023.

Ransomware Threats **at a Glance**

- Ransomware attacks in 2023 **nearly doubled** to around 4,200, as compared to around 2,200 in 2022.
- **Professional Services, Manufacturing,** and **Construction** sectors remained the most attacked sectors throughout 2023.
- Even though 2023 saw a rise in ransomware attacks against all industry sectors - **Healthcare, Transportation & Logistics,** and **Energy & Utilities** sectors faced some of the most brutal attacks.
- **LOCKBIT, ALPHV,** and **CL0P** were responsible for over 42% of ransomware attacks this year.
- Ransomware attacks spread across 117 countries around the world in 2023, with the **United States,** the **UK, Canada, Germany,** and **Italy**-based organizations accounting for 65% of total ransomware attacks.
- **32 new ransomware groups emerged in 2023** - Dark Power, DarkB!t, MortalKombat, Money Message, Nevada, Rorschach, Cylance, CROSSLock, RTM Locker, Dark Race, Dunghill, La Piovra, Trigona, NoEscape, Akira, Rancoz, BlackSuit, RA Group, Malas, CryptNet, Rhysida, 8Base, Obsidian ORB, Buhti, Cactus, INC Ransom, Metaencryptor, ThreeAM, Knight, Cyclops Group, and MedusaLocker.
- As predicted about possible future collaborations between APT groups and Ransomware groups, the prolific APT group Scattered Spider has been reported to synergize with the ALPHV ransomware group.
- Aggressive extortion mechanisms such as contacting the customers of victim organizations or filing SEC disclosures were adopted by groups such as Lorenz and ALPHV to further tarnish the reputation of organizations and pressurizing them to pay a ransom – thus establishing an audacious precedent of weaponizing cyber security regulations themselves, for their nefarious objectives.
- Ransomware groups such as LOCKBIT, ALPHV, 8Base, and CL0P launched and outrightly threatened Supply Chain Attacks.
- Ransomware groups continue to add evasion tactics and upgrade their ransomware variants to remain formidable, a trend we continued to observe in 2023. LOCKBIT, BlackByte, Royal, CL0P, IceFire, Qilin, ALPHV, Mallox, Akira, Trigona, Abyss, and Yashma were observed to be reorganizing their operations.
- Hive, RagnarLocker, and ALPHV ransomware operations **were seized as a result of coordinated LEA operations.** However, ALPHV resuscitated their operations and continued to torment businesses.
- Brand sustainability for ransomware groups is increasingly becoming more challenging due to declining ransom payments, increased enforcement actions by LEA, the cost of continued innovation to remain pertinent and evade detection, the disintegration of affiliate networks to launch their own services, and the emergence of small and stealthy groups that are ready to settle for less. Hence, existing ransomware groups like BianLian have changed their tactics to extortion from encryption.

Ransomware **Attack Vectors from 2023**

- Compromised accesses via Stealer Logs, Social Engineering, and Phishing remained the most common attack vectors employed by ransomware groups.
- Increasing use of AI for designing sophisticated targeted reconnaissance campaigns.
- Use of Living off the Land (LOLBins) techniques to avoid detection.
- The use of Active Directory discovery tools to enumerate systems and networks.
- Leveraging system tools to extract system details, including the hostname, operating system version, BIOS information, etc.
- Sophisticated and seemingly legit tools to disable Endpoint Detection and Response (EDR) processes, antivirus software, and erase log files.
- Exploiting vulnerable Managed File Transfer products.
- Increased use of automation to design exploits for recently reported or known vulnerabilities.
- DLL hijacking to execute ransomware binaries without detection.
- Hypervisor Jackpotting, involving attacking VMware ESXi hypervisors.
- HTTP tunneling to impersonate privileged services.
- Novel malware delivery techniques in different phases of attacks.

Every cyberattack has an attack vector, and Ransomware is no exception. While a plethora of techniques have been used to deliver Ransomware attacks and ensure that the targeted data is encrypted and compromised, there is a worrying pattern of leveraging vulnerabilities and exposed assets – a trend that has only seemed to intensify over the past year. The next section covers the major vulnerabilities we observed being leveraged by Ransomware gangs to carry out their attacks, as well as the specific regions and sectors where they were exploited.

Vulnerabilities Leveraged by **Ransomware Groups**

In 2023, there was a concerning trend observed as ransomware groups strategically targeted various Common Vulnerabilities and Exposures (CVEs), exploiting vulnerabilities within internet-exposed assets. A snapshot of vulnerabilities exploited by ransomware groups in 2023 is as follows.

CVE-2023-0669
Fortra
GoAnywhere MFT
Lockbit3.0 and Cl0P

CVE-2022-44698
Microsoft
Windows SmartScreen Security
Magniber

CVE-2023-28252
Microsoft
Windows Common Log File System Driver
Nokoyawa

CVE-2023-27532
Veeam
Veeam Backup & Replication component
Cuba

CVE-2023-34362
Progress
MOVEit
Cl0P

CVE-2023-20269
Cisco
Adaptive Security Appliance and Firepower Threat Defense
Akira and Lockbit3.0

CVE-2023-41266
Qlik
Sense
Cactus

CVE-2023-41265
Qlik
Sense
Cactus

CVE-2023-27350
PaperCut
NG/MG
Lockbit3.0, Bl00dy, Buhti and Cl0P

CVE-2023-46604
Apache
ActiveMQ
HelloKitty

CVE-2023-4966
Citrix
NetScaler ADC and Gateway appliances
Lockbit3.0

CVE-2022-47986
IBM
Aspera Faspex
IceFire

Ransomware Attacks **Across Geographies**

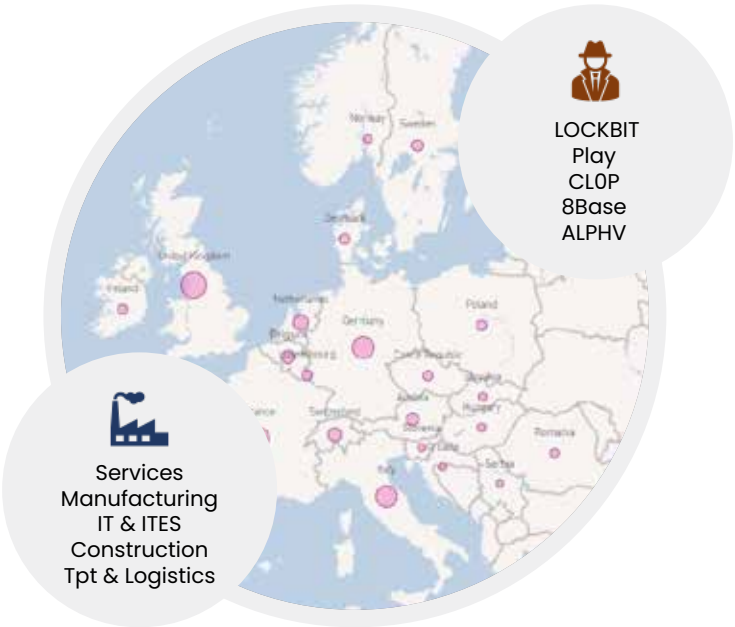
Americas, followed by Europe, faced the greatest number of ransomware attacks in 2023. Both regions accounted for over 70% of the attacks, followed by APAC.

AMERICAS

- The United States compromised of 46% of the victims in the Americas with Canada and Brazil being the next most targeted countries in the region.
- LOCKBIT, CL0P, and ALPHV were the most active groups in the region owning to the stringent breach disclosure regulations in the US.
- Professional Services was the most targeted sector, with IT firms being the second most impacted, leading to supply chain attacks.
- US law enforcement operations against cybercrime led to seizure and dismantling of nefarious Hive ransomware group infrastructure.

EUROPE & UK

- 60% entities targeted in the region have businesses in the UK, Germany, Italy, and France.
- The effects of stalemate in Russia-Ukraine conflict were observed with increase in cyberwar operations, and possible involvement of ransomware groups to target Critical Infrastructures across the region.
- EU Law Enforcement Agencies in a joint operation knock down the operations of RagnarLocker ransomware group, active since 2019.
- Active for a short duration in May 2023, Spanish-speaking Malas ransomware group mainly targeted Russian corporations.

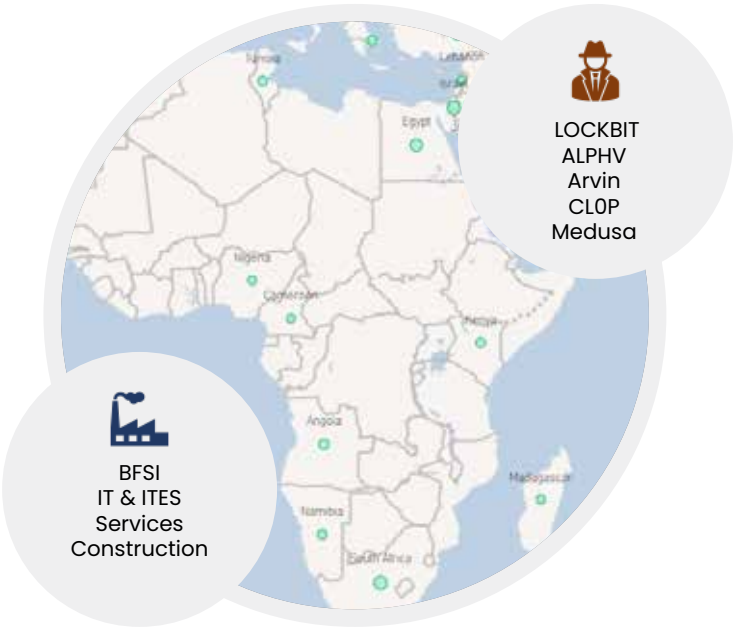


APAC

- Australia, India, and Indonesia were the most targeted countries in the region.
- Growing economies like Singapore, South Korea, Vietnam, Malaysia, Thailand, and Philippines drew increased attention of ransomware groups.
- Geopolitical tensions in South China and the possibility of a cyber war between China and Taiwan may lead to an increase in ransomware attacks in 2024.
- APAC region had victims spread over different countries with those of notoriety are the big banks and manufacturers from China, Taiwan-based Technology giants and Japanese conglomerates.

MIDDLE EAST, AFRICA & TURKEY

- The UAE, South Africa, Turkey and Israel contributed to over 50% of the victims from this region.
- The Arab nations continued to be the most impacted countries among the bunch, with LOCKBIT being a prominent player targeting Construction and Manufacturing firms.
- There is a sectoral shift in ransomware attacks towards BFSI and IT & ITES in the META region from earlier observed widespread attacks against the Manufacturing, Construction, Healthcare, Hospitality, and Food & Beverages sectors.
- Arvin Club ransomware emerged in the ransomware scenes again after a prolonged gap to primarily target Iranian entities.

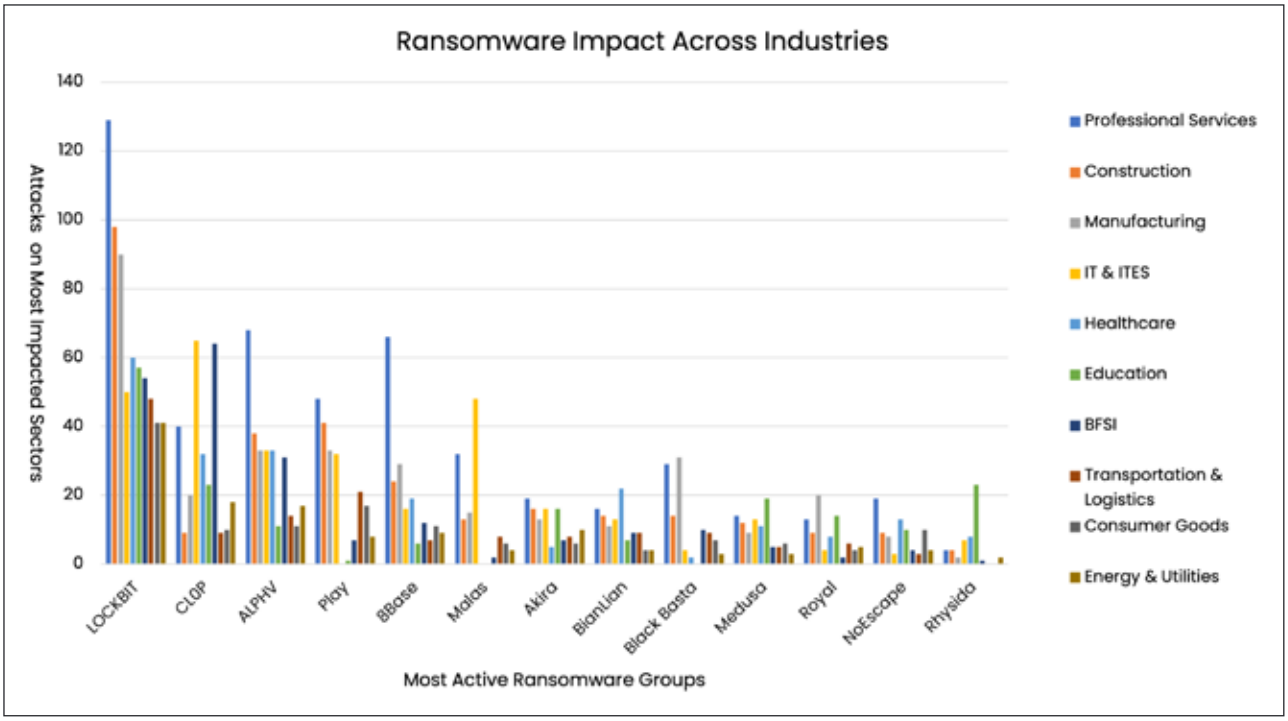


Ransomware Shift Across **Businesses & Critical Infrastructure**

The graph below highlights the most active ransomware groups and their sectoral distribution. The alarming trends and crucial findings from the industry standpoint are important to understand how the new ransomware threat landscape will emerge in the coming months.

- Newly emerged ransomware groups such as 8Base - a variant of Phobos ransomware - and Akira - from the shadows of Conti - emerged to be among the 10 most active ransomware groups.
- As predicted in our Q2-2023 Ransomware Threat Landscape Report, the **Transportation and Logistics** sector, being the most important sector in the value chain, suffered a 110% increase in ransomware attacks as compared to 2022. The Russia-Ukraine war and conflict in Gaza, alongside the state influence on several ransomware groups also could be a contributing factor to this precarious state of the industry.
- Companies involved in component manufacturing for the **Technology** industry, including those responsible for the production of Semiconductors, IoT devices and services, Industrial Automation, Smart Home Automation, Electronic supply chain, Data Centers, and Robotics, were aggressively targeted.
- Industries involved in the **Manufacturing** of critical components for several Critical Industries were vigorously targeted in the second half of 2023. The ransomware groups exfiltrated troves of technical data and blueprints from these companies that could be used for further exploiting the security gaps and launching component-level supply-chain attacks.

- Amongst **IT & ITES** sectors, the companies involved in developing and hosting specific applications and platforms supporting industries like Healthcare, Pharmaceutical & biotechnology, Energy & Utilities, Government, Transportation & Logistics, and BFSI also witnessed comparatively higher attacks.
- The **Banking, Financial Services, and insurance** institutions suffered 66% higher attacks this year; primarily in APAC and META regions.
- **Professional Services** companies involved in the physical security of Government, Aerospace & Defense, and Strategic National Assets also remained a lucrative target for ransomware groups.
- Ransomware Groups showed peculiar interest in **Healthcare** and **Pharmaceutical** companies involved in the research and development of advanced drugs, neuromodulation devices, natal healthcare equipment, and gene studies.
- The companies under the gambit of the **Energy & Utilities** sector, like those involved in Waterworks, providing Industrial Control Systems (ICS) and Operational Technology (OT), and Oil & Gas companies, suffered significant downtime and data loss due to ransomware incidents.
- The value-chain companies providing **Telecommunication** equipment, associated service sector contributing to the expansion of 5G infrastructure, and big-ticket Telecommunication Companies from the US, UK, Spain, India, Taiwan, Indonesia and Hong Kong saw an increase in ransomware attacks.
- **Automotive** sector component manufacturers from the US, UK, Germany, Japan, Taiwan, and China, manufacturing autonomous and connected devices, IoT components, electronic components, and chipsets, were also observed to be in the crosshairs of ransomware groups.



The cyber threat landscape often mirrors and is impacted by geopolitical events, even more so in the past year with two ongoing regional conflicts and an increase in cyber espionage, proxy warfare, and politically motivated Hacktivism that we have observed. The following section breaks down the impact of these geopolitical events and developments that have had a cascading impact on the threat landscape and the unique risks that have appeared from a cyber perspective.

Geostrategic Risks and **Ensuing Cyber Security Risks**

The geopolitical-verse in 2023 was highly volatile due to brewing cross-border conflicts, shifting trade boundaries, multi-polarization of world politics, and fear of yet another global recession. These events unfolded a new 'Squid Game' for the governments, businesses, and citizens to safeguard the world order from partial/total collapse. These incidents led to a parallel launch of 'Dark Squid Games' in the cyber-verse, offering a complex playground to states to guise their cyber incursions and to cyber-activists in advancing their propaganda.

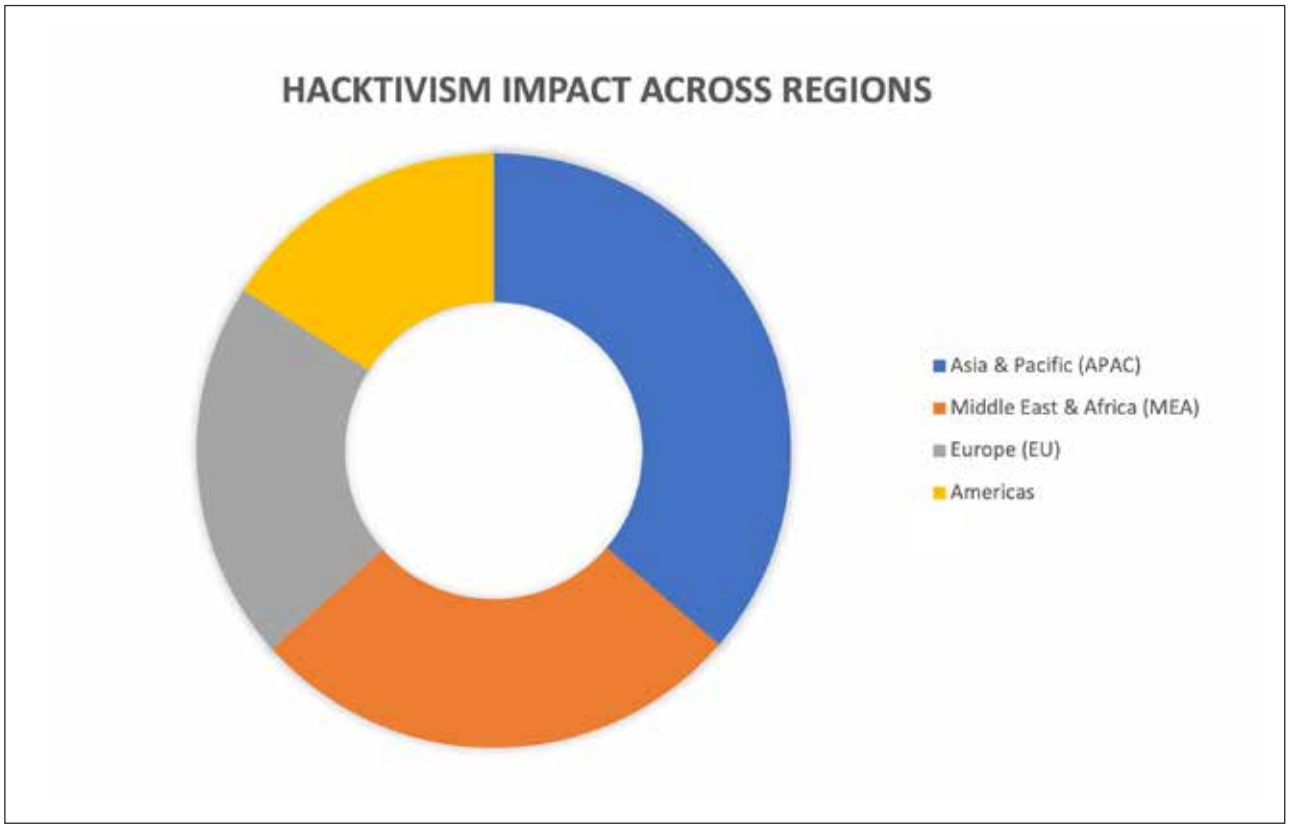
Let's flyby across these global events to decipher the cause and effect of cyber-verse incidents that emerged in hindsight:

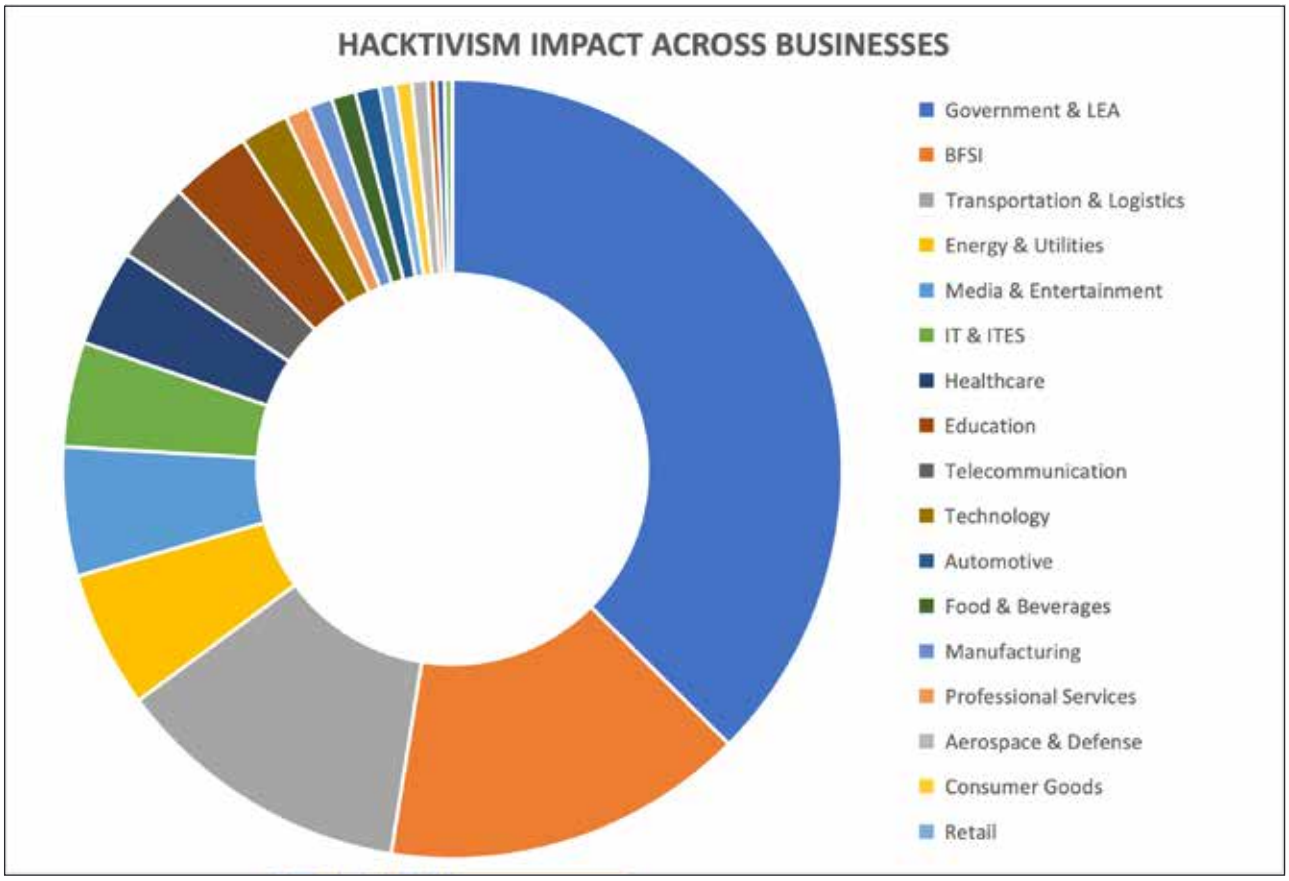
- **Russia-Ukraine Conflict:** The 600-day conflict does not seem to be ending anytime soon and has resulted in cyber escalations between both hostile nations. The situation has also been leveraged by several hacktivist groups since 2022, and the same trend continued in 2023 with prolific hacktivist groups such as Killnet, Noname, GhostSec, and Anonymous Sudan targeting allied countries from both sides.
- **Israel-Gaza Tensions & Ensuing Conflict:** Israel has been in the crosshairs of Hacktivists since the beginning of 2023, be it the Al-Aqsa Mosque incident or the Islamophobia propaganda against the country and, very recently, the Gaza conflict that led to the emergence of new hacktivist groups and others former groups to collectively overwhelm the Israeli websites and critical infrastructure. Over 250 threat groups tracked by CRIL have been involved in hacktivism-related incidents targeting both the warring countries and any countries that have not explicitly condemned the military actions by Israel, have also been targeted by these groups. Besides these, CRIL also noticed several groups sympathizing with the Hamas **ideology,** running propaganda campaigns against Israel and fundraising campaigns across several social media channels.
- **Sudan Civil War:** The outbreak of a civil war in Sudan in April 2023, and due to international condemnation of Sudanese military actions, the Hacktivist group Anonymous Sudan launched several attacks on French and American domains. They also launched overwhelming attacks on the Kenyan government and financial institutions.
- **Military Coup in Niger:** Following a military coup in Niger in July 2023, the Hacktivist Group Anonymous Sudan initiated attacks on Nigerian enterprises in retaliation to Nigeria's support to the Economic Community of West African States' (ECOWAS) anticipatory military response against Niger.
- **India Anchoring G20 Summit:** India hosted the G20 summit in September 2023, and to condemn India hosting this event, several hacktivist groups launched coordinated DDoS Attacks on over 3000 Indian domains comprising that of Indian government entities, national banks, educational institutions, media houses, and several other businesses.
- **Quran Desecration in Europe:** The Quran burning incidents in Denmark, Norway, and Sweden incited several hacktivism campaigns by groups like Anonymous Sudan, Hacktivist Indonesia, Mysterious Team, Team_insane_pk, and several other pro-Islamic groups against these countries. After a series of DDoS attacks in the Scandinavian region, Anonymous Sudan continued to target Sweden-based Scandinavian Airlines, SAS and demanded a ransom of USD 175,000 to stop the attacks.
- **Volatility in the Middle East:** Be it the Yemen situation, skirmishes with Iran, or the ongoing conflict in Gaza, hacktivists were observed carrying out numerous cyberattacks on government organizations, financial institutions, telecommunications companies, media outlets, and retail organizations in Saudi Arabia, the United Arab Emirates, Bahrain, Egypt, Qatar, and Kuwait.
- **US Anti-transgender Legislations:** SiegedSec carried out DDoS attacks and leaked compromised data from the City of Fort Worth, Texas, in June 2023. The hacktivist group launched their attack to show their solidarity with the state-wide protests against the anti-transgender legislation in Texas.

- **Australian Fashion Show Row:** A fashion show in Australia in March 2023 displaying clothing lines in Arabic texts referring to Allah incited Mysterious Team Bangladesh to target the Australian government, banking, and several other entities under the Opsjentik campaign.
- **Japan-Israel Cybersecurity Cooperation Agreement:** The hacktivist group GhostClan in retaliation to the Japan-Israel cybersecurity cooperation agreement announced in February 2023, claimed hacking 18 Japanese websites, including government websites.
- **Japan Expands Embargo on Russia:** In another incident, pro-Russian hacktivist group NoName targeted Japanese organizations, including railway services, in retaliation to Japanese sanctions against Russian individuals and organizations.
- **Arrest of Colombian Hacker:** In the aftermath of the arrest of threat actor "Org0n" by Colombian law enforcement in May 2023, various hacktivists voiced their resentment by actively participating in #OpColombia and #FreeOrg0n propaganda campaigns. Significant being SiegedSec hacktivist group's operations against various Colombian entities, including 30 radio broadcasts and 8 government-affiliated satellite receivers, internet-exposed Industrial Control Systems (ICS) components, Power Supply Controllers and Fuelling Systems in Colombia.
- **Rohingya Refugee Crisis:** Following the exodus of the Muslim ethnic minority group, Rohingyas from Myanmar due to the internal conflict to safer havens in Southeast Asia in Indonesia and Bangladesh, several pro-Indonesian and pro-Bangladeshi hacktivist groups targeted the United Nations, Red Cross, and other institutions to highlighting their inability to contain the situation.

CRIL analyzed hundreds of Hacktivism incidents across the globe in 2023 by several Hacktivist groups and their motivations to assess their impact on different continents and businesses. The graphs below highlight that APAC, followed by the Middle East due to multiple dynamics in play were the most affected regions.

The economic impact of these incidents, besides the Government & LEA being the obvious targets of these propagandistic activities, was evident in key economic catapults such as BFSI, Transportation & Logistics, Energy & Utilities, and Media enterprises.





APT groups comprise some of the most potent threats in cyberspace, with state-backed machinery enabling a high degree of sophistication, scale, and motivation, empowering these adversaries with funding, know-how, and capabilities. The following section dives into the various APT campaigns that were observed in 2023 and their resultant impact.

APT Campaigns **in 2023**

An Advanced Persistent Threat (APT) denotes a highly sophisticated and long-lasting cyber assault executed by adept adversaries, frequently backed by states or well-funded entities. These threats utilize advanced methods like tailored malware, exploits for undiscovered vulnerabilities, and social engineering, enabling them to operate persistently without detection. We have compiled some Important APT activities of 2023 in this section.

- In March 2023, CRIL reported[1] that SideCopy set its sights on DRDO using a DLL Sideloading attack. The typical approach of SideCopy APT includes the use of malicious LNK files to kickstart an intricate infection chain, employing various HTAs and loader DLLs, ultimately resulting in the deployment of final payloads.
- On April 18, 2023, UK and US cybersecurity and intelligence agencies reported[2] that the Russian nation-state actor APT28 employed a patched remote code execution vulnerability in Cisco network appliances for espionage and malware deployment. APT28 took advantage of an outdated vulnerability, identified as CVE-2017-6742[3], which is a remote code execution vulnerability in Cisco IOS and IOS XE software.
- On May 09, 2023, CISA issued an advisory[4] outlining the measures to dismantle the Snake malware infrastructure which is developed and employed by Center 16 of Russia's Federal Security Service (FSB), also known as Turla.
- On June 01, 2023, CRIL shared details of a campaign[5] orchestrated by SharpPanda APT, specifically targeting high-ranking government officials from G20 nations. This attack employed a spearphishing email technique, which delivers a backdoor into the compromised system.
- On August 31, 2023, CISA and Five Eyes released a joint advisory[6], which highlighted Sandworm's use of Infamous Chisel to target Ukrainian military entities. This Infamous Chisel operates over the Tor network, provides persistent access to Android devices, and collects sensitive information from the victim's Android devices.
- Higaisa APT resurfaced[7] via phishing site after 2021, posing as OpenVPN software customized for Chinese users. This malicious software allows Threat Actors to take control of the compromised system using a Go Compiled shellcode.
- Quietly conducting a sophisticated spying operation in the Middle East, Scarred Manticore, an Iranian cyber threat group associated with MOIS (Ministry of Intelligence & Security), was revealed[8] by Checkpoint on October 31, 2023. Employing their latest malware tools framework, LIONTAIL, the APT group successfully operated discreetly for over a year.
- On November 1, 2023, CRIL discovered[9] a new version of Android malware linked to DoNot APT, potentially targeting individuals in India's Kashmir region. The TAs behind this group have enhanced the capabilities of Android malware, including recording VoIP calls, collecting messages from various apps, and gathering diverse data types.

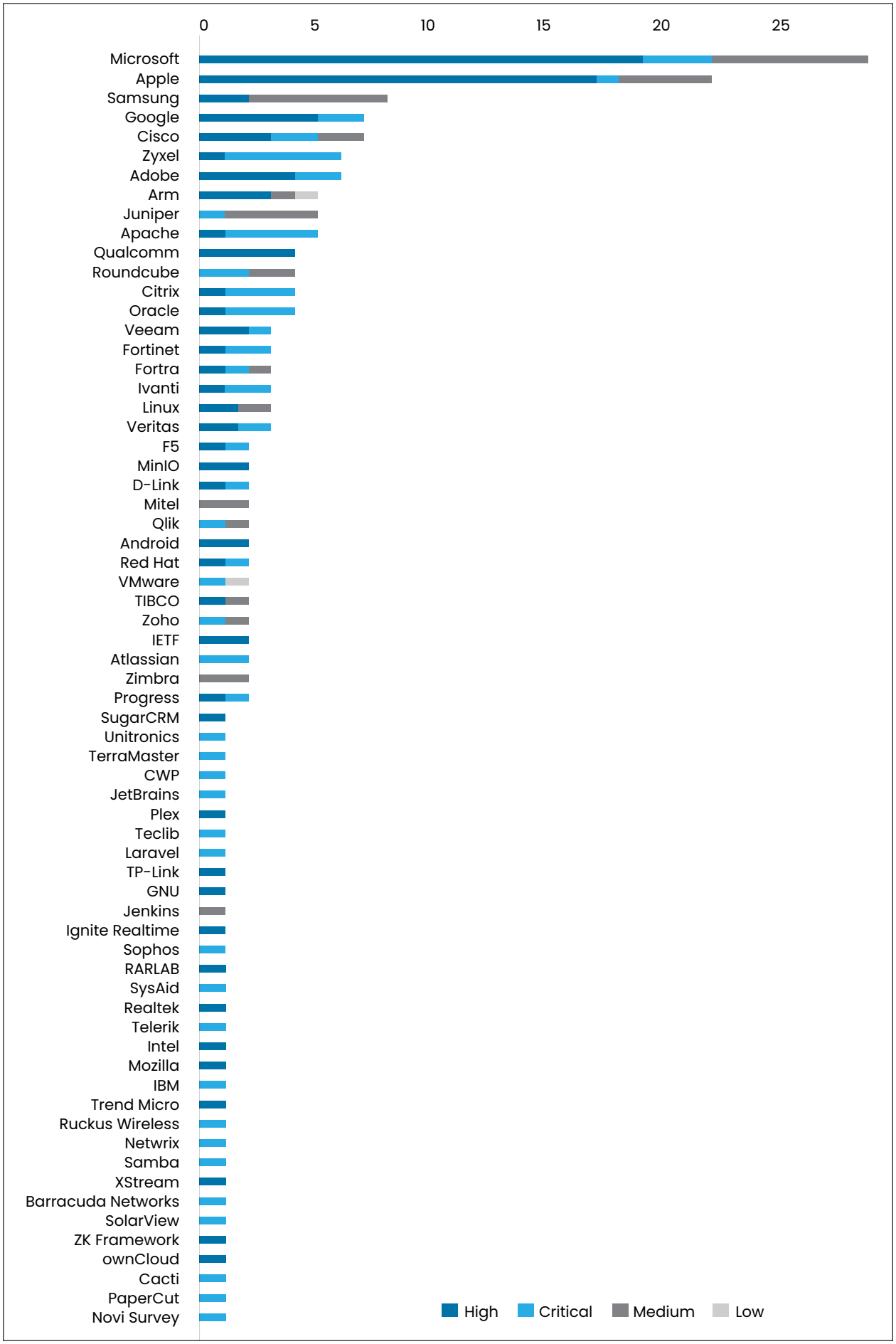
Vulnerabilities have always been a common vector for cyberattacks. As the world continues to digitize at a faster rate, the scope for exploitable vulnerabilities increases proportionally. In 2023, we observed a rise in major vulnerabilities in commonly used products and critical technologies that opened the door to cyberattacks. The following section details some of these vulnerabilities and how Threat Actors exploited and weaponized them in 2023.

1. https://cyble.com/blog/notorious-sidecopy-apt-group-sets-sights-on-indias-drdo/
2. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-108
3. https://nvd.nist.gov/vuln/detail/CVE-2017-6742
4. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-129a
5. https://cyble.com/blog/sharppanda-apt-campaign-expands-its-arsenal-targeting-g20-nations/
6. https://www.cisa.gov/news-events/analysis-reports/ar23-243a
7. https://cyble.com/blog/higaisa-apt-resurfaces-via-phishing-website-targeting-chinese-users/
8. https://blog.checkpoint.com/security/unraveling-the-scarred-manticore-saga-a-riveting-epic-of-high-stakes-espionage-unfolding-in-the-heart-of-the middle-east/
9. https://cyble.com/blog/donot-apt-expands-its-arsenal-to-spy-on-victims-voip-calls/

Lessons from the Past: **Vulnerabilities of 2023**

In the span from January 01, 2023, to December 11, 2023, public and private entities have observed Threat Actors weaponizing vulnerabilities to accomplish their illicit motives.

- In 2023, the rapid exploitation of CVEs has been evident, with threat actors being extremely quick to exploit their vulnerabilities of choice. Additionally, malicious threat actors continued the exploitation of vulnerable internet-exposed assets.
- The majority of ransomware attacks worldwide originated due to the exploitation of vulnerabilities within network devices and Managed File Transfer (MFT) applications.
- Analysis indicates diversity in the **193 CVEs that were actively exploited** by malicious actors, notably products from prominent vendors such as Microsoft, Apple, Samsung, Cisco, and Zyxel were under active exploitation in the year 2023.
- Out of 193 vulnerabilities actively exploited, **36 vulnerabilities were exploited by known attackers,** which included multiple ransomware groups.
- Threat Actors carried out mass exploitation targeting products from Vendors Progress, Citrix, Apache, and Atlassian.
- **Cl0P, Bl00dy, and Lockbit3.0** ransomware groups shared a common interest in exploiting MFT applications.


0
5
10
15
20
25
Microsoft
Apple
Samsung
Google
Cisco
Zyxel
Adobe
Arm
Juniper
Apache
Qualcomm
Roundcube
Citrix
Oracle
Veeam
Fortinet
Fortra
Ivanti
Linux
Veritas
F5
MinIO
D-Link
Mitel
Qlik
Android
Red Hat
VMware
TIBCO
Zoho
IETF
Atlassian
Zimbra
Progress
SugarCRM
Unitronics
TerraMaster
CWP
JetBrains
Plex
Teclib
Laravel
TP-Link
GNU
Jenkins
Ignite Realtime
Sophos
RARLAB
SysAid
Realtek
Telerik
Intel
Mozilla
IBM
Trend Micro
Ruckus Wireless
Netwrix
Samba
XStream
Barracuda Networks
SolarView
ZK Framework
ownCloud
Cacti
PaperCut
Novi Survey
High
Critical
Medium
Low

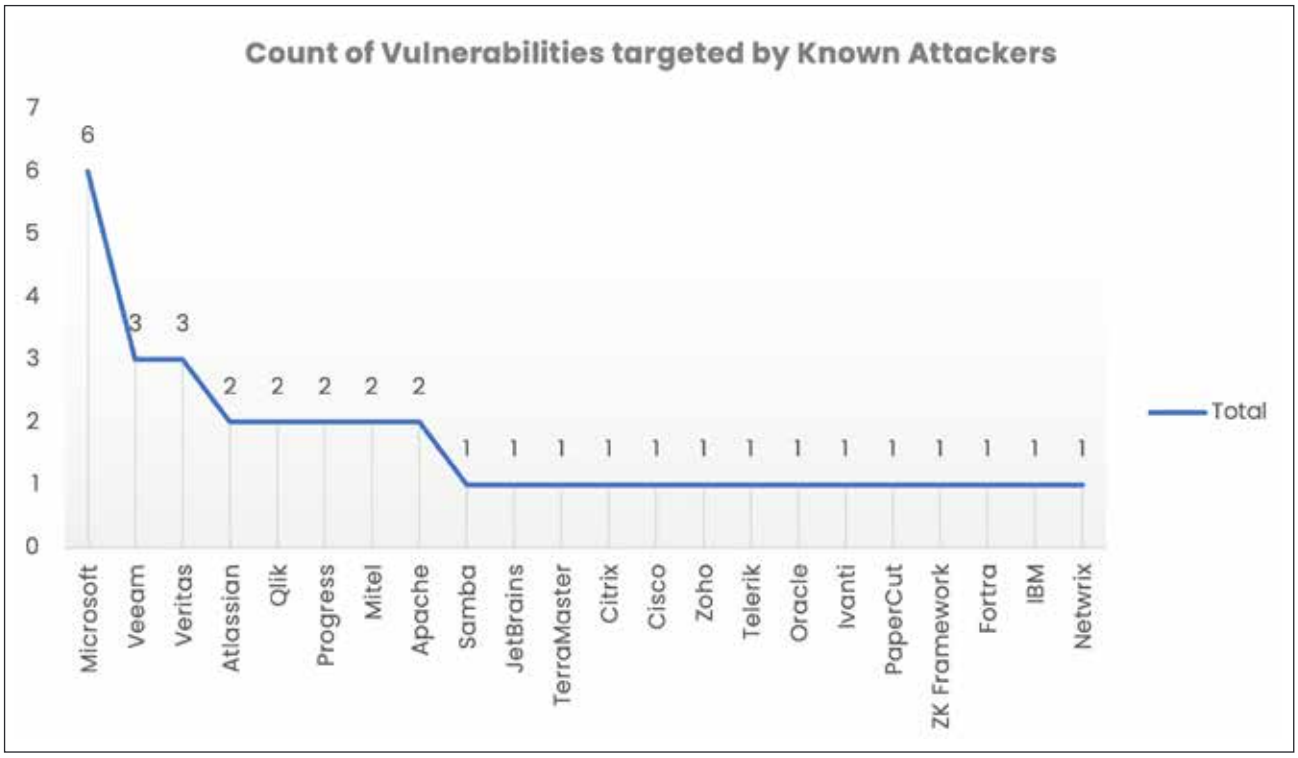
Known Exploited **Vulnerabilities**

In 2023, we observed that the majority of vulnerabilities targeted by Threat Actors were from two specific vendors – "Microsoft" and "Apple". With **network devices** and **Managed File Transfer Systems** being major vectors of exploitation for the TAs, vulnerabilities within **WinRAR** (CVE-2023-38831) and **Atlassian Confluence** (CVE-2023-22518) were also actively exploited.

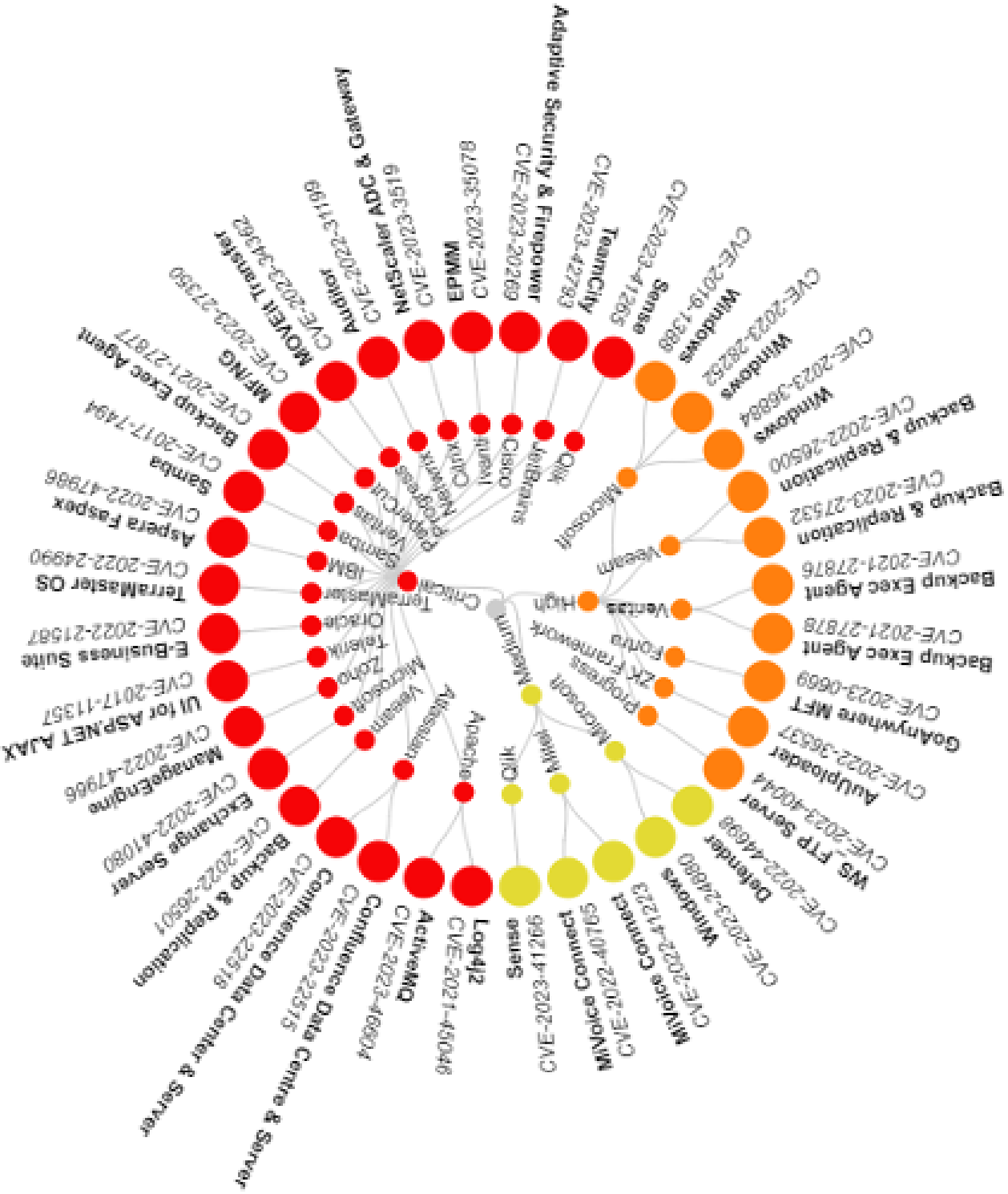
As illustrated in the graph below, the majority of vulnerabilities exploited by TAs fall under the **High severity (94 instances) category,** followed by the **Critical severity (62 instances) category**.

Vulnerabilities Leveraged by Known **Threat Attackers**

In 2023, Threat Actors demonstrated significant interest in several vulnerabilities, exploiting them to launch ransomware attacks globally. Displayed below is a visual representation illustrating the number of vulnerabilities across different vendors whose products were specifically targeted by known Threat Actors in 2023.



The image below highlights the Critical, High, and Moderate CVEs of vendors and products targeted by known attackers.



Weaponization of Major Vulnerabilities as seen on **Cybercrime Forums**

- Modified exploits of the Citrix Bleed vulnerability (**CVE-2023-4966**), impacting Citrix NetScaler web application delivery control (ADC) and NetScaler Gateway appliances, were shared by threat actors **cccp, TonyRzGz,** and **xai** on BreachForums and XSS. The vulnerability was also reported to be mass weaponized by ransomware operators, including RansomExx and LockBit 3.0.
- On its Telegram channel, the **BI00dy ransomware group** enquired about a working exploit for **CVE-2023-39143,** affecting PaperCut NG and PaperCut MF before 22.1.3 on Windows. In another instance, the same group leveraged the vulnerability, **CVE-2023-27350,** in PaperCut NG 22.0.5 to establish initial access to the network of an Indian educational institution. The vulnerability is on the radar of threat actors, and they are performing mass scans for vulnerable PaperCut Servers to perform large-scale attacks.
- Threat actor **0xCee** weaponized the F5 BIG-IP Missing Authentication Vulnerability (**CVE-2022-1388**) to gain unauthorized access to an African bank's infrastructure. The vulnerability is also listed in the top exploitable vulnerability list of 2022, released by CISA.
- In June 2023, the threat actors **johndoe7** and **LORD1** on XSS and Exploit offered a custom malicious script to exploit the Progress MOVEit Transfer vulnerability (CVE-2023-34362). In May 2023, the CL0P ransomware group targeted Progress Software's MOVEit Transfer, which is commonly used by organizations to manage file transfer operations. They exploited the SQL injection zero-day vulnerability (**CVE-2023-34362**) to infiltrate MOVEit Transfer web applications to obtain unauthorized access to stored databases.
- Threat Actor **NRO** on BreachForums was selling a zero-day exploit for **CVE-2023-35081** impacting **Ivanti EPMM** versions (11.10.x < 11.10.0.3, 11.9.x < 11.9.1.2 and 11.8.x < 11.8.1.2). This is a critical remote unauthenticated API access vulnerability, which allows remote attackers to gain access to sensitive information, add an EPMM admin account, and modify configuration via authentication bypass.
- We observed threat actors **d3vilHunt3r, AegisCrypter,** and **H4rDw4Y** on Exploit, XSS, and BreachForums offered exploits for **CVE-2023-38831** to target vulnerable **WinRAR** application before 6.23. The exploitation of this vulnerability was also seen being incorporated in White Snake Stealer.

Critical Infrastructure forms the backbone of any nation's industry, finance, security, and overall functioning, spanning Industrial Control Systems, Operational Technology, and other critical organs of a nation's production, economy, governance, and national security. Naturally, this makes this sector a particularly lucrative target for TAs and APT groups looking to compromise these key functions in an organization. The following section covers the attacks that we observed on Critical Infrastructure with a focus on how they occurred, the motivation behind them, and their impact.

Critical Infrastructure (CI) **Sector Threat Landscape**

Critical Infrastructure faced a spectrum of assaults, including exploitation of CVEs in ICS assets, DDoS attacks, ransomware attacks, physical breaches, and targeted attacks toward organizations operating within the CI sector.

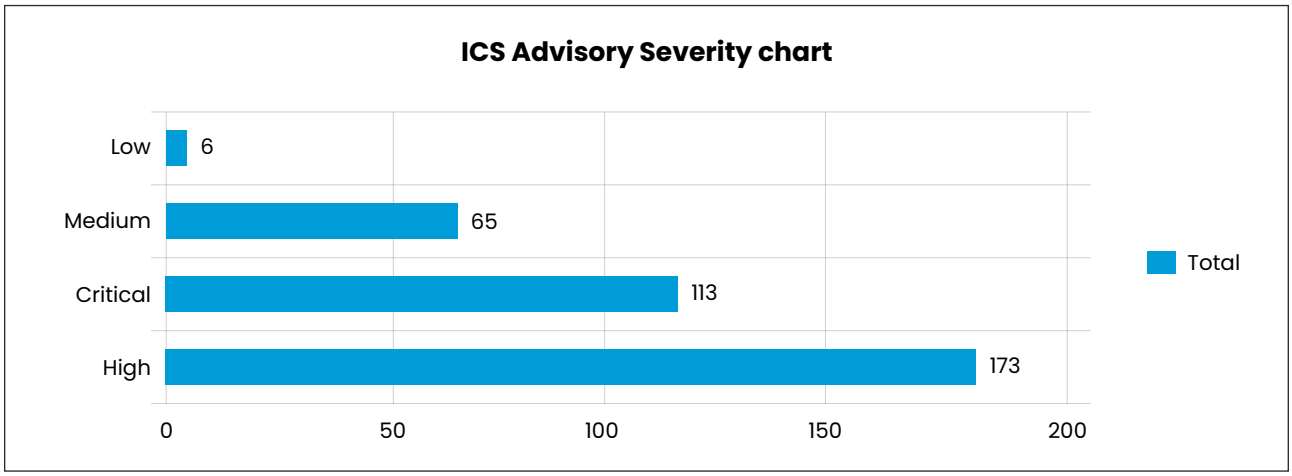
Below, we have listed a few incidents that highlight notable attacks toward the Critical Infrastructure sector:

- Geopolitical events continued to mold hacktivist attacks towards publicly exposed ICS assets such as Unitronics PLC, HMI, and SCADA systems connected via VNC, devices communicating via ICS-specific protocols.
- Volt Typhoon, a China-backed hacking group, targeted US critical infrastructure using living-off-the-land techniques. It was observed that the group achieved initial access to targeted organizations via internet-facing Fortinet FortiGuard devices.
- In May 2023, a coordinated cyber-attack targeted 16 Danish energy companies, utilizing the CVE-2023-28771 vulnerability in Zyxel firewalls, compromising 11 companies. The result was that the attackers gained access to some of the companies' Industrial Control Systems, and several companies had to go into "island mode operation", where an ICS network or component operates in isolation or independently from external networks or systems.
- In June 2023, a cyberattack hit Suncor, a major Canadian energy company, disrupting some services at its gas station chain Petro-Canada, leaving Canadian motorists unable to make gas transactions and electronic payments.
- The Canada Border Services Agency (CBSA) recently reported that the attack campaign was responsible for the intermittent connectivity issues that affected kiosks and electronic gates at airports on September 17, 2023.
- CRIL alerted the threat towards PV plants via internet-exposed PV monitoring solutions, such as SolarView, on July 5, 2023. Subsequently, Fortinet reported mass exploitation of the command injection vulnerability of SolarView. On July 13, 2023, CISA added the SolarView Compact Command Injection Vulnerability (CVE-2023-29303) vulnerability in their KEV catalogue indicating active exploitation.
- CRIL alerted exploitation of internet-exposed Unitronics devices that were targeted in the Al-Aqsa Mosque incident #OpIsrael. It was later observed that these same devices were targeted in the US to target Water and Wastewater Systems.
- In March 2023, CRIL investigated Global Navigation Satellite System (GNSS) receivers and Satellite Modem attacks launched by GhostSec and Ukraine-based hacktivists and provided insights on the vast attack surface of publicly exposed GNSS systems. It was observed that hacktivist groups continued targeting these assets in the year 2023.

Industrial Control System **Vulnerabilities Trend 2023**

From January 01, 2023, to December 11, 2023, CRIL analyzed Industrial Control Specific specific vulnerabilities published by the Cybersecurity and Infrastructure Security Agency (CISA) and observed that a collective of **116 vendors issued a sum of 357 ICS advisories**. The majority of vulnerabilities fall under the **High and Critical Severity category**.

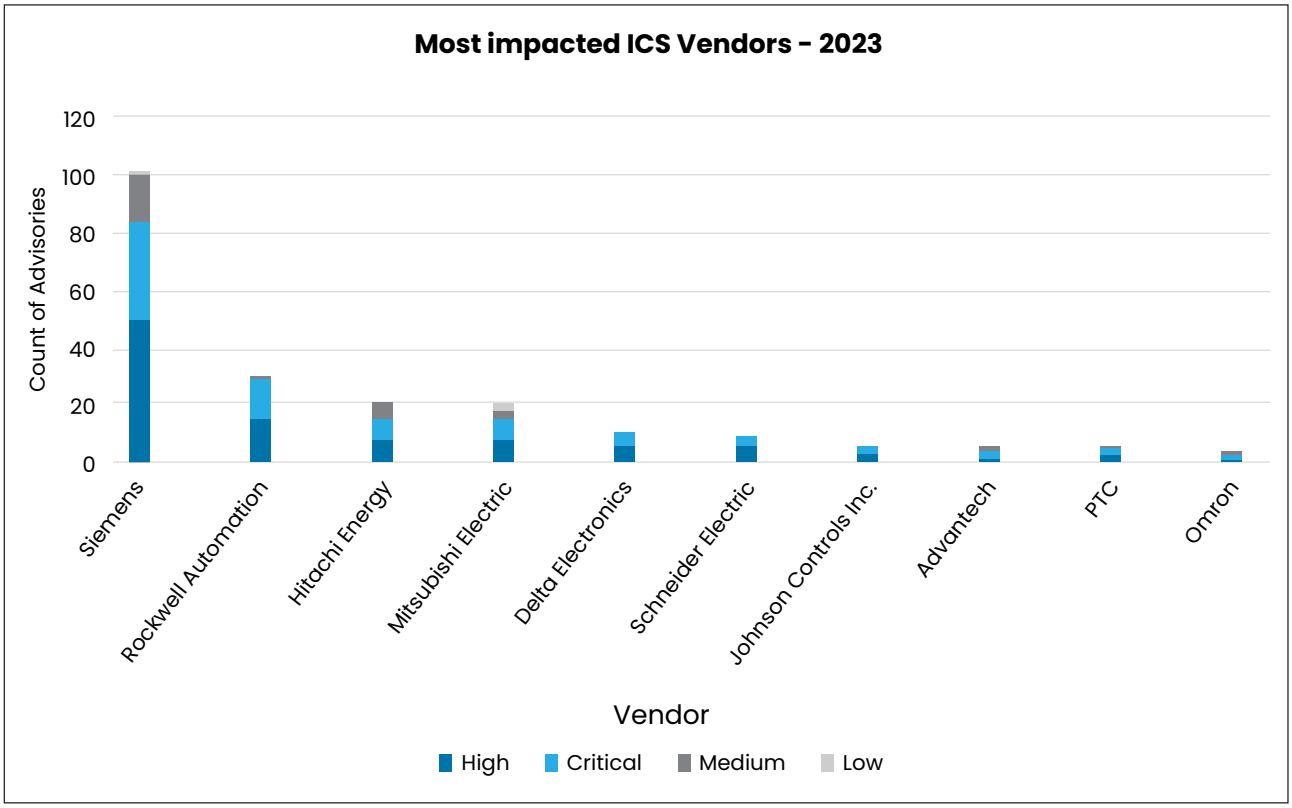
The graph below shows the severity of the following advisories released:



CRIL observed that the most vulnerable ICS assets for the year 2023 fall under the 3 categories given below.

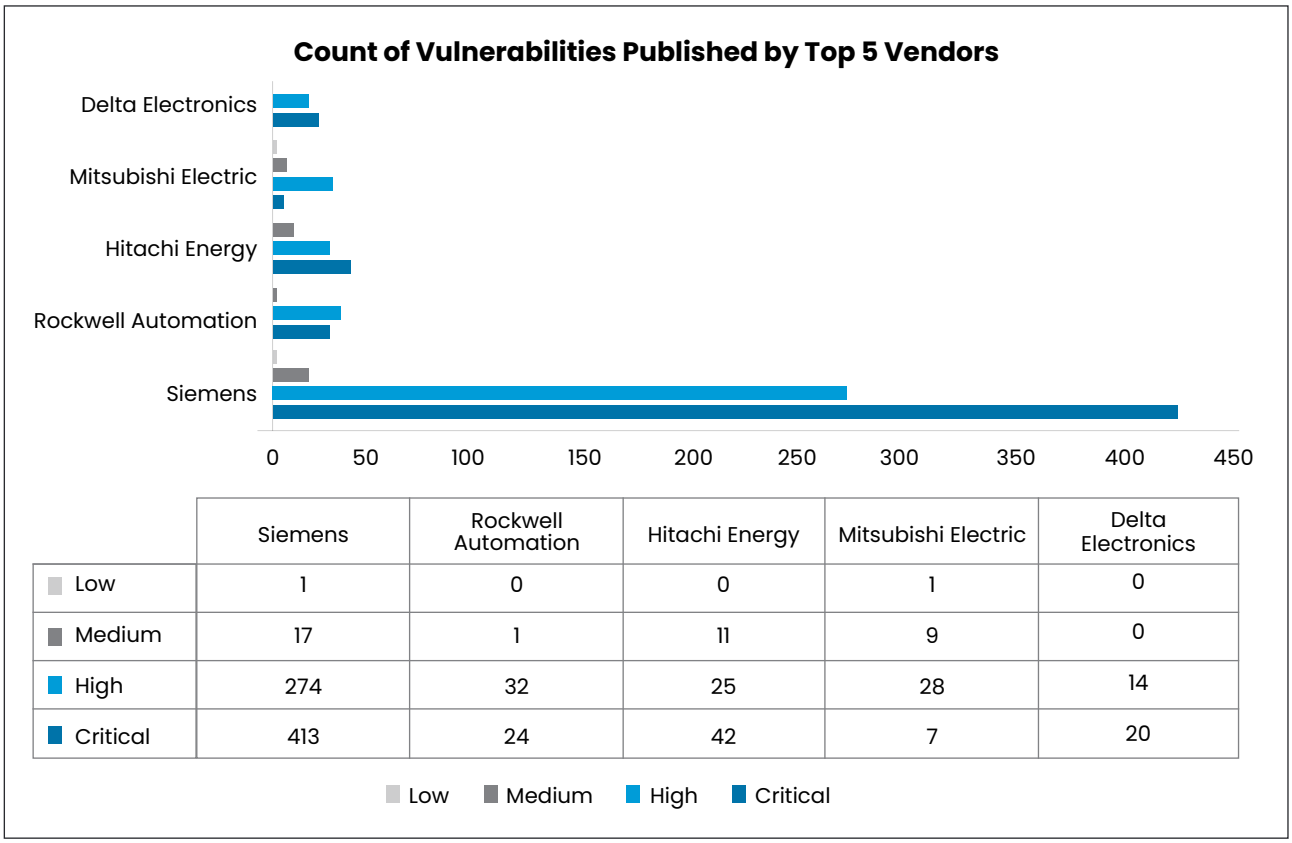
- Operation System (Manufacturing Execution System, Product Lifecycle Management, Energy Management System, Network Management System, Computerized Maintenance Management System, Enterprise Performance Management, Remote Sensing)
- Field Controller/Remote Terminal Units /Programmable Logic Controller/Intelligent Electronic Device /IoT Edge
- Switch/Wireless Access Point/Router/Gateway/Firewall/Remote Access/Process Communication Unit

CRIL observed that the majority of vulnerabilities disclosed in 2023 originated from vendors such as Siemens, Rockwell Automation, and Hitachi Energy. The bulk of the Critical and High Severity category vulnerabilities were reported by **Siemens and Rockwell Automation**. The graph below represents vendors that reported the most number of vulnerabilities.



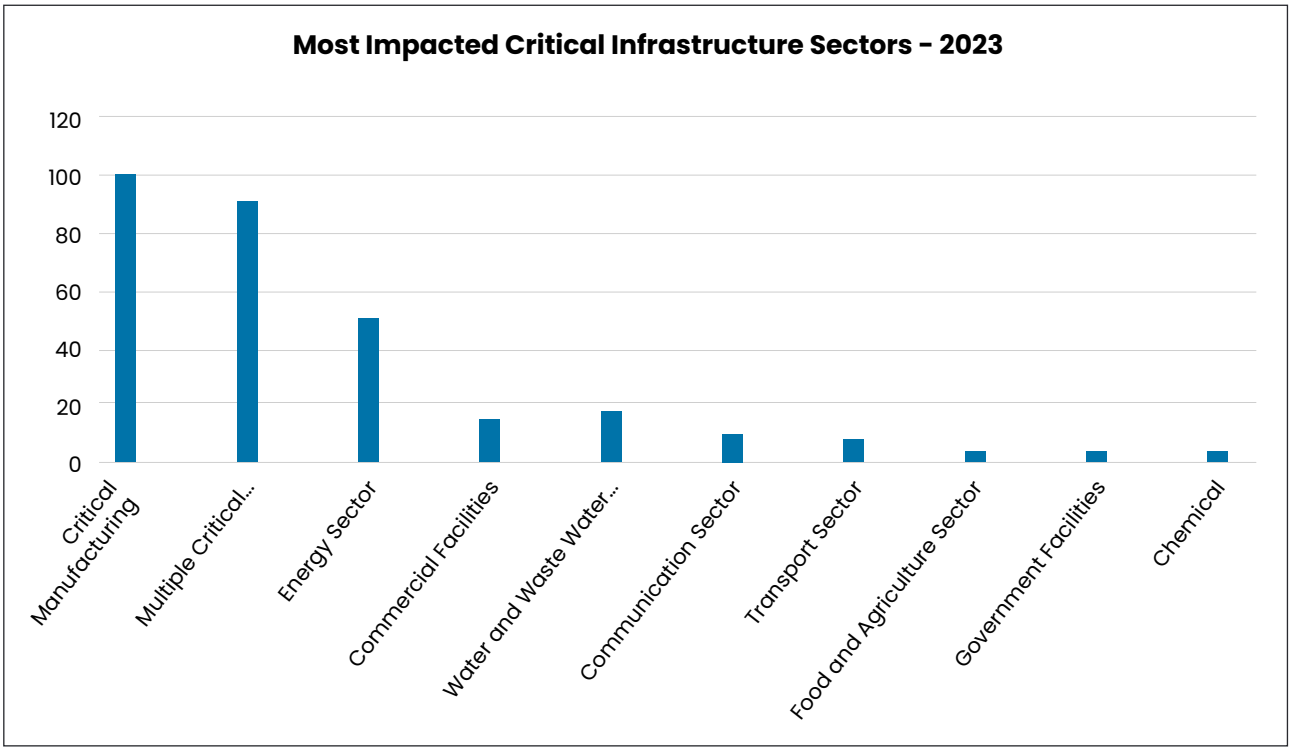
As per the analysis, it was observed that 1,342 vulnerabilities were published by CISA, out of which over 700 vulnerabilities covered vulnerabilities within Siemens alone.

The graph below depicts the count of vulnerabilities published by the Top 5 Vendors.



	Siemens	Rockwell Automation	Hitachi Energy	Mitsubishi Electric	Delta Electronics
Low	1	0	0	1	0
Medium	17	1	11	9	0
High	274	32	25	28	14
Critical	413	24	42	7	20

Analysis by CRIL researchers indicates that the vulnerabilities within ICS products are widely used in the **Critical Manufacturing, Multiple Sectors, and Energy Sector,** as shown in the graph below.



As individuals, organizations, government entities, and law enforcement continue to adapt their cyber threat posture to secure themselves against cyber threats, threat actors are also continuously refining their Tactics, Techniques, and Procedures to bypass these new measures and remain operational and relevant as cyber threats. The following section covers some of the ways Threat Actors modified existing malware, adopted new threat vectors, and leveraged emergent technology in an attempt to stay ahead of the global cybersecurity community.

Emerging **Threats**

In 2023, Threat Actors (TAs) expanded their toolkit to include languages such as **Rust, Go, and Nim,** diverging from the more conventionally used languages such as Microsoft Visual C++, C# .Net, and Java. This evolution reflects a strategic adaptation by adversaries, suggesting a desire to explore diverse programming environments to create malicious threats. The utilization of these alternative languages introduces new challenges for cybersecurity defenders, as it necessitates an understanding of unconventional techniques and behavior associated with these platforms.

The statistics below illustrate the surge in malware incidents associated with programming languages such as Go, Rust, and Nim in 2023 as compared to 2022.

Figure 1 - Increase in malware written in Go, Rust, and Nim in 2023 compared to 2022 (Source: VirusTotal)

With the increase of new languages being used in the development of malware, certain techniques became more obvious, which include:

- The use of "living off the land" commands in Rust-based malware, such as SysJoker[10]
- Data exfiltration attempts prior to encryption and deleting Volume Shadow copies by 3AM[11] ransomware.
- The targeting of specific technology, such as the case with GoTitan[12] exploiting Apache ActiveMQ and HinataBot[13], a Go-based variant of Mirai, targeting Realtek SDK, Huawei routers, and Hadoop YARN servers.
- Nim-based Kanti[14] ransomware was observed adopting a selective encryption strategy to keep systems operational for potential ransom payments.

In 2024, the cybersecurity landscape is anticipated to face a rise in sophisticated threats employing alternative programming languages such as Rust, Go, and Nim. These languages enable adversaries to develop more resilient and evasive malware, posing a challenge to traditional defense mechanisms.

A noteworthy trend has emerged in the realm of cybersecurity in 2023, where multiple malware instances have been crafted using **Python**. Notably, TAs are increasingly leveraging various **open-source** malware as foundational templates to create malicious threats. This approach allows them to customize and deploy malware with greater efficiency. Moreover, there is a discernible shift in the tactics employed for data exfiltration, with TAs incorporating popular messaging platforms such as **Discord** and **Telegram** alongside traditional exfiltration methods.

The statistics below illustrate the spike in malware instances linked with Python in 2023 as compared to the previous year, 2022.

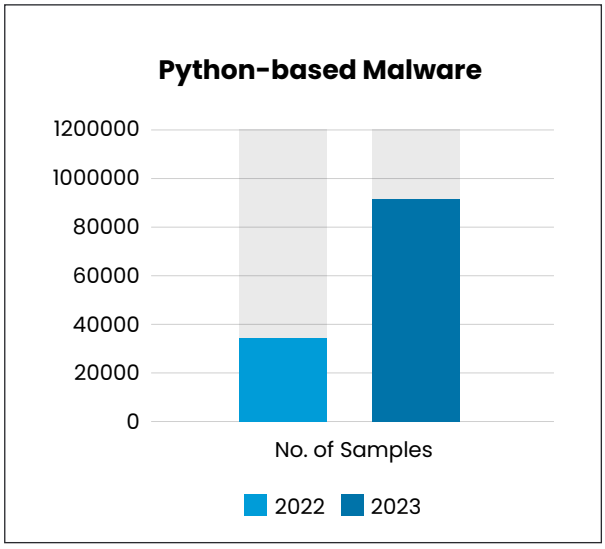


Figure 2 - Python-based malware rise in 2023 compared to 2022

Security researchers have identified a surge in Python-based malware, with examples like PY#RATION[15] RAT and Trap Stealer[16]. The former, distributed through phishing campaigns, is equipped with extensive capabilities such as network enumeration, keylogging, file

10. https://research.checkpoint.com/2023/israel-hamas-war-spotlight-shaking-the-rust-off-sysjoker/
11. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/3am-ransomware-lockbit
12. https://www.fortinet.com/blog/threat-research/gotitan-botnet-exploitation-on-apache-activemq
13. https://www.akamai.com/blog/security-research/hinatabot-uncovering-new-golang-ddos-botnet
14. https://cyble.com/blog/kanti-a-nim-based-ransomware-unleashed-in-the-wild/
15. https://www.securonix.com/blog/security-advisory-python-based-pyration-attack-campaign/
16. https://cyble.com/blog/new-open-source-trap-stealer-pilfers-data-in-just-6-seconds/

transfers, and detection of antivirus tools. Trap Stealer[17], constructed using an open-source builder, covertly extracts sensitive information like cookies and Discord tokens, with ongoing development efforts to optimize data exfiltration within a 6-second timeframe.

In September, a Python malware campaign[18] targeted Tatar language speakers, capturing screenshots using a PowerShell script and FTP for remote data transmission. CRIL also uncovered Exela[19] malware, utilizing Discord as a delivery mechanism with anti-debugging and anti-VM techniques. PySilon RAT[20], an open-source tool, is employed for advanced remote access, using Discord for Command and Control (C&C) while disguising itself through various software mimics. An emerging malware variant, Akira Stealer[21], disguises itself as free premium software, utilizing multi-level infection processes, obfuscation, and targeting financial data, uploading stolen data to gofile.io and Discord.

In 2024, the rise of Python-based malware, coupled with open-source malware, empowers TAs to efficiently customize and deploy sophisticated attacks. With advanced capabilities, these TAs increasingly leverage messaging platforms like **Discord** and **Telegram** for covert data exfiltration.

17. https://cyble.com/blog/new-open-source-trap-stealer-pilfers-data-in-just-6-seconds/
18. https://cyble.com/blog/tatar-language-users-in-the-crosshairs-of-python-screenshotter/
19. https://cyble.com/blog/exela-stealer-spotted-targeting-social-media-giants/
20. https://cyble.com/blog/emerging-threat-understanding-the-pysilon-discord-rats-versatile-features/
21. https://www.cyfirma.com/outofband/akira-stealer-an-undetected-python-based-info-stealer/

File Types Being Utilized in **Infection Flows**

In 2023, there was a notable surge in the strategic diversification of file types employed by TAs in their infection flows. TAs are increasingly utilizing LNK, BAT, CMD, and PowerShell to orchestrate sophisticated attacks. These files are exploited to conceal malicious payloads, adding to the complexity of their attack vectors.

Meanwhile, the versatile PowerShell scripting language remains the preferred choice for TAs, allowing for the download of malicious payloads, system reconnaissance, and lateral movement within networks. Previously, TAs employed Macros, VBS, JS, WSF, and various other scripts within the infection chain in their malware attacks.

The following data indicates a rise in the utilization of **LNK, BAT, and PowerShell** scripts within the infection chain of malware attacks in 2023, in contrast to the statistics from 2022.

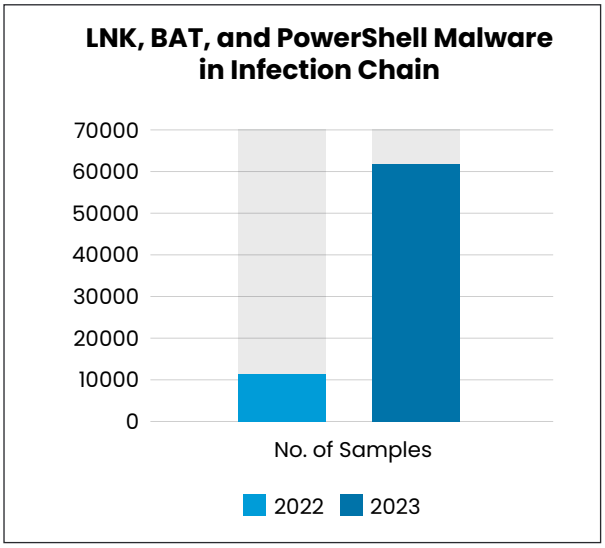


Figure 3 – Rise of LNK, CMD & PowerShell script usage in Malware attacks

Security researchers have uncovered evolving malware campaigns employing sophisticated code-based manipulation techniques. One identified[22] method involves exploiting an equation editor vulnerability in Excel documents to initiate a malware chain, utilizing PowerShell and steganography to conceal a .NET payload, and ultimately delivering a Remote Access Trojan (RAT) to the victim's system. In a separate instance, AgentTesla malware spread through spam emails featuring CPL[23] and CHM[24] files. These files executed PowerShell scripts, injecting the malware into system processes while employing obfuscated binary strings for concealment.

Mallox ransomware adopted a new approach, utilizing BatLoader in spam email attachments to deploy its new variant[25]. The infection involves obfuscated batch scripts and dynamic loading of the malware assembly using PowerShell injection techniques. Another campaign highlighted the dissemination of Apanyan Stealer[26] through adult websites, leveraging a WinRAR vulnerability to deploy malicious payloads, including a BAT file and additional malware like Murk-Stealer and AsyncRAT. Lastly, a PurpleFox[27] malware campaign utilized spam emails and steganography,

22. https://cyble.com/blog/threat-actor-employs-powershell-backed-steganography-in-recent-spam-campaigns/
23. https://cyble.com/blog/agenttesla-malware-targets-users-with-malicious-control-panel-file/
24. https://cyble.com/blog/agenttesla-spreads-through-chm-and-pdf-files-in-recent-attacks/
25. https://cyble.com/blog/mallox-ransomware-implements-new-infection-strategy/
26. https://cyble.com/blog/winrar-vulnerability-puts-illicit-content-consumers-at-risk-of-apanyan-stealer-murk-stealer-asyncrat/

employing VBA macros and PowerShell scripts to deliver an MSI payload camouflaged as a JPG file, unleashing malicious activities on victims' systems.

In 2024, cybersecurity professionals foresee a persistent trend in TAs utilizing a range of file types, including LNK, BAT, CMD, and PowerShell, to execute sophisticated cyber-attacks—a continuation of the patterns observed in 2023. The enduring prominence of PowerShell scripting is expected to continue, granting TAs the ability to carry out diverse activities within compromised networks.

Emergent technologies form a new frontier for individuals and organizations, and Threat Actors are no exception to that rule. With cyberspace constantly evolving, threat actors continue to innovate to target new technologies to increase their reach and target an even larger subset of potential victims. While Windows forms a large part of the overall connected systems in use, there is a growing trend of Threat Actors switching their focus to specifically target a rapidly growing user base of Android and Apple devices (particularly macOS). In the following section, we will discuss this pattern of targeting new technologies with specific examples.

27. https://cyble.com/blog/purplefox-resurfaces-via-spam-emails-a-look-into-its-recent-campaign/

New Technologies Being Targeted by **Threat Actors**

2023 has seen a concerning surge in sophisticated threats targeting the Android ecosystem. New malware players like Hook[28], FluHorse[29], and GoldDigger[30], along with entities such as Chameleon[31], Gigabud[32], GoatRat[33], and Enchant[34], highlight the diversity in the evolving threat landscape.

Tactics for distributing banking trojans through the Google Play Store have evolved, with Threat Actors (TAs) actively promoting "Dropper-as-a-Service" on underground forums. Despite Google's restrictions, a recent discovery unveils a novel threat named "SecuriDropper[35]," effectively outsmarting Android's restricted settings and emphasizing the persistent arms race. Zombinder, an earlier platform, has reemerged as a dropper, aligning closely with the innovative functionality observed in SecuriDropper.

The recent discovery of DaaS highlights the ongoing and dynamic nature of the threat landscape, emphasizing the pivotal role played by innovative dropper services. We anticipate witnessing new droppers successfully bypassing such restrictions in 2024.

28. https://www.threatfabric.com/blogs/hook-a-new-ermac-fork-with-rat-capabilities
29. https://blog.checkpoint.com/security/fluhorse-check-point-research-exposes-a-newly-discovered-malware-disguised-as-east-asian-legitimate-popular-android-apps/
30. https://blog.checkpoint.com/security/fluhorse-check-point-research-exposes-a-newly-discovered-malware-disguised-as-east-asian-legitimate-popular-android-apps/
31. https://cyble.com/blog/chameleon-a-new-android-malware-spotted-in-the-wild/
32. https://cyble.com/blog/gigabud-rat-new-android-rat-masquerading-as-government-agencies/
33. https://cyble.com/blog/goatrat-android-banking-trojan-variant-targeting-brazilian-banks/
34. https://cyble.com/blog/new-enchant-android-malware-targeting-chinese-cryptocurrency-users/
35. https://www.threatfabric.com/blogs/droppers-bypassing-android-13-restrictions

Emerging **macOS** Targeting

As technology advances, so does the sophistication of cyber threats, and no operating system remains immune to the evolving landscape of cybersecurity risks. Recently, there has been a noticeable shift in focus, with TAs increasingly targeting **macOS** systems, posing a growing challenge in ensuring the security of these platforms. The image below illustrates statistics collected from VirusTotal for malicious **Mach-O** files submitted in the last three years.

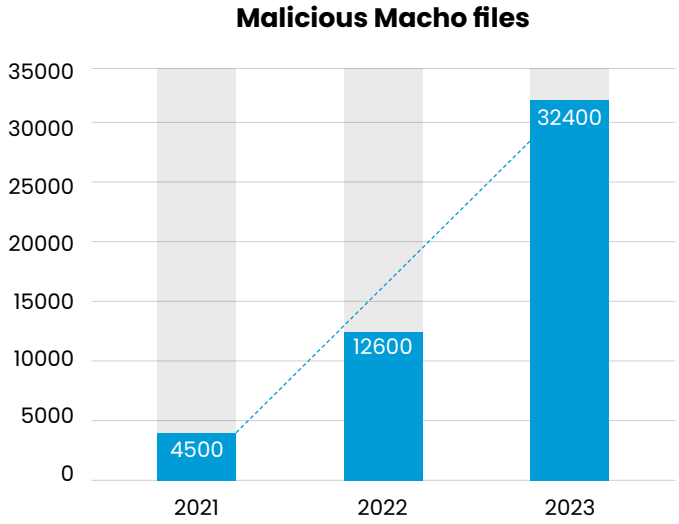


Figure 16 - Statistics of Malicious Macho files (Source: VirusTotal)

CRIL observed a rapid evolution in Malware-as-a-Service information stealers (MaaS infostealers), with a particular emphasis on macOS environments. Notable instances include the emergence of stealers like Atomic Stealer[36], MacStealer[37], Realst Stealer[38], ShadowVault[39], and XLoader[40] macOS Stealer.

In addition to the infostealers, there have been occurrences of major ransomware encryptors, specifically targeting Mac devices. On April 16, a security research team shared information on Twitter about a LockBit[41] ransomware variant specifically designed for Apple's macOS arm64 architecture. First-ever major Instance of Ransomware Targeting macOS.

Additionally, the North Korean Lazarus hacking group introduced 'KandyKorn[42],' a stealthy macOS backdoor targeting blockchain engineers. The utilization of Cobalt Strike on macOS, with the introduction of 'Geacon[43],' highlights the dynamic and evolving risk landscape for Apple's devices. In the forthcoming year, as macOS becomes a focal point, TAs may incorporate new and advanced malware into their arsenals.

36. https://cyble.com/blog/threat-actor-selling-new-atomic-macos-amos-stealer-on-telegram/
37. https://www.uptycs.com/blog/macstealer-command-and-control-c2-malware
38. https://www.sentinelone.com/blog/apple-crimeware-massive-rust-infostealer-campaign-aiming-for-macos-sonoma-ahead-of-public-release/
39. https://cyble.com/blog/malicious-tools-in-the-underground-investigating-their-propagation/
40. https://www.sentinelone.com/blog/xloaders-latest-trick-new-macos-variant-disguised-as-signed-officenote-app/
41. https://www.sentinelone.com/blog/lockbit-for-mac-how-real-is-the-risk-of-macos-ransomware/
42. https://www.elastic.co/security-labs/elastic-catches-dprk-passing-out-kandykorn
43. https://www.sentinelone.com/blog/geacon-brings-cobalt-strike-capabilities-to-macos-threat-actors/

Sophisticated Threats in the **Android Ecosystem**

The year 2023 has witnessed a concerning surge in sophisticated threats targeting the Android ecosystem. Within the realm of emerging threats, 2023 introduces several new players in the malware landscape, including Hook[44], FluHorse[45], and GoldDigger[46]. Concurrently, Cyble's vigilant research brings light to the presence of malicious entities such as Chameleon[47], Gigabud[48], GoatRat[49], Enchant[50], and more, underscoring the diversity and dynamism of the evolving threat landscape.

The underground cyber economy has seen an increase in illicit services, notably the rise of "dropper-as-a-service[51]" and "Google Play loader[52]" offerings on dark web markets. These services have become instrumental in the distribution of Android malware, providing threat actors with turnkey solutions for deploying malicious payloads. Concurrently, the surge of Android banking Trojans and other malware has increased, with threat actors increasingly leveraging advanced evasion techniques.

A notable escalation in ATS-based banking trojans has been observed throughout 2023, with a particular focus on Brazilian banks. Noteworthy malware entities such as PixPirate[53], PixBankBot[54], GoatRAT[55], and its variants (Criminal bot and Fantasy banking trojan) strategically target the Pix platform, signifying a shift in the focal points of financial threat vectors.

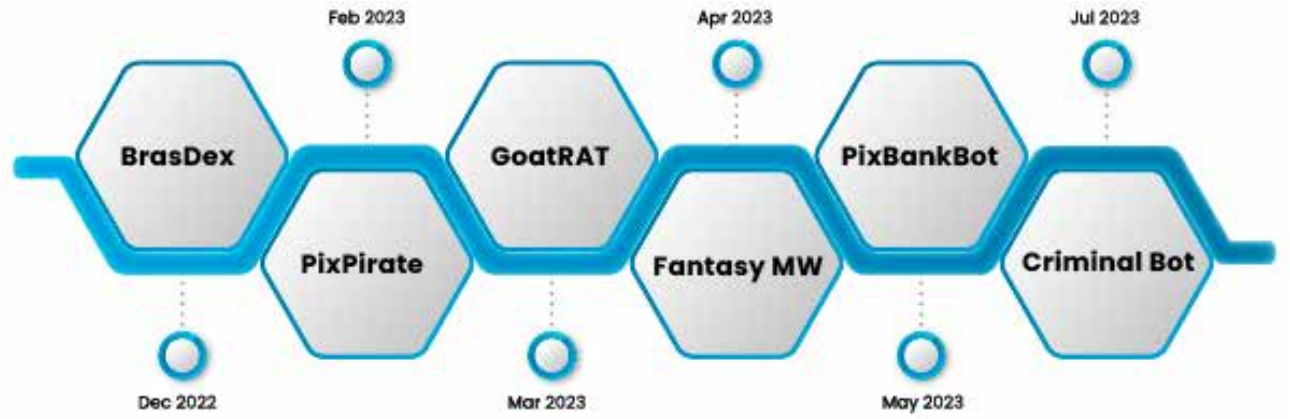


Figure – Timeline of ATS-based banking trojan targeting Brazilian banks

The prevalence of ATS-based malware highlights the evolving challenges confronting financial institutions in the digital payments era, emphasizing the necessity for adaptive security measures. For 2024, our prediction based on current findings and trends is that the sophistication and prevalence of ATS-based banking trojans will continue to increase, posing an even greater risk to financial systems worldwide.

44. https://www.threatfabric.com/blogs/hook-a-new-ermac-fork-with-rat-capabilities
45. https://blog.checkpoint.com/security/fluhorse-check-point-research-exposes-a-newly-discovered-malware-disguised-as-east-asian-legitimate-popular-android-apps/
46. https://blog.checkpoint.com/security/fluhorse-check-point-research-exposes-a-newly-discovered-malware-disguised-as-east-asian-legitimate-popular-android-apps/
47. https://cyble.com/blog/chameleon-a-new-android-malware-spotted-in-the-wild/
48. https://cyble.com/blog/gigabud-rat-new-android-rat-masquerading-as-government-agencies/
49. https://cyble.com/blog/goatrat-android-banking-trojan-variant-targeting-brazilian-banks/
50. https://cyble.com/blog/new-enchant-android-malware-targeting-chinese-cryptocurrency-users/
51. https://www.threatfabric.com/blogs/droppers-bypassing-android-13-restrictions
52. https://securelist.com/google-play-threats-on-the-dark-web/109452/
53. https://www.cleafy.com/cleafy-labs/pixpirate-a-new-brazilian-banking-trojan
54. https://cyble.com/blog/pixbankbot-new-ats-based-malware-poses-threat-to-the-brazilian-banking-sector/
55. https://cyble.com/blog/goatrat-android-banking-trojan-variant-targeting-brazilian-banks/

Deception is at the core of any subtle cyberattack, which explains why Threat Actors leverage deception techniques so widely. These can range from known vectors such as phishing and fraud to the increasing sophistication we have observed in the fields of Malvertising, SEO poisoning, and targeting widely adopted technology such as QR codes. The following sections aim to cover how deception-based attacks form a formidable threat in cyberspace, leveraging deceptive tactics to camouflage their true intent.

Rise of Deception-**Based Attacks**

2023 saw a significant uptick in supply chain attacks, particularly in the realm of malicious code packages. This increase is driven by attackers looking for new and lasting ways to breach systems. Malicious code package attacks involve spreading harmful packages or injecting malicious code into legitimate ones, distributed through online repositories and package managers trusted by users such as PyPI and npm.

A recent incident report[56] from PyPI administrators on May 20, 2023, unveiled a disruption in the Python Package Index. To counter a surge in malicious users and projects, new registrations were temporarily suspended. PyPI, a lynchpin in the Python ecosystem, simplifies development but now faces severe challenges in maintaining integrity and security.

Insights from Cyble Research and Intelligence Labs (CRIL) exposed[57] the gravity of the situation. A thorough investigation identified 160 malicious Python packages with over 45,000 cumulative downloads. Malware such as Downloaders, Creal Stealer, and Hazard Token Grabber were discovered, signaling a worrisome trend in their adoption.

CRIL also uncovered a threat in the form of typo-squatted packages. For instance, a misspelled package, 'reaquests,' mimicking the popular 'requests,' poses a significant risk. Users may unknowingly install malicious content, thinking it's the authentic package.

56. https://status.python.org/incidents/qy2t9mjjcc7g
57. https://cyble.com/blog/over-45-thousand-users-fell-victim-to-malicious-pypi-packages/

NPM Packages

- The Node Package Manager (npm) is vital for Node.js projects but presents security challenges. With over a million packages, npm's collaborative nature becomes a breeding ground for malicious intent. Packages can execute destructive commands during installation, compromising systems. Notably, TurkoRAT, a 2023 malware strain, highlighted the exploitation of npm for nefarious purposes.
- The significance of npm lies in the widespread use of JavaScript, powering almost 98% of websites. However, the ease with which open-source tools can be downloaded and modified for malicious use poses a significant risk. TurkoRAT[58] exemplifies the threat, masquerading as an open-source tool for "testing" but easily repurposed by threat actors.
- In the relentless battle against supply chain risks, staying vigilant and adopting robust security measures are imperative for developers and organizations navigating the open-source coding landscape.

In 2024, a surge in supply chain attacks will drive a heightened focus on security measures within open-source coding packages. Expect the incorporation of advanced technologies to bolster authentication and fortify the integrity of the supply chain.

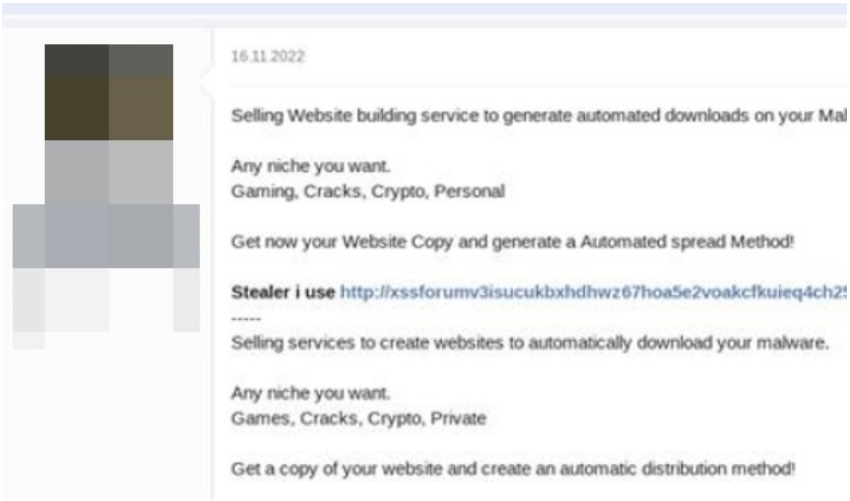
58. https://www.reversinglabs.com/blog/rats-found-hiding-in-the-npm-attic

SEO Poisoning and **Malvertising**

In 2023, SEO poisoning has emerged as a prevalent cyber intrusion technique. Threat actors use tactics like typosquatting, manipulating search engine algorithms with strategic keywords, malvertising through ad space purchases, and compromising small businesses' low-security websites for SEO poisoning and command-and-control infrastructure.

According to a report from Confiant[59], the security violation (attempts to compromise the user) rate associated with malvertising in Q1 2023 reached its highest level in four years, indicating a significant surge in attempts to compromise user security. Notably, during the first half of 2023, users of Firefox for Windows faced the highest rate of security issues, closely followed by Windows Edge users. In contrast, Chrome demonstrated strong performance in terms of security across all platforms; however, it exhibited relatively lower performance in terms of overall quality.

CRIL also observed TAs using SEO poisoning to distribute malware. The figure below shows a post on cybercrime forums regarding the usage of SEO poisoning to spread malware.



Technical analyses, such as DFIR Report's 'A Gootloader Story[60],' provide a detailed look into how threat actors leverage SEO poisoning for successful intrusions and their ensuing consequences.

Gootloader, identified by Sophos in March 2021, represents a case where threat actors employ SEO poisoning to elevate compromised websites hosting malware to the top of specific search queries. Users searching for phrases are directed to forum-like web pages and instructed to download a file, inadvertently executing malware. The Gootloader case exemplifies the evolving landscape of cyber threats, emphasizing the need for heightened cybersecurity awareness and proactive measures to counteract the risks posed by SEO poisoning techniques.

In 2024, Cyber adversaries will continue evolving tactics like SEO poisoning and malvertising, necessitating organizations to invest in sophisticated threat detection tools and machine learning algorithms. Predictions suggest a rise in AI-driven attacks and the emergence of novel evasion techniques.

59. https://www.confiant.com/news/h1-2023-maq-summary#:~:text=The%20report%20identifies%20that%20during,security%20risk%20to%20the%20user.
60. https://thedfirreport.com/2022/05/09/seo-poisoning-a-gootloader-story/

QR Codes **Under Siege**

"QR fraud" generally refers to fraudulent activities or scams that involve the use of QR codes. TAs may exploit QR codes to trick individuals into providing sensitive information, make unauthorized transactions, or distribute malware. Microsoft has shared[61] some common scams associated with QR codes.

Scammers use "quishing" tactics, sending phishing emails with QR codes to deceive recipients. Pretending to represent reputable companies, these emails falsely claim issues like failed online payments, urging victims to scan QR codes to re-enter credit card details. Some emails come from free addresses or recently registered domains, and a few include the Microsoft Security logo to boost credibility, illustrating the diverse methods employed in these deceptive campaigns. Malwarebytes[62] shared an example of such an attack in August 2023. The figure below shows the malicious QR code masquerading as Microsoft Multi-Factor Authentication.

Quishing is a very potent initial infection vector for threat actors, and QR codes give social engineering attacks a new edge. The attacks have been prevalent for many years, and they will get more popular in the upcoming years as multiple organizations are going paperless.

61. https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/five-common-qr-code-scams
62. https://www.malwarebytes.com/blog/news/2023/08/qr-codes-deployed-in-targeted-phishing-campaigns

Social Media **Deception**

In 2023, a notable increase in cyber threats has been observed[63] targeting **social media platforms**, posing significant risks to users. The surge includes the proliferation of phishing pages on these platforms, where users unknowingly download malicious files.

LinkedIn, a prominent professional network, is also under attack as TAs pose as recruiters, posting fake job opportunities to trick employees into engaging with potential malicious threats[64]. Additionally, a phishing campaign[65] employing LinkedIn Smart Links has been identified, manipulating recipients into clicking on seemingly harmless links that lead to phishing sites. This growing trend highlights the dynamic and evolving nature of cybersecurity threats on established social media platforms, suggesting that TAs may increasingly target emerging platforms with innovative infiltration tactics.

63. https://cyble.com/blog/the-growing-threat-of-chatgpt-based-phishing-attacks/
64. https://www.welivesecurity.com/en/eset-research/lazarus-luring-employees-trojanized-coding-challenges-case-spanish-aerospace-company/
65. https://cofense.com/blog/linkedin-smart-links-credential-phishing-campaign/

Deceptive **Proof of Concepts**

Proof of Concepts (PoCs) play a vital role for security researchers, facilitating benign testing to identify vulnerabilities. Nevertheless, certain deceptive PoCs mask malicious intentions by incorporating covert backdoors, feigning legitimacy while harbouring persistent threats. In 2023, there were instances of targeted attacks on security researchers involving deceptive PoCs.

- In early May 2023, the VulnCheck[66] team came across numerous misleading GitHub repositories that falsely purported to be zero-day exploits for well-known applications. Upon investigation, it was determined that these repositories were, in fact, delivering malware payloads onto the machines of unsuspecting victims.
- In July 2023, a deceptive PoC linked to CVE-2023-35829[67] demonstrated a vulnerability while clandestinely embedding a backdoor. Unearthed by the Uptycs[68] threat research team, the discovery significantly impacts the security research community.
- In September 2023, Palo Alto's Unit42 exposed[69] a deceptive PoC linked to CVE-2023-40477[70]. Analysis revealed an infection chain leading to the installation of a VenomRAT payload.

66. https://vulncheck.com/blog/fake-repos-deliver-malicious-implant
67. https://nvd.nist.gov/vuln/detail/CVE-2023-35829
68. https://www.uptycs.com/blog/new-poc-exploit-backdoor-malware
69. https://unit42.paloaltonetworks.com/fake-cve-2023-40477-poc-hides-venomrat/
70. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40477

Predictions

1. In the landscape of 2024, a noticeable surge is anticipated in the trade of ICS-specific exploits over the DarkWeb forums. This forecast stems from the substantial uptick in vulnerabilities unveiled throughout 2023 within ICS-specific assets.

2. The spread of disinformation and fake news might lead to public distrust and confusion, making it a significant cybersecurity concern in 2024. The erosion of public trust due to widespread disinformation and confusion can impact collective cybersecurity resilience.

3. The proliferation of AI technology in 2023 is expected to significantly enhance the potency of social engineering attacks. AI-driven advancements enable attackers to craft highly personalized and convincing social engineering tactics.

4. Additionally, the historical cybercrime forums activities from 2022 and 2023 clearly indicate an alarming growth in cyber threat incidents. Cyber security executives must note that our research during 2023 had found significant artifacts indicating a surge in mass exploitation of historical vulnerabilities to target organizations irrespective of their business size, that will continue to incite attacks in 2024.

5. 2023 also marked a record number of incidents impacting organizations in India, followed by the United States. Therefore, we foresee a surge in the use of ready-made exploit kits and open-source penetration testing tools to weaponize historical vulnerabilities for targeting organizations in countries with vast and developing digital infrastructure.

6. We also observed a prudent shift in the tactics where threat actors that were apparently acting stand-alone for a long time are now collaborating with other threat actors and groups. This tactic observably led cybercriminals to share skill sets, diversify attack methodology, minimize exploitation time, and fetch shared profits on compromises and data breaches.

7. Forums will continue to be a breeding ground for exploits, vulnerabilities, and data breaches, with any notable shutdowns being met with multiple new forums to take their place. Threat actors continue to jockey to stake their claim as being foremost in their fields by sharing and selling exploited datasets.

8. Ransomware growth shows no sign of slowing down, positioning ransomware to continue to be one of the largest threats to organizations. AI will significantly impact this industry as crafting emails, personas, delivery methods, and even the malware will become trivial to do, enabling operators to continue their “pray and spray” methodology. Operators have already been observed adding new tricks to their repertoire, such as filing SEC breach notifications, all in an effort to extort their victims for more and more money. Expect tactics like this to continue to evolve and mature into standard extortion practices, and have a response plan in place in the event that your organization is impacted by ransomware. Have a Disaster Recovery/Data Recovery plan in place and practice it regularly.

9. With global conflicts showing little signs of slowing down, expect hacktivism to continue to be a threat to certain organizations. Most organizations will not feel the impact of hacktivism unless they are particularly involved with the countries or regions affected by conflicts or geopolitical turmoil. However, the risk of supply chain impacts could impact organizations not even related to the conflict.

10. We believe the overall trends and constant evolution in tactics will continue to pose a major challenge for the information security industry and its executives to protect the global digital infrastructure from fast-paced and potentially recurring cyber-attack campaigns.

Next-Generation AI-Powered Cybersecurity Tailored for Enterprises, Government, & Law Enforcement

Our vision: Democratize threat intelligence for all—enterprises, governments, individuals, and researchers. Empower everyone to protect their digital assets and privacy. A future where knowledge is power, accessible to all.

CYBLE VISION

Award-Winng Cyber Threat Intelligence Platform

CYBLE HAWK

Built For Govt., Law Enforcement, National Defence

AMIBREACHED POWERED BY CYBLE

Helps Individuals/Enterprises Search Their Dark Web Exposure

ODIN by CYBLE

Built for Information Security Teams

THE CYBER EXPRESS By CYBLE

#1 Cybersecurity News & Magazine

www.cyble.com