HivePro's Annual Threat Report

CYBER HORIZON

2023

APRIL 2024

CYBER HORIZON

HivePro's Annual Threat Report

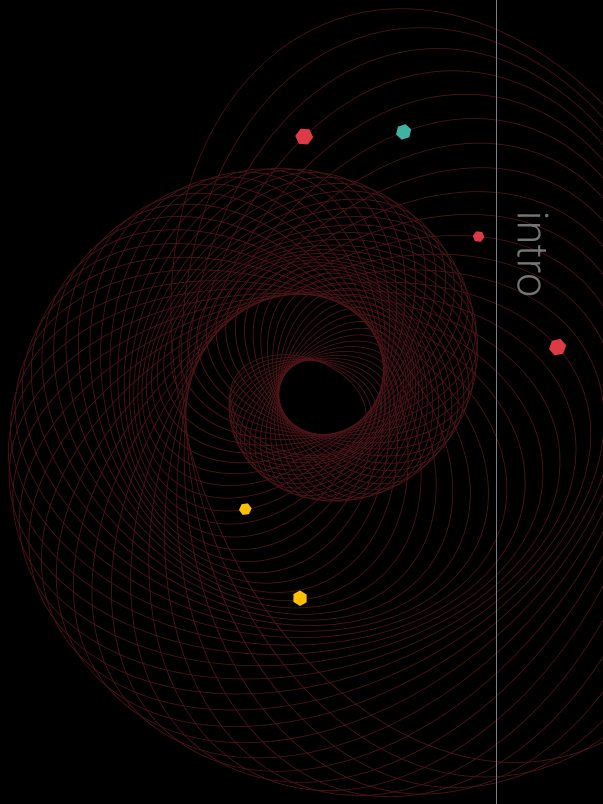
CYBER HORIZON

HivePro's Annual Threat Report

01

Executive Summary

1.1 Introduction



intro

HiveForce Labs, the Threat Research division of Hive Pro Inc., presents its annual threat report for the year 2023 and forecasts the cybersecurity landscape for 2024. As a leading threat exposure management company and among the pioneers of the space, HiveForce Labs continuously monitors cyber threats, attacks, threat actors, vulnerabilities, and exploits worldwide to provide insights into the evolving cybersecurity landscape.

In 2023, cyber threats continued to escalate, with a notable increase in ransomware attacks, supply chain compromises, and sophisticated cyber espionage campaigns. Threat actors demonstrated greater sophistication, often leveraging advanced techniques and tools to breach organizations' defenses. Nation-state-sponsored attacks also remained a significant concern, with several high-profile incidents highlighting the geopolitical aspects of cybersecurity.

Executive Summary

1.1 Introduction

One of the key trends observed in 2023 was the increasing impact of cloud and AI technologies on cybersecurity. While cloud services offered scalability and flexibility to organizations, they also introduced new security challenges. Similarly, the rise of AI-powered threats posed new challenges for cybersecurity professionals, as threat actors began to leverage AI for reconnaissance and attack automation.

Looking ahead to 2024, HiveForce Labs predicts that cyber threats will continue to evolve, with ransomware attacks remaining a top concern for organizations. Nation-state-sponsored attacks are expected to become more sophisticated and widespread, targeting critical infrastructure and sensitive data. Additionally, the integration of AI and machine learning into cyber attack tools and techniques is expected to increase, making it essential for organizations to enhance their security measures.

This report provides a comprehensive overview of the cyber threats observed in 2023, analyzes key trends and developments, and offers recommendations for organizations to strengthen their cybersecurity posture in 2024.

1.2

trends & insights

Zero-day vulnerabilities

They have been the sweet spot for exploitation by ransomware groups, resulting in a significant increase in global ransom payments, surpassing the **$1 billion** mark. The Cl0p ransomware group orchestrated significant attacks campaigns leveraging zero-day vulnerabilities, notably targeting platforms such as GoAnywhere MFT, PaperCut, MOVEit, and SysAid.

Ransomware Proliferation

Ransomware attacks continued to dominate the cybersecurity landscape in 2023, targeting organizations of all sizes and sectors. A ***95% surge*** in victims, totaling 4,769 was observed in 2023 with the United States witnessing the most number of attacks by volume followed by the UK and Canada.
The use of ransomware-as-a-service (RaaS) platforms and double extortion tactics became increasingly prevalent, leading to a surge in ransomware incidents globally.

Insights

executive summary

Supply chain attacks

Supply chain attacks have reached their peak, leading to numerous high-profile incidents resulting in data breaches, ransomware attacks, and intellectual property theft. The **global cost** of software supply chain attacks for the year 2023 was nearly $48B which is predicted to have a **15% growth** year-on-year with a target of **$138B by 2031**.

The United States alone witnessed 242 claimed software supply chain attacks in 2023 which is the highest reported number in the last 5 years and has increased by over 115% from the year 2022.

Emergence of New Threat Actors

The year witnessed the emergence of new ransomware groups, such as "**RA Group**" and "**Dark Power**", leveraging sophisticated attack techniques and targeting critical infrastructure sectors. These groups posed a significant threat to organizations worldwide, highlighting the need for enhanced cybersecurity measures.

Advanced Evasion Techniques

Threat actors continued to evolve their tactics, using fileless ransomware, zero-day vulnerabilities, and anti-analysis techniques to evade detection. These advanced evasion techniques made it challenging for organizations to defend against ransomware attacks effectively.

2023 2031

Insights

executive summary

Nation-State Sponsored Attacks

Nation-state sponsored cyberattacks remained a significant concern in 2023, with several countries engaging in cyber espionage and cyber warfare activities. These attacks targeted critical infrastructure, government agencies, and military institutions, highlighting the need for enhanced cybersecurity measures at a national level.

Data Exfiltration and Double Extortion

Double extortion tactics, involving the exfiltration of sensitive data before encryption, became increasingly common in 2023. This approach added a new dimension to ransomware attacks, as threat actors threatened to leak or sell stolen data if ransom demands were not met.

Impact of Cloud and AI

The increasing adoption of cloud services and artificial intelligence (AI) posed both opportunities and challenges for cybersecurity. While cloud services offered scalability and flexibility, they also introduced new security risks. Similarly, AI-powered attacks became more sophisticated, requiring organizations to deploy advanced AI-driven security solutions to mitigate these threats.

Forecasting 2024 executive summary 1.3

Increased Ransomware Sophistication

Ransomware attacks are expected to become more sophisticated in 2024, with threat actors leveraging AI and machine learning to enhance their attack capabilities. The use of RaaS platforms will also continue to rise, making it easier for attackers to launch targeted attacks against organizations.

Geopolitical Impact on Cybersecurity

Geopolitical tensions will have a significant impact on cybersecurity in 2024, with nation-state sponsored attacks becoming more prevalent. Countries will increasingly use cyberattacks as a tool for espionage and warfare, leading to a rise in cyber conflicts.

Focus on Cyber Resilience

In response to the growing cyber threats, organizations will focus on enhancing their cyber resilience. This includes investing in threat intelligence, cybersecurity training, and incident response capabilities to quickly detect, respond to, and recover from cyberattacks.

Forecasting 2024 executive summary 1.3

Quantifying Cyber Risk

Chief Information Security Officers (CISOs) will be increasingly tasked with quantifying **cyber risk in financial terms** to effectively communicate with executive stakeholders. This will require a deep understanding of cyber risks and their potential impact on the business.

Simplification of Security Stack

CISOs will prioritize the simplification of their security stack, focusing on making security operations more efficient. Automation will play a crucial role in this process, allowing teams to focus on addressing the most critical threats.

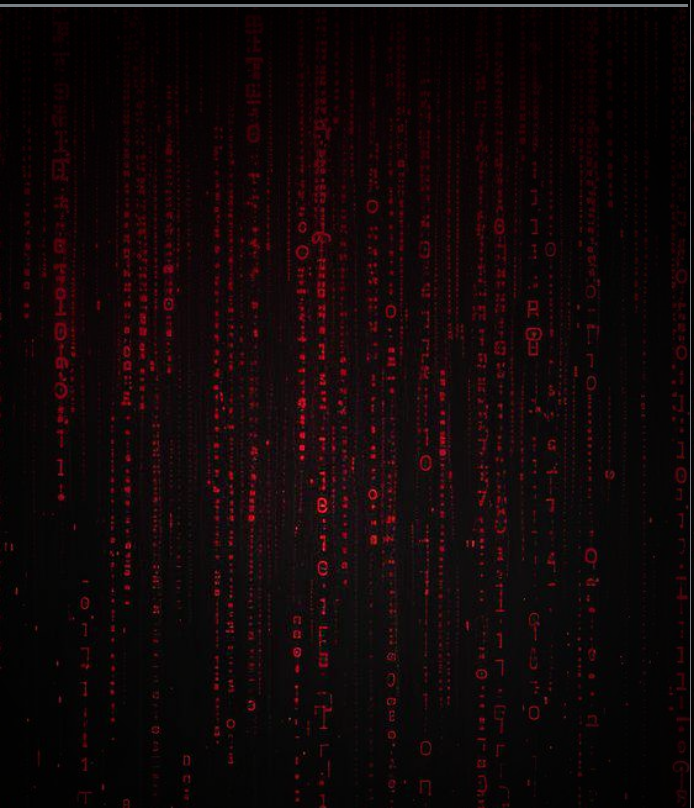
AI Support and Skill Development

AI deployments will support security teams by **automating low-level tasks and augmenting team productivity**. However, AI will not replace humans but rather empower them to make a lasting impact within their roles. Skill development and well-being of team members will be a critical focus for IT leadership.

Focus on Frontline Defense

Insider threats remain a significant concern, and IT leaders will need to help teams understand their responsibilities in preventing credential and data exploitation. Collaboration with other departments for effective security training and awareness will be key.

The New Normal: Shift Left, Monitor, Collaborate, Verify



As the cybersecurity landscape continues to evolve rapidly, it is imperative for organizations and cybersecurity professionals to adopt proactive measures to defend against emerging threats. To safeguard against cyber attacks, a transition towards a "shift left" approach is essential, focusing on early integration of security into the development process. This approach ensures that security is not an afterthought but an integral part of the entire software development lifecycle.

Implementing a continuous threat exposure management program is crucial to identify and mitigate vulnerabilities and threats proactively. By continuously monitoring and analyzing their security posture, organizations can detect and respond to threats in real-time, reducing the risk of a successful cyber attack.

In addition, the adoption of cyber mesh architectures can help organizations create a more resilient and adaptive security framework. Cyber mesh enables different components of the security ecosystem to work together seamlessly, sharing threat intelligence, security findings data and responding to threats collectively. This approach enhances the overall security posture of an organization, making it more difficult for threat actors to exploit vulnerabilities.

Furthermore, adopting a zero-trust security model is essential to prevent unauthorized access to critical systems and data. By verifying every user and device trying to access the network or data assets, organizations can ensure that only legitimate users gain access, reducing the risk of a data breach.

In conclusion, cybersecurity professionals must embrace a proactive approach to cybersecurity, focusing on early detection and mitigation of threats. By implementing continuous threat exposure management programs, cyber mesh architectures, and zero-trust security models, organizations can significantly enhance their cybersecurity posture and protect against evolving cyber threats.

2024...

Note to Cyber Practitioners 1.4

executive summary

Reactive approach to **proactive approach**

Vulnerability Risk Focus to **Threat Focus**

Siloed to **consolidated** data and technology

Uncontextualized to Contextualized **Remediation**

Hive Pro

02

"Navigating the Dynamic Threat Terrain"

Cyber Threat Landscape

The year 2023 marked a significant escalation in cyber threats, with organizations facing an unprecedented wave of attacks growing in both frequency and sophistication aimed at compromising their networks, stealing sensitive data, and disrupting operations. A significant surge is observed in cyber threats targeting cloud infrastructure, highlighting the growing challenges faced by organizations in securing their digital assets.

According to recent statistics, there has been a significant increase in the number of cyber attacks targeting cloud services in the year 2023, with a ***75% rise in cloud-related security*** incidents compared to the previous year. These attacks range from ransomware campaigns targeting critical infrastructure to data breaches affecting millions of users. The growing complexity and sophistication of cyber attacks has made it challenging for organizations to detect and respond to these threats effectively.

> *The United States witnessed the highest number of software supply chain attacks in the last five years.*

Exploitation of software supply chains emerged as a common attack vector, with a global cost of nearly $48 billion and a predicted 15% year-on-year growth, highlighting the need for robust vendor risk management strategies. The United States alone witnessed 242 claimed software supply chain attacks, the highest reported number in the last five years, showcasing the increasing frequency and impact of these attacks across various sectors.

Global cost of *$48B* in 2023, predicted growth to *$138B* by 2031

Ransomware attacks saw a dramatic transformation in 2023, with a 95% surge in victims compared to the previous year, fueled by both traditional ransomware and more sophisticated mega-ransomware. Notable ransomware leaders LockBit 3.0, ALPHV, and Cl0p continued to dominate the landscape, with ransomware payments surpassing the $1 billion mark for the first time. The business services sector was the most targeted, with 1,265 cases, while the media, leisure, and entertainment sector experienced the greatest number of vulnerabilities exploited in ransomware attacks.

Increase in global ransom payments, *exceeding $1 billion.*

Target Locked: Business Services Bullseye with 1,265 Cases !

Data breaches remained a significant challenge, with human error and external actors being major contributors. Ransomware was present in 24% of breaches, highlighting its steady impact across industries. The global average cost of a data breach reached $4.45 million, with 51% of organizations planning to increase security investments post-breach. Despite the importance of internal detection, only one-third of breaches were discovered internally, emphasizing the need for improved threat detection capabilities.

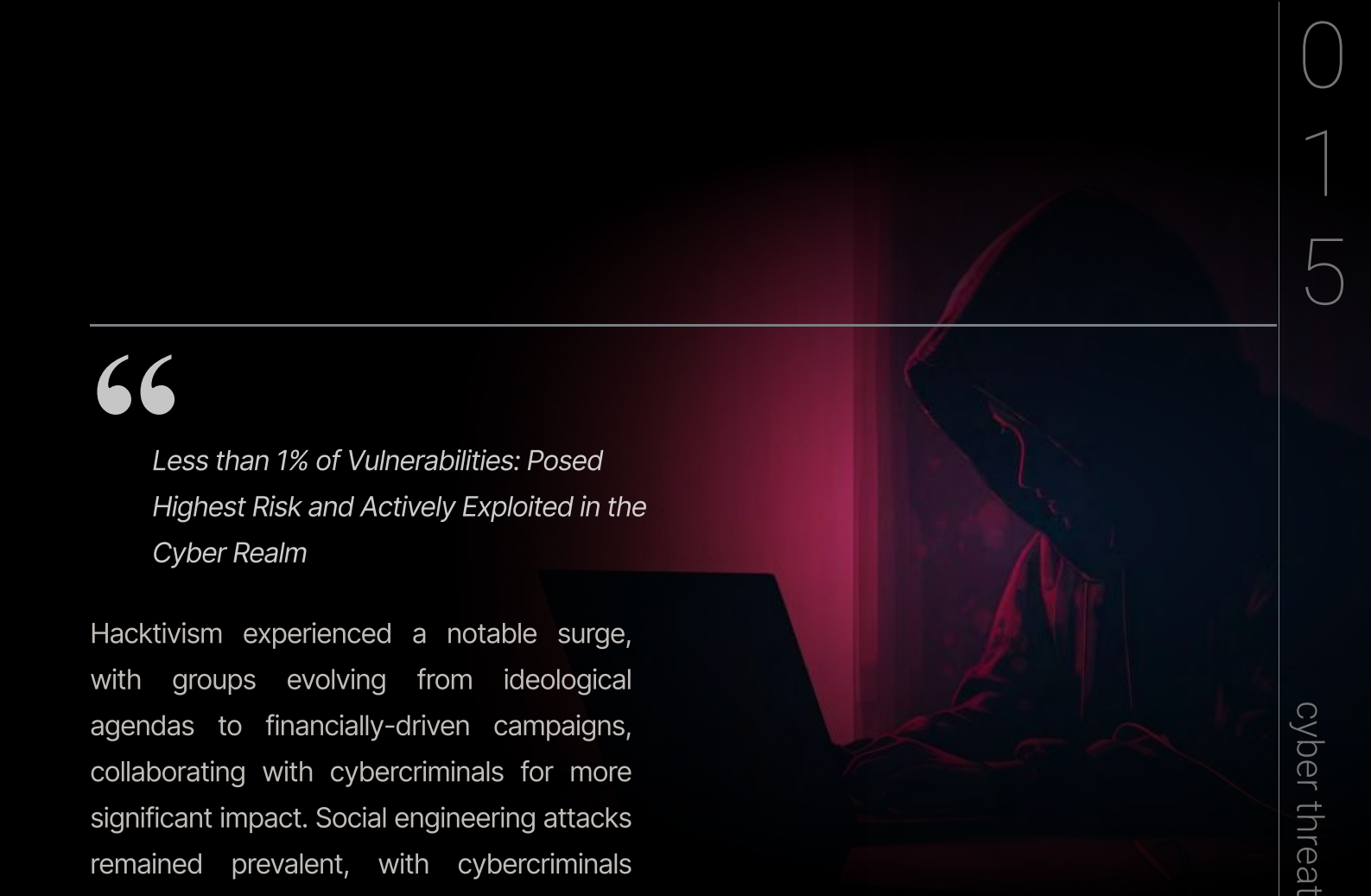
Data Breach Dents Wallets, Global Average Cost Hits $4.45 Million.

> *Data Breach Blind Spots: Two-thirds of data breaches eluded detection by existing security controls*

Evolving Strategies, Nation-State Cyber Espionage Takes a Stealthy Turn

Cyber espionage campaigns conducted by nation-state actors shifted towards more stealthy and persistent operations focused on espionage, targeting government or private-sector organizations involved in critical infrastructure. Russian and Iranian state-sponsored actors reduced the frequency of destructive attacks in favor of espionage campaigns, while Chinese state actors expanded their targeting to include U.S. defense infrastructure and partners in the Belt and Road Initiative. North Korea emerged as a significant player in cyber espionage, enhancing the sophistication of its operations.

Cyber espionage takes center stage as state-sponsored actors wage silent battles for strategic advantage.



> *Less than 1% of Vulnerabilities: Posed Highest Risk and Actively Exploited in the Cyber Realm*

Hacktivism experienced a notable surge, with groups evolving from ideological agendas to financially-driven campaigns, collaborating with cybercriminals for more significant impact. Social engineering attacks remained prevalent, with cybercriminals employing various techniques to deceive individuals and gain unauthorized access to sensitive information. The cybersecurity landscape also saw a notable surge in vulnerabilities, with less than 1% of these vulnerabilities posing the highest risk and actively exploited in the wild.

Overall, the cybersecurity landscape of 2023 underscored the need for organizations to adopt a proactive and multifaceted approach to cybersecurity to mitigate evolving and sophisticated cyber threats effectively. Later in this section, we will discuss some significant attacks that expanded the global cyber threat landscape in 2023.

"The cybersecurity landscape of 2023 posed significantly greater risks compared to 2022, grappling with severe software supply chain attacks, relentless ransomware assaults, substantial data breach threats, escalating cyber espionage endeavors, and intricate hacktivism activities."

Notable Events 2.1

cyber threat landscape

Millions of windows user impacted by attack on Microsoft's build infrastructure

Microsoft disclosed a supply chain attack in February 2023 that targeted its build infrastructure. The attackers compromised a build server used to compile and package software updates for Microsoft products. This allowed them to insert a malicious backdoor into legitimate software updates, which could potentially impact millions of Windows users worldwide. Microsoft took immediate action to address the issue and advised customers to update their systems to protect against the threat.

3000+ Airbus suppliers data breached in a supply chain attack initiated through customer Turkish Airlines

The alias USDoD, a threat actor and alleged ransomware operator, leaked data of over 3,000 suppliers of Airbus after purportedly penetrating the organization's systems using a hacked customer account from Turkish Airlines. USDoD, known for offering data from the FBI's InfraGard system on underground forums, claimed to have joined the ransomware crew Ransomed and leaked personal information of Airbus's suppliers. They accessed Airbus via Turkish Airlines, where a pirated Microsoft .NET framework led to an infostealer infection. This incident highlights the importance of supply chain security and the need for organizations to prepare for and respond to such attacks.

Notable Events 2.1

cyber threat landscape

$250M, estimated cost of ransomware attack on semiconductor giant Applied Materials

Another notable attack in the same month was the ransomware attack on semiconductor giant Applied Materials, originating from a business partner, which is estimated to cost the company $250 million. The attack, linked to a breach at Applied Materials's supplier MKS Instruments, disrupted shipments and highlighted vulnerabilities in the semiconductor supply chain. The incident underscores the growing cybersecurity risks in the semiconductor industry and the potential for widespread impact on various sectors reliant on electronic components.

239K+ devices and 1800+ companies affected by attack on VoIP software provider 3CX

3CX, a leading provider of VoIP software, experienced a supply chain attack in March 2023 that affected over 239,000 publicly exposed devices and 1800+ companies. The attack was traced back to a 2022 incident involving a manipulated X_TRADER installer from Trading Technologies, highlighting the persistent risks in software supply chains. As a result of the breach, the core desktop application was compromised, leading to the distribution of IconicStealer and UpdateAgent malware on Windows and MacOS platforms, respectively.

Notable Events 2.1

cyber threat landscape

11% fall in Okta's market capitalization following data breach

Okta, a leading identity and access management provider, experienced a data breach in October 2023 originating from an employee's compromised personal Google account. Attackers gained access to Okta's support system and extracted session tokens from customers, including 1Password, BeyondTrust, and Cloudflare. Okta responded by engaging law enforcement, notifying regulators, and enhancing security measures, including implementing multi-factor authentication and strengthening session security. The breach affected files associated with 134 Okta customers, leading to a loss of customer trust, operational disruptions, and potential account takeover attempts. Okta's shares fell by 11% following the incident.

$75M+ revenue generated by attack campaigns exploiting MOVEit vulnerability

In May 2023, a critical vulnerability, CVE-2023-34362, was discovered in the MOVEit Transfer solution, leading to risks of escalated privileges and unauthorized access. This vulnerability had been actively exploited since May 27, with indications that threat actors had been experimenting with it as early as 2021. High-profile victims of this exploitation include BBC, British Airways, and Nova Scotia's government. The Cl0p ransomware group orchestrated a widespread exploitation of this vulnerability, with an estimated expected revenue of 75 million dollars from their activities.

Notable Events 2.1

cyber threat landscape

$70M ransom demanded by LockBit Ransomware gang

In June 2023, the LockBit group targeted Taiwan Semiconductor Manufacturing Company (TSMC) and managed to breach one of its IT hardware suppliers, Kinmax Technology. The attackers demanded a $70 million ransom, suggesting they had stolen sensitive information. TSMC stated that the incident did not affect its business operations or compromise customer information, as the supplier's breach only involved information related to server setup and configuration. Kinmax confirmed the breach, noting that leaked information included system installation preparation provided to customers as default configurations. TSMC terminated its data exchange with Kinmax and enhanced their security measures.

State sponsored actors exploiting WinRAR vulnerability for various attack campaigns

Multiple government-backed hacking groups exploited the WinRAR vulnerability, CVE-2023-38831, highlighting the ongoing threat of zero-day exploits. Even after a patch was available, many users remained vulnerable, leading to various cybercrime campaigns. These attacks included phishing campaigns impersonating legitimate organizations and delivering malware, such as the Rhadamanthys infostealer. The exploitation of CVE-2023-38831 underscores the critical importance of prompt patching and robust cybersecurity measures to protect against known vulnerabilities.

Notable Events cyber threat landscape 2.1

NATO Allies severely impacted by the humanitarian crisis

On January 30, the Russian Hacktivist Group KillNet launched a disruptive DDoS attack on 14 U.S. medical centers, including Stanford Healthcare, Duke University Hospital, and Cedars-Sinai. This cyber assault severely hindered critical resource access, impacting both patients and healthcare staff. Concurrently, Tallahassee Memorial Healthcare in North Florida faced a two-week emergency downtime following a cyberattack, leading to rescheduled surgeries and the exposure of 20,376 individuals' Social Security numbers. In Ohio, Medina Hospital experienced operational disruptions as an unauthorized third party gained server access, redirecting emergency ambulances and forcing the rescheduling of elective procedures at the Ohio Medical Center.

60+ credit unions, hospitals and financial unions in the US breached by CitrixBleed

Multiple ransomware groups have caused significant disruptions by targeting over 60 credit unions, hospitals, financial services, and more in the US. Exploiting the CitrixBleed vulnerability in Netscaler, these groups targeted organizations like Boeing, Ongoing Operations LLC, and HTC Global Services, demanding extortion payments. This highlights the pervasive threat of ransomware groups, which, despite being often staffed by teenagers, are capable of disrupting critical infrastructure and causing widespread impact. The situation underscores the urgent need for improved cybersecurity practices, including prompt patching and secure software development.

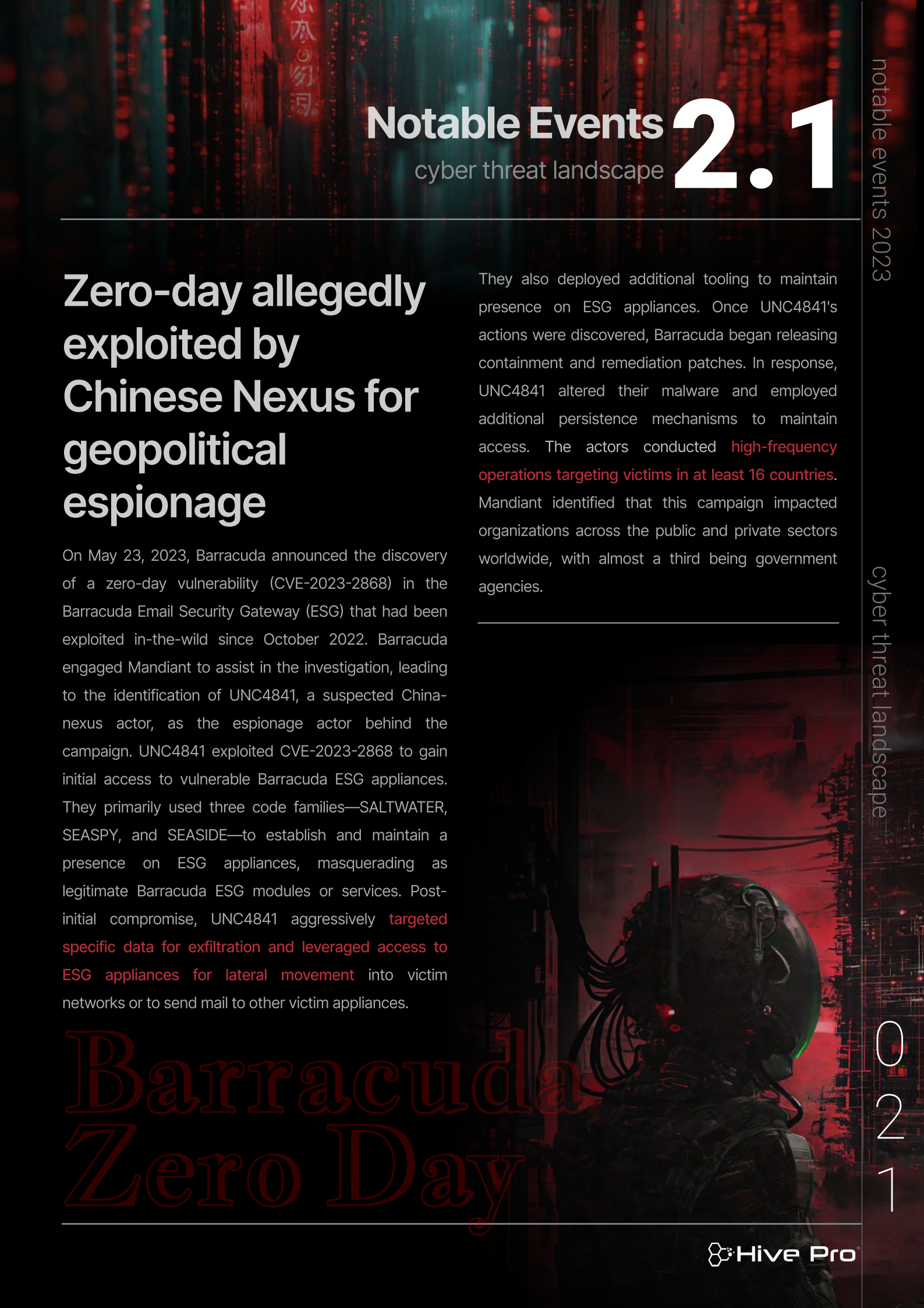
Notable Events 2.1

cyber threat landscape

Zero-day allegedly exploited by Chinese Nexus for geopolitical espionage

On May 23, 2023, Barracuda announced the discovery of a zero-day vulnerability (CVE-2023-2868) in the Barracuda Email Security Gateway (ESG) that had been exploited in-the-wild since October 2022. Barracuda engaged Mandiant to assist in the investigation, leading to the identification of UNC4841, a suspected China-nexus actor, as the espionage actor behind the campaign. UNC4841 exploited CVE-2023-2868 to gain initial access to vulnerable Barracuda ESG appliances. They primarily used three code families—SALTWATER, SEASPY, and SEASIDE—to establish and maintain a presence on ESG appliances, masquerading as legitimate Barracuda ESG modules or services. Post-initial compromise, UNC4841 aggressively targeted specific data for exfiltration and leveraged access to ESG appliances for lateral movement into victim networks or to send mail to other victim appliances.

They also deployed additional tooling to maintain presence on ESG appliances. Once UNC4841's actions were discovered, Barracuda began releasing containment and remediation patches. In response, UNC4841 altered their malware and employed additional persistence mechanisms to maintain access. The actors conducted high-frequency operations targeting victims in at least 16 countries. Mandiant identified that this campaign impacted organizations across the public and private sectors worldwide, with almost a third being government agencies.



APT Campaigns 2.2
cyber threat landscape

Operation Magalenha: A Persistent Threat to Portuguese Financial Institutions

Operation Magalenha is a long-running campaign targeting users of Portuguese financial institutions, conducted by a Brazilian threat group. This campaign, which began in 2021 and was last observed in the first quarter of the year 2023, has evolved to target users of over 30 financial institutions. The attackers aim to steal credentials and exfiltrate users' personal information, which can be exploited for malicious activities beyond financial gain. To maximize their attack potency, the **threat group deploys two backdoor variants simultaneously**. In response to stricter anti-abuse measures by some IaaS providers, the threat actor has **shifted its infrastructure hosting to Timeweb**, a Russian IaaS provider known for its more relaxed policies. This shift ensures uninterrupted operations for the threat group.

A Brazilian threat group's multi-year assault on 30+ financial institutions, culminating in a strategic shift to Russian servers to continue their expansive cyber heist

cve-2021-44228

Operation Blacksmith: Exploiting log4shell vulnerabilities for delivering DLang-based malware

Operation Blacksmith, a campaign employing new DLang-based malware by the Lazarus Group, targets manufacturing, agriculture, and security sectors. Exploiting Log4Shell (CVE-2021-44228), this marks a **shift in Lazarus' tactics with new DLang-based RATs and Telegram-based C2 communications**. The campaign overlaps with the Andariel APT group's TTPs, indicating coordination within Lazarus. 'NineRAT,' a new malware family, was first used in March 2023, is deployed alongside 'HazyLoad' and other DLang-based malware. Last year, Lazarus targeted energy providers using Log4j vulnerabilities.

APT Campaigns 2.2

cyber threat landscape

Operation Dream Job: Lazarus Group's Cyber Espionage Campaign Across Multiple Sectors

North Korea-linked Lazarus Group has been using trojanized versions of Virtual Network Computing (VNC) apps to target the defense industry and nuclear engineers in a campaign called Operation Dream Job. The group tricks job seekers on social media into opening malicious apps for fake job interviews. These apps operate discreetly to avoid detection, activating only when a user selects a server from the drop-down menu of the trojanized VNC client. Once launched, the counterfeit app retrieves additional payloads, including Lazarus Group malware like LPEClient, which can profile compromised hosts. The adversary also deploys an updated version of COPPERHEDGE, a backdoor known for running arbitrary commands and exfiltrating data, along with bespoke malware for transmitting files of interest to a remote server. Targets of this campaign include businesses directly involved in defense manufacturing, such as radar systems, unmanned aerial vehicles (UAVs), military vehicles, ships, weaponry, and maritime companies. Operation Dream Job involves contacting potential targets via suspicious accounts on platforms like LinkedIn, Telegram, and WhatsApp, offering lucrative job opportunities to trick them into installing malware.

Bluebottle: $11M stolen in 30+ targeted attacks on the financial sector

Bluebottle, a cyber-crime group targeting the financial sector, continues attacks on banks in Francophone countries using living off the land techniques and commodity malware. Symantec's observations, published in January 2023, running from July to September 2022, show new tactics, including the use of ISO files, GuLoader, and kernel drivers to disable defenses. They also employed Netwire RAT, Quasar RAT, and Cobalt Strike Beacon. The group targeted three financial institutions in Africa, compromising multiple machines in each. While Symantec cannot confirm monetization, Bluebottle's past success suggests ongoing threats to financial institutions, particularly in Francophone countries, with a possible expansion to other French-speaking regions.

HackForGood: Hacktivism against racism, fascism and apartheid targeting Israel

DarkBit ransomware, emerged in early 2023, has targeted educational institutions in Israel, claiming to be politically motivated against racism, fascism, and apartheid. Written in Golang, it follows other ransomware families using cross-platform languages. DarkBit's social media presence spreads details about attacks and victim data. Their ransom notes emphasize encrypted data recovery, threatening additional charges for delays. DarkBit excludes specific files from encryption and splits larger files for encryption, appending a ``.Darkbit'' extension. Early demands reached 80BTC (approx. $2 million USD). The group's political stance and encryption tactics set them apart in the ransomware landscape.

Impacting the Cloud 2.3

cyber threat landscape

Anonymous Sudan's DDoS attacks causing widespread failure of Microsoft cloud services

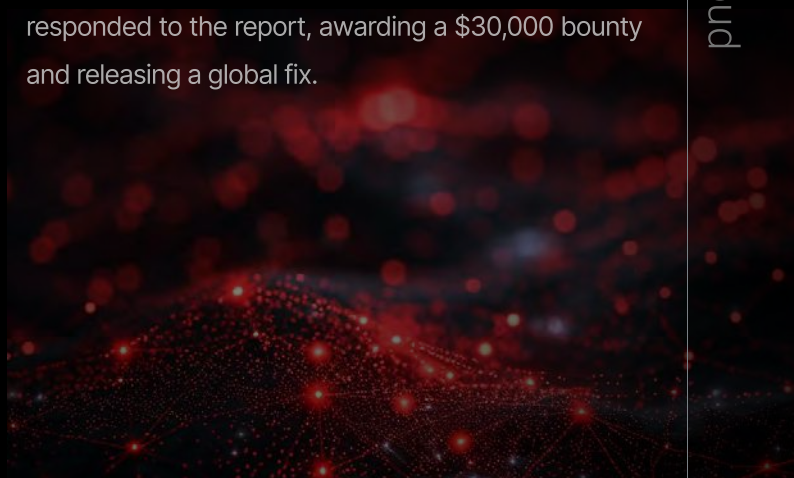
In June 2023, a number of Microsoft services, including Azure, Outlook, and OneDrive, experienced an outage that left many users unable to access these platforms. The outage was attributed to a sudden influx of traffic and was claimed to be orchestrated by the Attacker Group, also known as Anonymous Sudan. While the attack caused only service unavailability and there is no evidence of any data breach, it underscores the vulnerability of cloud services to large-scale disruptions. Established in January 2023, STORM-1359 has since been responsible for multiple Distributed Denial of Service (DDoS) attacks on government agencies, medical facilities, and various other organizations targeting cloud hosted services.

Misconfigured cloud environment exposes 260K Toyota customers' data

Toyota has revealed that approximately 260,000 customers' data was exposed online due to a misconfigured cloud environment, affecting customers in Japan, Asia, and Oceania. The data leak included information such as in-vehicle device IDs, map data updates, and creation dates, but not vehicle locations. The automaker has also implemented measures to enforce data handling rules and prevent future incidents.

EmojiDeploy vulnerability in Azure services allowing remote code execution

The EmojiDeploy vulnerability, discovered by Ermetic in late 2022 and publicly disclosed in January 2023, allows for remote code execution in various Azure services, including Function Apps, App Service, and Logic Apps. Attackers can exploit this vulnerability through CSRF on the SCM service Kudu, deploying malicious payloads to victim applications. The vulnerability enables threat actors to run code as the www user, steal or delete sensitive data, launch phishing campaigns, and take over app managed identities for lateral movement. Microsoft swiftly responded to the report, awarding a $30,000 bounty and releasing a global fix.



Despite the breach, Toyota confirmed that there is no evidence of secondary use or third-party copies of the data remaining online. This incident follows a previous data leak reported by Toyota last year, highlighting the ongoing challenges companies face in securing sensitive customer information in the digital age.

Impacting the Cloud 2.3
cyber threat landscape

38TB of Private Data accidently exposed by Microsoft's AI Research Team

Microsoft's AI research team inadvertently exposed 38 terabytes of private data, including a disk backup containing sensitive information such as passwords, private keys, and over 30,000 internal Microsoft Teams messages. The exposure occurred while the team was publishing a bucket of open-source training data on GitHub, using an Azure feature called SAS tokens to share data from Azure Storage accounts. Unfortunately, the link was misconfigured to grant access to the entire storage account instead of specific files, leading to the accidental exposure of additional private data. This incident highlights the challenges organizations face in securing massive amounts of data as they leverage AI more broadly, emphasizing the need for additional security measures and safeguards.

Rapid Reset DDoS attack targeting AWS services with 155M requests per second

Amazon Web Services (AWS) faced a significant Distributed Denial of Service (DDoS) attack in 2023, flooding websites and applications with over 155 million requests per second. AWS CEO Adam Selipsky praised the swift response of AWS engineers, ensuring minimal disruption to customers. The attack, known as the HTTP/2 Rapid Reset attack, targeted customers with an unprecedented volume of HTTP requests, making websites and applications temporarily unavailable. This attack stands out due to its size and scale, posing challenges in processing normal traffic. AWS, along with Google and Microsoft, successfully mitigated this attack, underscoring the importance of robust cybersecurity measures in today's digital landscape. The attack exploited a zero-day vulnerability in the HTTP/2 internet protocol, emphasizing the need for continuous vigilance and rapid response capabilities to counter evolving cyber threats.

Inheritable Threats 2.4

cyber threat landscape

Vulnerable WordPress plugins impacting millions of websites globally

In 2023, several notable vulnerabilities were discovered in WordPress plugins, highlighting the ongoing security challenges faced by WordPress site owners and developers. These vulnerabilities ranged from critical to moderate, affecting a wide range of plugins used by millions of websites globally. One such vulnerability was found in the popular plugin "Ultimate Member WordPress" which could allow unauthenticated attackers to elevate privileges and assume site administrator role effectively taking over the site. Another significant vulnerability was discovered in the "WooCommerce" plugin, which could enable attackers to bypass authentication and gain unauthorized access to sensitive data. These vulnerabilities underscore the importance of regularly updating plugins and maintaining strong security practices to protect WordPress websites from potential exploits.

1/5 Python applications impacted by dependency vulnerabilities

Vulnerabilities in Python libraries led to a substantial increase in security incidents in the year 2023, with a notable rise of over 200% in reported attacks compared to the previous year. These vulnerabilities affected a wide range of applications, impacting approximately 1 in every 5 Python-based projects globally. These vulnerabilities led to potential security risks for applications and systems relying on these libraries. One such vulnerability was found in the widely used "requests" library, which could allow an attacker to execute arbitrary code if a malicious server responded to a request. Another significant vulnerability was discovered in the "urllib" module, which could be exploited to bypass SSL/TLS certificate validation, potentially exposing sensitive data to interception. These vulnerabilities highlight the importance of regular updates and secure coding practices when using third-party libraries in Python applications.

Protocol and framework vulnerabilities causing widespread chaos

The year 2023 witnessed several significant vulnerabilities that were discovered in widely used protocols and frameworks, leading to a range of cyberattacks. These flaws exposed critical systems to exploitation, resulting in data breaches, service disruptions, and other security incidents. Notable incidents included attacks exploiting vulnerabilities in the HTTP/2 protocol, impacting AWS and other major cloud providers, as well as flaws in widely used frameworks like Django and Flask, which left web applications vulnerable to various attacks.

The "TunnelCrack" vulnerabilities affect various VPN services. These vulnerabilities exposed a wide range of VPN users to potential exploitation, highlighting the risks associated with insecure VPN implementations. Additionally, the year saw the emergence of new attack vectors, such as flash loan attacks targeting protocols like Jimbo's Protocol. These attacks exploited vulnerabilities in decentralized finance (DeFi) platforms, demonstrating the need for robust security measures in the rapidly evolving blockchain and cryptocurrency ecosystem.

Fake PoC exploits targeting cyber researchers with VenomRAT

A malicious threat actor distributed a fake proof-of-concept (PoC) via GitHub, claiming to exploit a Remote Code Execution (RCE) vulnerability in WinRAR, identified as CVE-2023-40477 in September 2023. Their objective was to compromise users who downloaded this code by introducing the VenomRAT malware. It's crucial to underscore that this PoC is counterfeit and incapable of exploiting the intended vulnerability; rather, it is based on publicly available PoC code related to a GeoServer vulnerability documented under CVE-2023-25157.

This deceptive PoC is a Python script contained within a ZIP archive named CVE-2023-40477-main.zip, specifically labeled as poc.py. Upon execution, instead of triggering an exploit, the PoC generates a batch script. This batch script, in turn, retrieves an encoded PowerShell script and proceeds to execute it on the host system.

The purpose of this PowerShell script is to download the VenomRAT malware and establish a scheduled task to run it every three minutes. Once VenomRAT gains a foothold on a Windows device, it activates a keylogger, capturing and storing all keystrokes in a locally saved text file. The VenomRAT client implicated in this incident begins logging keystrokes, with the captured keystrokes saved in %APPDATA%\MyData\DataLogs_keylog_offline.txt. Subsequently, the client establishes communication with its Command and Control (C2) server, processing the server's commands as they are received. Although the attack has now ceased, it serves as a clear reminder of the inherent risks associated with obtaining PoCs from GitHub and executing them without conducting a comprehensive assessment to ensure their security.

cve-2023-40477

DecoyDog

Utilizing well-formed DNS requests for command and control

In April 2023, a sophisticated malware toolkit called DecoyDog was discovered, utilizing the Domain Name System (DNS) for command and control (C2) communication. Unlike conventional malware, DecoyDog's C2 operations rely on DNS traffic, making it highly elusive and challenging to detect. Initially based on the Pupy open-source remote access trojan (RAT), DecoyDog exhibits a level of sophistication beyond its predecessor. While Pupy is commonly used by penetration testers, DecoyDog's capabilities go far beyond those of a typical RAT. DecoyDog's behavior has raised serious concerns among security experts.

The malware responds to all well-formed DNS requests, exhibiting a wildcard-type behavior that is unusual among most malware, which often tries to avoid detection. This deliberate and sophisticated approach has allowed DecoyDog to evade identification and remain concealed for extended periods. The motives behind DecoyDog's development remain unclear, as no specific victims have been identified. The malware has been traced to at least three different threat actors, adding to the mystery surrounding its purpose and potential targets. The malware's behavior also indicates a level of sophistication and intentionality that raises concerns about the motives behind its development.

Due to its encryption methods, understanding the specific data being communicated by DecoyDog has proven challenging. Nonetheless, researchers have been able to identify the types of messages sent and profile the overall communication behavior of the malware.

Diversifying roles in multi-strain ransomware-as-a-service

A highly proficient threat actor, widely recognized as farNetwork and fluent in Russian, has intricately **associated itself with five distinct ransomware-as-a-service (RaaS) programs, assuming diverse roles within each.** As the orchestrator of the Nokoyawa ransomware-as-a-service, farNetwork cultivated expertise in the digital realm of underground forums. Operating under various pseudonyms, their engagements spanned from 2019 to 2023, during which they actively contributed to the JSWORM, Nefilim, Karma, and Nemty affiliate programs by overseeing malware development and operational management. farNetwork subjected potential affiliates to rigorous assessments, providing them with corporate account credentials sourced from the Underground Cloud of Logs service, which trades in logs pilfered by info-stealers like RedLine, Vidar, and Raccoon.

Affiliates were expected to escalate their privileges within target networks, exfiltrate files, execute the encryptor, and subsequently demand ransom payments. In the RaaS framework, affiliates stand to gain 65% of the ransom proceeds, while the botnet owner retains 20%. The ransomware developer, in this model, claims 15% of the overall share, with the possibility of a reduction to 10%. farNetwork recently declared its retirement from the cyberscene, culminating in the October shutdown of the Nokoyawa RaaS program, accompanied by the exposure of data from 35 victims.

Abusing blockchain based decentralized peer-to-peer network communication protocols

A newly discovered multi-platform threat, NKAbuse, has been found using the decentralized, peer-to-peer network connectivity protocol NKN (New Kind of Network) for communication. NKN, a network protocol incorporating blockchain technology for resource management, offers a secure and transparent model for network operations. While NKAbuse primarily targets Linux desktops, its ability to infect MIPS and ARM systems also poses a threat to IoT devices. The NKN network protocol, with over 60,000 official nodes, is designed to optimize data transmission through various routing algorithms. Unfortunately, this efficiency has made NKN a target for exploitation by malware operators. **NKAbuse utilizes the NKN public blockchain protocol to execute flooding attacks and act as a backdoor within Linux systems**.

To infiltrate systems, the malware uploads an implant to the victim host, establishes persistence through a cron job, and installs itself in the host's home folder. NKAbuse takes advantage of an obsolete Apache Struts vulnerability, CVE-2017-5638, to target a financial company. Using the NKN public blockchain protocol, NKAbuse executes DDoS attacks that are challenging to trace back due to the novel protocol's lack of active monitoring by security tools. The malware client communicates with the botmaster through NKN, facilitating data exchange using various protocols

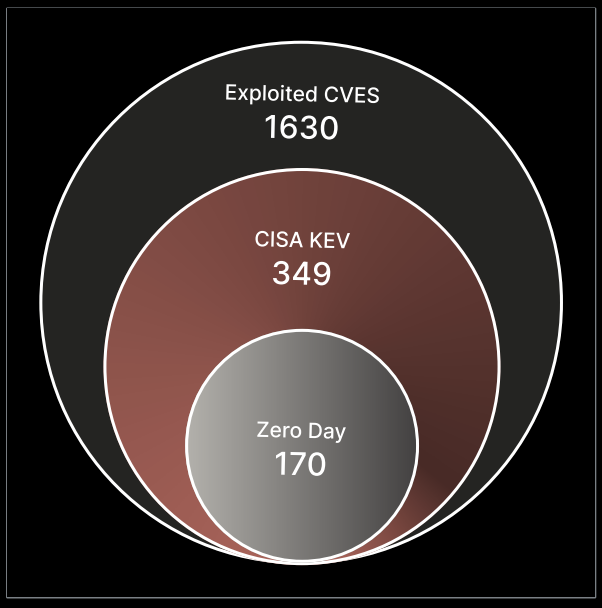
NKAbuse also acts as a potent RAT equipped with capabilities for persistence, command execution, and information gathering. Using the "Heartbeat" framework, it engages in regular communication with the botmaster, storing essential information about the infected host. Additionally, NKAbuse can capture screenshots of the infected machine through an open-source project. This multifaceted functionality makes NKAbuse a powerful tool for remote control and extensive information acquisition. The use of blockchain technology adds an extra layer of complexity, making defense against this threat exceptionally challenging.

03

"Decoding Vulnerabilities
A Deep Dive into the Anatomy of Cyber Weaknesses"

Vulnerabilities & Exploits

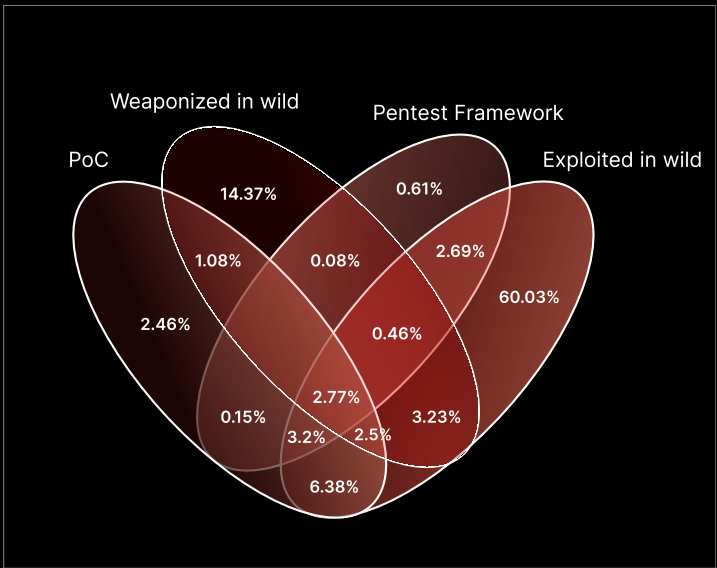
In 2023, a significant number of vulnerabilities, totaling 28,830, were identified and assigned CVE IDs. It's important to note that the actual count could be higher, considering vulnerabilities without CVE IDs. Additionally, cloud vulnerabilities were not included in CVE assignment, potentially expanding the overall vulnerability landscape. Moreover, a total of 1,630 vulnerabilities were exploited, with 349 carrying CISA Known Exploited Vulnerabilities (KEV) tags and 170 being zero-day vulnerabilities. Furthermore, 1,264 vulnerabilities lacking both Zero-day and CISA KEV tags were exploited in the wild.



3.1 Vulnerabilities and exploit

Analyzing Exploited Vulnerabilities: From Active Wild Exploits to Penetration Testing Toolkits

The distribution of exploited vulnerabilities shows that **81% were actively exploited in the wild**. Another 25% were weaponized, indicating that threat actors tailored vulnerabilities to their needs, seamlessly integrating them into their attack strategies. This type of weaponization, marked by inventive tactics, is typically orchestrated by technically proficient adversaries with specific objectives. Additionally, 19% of vulnerabilities had Proof of Concept, providing a foundational element for threat actors to create comprehensive tools for initial access, lateral movement, and privilege escalation. Finally, **10% of vulnerabilities were utilized in penetration testing frameworks** such as Metasploit, Acunetix, and Nessus, making them easily accessible for potential attacks and serving as a convenient toolkit for script kiddies.



3.2 PoC to Wild: Vulnerabilities Snapshot

Moreover, numerous vulnerabilities, not categorized as Zero-day or CISA KEV, were significantly exploited. The focus on prioritizing Zero-day or CISA KEV vulnerabilities often neglects those with straightforward initial vectors susceptible to exploitation. This alternative perspective enhances understanding of the threat landscape, enabling fair prioritization in remediation efforts. A key contributing factor to this scenario is the delay in promptly applying patches released by vendors. Ignorance also plays a role in enabling the exploitability of N-day vulnerabilities. The primary vectors facilitating these exploits include:

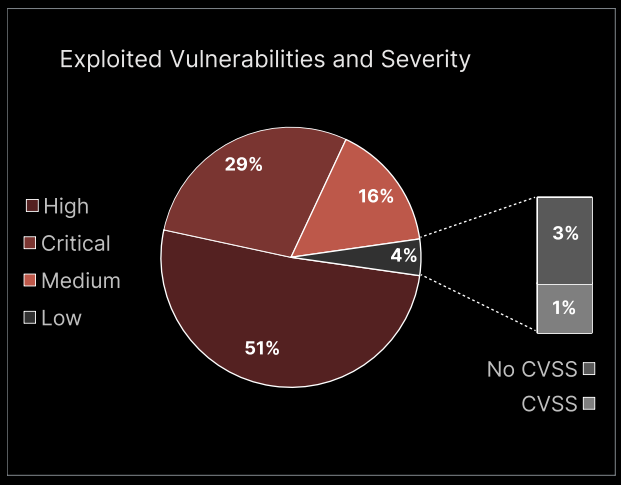
- **CWE-79**, resulting from inadequate sanitization or validation of input during web page generation, exposing vulnerabilities to attacks like Cross-Site Scripting (XSS).
- **CWE-89**, which involves mishandling special characters in SQL commands, leading to SQL injection vulnerabilities.
- **CWE-352**, or Cross-Site Request Forgery (CSRF), where attackers deceive a user's browser to execute undesired actions on trusted sites.
- **CWE-22**, addressing issues where software fails to restrict access to directories properly, potentially allowing unauthorized access to sensitive data or system files.
- **CWE-20**, emphasizing vulnerabilities arising from insufficient validation of user input, highlighting the critical importance of proper input validation to mitigate security threats, including buffer overflows and injection attacks.

CVSS Analysis 3.1
vulnerabilities and exploits

2023 Vulnerability Impact: A CVSS Score Analysis of Severity and Exploitation Trends

Analysis of exploited vulnerabilities unearthed in 2023 through the lens of Common Vulnerability Scoring System (CVSS) shows that **20% had a severity rating below 7,** categorizing them as Low, Medium, or having no CVSS Score. Furthermore, **29% of exploitations were linked to Critical severity vulnerabilities,** indicating heightened awareness and prompt patching, in contrast to **High Severity vulnerabilities, which constituted 51%** of exploitations. Additionally, a thorough examination of all vulnerabilities identified in 2023 reveals that over **800 vulnerabilities are awaiting severity score assessment**.

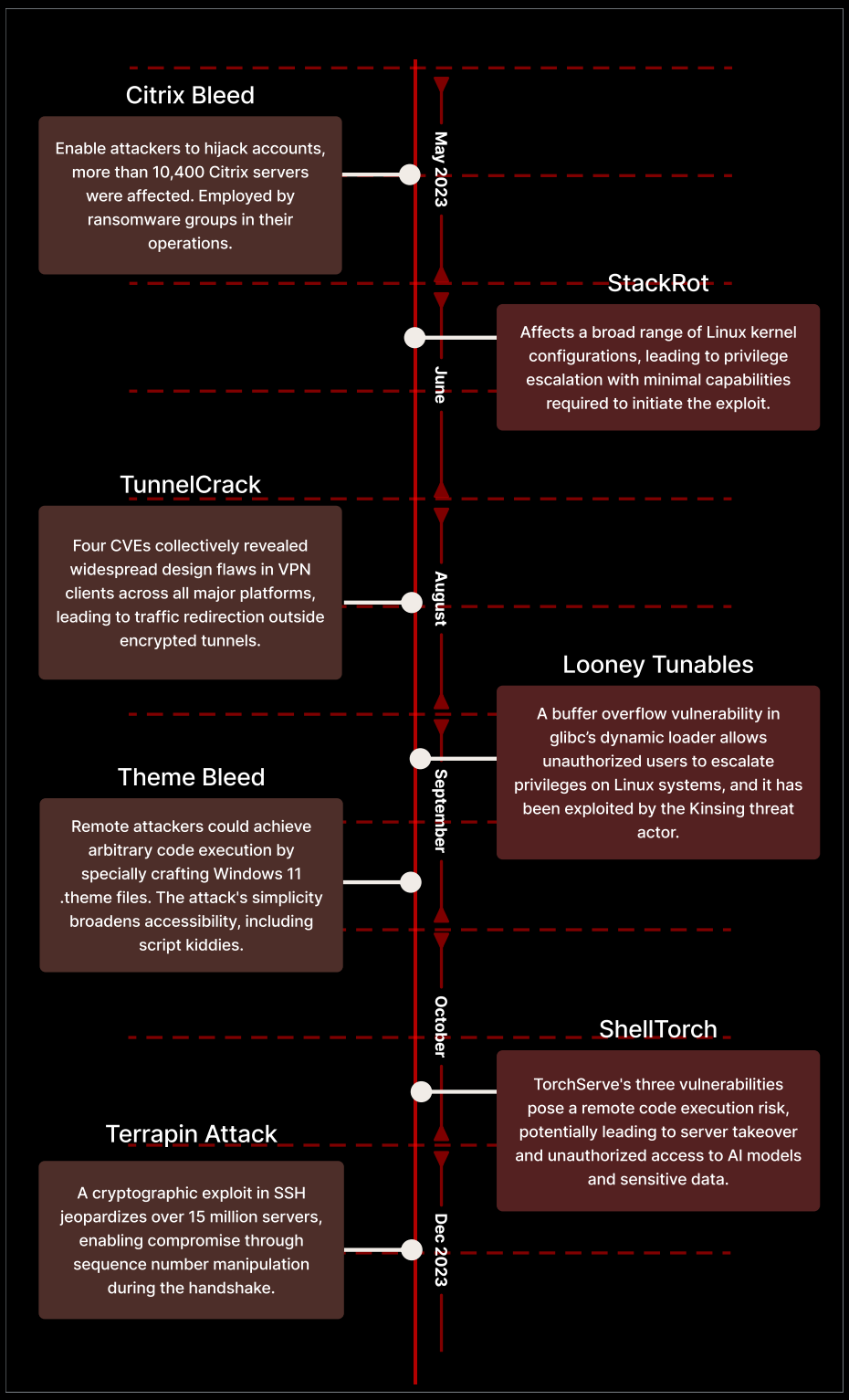
3.3 exploited vulnerabilities and severity



Celebrity Vulnerabilities 3.2
vulnerabilities and exploits

Celebrity vulnerabilities are widely recognized software flaws that have had far-reaching and devastating effects across various operating systems, software platforms, and hardware components. These vulnerabilities provide malicious actors with a gateway into sensitive systems, potentially leading to unauthorized access and compromise of critical information, with motives ranging from data theft to complete system disruption. As a result, businesses face significant consequences, including financial losses, damage to reputation, and potential legal actions.

In 2023, a series of celebrity vulnerabilities were identified, proving to be impactful as they were exploited by ransomware groups in coordinated campaigns facilitated by initial access brokers. These vulnerabilities were also **marketed as premium features on underground forums**. The exploitation of these vulnerabilities and their integration into adversaries' attack chains are causes for concern.



Two notable vulnerabilities, **Citrix Bleed** (CVE-2023-4966) and **Looney Tunables** (CVE-2023-4911), have caused significant disruption due to their widespread use in affected products or services, expanding the threat landscape. Citrix Bleed, disclosed in August 2023, was initially exploited in Zero-day attacks in May 2023 by the LockBit ransomware gang, with later exploitation by the Medusa ransomware and LockBit affiliates.

This vulnerability allowed attackers to steal authentication sessions and hijack accounts, gaining complete control of devices. On the other hand, Looney Tunables, affecting major Linux systems, is a buffer overflow vulnerability in Glibc's dynamic loader exploited for local privilege escalation. The Kinsing threat actor exploited this vulnerability to steal credentials and secrets from AWS environments.

Aged Vulnerabilities 3.3
vulnerabilities and exploits

In 2023, HiveForce Labs witnessed over 90 vulnerabilities from previous years, dating back to 2013, were widely exploited and capitalized upon in multiple attacks. Threat Actors have taken advantage of these vulnerabilities, leveraging them in active attacks, despite patches to fix these flaws have been made available.

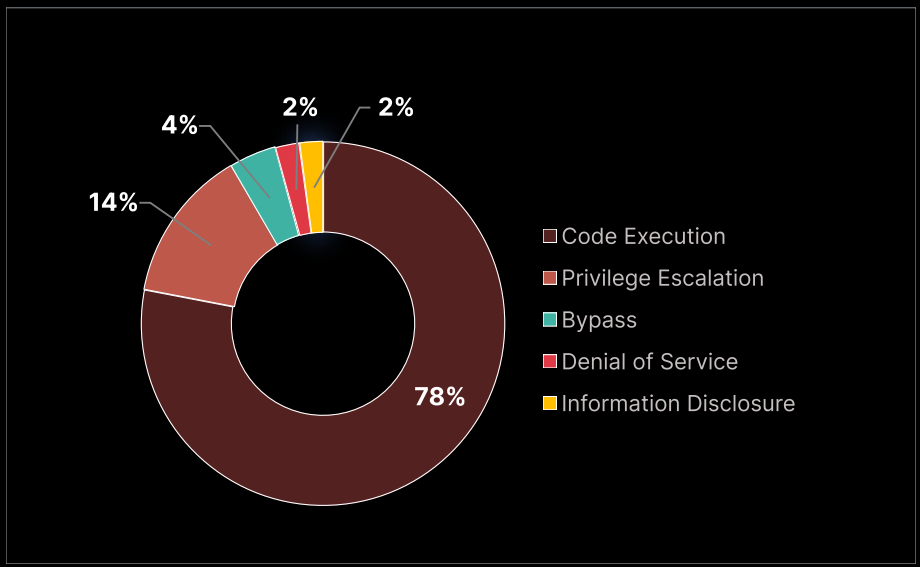
The persistence of these exploits can be attributed primarily to **negligent maintenance of devices or applications**. Throughout the year, these vulnerabilities were extensively exploited, with several Advanced Persistent Threat (APT) groups actively weaponizing them for various malicious activities.

The top three APT groups exploiting these vulnerabilities include APT28,Cadet Blizzard and the Lazarus Group

Additionally, ransomware groups like AvosLocker and Lockbit have been observed leveraging and incorporating these vulnerabilities into their operations.

Notably, 78% of these vulnerabilities allow for code execution, effectively acting as backdoors for threat actors within the infrastructure. This provides them with continued access and execution of their commands, posing significant security risks. Some prominent ongoing threats include the Microsoft Office Memory Corruption Vulnerability (CVE-2017-11882), the Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228), the Microsoft Windows Support Diagnostic Tool Remote Code Execution Vulnerability (CVE-2022-30190), and the Microsoft Office/WordPad Remote Code Execution Vulnerability with Windows API (CVE-2017-0199).

3.5 exploited vulnerabilities and impact



Aged Vulnerabilities 3.3

Vulnerabilities Exploitation Analysis

Some prominent ongoing threats include the Microsoft Office Memory Corruption Vulnerability (CVE-2017-11882), the Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228), the Microsoft Windows Support Diagnostic Tool Remote Code Execution Vulnerability (CVE-2022-30190), and the Microsoft Office/WordPad Remote Code Execution Vulnerability with Windows API (CVE-2017-0199).

One noteworthy instance involves the exploitation of CVE-2021-44228 in an operation executed by the Blacksmith LockBit ransomware, a highly impactful Ransomware-as-a-Service (RaaS) variant targeting critical sectors globally. Another case involves the weaponization of CVE-2022-30190 in a persistent cyber threat known as **MEME#4CHAN**. This threat is characterized by an intricate phishing campaign, utilizing a unique attack chain methodology to successfully infiltrate targeted systems and distribute the XWorm malware.

The GoldenJackal APT group exploited the flaw to gain initial access. In July 2023, Lokibot targeted worldwide by leveraging this vulnerability with the explicit purpose of amassing delicate information from compromised machines.

Zero Day Analysis 3.4
vulnerabilities and exploits

Zero Day Exploits, with their aura of mystery, present a unique cybersecurity challenge.

These vulnerabilities, often unknown to both vendors and defenders, possess a special power, allowing attackers to exploit systems with unmatched stealth and efficiency. Understanding these zero-days reveals the complex web of exploitation tactics and highlights the critical need for proactive defense measures in a constantly evolving threat landscape. In 2023, we encountered **over 90** actively exploited zero-day vulnerabilities, used by malicious software, ransomware groups, and Advanced Persistent Threats (APTs). These exploits resulted in severe consequences, inflicting significant financial losses on the victims. Several zero-days garnered significant attention due to their widespread and intensive exploitation.

- CVE-2023-0669: **Fortra GoAnywhere** MFT Remote Code Execution Vulnerability, This vulnerability affected 1,000 GoAnywhere instances exposed online, with only 135 on ports 8000 and 8001 housing the vulnerable admin console. Notably, it was exploited by threats such as Cl0p ransomware, TrueBot, LockBit ransomware, and the Graceful Spider APT group between February and May 2023.

- CVE-2023-4966: **Citrix Bleed** This vulnerability allowed attackers to extract valid session tokens from the memory of internet-facing vulnerable NetScaler devices. These compromised session tokens could be used to impersonate active sessions, bypassing authentication, including multi-factor, and gaining complete access to the appliance. Notably, this vulnerability persisted even after patching and rebooting, as copied tokens remained valid unless additional mitigation measures were taken.

- CVE-2023-38606: **Apple Buffer Overflow** Vulnerability This vulnerability was the third security flaw discovered in connection with **"Operation Triangulation,"** an iOS cyber-espionage spy campaign ongoing since 2019. The campaign utilized multiple zero-day vulnerabilities to bypass security measures in iPhones, posing an ongoing threat to user privacy and security.

Zero Day Analysis 3.4
vulnerabilities and exploits

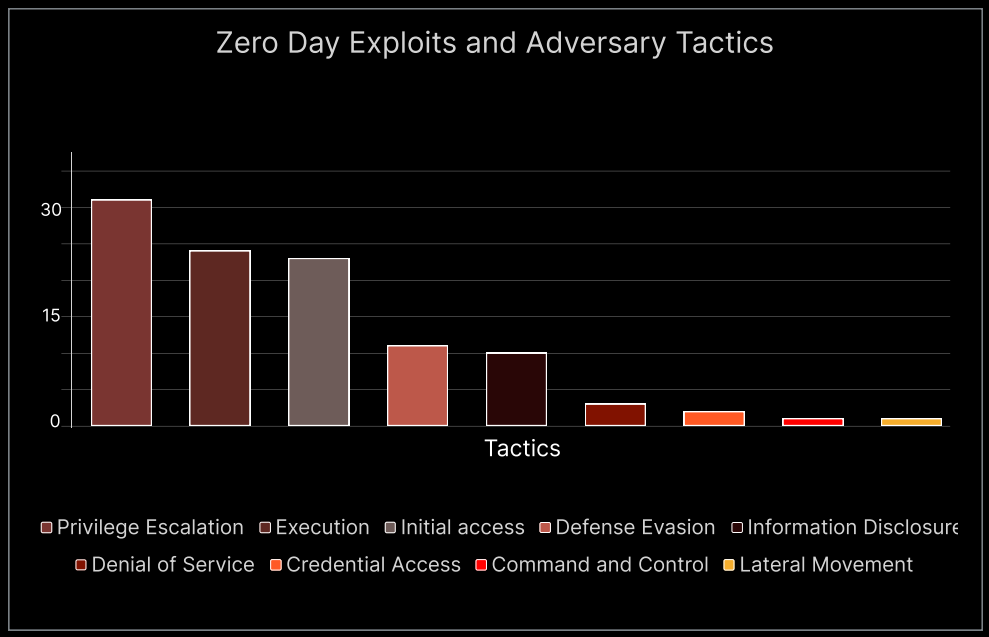
- CVE-2023-29059: **Arbitrary Code Execution** in 3CXDesktopApp The 3CX desktop app was compromised through a trojanized, multi-stage supply attack chain in the SmoothOperator campaign, enabling arbitrary code execution.

- CVE-2023-38831: **RARLAB WinRAR Code** Execution Vulnerability - The WinRAR code execution vulnerability emerged as a favored tool for threat actors, frequently employed in attack chains for Initial Access. Its exploitation technique is notably trivial, leading to its widespread adoption by seven distinct threat actors, who utilized a total of 14 distinct malware strains.

- CVE-2023-34362: **Progress MOVEit Transfer** SQL Injection Vulnerability A SQL Injection vulnerability, culminating in data exfiltration, was extensively exploited by the **FIN11 Threat group**, causing significant impact on major corporations such as Siemens, Shell, IBM, and Microsoft.

Adversaries have incorporated these zero-day vulnerabilities into their attack chains. The following illustration maps adversary tactics to zero-day vulnerabilities, showcasing the tactics employed upon exploiting these zero-days.

3.6 Zero day exploits and adversary tactics

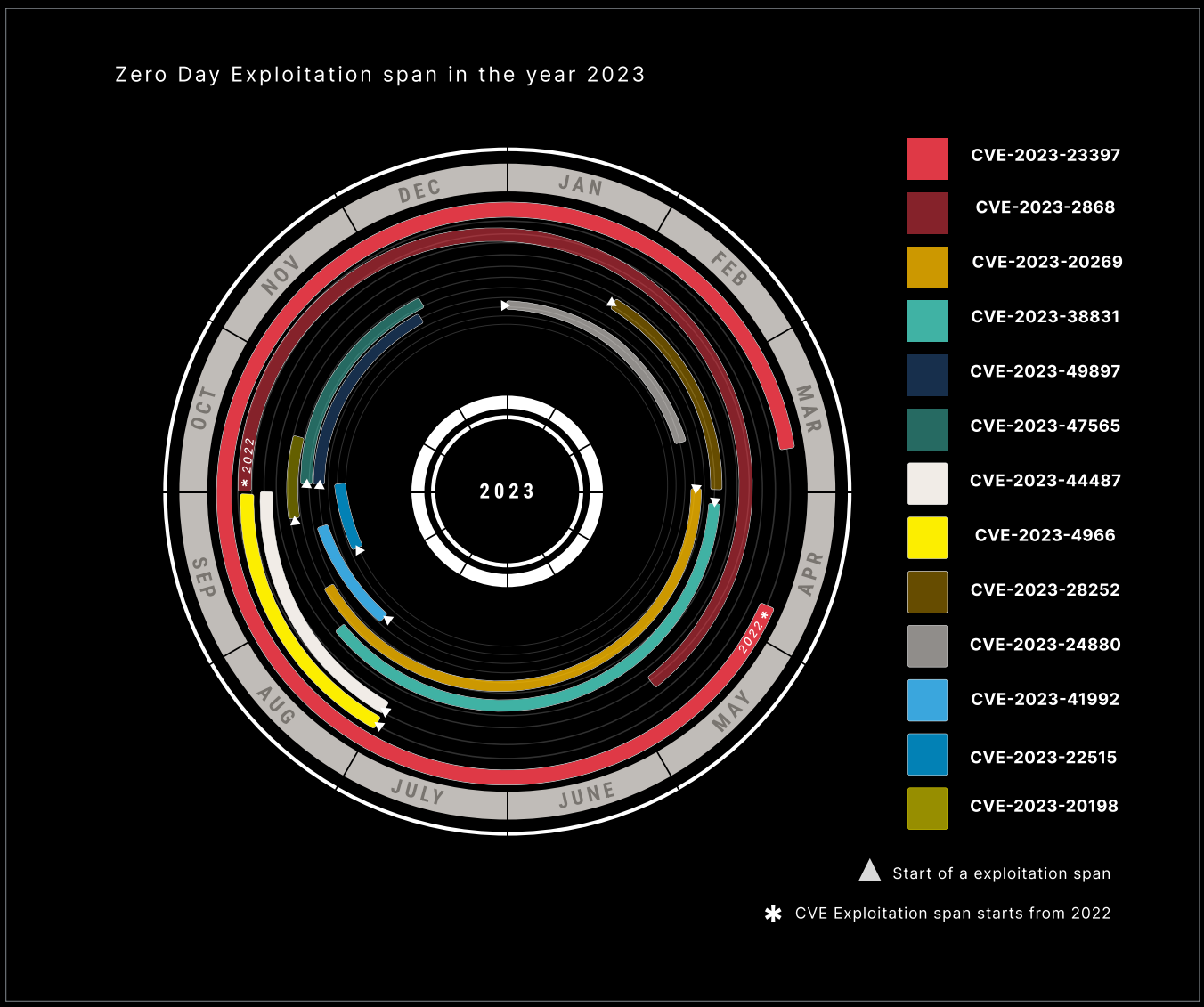


"An effective and meaningful log monitoring system is crucial for detecting adversary Privilege Escalation tactics. This involves enabling and forwarding system and application logs to a centralized system, where rules are created to monitor changes in user privileges."

Zero Day Analysis 3.4
vulnerabilities and exploits

Moreover, The temporal disparity between zero-day exploitation and patch availability significantly heightens the associated risks. In the year 2023, several zero-day vulnerabilities persisted without patches for more than a month, remaining within the reach of adversaries. During this window, attackers could infiltrate systems, exfiltrate sensitive data, and unleash havoc without fear of immediate mitigation measures.

The gap between the exploitation of zero-day vulnerabilities and the availability of patches epitomizes the perpetual cat-and-mouse game inherent in cybersecurity. Addressing **this disparity necessitates the development of a resilient cyber infrastructure** founded on realistic simulations of attack scenarios, ongoing cyber validation, agile response mechanisms, and actionable threat intelligence.



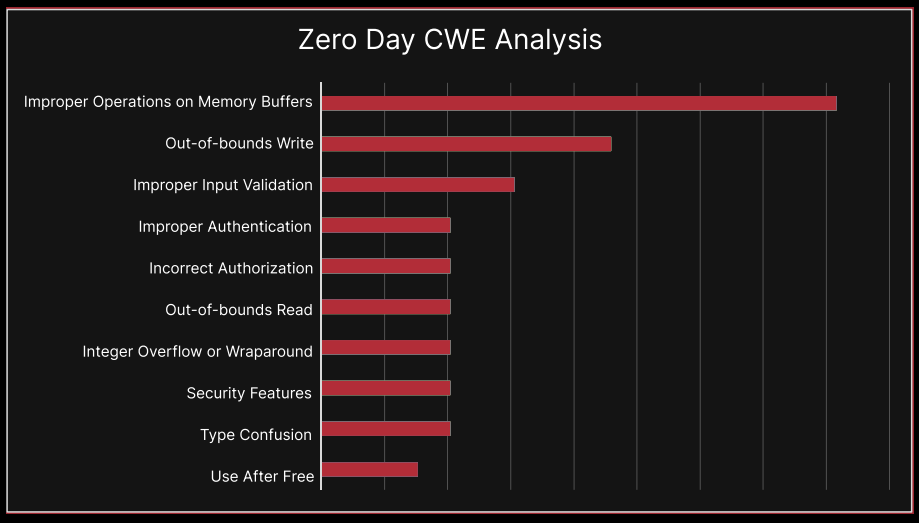
3.7 Zero Day Exploited date to Patch Availability date in Months

Zero Day CWE Analysis 3.5
vulnerabilities and exploits

Zero-days CWE Analysis

Analysis of zero-day vulnerabilities using the Common Weakness Enumeration (CWE) framework shows that approximately **one-third of these vulnerabilities originate from Memory Corruption or mishandling of Memory Operations.** Close behind are issues with input validation, as well as problems with authorization and authentication checks.

Software Development Life Cycle (SDLC) processes should give high priority to thorough checks for these weaknesses to proactively mitigate future risks. Memory-related problems can be prevented by emphasizing robust memory management techniques or by using programming languages that are highly memory-safe.



3.8 CWE Analysis

Vulnerability Fusion: the Power of Chained flaws 3.6

Vulnerability chaining involves exploiting multiple vulnerabilities in a sequential or simultaneous manner. This tactic is often used by adversaries to achieve a higher level of compromise than what is achievable with a single vulnerability alone. Moreover, this tactic often **puts low or medium-severity vulnerabilities in action**, effectively orchestrating them in tandem to create a chain reaction that complements each other, ultimately leading to successful exploitation. In 2023, several notable vulnerability chaining incidents occurred, showcasing the potential risks posed by this technique -

Zero-Click Outlook Remote Code Execution

CVE-2023-36710, a Remote Code Execution vulnerability in Windows Media Foundation core, necessitates user execution for successful exploitation. Combined with CVE-2023-35384, a security feature that bypasses vulnerability in the MSHTML platform, it satisfies the exploitability criteria, potentially resulting in Zero-click Outlook Remote Code Execution. Notably, both vulnerabilities individually possess a medium severity rating.

Server Bricking via MegaRAC BMC flaws

Two vulnerabilities were uncovered in MegaRAC BMC firmware, following the public disclosure of stolen firmware source code by the RansomEXX ransomware gang. CVE-2023-34329, an authentication bypass flaw, and CVE-2023-34330, a code injection flaw, work to assist adversaries in gaining remote code execution on servers running vulnerable firmware. The ramifications of these vulnerabilities are severe, including the remote takeover of compromised servers, rendering motherboard components useless (bricking), potential physical harm to servers such as over-voltage or firmware bricking, and the initiation of indefinite reboot loops.

Ivanti EPMM Unauthenticated Remote Code Execution

CVE-2023-35081, recognized as a remote arbitrary file write vulnerability in Ivanti EPMM, has been exploited in real-world attacks. This vulnerability was employed in conjunction with CVE-2023-35078, utilizing a chaining technique that facilitated the unauthenticated remote execution of malicious code on compromised systems.

Diplomats Surveillance and 3 iOS flaws

Three iOS vulnerabilities (CVE-2023-41991, CVE-2023-41992, and CVE-2023-41993) were chained together in a targeted attack aimed at deploying Predator spyware. These vulnerabilities were exploited in an exploit chain against a former Egyptian Member of Parliament. Predator, developed by Intellexa/ Cytrox, was utilized to conduct surveillance on targeted mobile devices.

Unauthenticated SharePoint Remote Code Execution

A pre-authentication Remote Code Execution scenario can be orchestrated by linking CVE-2023-24955 and CVE-2023-29357. CVE-2023-24955 empowers a site owner to execute code remotely on the SharePoint server. In tandem, CVE-2023-29357 facilitates JSON Web Tokens (JWTs) spoofing, granting the essential privileges to exploit CVE-2023-24955 effectively, culminating in code execution.

> *"These examples underscore the serious threat posed by vulnerability chaining, demonstrating how attackers could combine low or medium-severity flaws to execute highly damaging attacks. The dangers associated with vulnerability chaining emphasize the need to move away from solely focusing on vulnerabilities with critical severity ratings. Prioritizing vulnerabilities based on their potential to be exploited in real-world scenarios is crucial for effectively managing security risks "*

04

1

threat actor of the year

YORO-TROOPER

most notorious

high-impact activities in 2023

APT29

Lazarus

Threat Actors

In Action

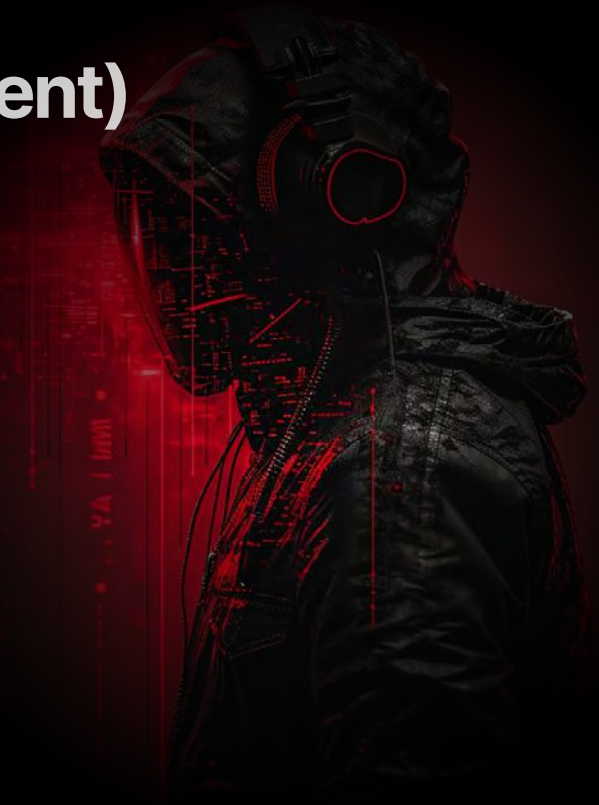
“

In 2023, HiveForce labs tracked over 100 distinct threat actors disrupting cyberspace, impacting technology giants and even security software by exploiting inherent flaws. Notable among these were the following actors, predominantly engaged in disruptive activities throughout the year.

Notable Actors 4.1
threat actors in action 2023

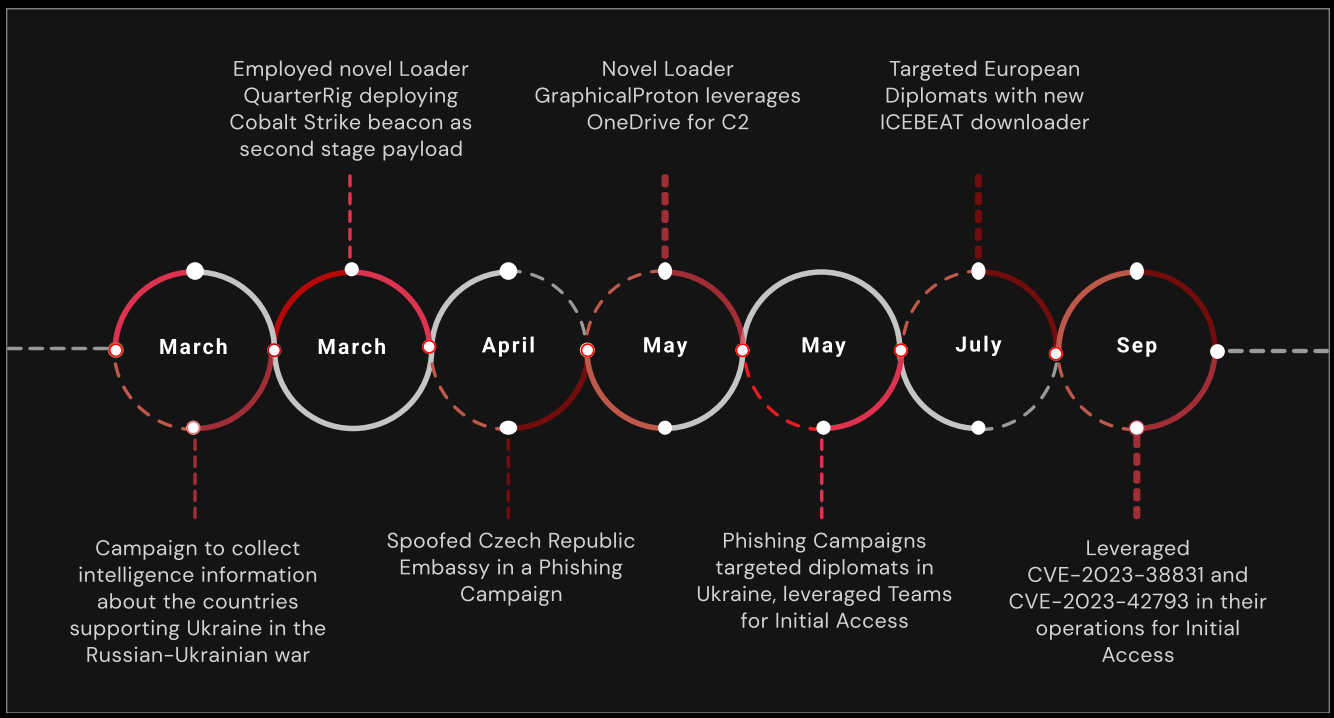
APT29 (2008-Present)

Russian state-sponsored actor

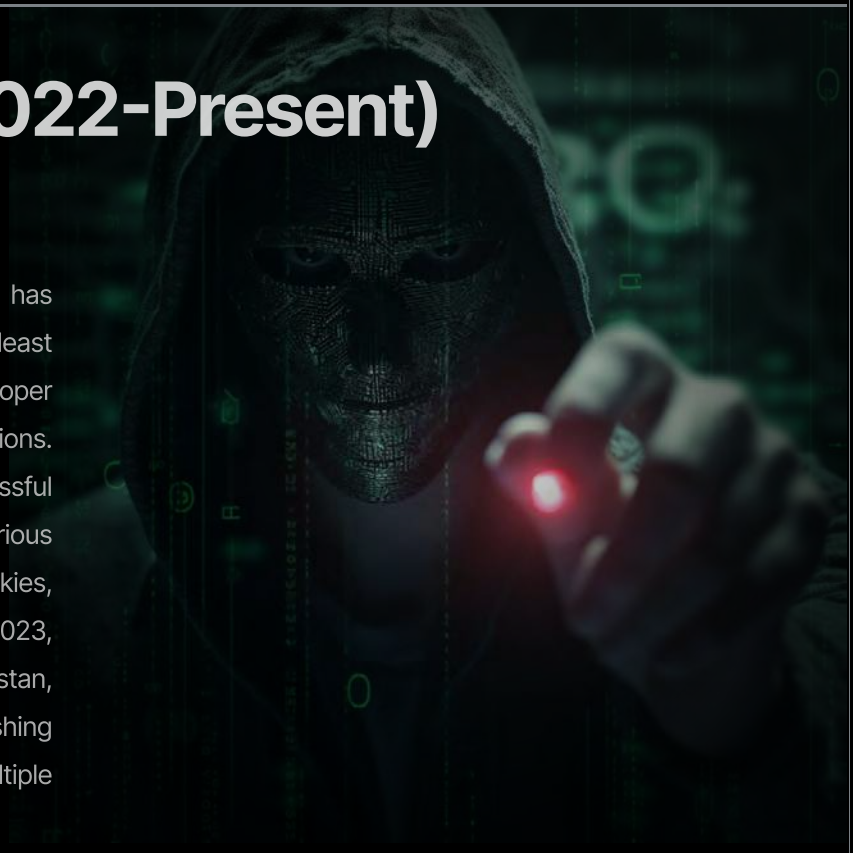


APT29, a Russian state-sponsored actor, targets foreign diplomats and ambassadors through large-scale spear-phishing campaigns. They capitalized on WinRAR vulnerability CVE-2023-38831 for Initial Access and exploited authentication bypass vulnerability CVE-2023-42793 in TeamCity Servers. Notable activities include **targeting European Diplomats with ICEBEAT downloader.**

4.1.1 APT29 activity timeline



Notable Actors 4.1
threat actors in action 2023

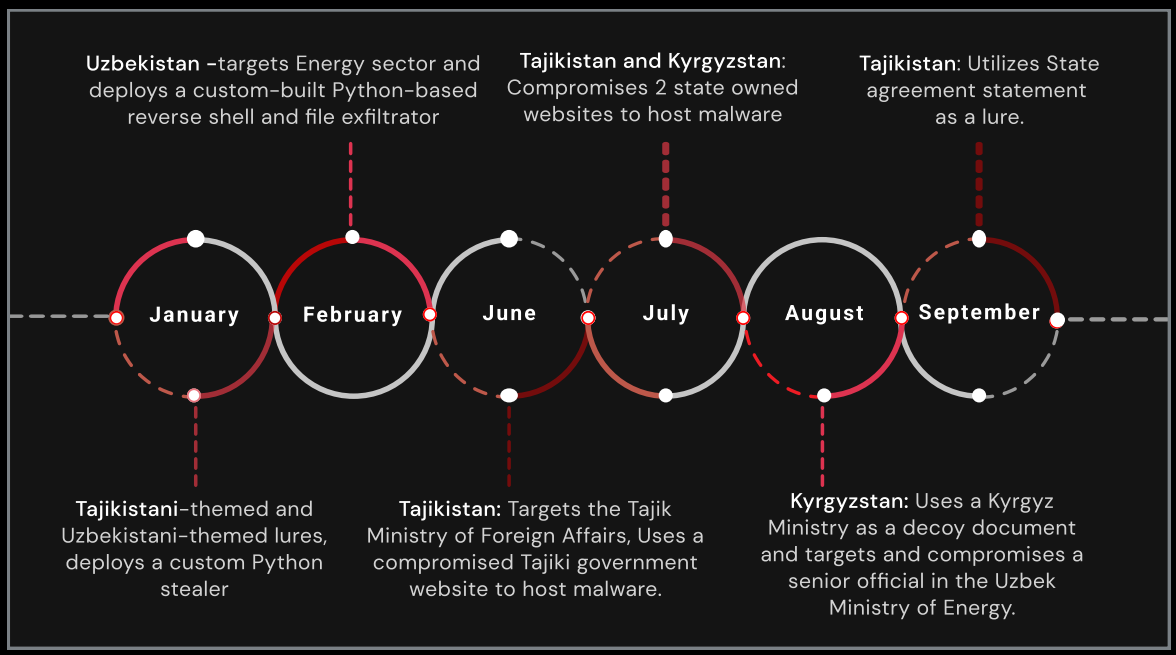


YoroTrooper (2022-Present)

A Stealthy digital espionage

An espionage-focused threat actor that has conducted successful campaigns since at least June 2022. The primary targets of YoroTrooper include government and energy organizations. The information stolen during successful compromises includes credentials from various applications, browser histories and cookies, system information, and screenshots. In 2023, YoroTropper was actively targeting Uzbekistan, Tajikistan, Kyrgyzstan with their targeted phishing lures and even compromised multiple government websites for hosting payloads.

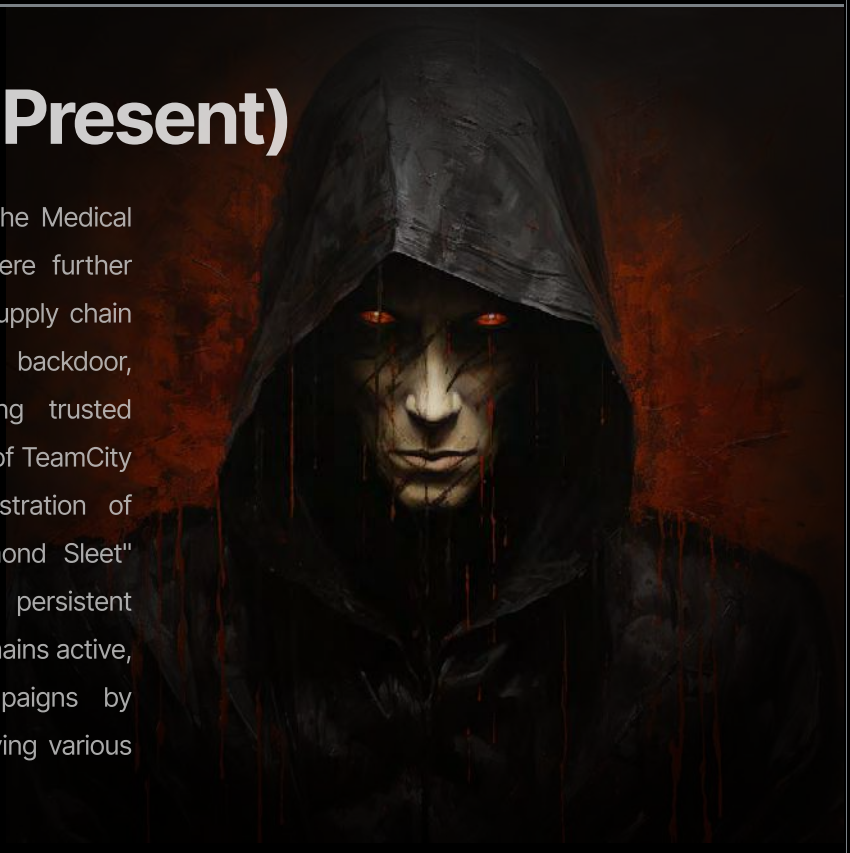
4.1.2 Yorotropper activity timeline



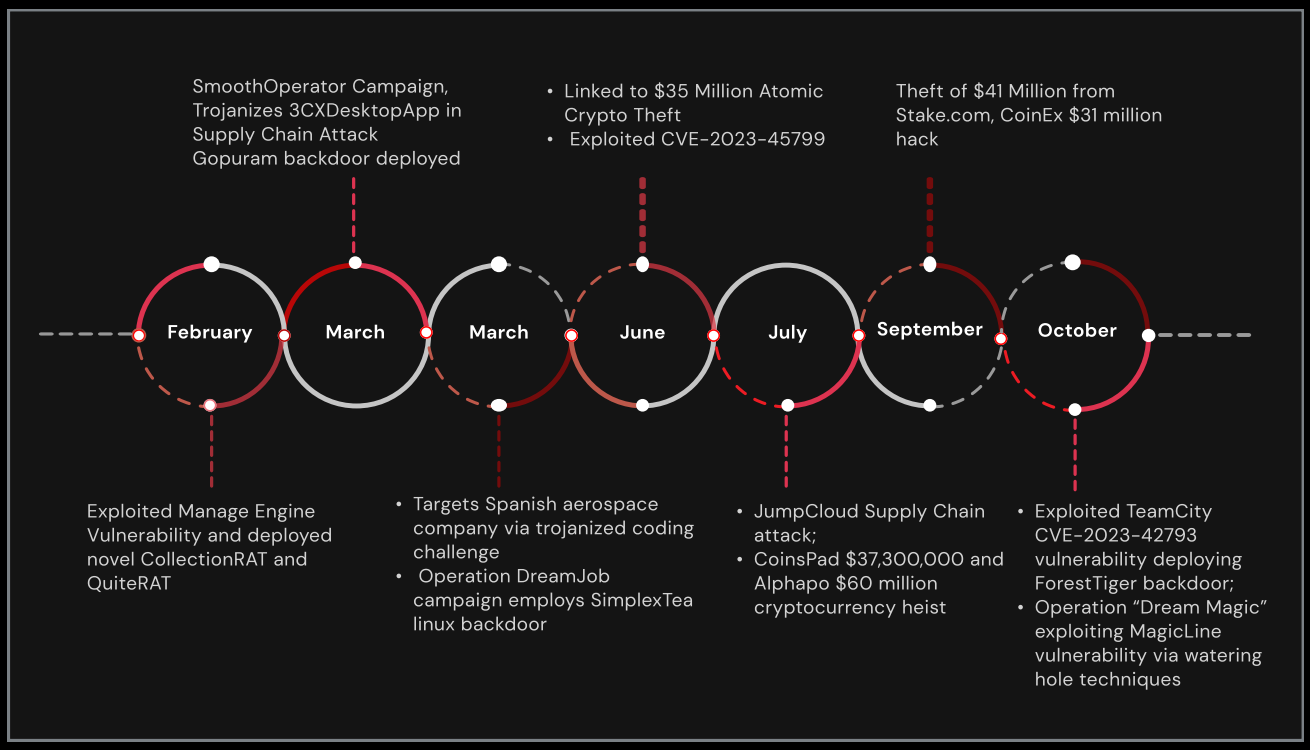
Notable Actors 4.1
threat actors in action 2023

Lazarus (2007-Present)

Lazarus group kickstarted 2023 targeting the Medical Research and Technology Sector, they were further found to be actively engaged in the 3CX supply chain attack and deployed the Gopuram backdoor, showcasing their adeptness at infiltrating trusted software channels. The group's exploitation of TeamCity CVE-2023-42793 in October and orchestration of operations like "Dream Magic" and "Diamond Sleet" highlighted their evolving techniques and persistent threat to global cybersecurity. The group remains active, consistently engaging in malicious campaigns by exploiting multiple vulnerabilities and deploying various malware strains.



4.1.3 Lazarus activity timeline

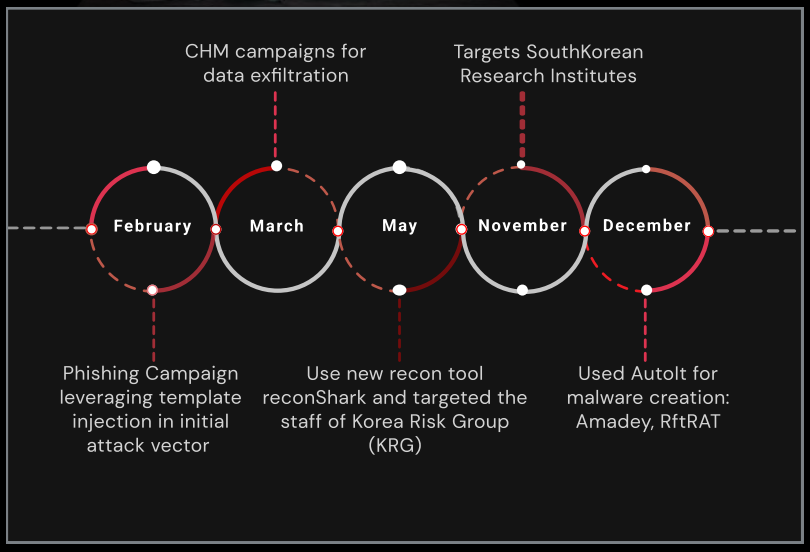


Notable Actors 4.1
threat actors in action 2023

KimSuky (2012-Present)

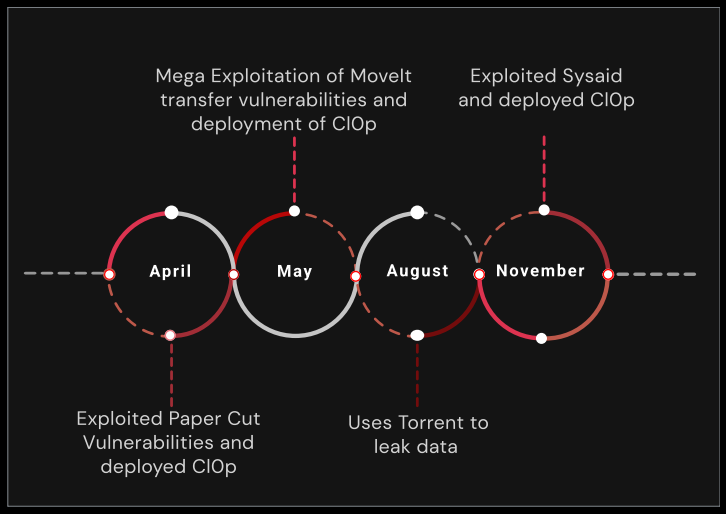
Kimsuky is believed to be engaged in Intelligence Collection and Espionage Activities for the North Korean Government Since 2012. The Kimsuky Group Leads the Way in Malware Delivery via CHM Files, running multiple CHM-Based Malware Campaigns in early 2023. The group has spearheaded social engineering tactics, employing various file types such as HWP documents and OneNote files to deliver initial stage payloads. They also utilize multi-level persona interaction during phishing campaigns to engage targets effectively.

4.1.4 Kimsuky activity timeline



FIN11 (2016 – Present)

FIN11 deploys the Cl0p ransomware and extracts data from compromised networks. They exploit vulnerabilities in software like SysAid and PaperCut to gain unauthorized access to systems.



4.1.5 FIN11 activity timeline

Emerging Groups 4.2

threat actors in action 2023

2023 also saw the rise of a number of formidable new adversaries, introducing novel tactics, techniques, and procedures (TTPs) that disrupted traditional security paradigms and challenging the resilience of digital environments. These new threat actors, driven by diverse motivations ranging from financial gain to ideological fervor, underscored the evolving nature of cyber threats. Understanding their modus operandi, targets, and impact becomes imperative in fortifying defenses and mitigating risks in an increasingly interconnected world. In this discourse, we delve into the landscape of cyber threats, unraveling the identities and characteristics of the new threat actors that came to prominence in 2023.

A cohort of formidable new adversaries has surfaced, unsettling traditional security standards with pioneering strategies and diverse motivations.

DragonBreath

AtlasCross

Clasiopa

It is paramount to dissect their strategies, discern their targets, and comprehend their impact to reinforce formidable defenses against the ever-shifting landscape of cyber warfare.

Emerging Groups 4.2
threat actors in action 2023

- **Atlas Cross -** A sophisticated Advanced Persistent Threat (APT) actor, referred to as Atlas Cross, was discovered employing a new attack process rooted in phishing documents. This actor exhibits high technical proficiency, employs cautious attack methodologies, and has been involved in targeted strikes on specific entities. The phishing activity serves as the primary method for infiltrating in-domain penetration. It introduces two **new Trojan horse programs, AtlasAgent and DangerAds**, and its attack chain indicates that while AtlasCross has a limited scope, its attack processes are characterized by high robustness and maturity.

- **Clasiopa**: Clasiopa stands out for its unique toolset, featuring a custom malware known as Backdoor.Atharvan. The precise infection vector employed by Clasiopa remains unidentified, but there are indications that the attackers may have gained access through brute force attacks targeting public-facing servers. **The tools used by Clasiopa include Atharvan, Thumbsender, and a custom proxy tool.** Notably, this previously unknown threat group has been detected targeting a materials research organization based in Asia.

- **UNC4841**: UNC4841 is a well-resourced threat actor known for employing a diverse array of malware and custom tools to support their global espionage operations. Their strategic targeting involves selectively deploying specific malware families, with SKIPJACK being the most frequently used. The primary focus of UNC4841 is on government and technology organizations, although they have been observed targeting other sectors as well. Their activity, observed in victims affected by **the exploitation of CVE-2023-2868, spanned from October 2022 to June 2023**. UNC4841 utilizes new and innovative malware, such as a passive backdoor named SKIPJACK, which involves trojanizing legitimate Barracuda ESG modules by injecting malicious Lua code.

Emerging Groups 4.2

threat actors in action 2023

- **DEV-0147 :** DEV-0147, a cyber espionage group based in China, known for data exfiltration operations by targeting government agencies and think tanks in Asia and Europe. Recently, the group has **breached diplomatic targets in South America**. DEV-0147 employs QuasarLoader, a webpack loader, to distribute malware, and maintains access using ShadowPad, a remote access trojan connected to other Chinese threat actors. In South America, the group conducts post-exploitation activities such as utilizing Cobalt Strike for command and control, data exfiltration, and exploiting on-premises identity infrastructure for reconnaissance and lateral movement.

- **Dragon Breath APT**: The Dragon Breath APT (also known as Golden Eye Dog & APT-Q-27) is a threat actor group specializing in targeting the online gambling sector and its participants. In their evolving attack techniques, the group has **introduced a double-clean-app method and innovative DLL sideloading tactics** specifically aimed at the gambling industry. These campaigns are primarily directed at Chinese-speaking Windows users, enticing victims with trojanized versions of popular applications. Furthermore, the group has increased the sophistication of its attacks by employing double DLL sideloading tactics, adding layers of complexity to evade detection.

- **CL-STA-0043** : CL-STA-0043, denoting a cluster with state-sponsored motivation, purports to be a nation-state actor with sophisticated capabilities. This threat actor **targets government entities in Africa and the Middle East**, employing advanced evasion techniques and tools to achieve their objectives. Among these techniques is the use of an **in-memory VBS implant to clandestinely execute webshells**, along with a rare credential theft method observed for the first time in the wild. To gain access to target networks, CL-STA-0043 exploits vulnerabilities in Microsoft Exchange and Internet Information Services (IIS) hosted on-premises. Once inside, they conduct reconnaissance to locate critical resources and utilize built-in Windows capabilities for privilege escalation. A notable observation was the detection of suspicious activity originating from the Exchange Server's w3wp.exe process, which investigation revealed to be caused by an in-memory VBScript implant deployed by the threat actor.

> *In essence, the ascent of these novel threat actors illuminates the perpetual necessity for security fortifications.*

05 MALWARE

most notorious high-impact activities in 2023

malware trends

XLoader

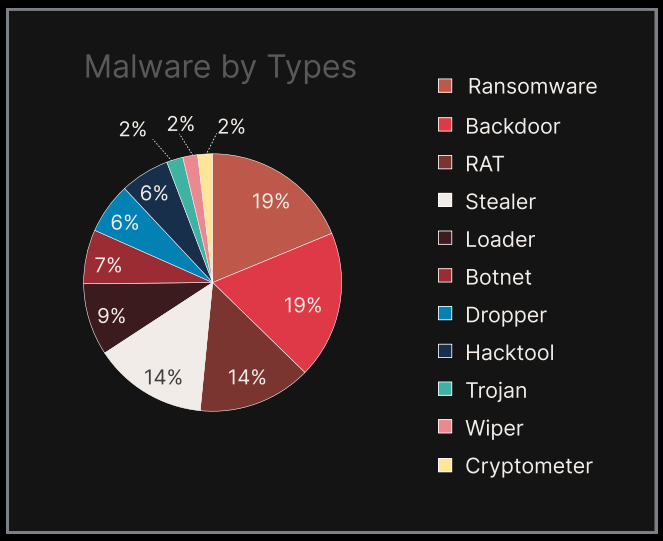
notable malwares

Agent Tesla

> HiveForce labs has identified over 400 unique malware strains actively used in major attack campaigns, with many evolving and adopting new tactics. The malware-as-a-service market on the dark web offers these tools for as little as under $10, complete with technical support services. Some models cater specifically to non-technical users, offering simplified operations and user-friendly interfaces.

Latest Trends 5.1
malware trends

Ransomware and backdoors have emerged as significant threats, followed by remote access trojans (RATs) and data stealers. These threats often originate from malware-as-a-service platforms or are developed by highly sophisticated actors. Many variants are adapted and customized from open-source software to fit specific campaign needs.



5.1 Malware types

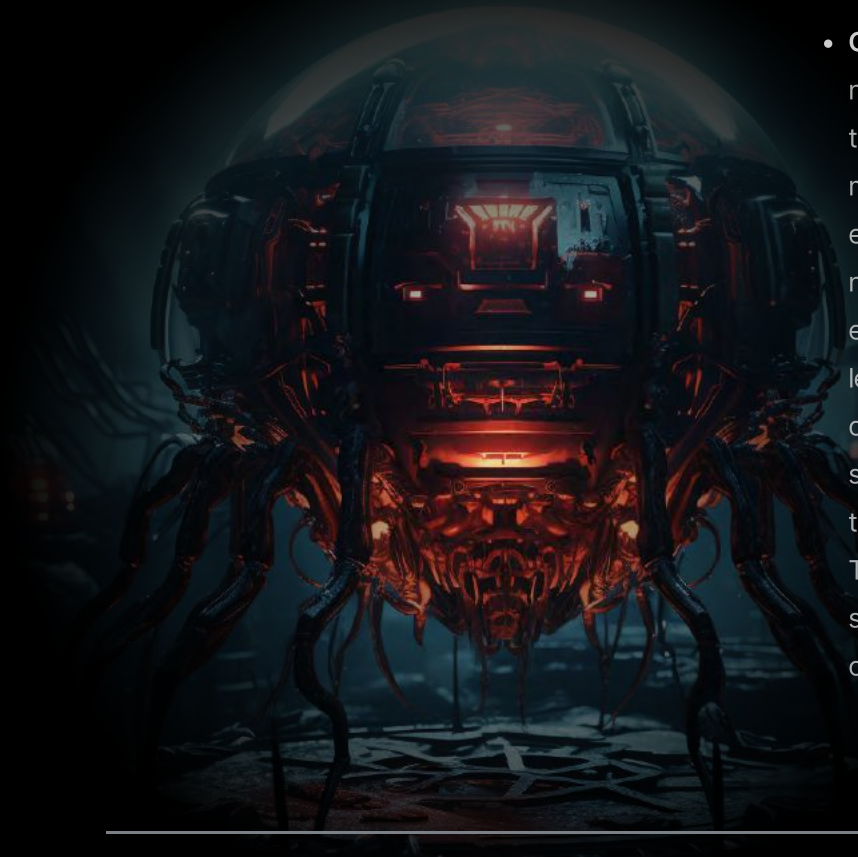
As AI technology continues to evolve, cybersecurity measures must also adapt to effectively counter these emerging threats.

- **Leveraging AI :** The rise of AI-driven threats is a major concern in cybersecurity. Although current trends mainly involve the use of AI for reconnaissance and early stages of attacks, there is a looming potential for its advancement into **more complex and comprehensive attack chains**. This evolution could **enable attackers to automate and enhance various stages of cyber attacks**, making them more sophisticated and difficult to detect and mitigate. As AI technology continues to evolve, cybersecurity measures must also adapt to effectively counter these emerging threats.

- **Takedown and Resurgence :** Despite numerous multi-state, multi-agency coordinated takedown operations on malware service infrastructure, the malware operators have demonstrated resilience by quickly rebounding from these setbacks. Despite periods of limited activity, they resurge within months, underscoring the challenges of combating sophisticated cyber threats and the agility of malicious actors. For instance, the QakBot Command and Control (C2) infrastructure was dismantled in August; however, it resurfaced within a remarkably short span of three months.

Latest Trends 5.1
malware trends

- **Malware-as-a-Service (MaaS) :** MaaS platforms present significant challenges, with subcategories including Packer-as-a-Service, Ransomware-as-a-Service, and Phishing-as-a-Service, posing significant threats in 2023. These markets operate on an affiliate model, wherein operators lease their services, including malware deployment, control panel access for managing attacks, and technical support services. Their user-friendly interfaces enable individuals with minimal technical expertise to purchase and utilize these services, significantly amplifying their potential as weapons for a broader spectrum of attackers.



- **Open Source Software Abuse**: There is a noticeable rise in the adoption of open-source tools by malware developers to create new malware strains. This trend involves customizing existing open-source software to meet specific needs, enhance stealth, and maximize effectiveness in cyberattack campaigns. By leveraging the flexibility and functionality of open-source tools, attackers can quickly develop sophisticated malware variants that are tailored to exploit vulnerabilities and evade detection. This approach allows them to stay ahead of security measures and pose a greater threat to organizations and individuals alike.

FormBook (xLoader)

FormBook, also known as xLoader, is classified as a high-level threat and falls under the category of stealers. It is primarily distributed through phishing attacks. FormBook has been in operation since 2016 and is offered as a Malware-as-a-Service (MaaS) on underground hacking forums. **Known for its effective evasion techniques and affordability,** FormBook is particularly adept at stealing and exfiltrating data. In 2023, FormBook expanded its distribution strategy by utilizing malvertising, leveraging the MalVirt Loader to avoid detection. With the decline of Qbot, FormBook has emerged as one of the most prevalent malware strains. Its ability to steal data, adapt to new environments, and evolve continuously has cemented FormBook's position as a persistent threat in the cybersecurity landscape.

Agent Tesla (Negasteal)

Agent Tesla, also known as Negasteal, is classified as a high-level threat and is categorized as a Remote Access Trojan (RAT). It is primarily distributed through phishing attacks. Since February 2023, Agent Tesla has been a persistent threat, utilizing GuLoader in new phishing campaigns targeting various sectors and countries. In an August phishing campaign, a new version of Agent Tesla was distributed through a carefully crafted Microsoft Excel document, **exploiting a long-standing memory corruption vulnerability in Microsoft Office's Equation Editor**. In November, a new variant of Agent Tesla emerged, delivered via a lure file using the ZPAQ compression format, with the aim of harvesting data from multiple email clients and nearly 40 web browsers.

Emerging Threats 5.3
malware mavericks

Greatness

A Phishing-as-a-Service (PhaaS) platform, has been active since mid-2022, experiencing notable spikes in activity during December 2022 and March 2023. This platform equips attackers with tools to orchestrate convincing campaigns aimed at stealing login credentials and session cookies. **It automatically generates pages with realistic details,** allowing attackers to harvest credentials entered on these fake pages. Greatness boasts features such as bypassing multi-factor authentication, employing location-based victim filtering, and integrating with Telegram bots for real-time monitoring. Its user-friendly interface **enables individuals with minimal technical expertise** to procure and deploy Greatness, thus expanding its potential as a weapon for a wider spectrum of attackers.

RustBucket

A macOS-targeting malware family, has been active since April 2023 and is attributed to the North Korean threat actor group, **BlueNoroff**, renowned for its sophisticated cyberattacks. Operating as a multi-stage malware, RustBucket employs various phases to evade detection and achieve its malicious objectives. In its initial stage, typically an AppleScript component, RustBucket establishes persistence and downloads the next stage payload. The malware retrieves a second-stage payload — a Rust-based binary equipped with features for gathering extensive information and executing additional Mach-O binaries or shell scripts on the compromised system.

Pikabot

A malicious backdoor that surfaced in early 2023, has emerged as a significant threat in malvertising campaigns, notably through search engine advertisements. The malware exhibits a modular structure, comprising a loader and a core component responsible for executing most functionalities. Notably, Pikabot bears resemblances to the **Qakbot trojan**, evident in its distribution methods, campaign strategies, and malware behaviors. PikaBot, attributed to the **TA577** threat actor and associated with **Blackbasta ransomware** distribution, employs sophisticated tactics such as decoy websites and fingerprinting, underscoring the dynamic nature of cyber threats. Additionally, the threat actor **Water Curupira** has been actively disseminating the PikaBot loader malware through spam campaigns.

Ransomware Roundup 06

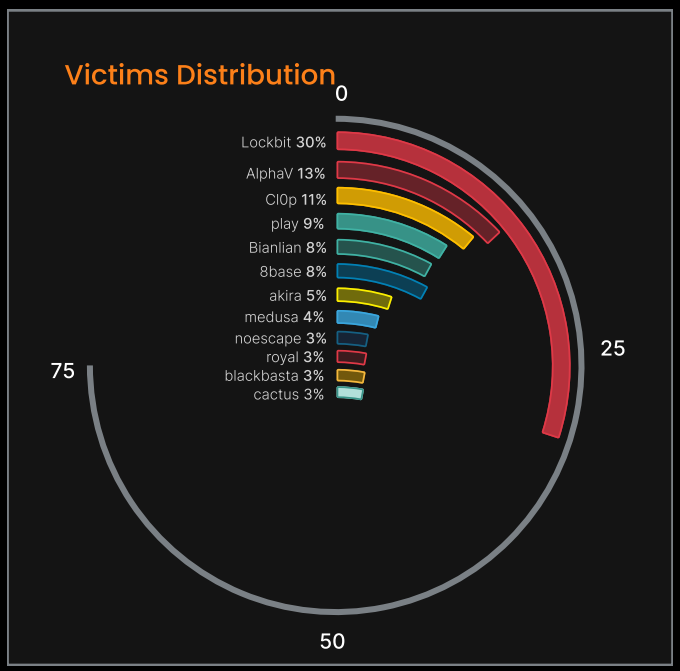
ransom rampage

Ransomware Roundup

Ransomware remains a persistent threat and continues to flourish, particularly within the affiliate or Ransomware-as-a-Service model. Year over year, there has been a **67% increase** in victim postings, with the victim volume nearly doubling, resulting in 4,769 victims across diverse industries and countries. Additionally, there have been 63 unique ransomware groups identified, utilizing encryption, data exfiltration, and other coercive techniques.

The dataset sourced from dark web forums provides only a partial view, highlighting major ransomware operators while overshadowing smaller ones. These lesser-known ransomware operators, though not active on dark web forums, still pose significant threats to the resilience of IT systems. Their operations, albeit less visible, contribute to the ongoing challenges faced by organizations in combating ransomware attacks.

6.1 Victim's Distribution



In 2023, ransomware had a profound impact, affecting 1 in 10 organizations globally. The targets were not limited to businesses; hospitals, schools, and government agencies were also victims, leading to disruptions and potential data breaches. The financial implications were substantial, as cybercriminals collected record ransoms. However, the human toll was equally significant, with individuals experiencing anxiety and inconvenience due to disruptions in critical services. This surge in ransomware attacks served as a stark reminder of the importance of enhancing cybersecurity measures, providing employee training, and fostering international collaboration to address this evolving threat.

In 2023, ransomware significantly impacted global organizations across sectors, highlighting the critical need for enhanced cybersecurity, employee training, and international collaboration.

Ransomware Roundup 06

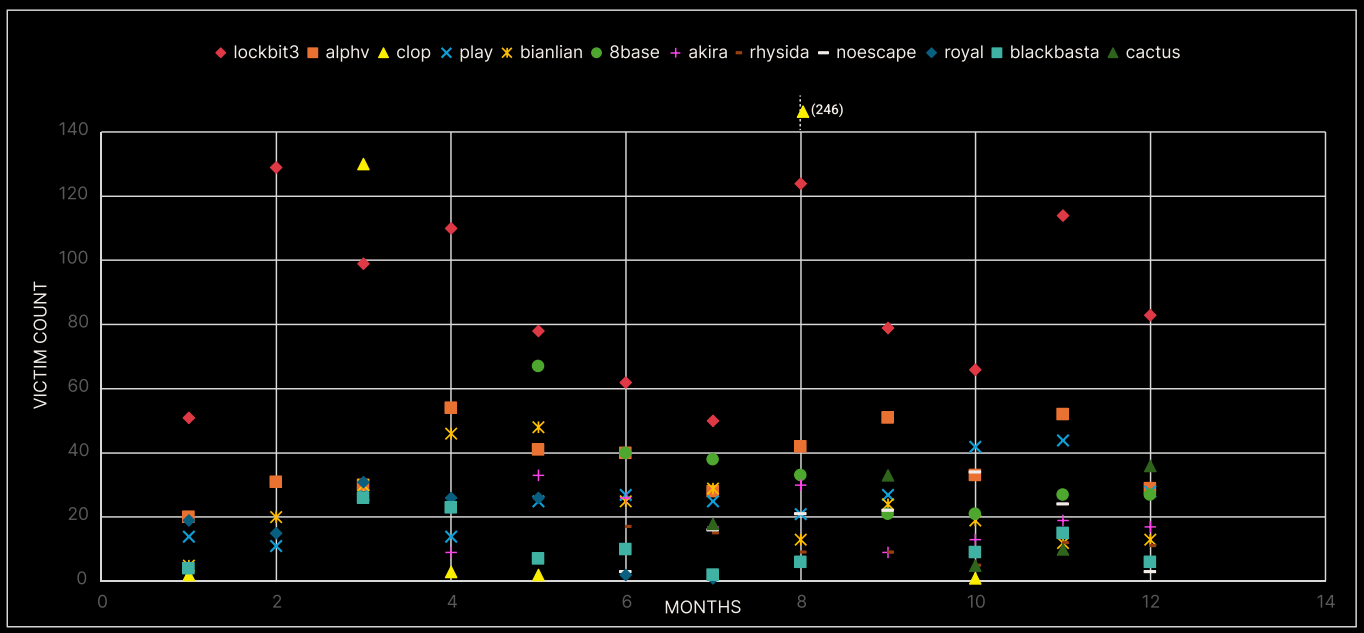
ransom rampage

In 2023

Analysis of ransomware victims over the past 12 months underscores the enduring threat posed by Lockbit, which has remained consistently active throughout the year. The Cl0p group experienced a surge in activity, notably in March through the exploitation of the GoAnywhere vulnerability, and again in August due to the widespread exploitation of the MoveIT zero-day vulnerability. The Cl0p group's exploitation of MoveIt resulted in a staggering $75 million in gains.

Lockbit remains a formidable ransomware threat, with a 7% increase in victim counts compared to the previous year, capturing 30% of the victim share. **AlphV**, in contrast, has nearly doubled its victim count. **Cl0p**, a newcomer to the top list, has witnessed a staggering 1100% increase in victim count.

RANSOMWARE VICTIMS OVER 12 MONTHS



6.2 Ransomware victims over 12 months

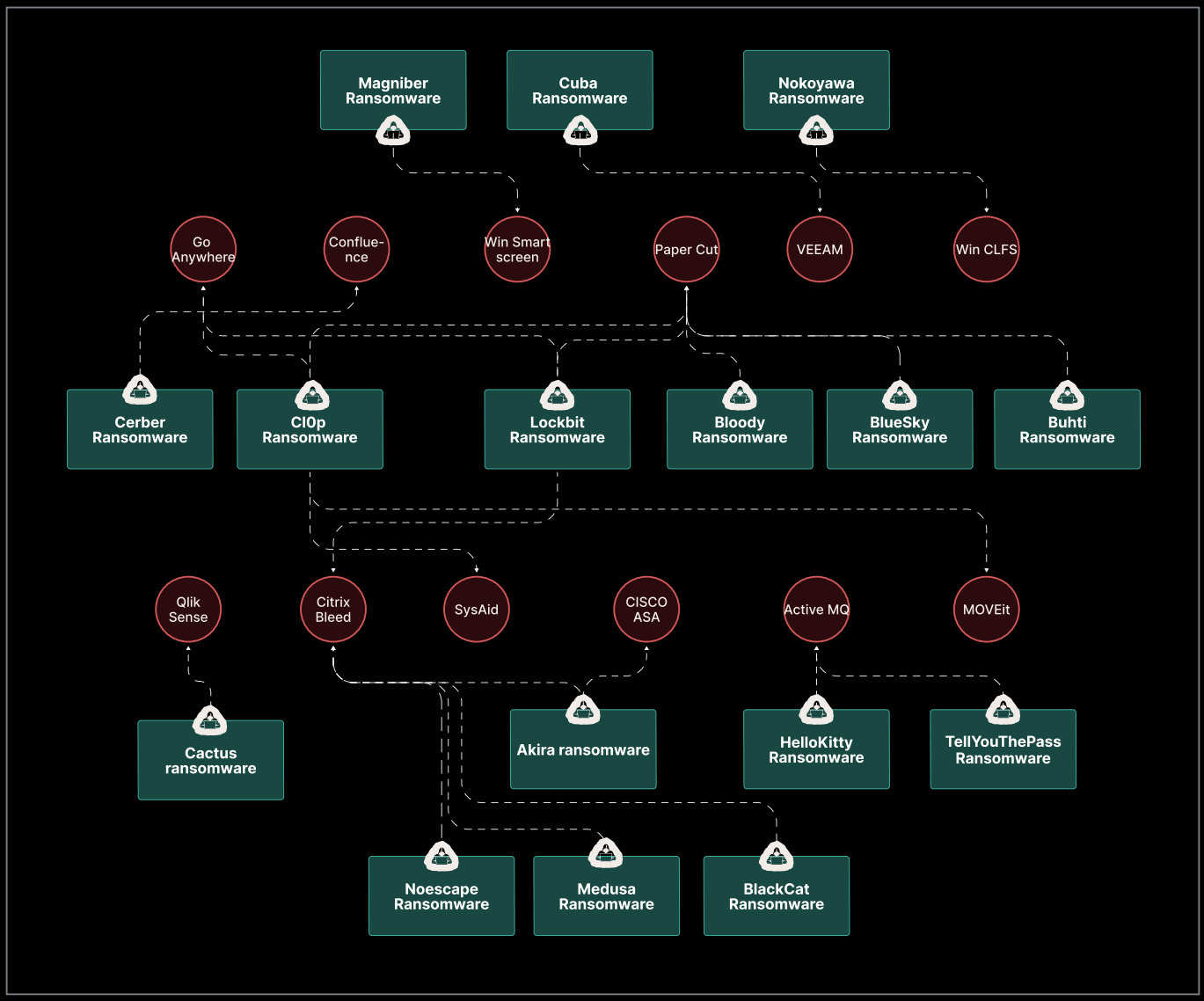
Ransomware Roundup 06

ransom rampage

A Tale of Two Forces: CVEs and Ransomware's Unlikely Bond

2023 also witnessed multiple ransomware groups emerging as pioneers in exploiting vulnerabilities, utilizing them primarily for initial access, which subsequently escalated to full-fledged system compromise, culminating in the deployment of ransomware.

CVE-Ransomware Relationship



6.3 CVE-Ransomware Relationship infographics

Notable Campaigns 6.1

ransomware roundup

Lockbit

LockBit ransomware, also known as ABCD Ransomware, poses a high threat level and operates using various delivery methods, including phishing, exploiting vulnerabilities, and brute-forcing exposed Remote Desktop Protocol (RDP) and Virtual Private Network (VPN) services. Active since September 2019, LockBit functions under a Ransomware-as-a-Service (RaaS) model, allowing affiliates to target critical infrastructure sectors worldwide. The group has evolved over time, with iterations like LockBit 1.0, 2.0, 3.0, and LockBit Green, each employing different tactics and tools.

In 2023, LockBit Green emerged as the latest variant, expanding its compatibility to include macOS alongside Windows, Linux, VMware/ESXi, and other platforms. Known for its dual-use tools and ability to move laterally within compromised networks, LockBit presents a significant challenge for organizations.

In 2023, notable LockBit attacks targeted entities such as TSMC, MCNA Dental, and CDW, demonstrating its widespread impact. LockBit 3.0 alone saw a surge from 393 cases in 2022 to 1,038 in 2023, marking a substantial 164% increase.

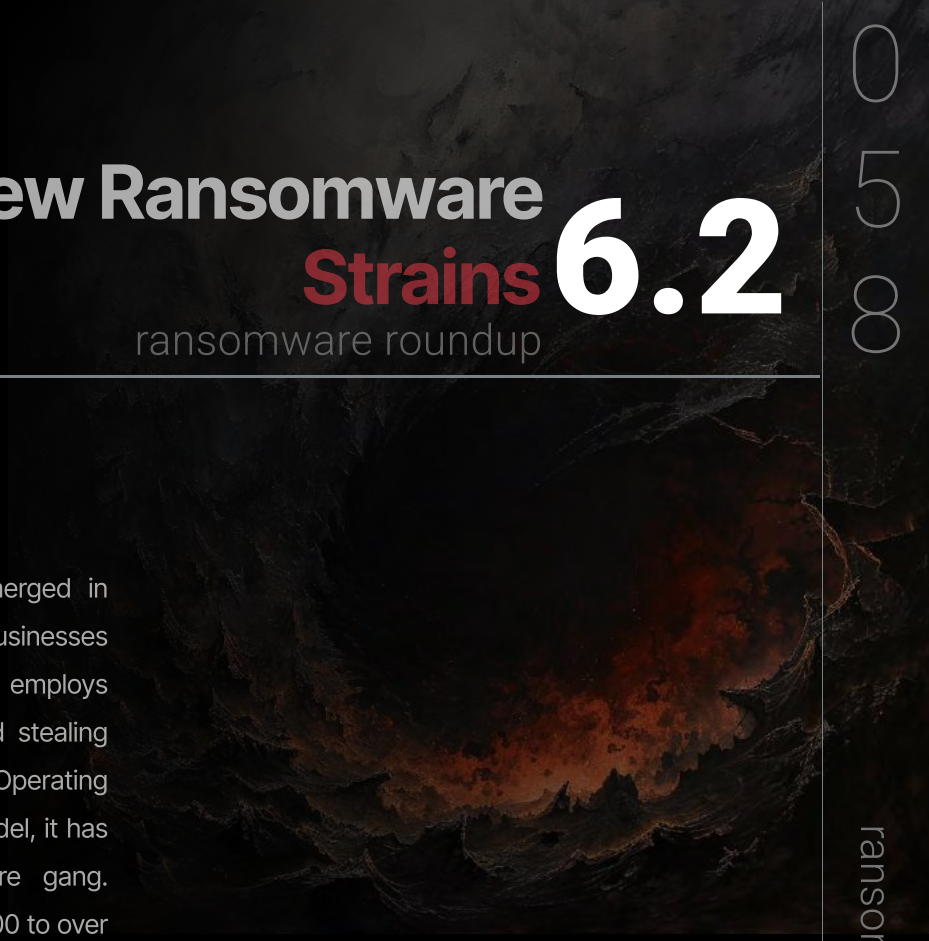
Cl0p

In 2023, the Cl0p ransomware, considered one of the most sophisticated variants, intensified its operations, utilizing pure extortion tactics such as **"encryption-less ransomware."** Managed by a Russian-speaking group, Cl0p operates on a Ransomware-as-a-Service (RaaS) model, engaging in more sophisticated attacks by leveraging zero-day vulnerabilities to demand higher ransoms.

The group strategically times its malicious operations ***during holidays*** to capitalize on reduced staffing levels in targeted companies. For instance, the MOVEit attack campaign was launched during the summer of 2023. In January, Cl0p disclosed targeting over 130 organizations by exploiting a zero-day vulnerability in GoAnywhere MFT's secure file transfer tool. Additionally, in May 2023, the group extensively used a SQL injection zero-day vulnerability to implant a web shell named LEMURLOOT on MOVEit Transfer web applications.

New Ransomware Strains 6.2

ransomware roundup



Akira

A sophisticated ransomware threat that emerged in March 2023 and is written in C++, targeting businesses primarily in the United States and Canada. It employs double extortion tactics, encrypting data and stealing sensitive information for added pressure. Operating under a Ransomware-as-a-Service (RaaS) model, it has ties to the now-defunct Conti ransomware gang. Ransom demands typically range from $200,000 to over $4 million. Akira deletes Windows Shadow Volume copies on affected devices and features a unique retro-style Tor leak site.

$200k to $4M

Dark Power

The Dark Power ransomware first surfaced in early 2023, employing a strategy of multi-extortion by threatening to expose victim data if demands are not met. Written in Nim, a versatile language that runs on multiple platforms, Dark Power also incorporates standard ransomware functions such as VSS removal. Upon infection, instead of a traditional ransom note, the ransomware drops a multi-page PDF file containing instructions for the victim. Dark Power attacks are not targeted towards specific industries or geographic locations but rather opportunistic in nature.

Dark Power's encryption mechanism relies on AES CTR (counter/block cipher mode), utilizing the Nimcrypto library. String encryption is achieved through a combination of base64 encoding and a hard-coded SHA256 key. Encrypted files are identified by the .darkpower file extension.

The ransomware attempts to terminate various services, including those related to Sophos, MailEnable, MSSQL, and any services with 'SQL' or 'Backup' in their names, to facilitate the encryption process. It also includes a predefined list of processes to terminate and specifies files and folders to exclude from encryption.

After encryption, Dark Power disables or destroys Volume Shadow Copy (VSS) volumes and tries to clear Windows Event Logs using WMIC. Dark Power demands extortion payments in XMR (Monero), with initial ransom amounts set at $10,000 USD in early campaigns. Victims are directed to contact the attacker through a .onion URL (TOR) and provided with a qTox messenger ID for direct communication.

Kadavro Vector

A specific variation of **NoCry ransomware** that emerged in 2023. It utilizes encryption to lock files on machines that have been compromised. The attackers then demand payment in Monero (XMR) cryptocurrency in exchange for the decryption of the files. Recent variants of the Kadavro Vector ransomware are being distributed disguised as fake Tor browser installers. Once executed, these variants encrypt files on the victim's computer and append them with a ".vector_" extension. A ransom message is then displayed on the victim's desktop, demanding $250 in Monero for file decryption. This ransom note is available in English, Russian, and Norwegian. Victims are given four attempts to enter a decryption key, which they are told will be provided after payment.

The ransomware warns that after four unsuccessful attempts, the encrypted files will be permanently lost. An older variant of Kadavro Vector encrypts files and appends the ".tor" extension. One of the most recent samples of Kadavro Vector includes a reference to a Pastebin page containing a ngrok address. Ngrok is a legitimate tool used for exposing local services to the internet, but threat actors often misuse its tunneling capabilities for Command and Control (C2) communication. This indicates a potential shift in tactics by the Kadavro Vector operators to use legitimate tools for malicious purposes.

RA Group

In April 2023, a new ransomware group known as RA Group emerged, appearing to utilize the leaked Babuk source code for their attacks, which was reportedly leaked by a **Babuk group** member in September 2021. Since then, several ransomware families, including **Rook, Night Sky, Pandora, Nokoyawa, Cheerscrypt, AstraLocker2, ESXIArgs, Rorschach, and RTM Locker**, have emerged, all leveraging this leaked code. The RA Group's operations are rapidly expanding, with successful attacks targeting three organizations in the U.S. and one in South Korea across various business sectors.

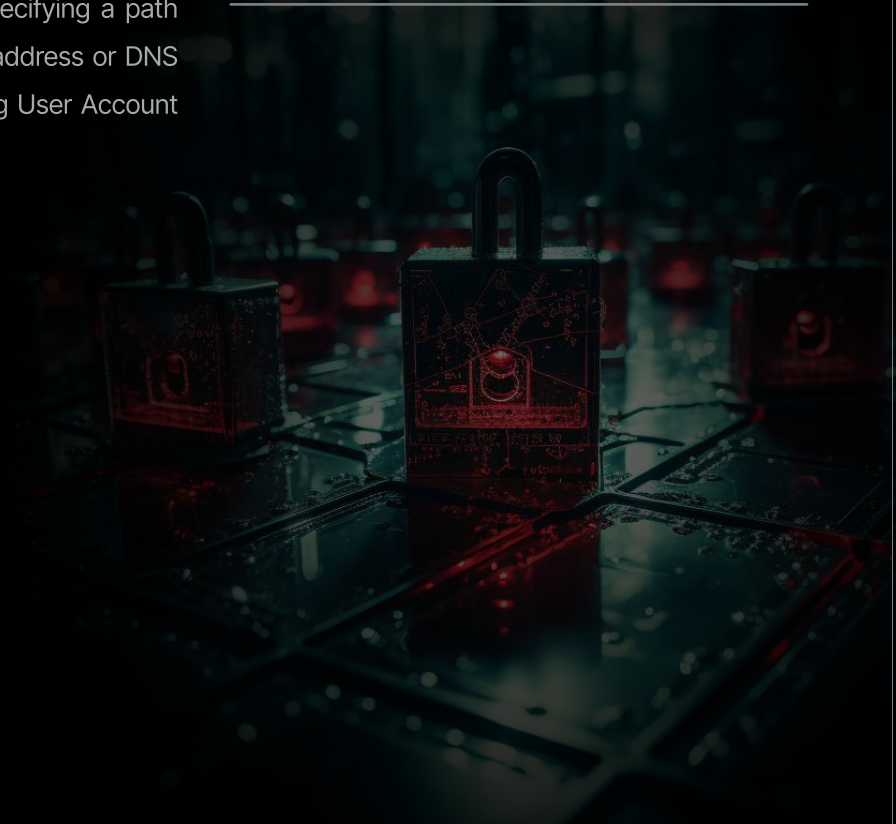
They employ double extortion tactics, enhancing the likelihood of victims paying the demanded ransom. Additionally, the group runs a data leak website where they threaten to release exfiltrated data if victims fail to comply with their specified time frame or ransom demands. Notably, the RA Group customizes each attack, using a unique ransom note titled "How To Restore Your Files.txt," tailored for each targeted organization. Furthermore, the executable file is named after the victim. The ransomware targets all logical drives on the victim's machine and network shares, attempting to encrypt specific folders while excluding those associated with the Windows system, boot, Program Files, and others. Encrypted files have the **".GAGUP"** and **".RAWLD"** extension appended to their filenames, while all volume shadow copies and Recycle Bin contents are wiped to impede easy data restoration.

CrossLock

CrossLock ransomware is a newly identified strain that stands out for being developed in the Go programming language. This choice of programming language provides the ransomware with cross-platform capabilities, making it harder to reverse engineer. The main objective of CrossLock is to encrypt the victim's data, thereby blocking access to it. What sets CrossLock apart is its use of a double extortion technique: **in addition to encrypting the data, it also exfiltrates it from the victim's system.**

The ransomware then threatens to publicly leak or sell the stolen data if the ransom demands are not met. Technical analysis of CrossLock reveals that it can be configured with various command line parameters for its execution. These parameters include specifying a path for encryption, designating a remote IP address or DNS name for network access, and bypassing User Account Control (UAC) for elevated privileges.

To avoid detection, CrossLock employs anti-analysis techniques like checking for the WINE environment and altering Event Tracing for Windows (ETW) functions. After patching ETW, the ransomware performs several data-cleaning actions on the infected system, such as deleting shadow copies, clearing event logs, and disabling the startup repair feature. The CrossLock Ransomware Group recently claimed responsibility for an attack on **Valid Certificadora**, a Brazilian IT & ITES company. This incident highlights the increasing threat posed by ransomware attacks against businesses and organizations worldwide, underscoring the need for robust cybersecurity measures.



07

"The Double-Edged Sword"

AI Risks & Security 2024...

"Artificial Intelligence (AI) has increasingly become a double-edged sword in the realm of cybersecurity, offering both innovative solutions and posing significant risks.

In 2023, the intersection of AI and cyber threats reached new heights, with advancements in AI technology presenting novel challenges. One of the key developments was the **exploitation of AI by malicious actors to enhance the sophistication of cyber attacks**, leading to a surge in AI-powered threats.

AI's Impact on Cybersecurity

AI Risks and Security

Understanding the Risks and Preparing for the Future

One of the primary risks posed by AI in cybersecurity is the potential for AI algorithms to be manipulated or biased, leading to erroneous decision-making in security systems. **Adversarial AI techniques, such as data poisoning and model evasion attacks, can deceive AI systems into making incorrect decisions, thus bypassing security measures.** In 2023, there were instances where cybercriminals used AI **to enhance the effectiveness of phishing attacks**, creating highly convincing and personalized messages that tricked users into divulging sensitive information.

Furthermore, the proliferation of AI-powered malware and ransomware presented significant challenges for cybersecurity professionals. Malware equipped with AI capabilities can adapt and evolve to evade detection, making it more challenging to defend against. For example, in 2023, there were instances of ransomware that used AI to analyze victims' behavior and determine the optimal time to launch an attack, maximizing the chances of a successful ransom payment.

Moreover, the use of AI in cyber attacks has raised concerns about the potential for autonomous cyber weapons that can target vulnerabilities at scale without human intervention. While such weapons have not yet materialized, the possibility remains a looming threat in the cybersecurity landscape.

On the defensive side, AI has been instrumental in improving threat detection and response capabilities.
AI-powered security tools can analyze vast amounts of data to identify patterns and anomalies indicative of a cyber attack, enabling organizations to respond swiftly and effectively. Additionally, AI has been used to enhance the accuracy of security analytics, enabling organizations to prioritize threats based on their severity and potential impact.

 # Challenges

Despite these advancements, there are challenges associated with the use of AI in cybersecurity. One of the key challenges is the **lack of transparency** and explainability in AI algorithms, making it difficult for cybersecurity professionals to trust AI-powered tools fully.
Moreover, the rapid pace of AI development has outpaced the ability of security professionals to keep up, leading to a skills gap in the cybersecurity workforce.

In conclusion, while AI has the potential to revolutionize cybersecurity, its adoption also comes with inherent risks. As we move forward, it is imperative for organizations to invest in AI-powered security solutions while also addressing the challenges posed by AI in cybersecurity. This includes ensuring transparency and accountability in AI algorithms and developing the skills necessary to effectively leverage AI for cybersecurity defense.

Future Outlook

The year 2023 marked a significant escalation in cyber threats, with organizations facing an unprecedented wave of attacks growing in both frequency and sophistication aimed at compromising their networks, stealing sensitive data, and disrupting operations. A significant surge is observed in cyber threats targeting cloud infrastructure, highlighting the growing challenges faced by organizations in securing their digital assets.

According to recent statistics, there has been a significant increase in the number of cyber attacks targeting cloud services in the year 2023, with a ***75% rise in cloud-related security*** incidents compared to the **previous year.** These attacks range from ransomware campaigns targeting critical infrastructure to data breaches affecting millions of users. The growing complexity and sophistication of cyber attacks has made it challenging for organizations to detect and respond to these threats effectively.

Predictions for 2024 8.1

future outlook

Increase in Ransomware Frequency and Sophistication

Ransomware attacks are expected to increase in frequency and sophistication, with a projected growth rate of over 40% compared to 2023. This growth is driven by the ease of access to ransomware-as-a-service (RaaS) platforms and the adoption of double extortion tactics, which have proven to be lucrative for cybercriminals.

Double Extortion Becomes the Norm

Double extortion tactics, where threat actors exfiltrate sensitive data before encrypting it, will become more prevalent. In 2023, **78%** of ransomware attacks involved some form of data exfiltration, and this trend is expected to continue in 2024. The average ransom demand for double extortion attacks is also expected to increase by 50%.

Supply Chain Attacks on Generative AI Ecosystems & Development Environments

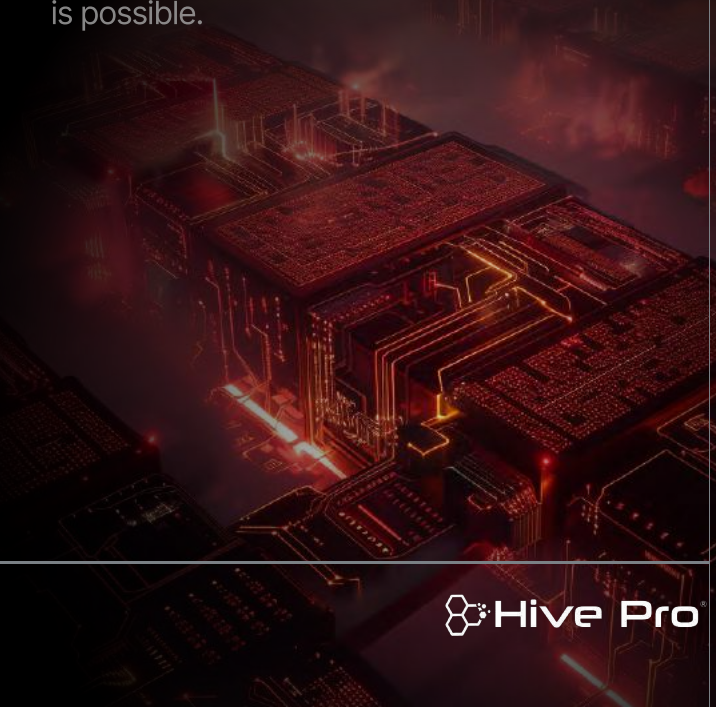
Supply chain attacks will target vulnerable generative AI ecosystems, exploiting weaknesses in various components beyond traditional attack vectors. A 25% increase in supply chain attacks targeting AI ecosystems compared to 2023, with a focus on poisoning AI training data and injecting malicious algorithms.

Ransomware-as-a-Service Innovation

Ransomware-as-a-Service (RaaS) will continue to evolve, empowering less-skilled cybercrime groups. Encryption-less attacks will become more prevalent, emphasizing the need for comprehensive zero trust protection strategies. A 50% increase in ransomware attacks compared to 2023 is possible, with an average enterprise ransom demand of $6.5 million and an average payment exceeding $150,000.

Rise in Man-in-the-Middle Attacks

Failure to implement a zero trust architecture will result in an increase in man-in-the-middle (MiTM) attacks. Phishing-as-a-Service toolkits will democratize sophisticated MiTM attacks, making them accessible to a broader range of threat actors. A 30% increase in MiTM attacks compared to 2023, with a significant impact on organizations' data security and privacy is possible.



Predictions for 2024 8.1

future outlook

Generative AI-Driven Attacks

The volume of generative AI-driven reconnaissance, exploitation, and phishing attacks will continue to grow. AI tools will be used to automate tasks such as identifying exposed assets and crafting sophisticated phishing emails, enhancing the efficiency and reach of malicious activities. A 40% increase in generative AI-driven attacks is expected compared to 2023, with a significant impact on organizations across all sectors.

Targeted Attacks on Critical Infrastructure

Critical infrastructure sectors such as healthcare, energy, and finance will face an increased risk of targeted ransomware attacks. These sectors are projected to account for over 60% of all ransomware incidents in 2024, up from 45% in 2023.

Evasion of Detection Mechanisms

Ransomware operators will continue to evolve their techniques to evade detection by security solutions. This includes using fileless ransomware, which is projected to increase by 25% in 2024, as well as leveraging zero-day vulnerabilities to bypass security controls.

Customized and Personalized Attacks

Cybercriminals will increasingly personalize their ransomware attacks to increase the psychological pressure on victims. In 2023, 85% of ransomware attacks included customized ransom notes, and this trend is expected to continue in 2024. Additionally, attackers will target specific industries based on their perceived ability to pay ransom demands.

Global Impact and Collaboration

Cybercriminals will increasingly personalize their ransomware attacks to increase the psychological pressure on victims. In 2023, 85% of ransomware attacks included customized ransom notes, and this trend is expected to continue in 2024. Additionally, attackers will target specific industries based on their perceived ability to pay ransom demands.

Expected Trends 8.2

future outlook

Quantifying Cyber Risk

Chief Information Security Officers (CISOs) will be increasingly tasked with quantifying cyber risk in financial terms to effectively communicate with executive stakeholders. This will require a deep understanding of cyber risks and their potential impact on the business.

Simplification of Security Stack

CISOs will prioritize the simplification of their security stack, focusing on making security operations more efficient. Automation will play a crucial role in this process, allowing teams to focus on addressing the most critical threats.

AI Support and Skill Development:

AI deployments will support security teams by automating low-level tasks and augmenting team productivity. However, AI will not replace humans but rather empower them to make a lasting impact within their roles. Skill development and well-being of team members will be a critical focus for IT leadership.

Focus on Frontline Defense

Insider threats remain a significant concern, and IT leaders will need to help teams understand their responsibilities in preventing credential and data exploitation. Collaboration with other departments for effective security training and awareness will be key.

Expected Trends 8.2
future outlook

Shifting focus towards critical infrastructure

Threat actors are expected to increasingly target Operational Technology (OT) systems in critical infrastructure such as power grids and transportation networks. These systems, lacking robust cybersecurity measures, will become vulnerable to cyber attacks capable of causing widespread disruptions with potentially catastrophic consequences.
Predictably, regulatory measures will be introduced to enforce cybersecurity requirements for OT systems, underscoring the importance of prioritizing cybersecurity measures and fostering effective collaboration to safeguard critical infrastructure.

Collaboration among government agencies, private sector organizations, and cybersecurity experts will prove essential in defending against these evolving threats.

Adoption of cross-platform programming languages

Threat actors are increasingly turning to cross-platform friendly programming languages for developing malware, exploiting their portability and adaptability across different operating systems. This trend raises security concerns as malicious actors seek to create resilient and stealthy malware that can evade traditional detection mechanisms. Examples of such languages include Rust, Go, Python, among others, highlighting the diversity in malware development approaches.

The cybersecurity landscape in 2024 will be characterized by increased complexity and sophistication of cyber threats. Organizations must prioritize investments in a zero trust architecture, AI-based security controls, and employee training to build resilience against evolving threats. By staying vigilant and proactive, organizations can effectively mitigate cyber risks and protect their digital assets in the coming year.

Appendix 09
Methodology and references

9.1 Research methodology

The methodology employed by HiveForce Labs for the annual threat report involved the collection and analysis of various cybersecurity threats, attacks, threat actors, vulnerability exploits, and zero-day publications on a daily basis throughout 2023. This data was sourced from internal monitoring systems, public reports, and threat intelligence feeds. The analysis included a detailed examination of all threat advisories published by HiveForce Labs in 2023, focusing on understanding the nature of threats, tactics used by threat actors, industries targeted, and the impact of these threats. Additionally, the findings from internal advisories were cross-referenced with external sources, such as known public attacks and breaches reported by other reputable threat intelligence companies, to corroborate the data.

Furthermore, HiveForce Labs conducted an analysis of geopolitical trends and threat actor behaviors based on the data collected from both internal and external sources. This analysis provided insights into the motives and strategies of threat actors operating in different regions and industries. The data collected from various sources was synthesized to identify key trends, patterns, and emerging threats in the cybersecurity landscape. Finally, the methodology and findings underwent a peer review process by cybersecurity experts within Hive Pro Inc. to ensure accuracy and reliability. Ethical considerations were also taken into account to ensure that no sensitive information or personally identifiable information (PII) was disclosed in the report.

9.2 Data Sources

- HivePro Vulnerability Database
- HiveForce Labs alert database
- National Vulnerability Database
- Shadowserver Foundation
- Malpedia
- Cybersecurity-help vulnerability Intelligence
- CISA KEV catalog
- MITRE
- Ransomwatch
- MISP
- Extensive Search over Internet

09

9.3 References

https://www.verizon.com/business/resources/T25e/reports/2023-data-breach-investigations-report-dbir.pdf

https://www.sangfor.com/blog/cybersecurity/list-of-top-ransomware-attacks-in-2023

https://www.ibm.com/downloads/cas/E3G5JMBP

https://www.idtheftcenter.org/publication/2023-data-breach-report/

https://cpl.thalesgroup.com/sites/default/files/content/research_reports_white_papers/field_document/2023-04/2023-data-threat-report-global-edition-usl.pdf

https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023

https://nordlayer.com/blog/data-breaches-in-2023/

https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023?rtc=1

https://www.infosecurity-magazine.com/news/cyber-espionage-france-2024/

https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2023/10/MDDR-2023-Blog-graphic-V3.jpg

https://www.trellix.com/assets/threat-reports/trelllix-threat-report-nov-2023.pdf

https://go.crowdstrike.com/rs/281-OBQ-266/images/GlobalThreatReport2024.pdf

https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

https://blog.qualys.com/vulnerabilities-threat-research/2023/12/19/2023-threat-landscape-year-in-review-part-one#:~:text=2023%20Vulnerability%20Threat%20Landscape,-Let's%20take%20a&text=Some%20highlights%20of%20their%20findings,likelihood%20of%20a%20successful%20attack.

https://securitybrief.asia/story/surge-in-hacktivism-aligns-with-geopolitical-tensions-in-2023

https://www.resmo.com/blog/social-engineering-statistics

https://thehackernews.com/2023/10/lazarus-group-targeting-defense-experts.html

https://www.sentinelone.com/anthology/darkbit/

https://cpl.thalesgroup.com/sites/default/files/content/CLOUD_AMI_pages/2023/2023-cloud-security-study-global-edition.pdf

https://attackerkb.com/

https://blog.qualys.com/vulnerabilities-threat-research/2023/10/03/cve-2023-4911-looney-tunables-local-privilege-escalation-in-the-glibcs-ld-so

https://www.sentinelone.com/resources/watchtower-end-of-year-report-2023/

9.3 References

https://www.aquasec.com/blog/loony-tunables-vulnerability-exploited-by-kinsing/
https://www.cyfirma.com/research/citrix-bleed-cve-2023-4966-vulnerability-analysis-and-exploitation/
https://blog.morphisec.com/responding-to-citrixbleed
https://tunnelcrack.mathyvanhoef.com/details.html
https://terrapin-attack.com/
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-325a
https://github.com/lrh2000/StackRot#stackrot-cve-2023-3269-linux-kernel-privilege-escalation-vulnerability
https://www.securonix.com/blog/securonix-threat-labs-security-meme4chan-advisory/
https://www.fortinet.com/blog/threat-research/lokibot-targets-microsoft-office-document-using-vulnerabilities-and-macros
https://securelist.com/goldenjackal-apt-group/109677/
https://securelist.com/operation-triangulation-the-last-hardware-mystery/111669/
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-Cl0p
https://blog.google/threat-analysis-group/government-backed-actors-exploiting-winrar-vulnerability/
https://www.cloudsek.com/blog/top-5-famous-software-supply-chain-cyber-attacks-in-2023
https://www.akamai.com/blog/security-research/chaining-vulnerabilities-to-achieve-rce-part-one
https://www.akamai.com/blog/security-research/chaining-vulnerabilities-to-achieve-rce-part-two
https://eclypsium.com/research/bmcc-lights-out-forever/
https://citizenlab.ca/2023/09/predator-in-the-wires-ahmed-eltantawy-targeted-with-predator-spyware-after-announcing-presidential-ambitions/
https://starlabs.sg/blog/2023/09-sharepoint-pre-auth-rce-chain/
https://www.interware.ca/blogs-01/formbook-malware-spreads-via-malvertising-using-malvirt-loader-to-evade-detection
https://blog.checkpoint.com/security/september-2023s-most-wanted-malware-remcos-wreaks-havoc-in-colombia-and-formbook-takes-top-spot-after-qbot-shutdown/
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/agent-teslas-unique-approach-vbs-and-steganography-for-delivery-and-intrusion/
https://blog.checkpoint.com/security/october-2023s-most-wanted-malware-njrat-jumps-to-second-place-while-agenttesla-spreads-through-new-file-sharing-mal-spam-campaign/

9.3 References

https://any.run/malware-trends/AgentTesla
https://www.cyfirma.com/outofband/tracking-ransomware-november-2023
https://blog.talosintelligence.com/new-phishing-as-a-service-tool-greatness-already-seen-in-the-wild/
https://www.elastic.co/security-labs/DPRK-strikes-using-a-new-variant-of-rustbucket
https://www.jamf.com/blog/bluenoroff-apt-targets-macos-rustbucket-malware/
https://www.zscaler.com/blogs/security-research/technical-analysis-pikabot
https://www.obrela.com/advisory/pikabot-a-new-emerging-threat/
https://www.itpro.com/security/ransomware/encryption-less-ransomware-warning-issued-over-emerging-attack-method-for-threat-actors
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-akira
https://www.trellix.com/about/newsroom/stories/research/akira-ransomware/
https://www.fortinet.com/blog/threat-research/lockbit-most-prevalent-ransomware
https://www.sans.org/blog/ransomware-cases-increased-greatly-in-2023/
https://www.cisa.gov/sites/default/files/2023-06/aa23-165a_understanding_TA_LockBit_0.pdf
https://blog.eclecticiq.com/chinese-state-sponsored-cyber-espionage-activity-targeting-semiconductor-industry-in-east-asia
https://cyble.com/blog/uncovering-the-dark-side-of-darkbit-ransomware/
https://unit42.paloaltonetworks.com/tag/cl-sta-0043/
https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/ra-group