Cyber Incidents and Intelligence: 2023

KPMG in Canada's Cyber Incident Response and Cyber Threat Intelligence Year-in-Review

March 2024

kpmg.ca

Contents

01

Introduction

As a rule, cybersecurity is an ever-evolving industry. Rapidly advancing technology, and equally as rapid and creative threat actors have ensured that the industry remains in a state of flux, requiring careful thought and decision making to keep organizations secure. 2023 was no exception to this rule.

The 2023 edition of KPMG in Canada's report on the state of the cyber security landscape will discuss major developments in malware, threat actor behaviour and the cyber defences needed to counter them. Our Incident Response, Cyber Threat Intelligence and Vulnerability Management teams have come together to share insights into interesting and novel cases resolved in the year, as well as thought leadership regarding potential outcomes in 2024 and beyond.

It should be noted that the opinions expressed within this report reflect real incidents and experiences through 2023. While descriptions of the events have been kept accurate, victim details have been obfuscated.

02

Incident Response

KPMG in Canada's Incident Response and Cyber Threat Intelligence teams have come together to provide this second edition report on the state of the cybersecurity landscape in 2023, as well as predictions for 2024. This includes reports and thoughts from KPMG's front line incident responders, cyber threat intelligence analysts, and thought leaders in the space.

It should be noted that the opinions expressed in this report reflect real incidents and experiences through 2023. While descriptions of the events have been kept accurate, victim details have been obfuscated.

IR Summary

2.1 Overview of Cybersecurity Concerns in 2023

Cybersecurity continued to be a primary concern for Canadian organizations in 2023. Organizations are increasingly under scrutiny not just from regulators and the public, but from their own board of directors and shareholders regarding leadership's management of cybersecurity incidents.

KPMG's report highlights some of the key cyber threats, intelligence, and trends observed in Canada in 2023. Ransomware continues to prevail across almost all industries, including organizations that provide essential services to Canadians such as schools, government entities, and utility providers. We highlight a continued focus on data exfiltration over the traditional single form of extortion by threat actor groups. In 2023, we have observed an increase in attacks on organizations in the **financial services and manufacturing industry.**

2.2 Notable Observations of 2023

Surge in Third-Party Compromises:
In 2023, third-party compromises have emerged as a prominent cybersecurity concern. Diverging from direct attacks on an organization's IT environment, third-party compromises are breaches within the IT networks or products belonging to external parties of our clients. This shift underscores the heightened involvement of third-party vendors, suppliers, and contractors in the landscape of data breaches, significantly increasing the complexity of incident response challenges faced by organizations.

Increase in 'Spray & Pray' Exploits: In 2023, KPMG observed an increase in automated 'spray and pray' tactics used by threat actors focused on exploiting vulnerable Internet-facing servers. The 'spray and pray' tactic is used by threat actors to automatically deploy malicious activities on a broad scale, often without specific targets in mind. Instead of meticulously selecting and targeting a particular organization, threat actors 'spray' their malicious efforts across a large number of potential victims. The rise of these easily automated vulnerability exploits underscores the need for organizations to reassess their patching schedules and re-examine their security posture related to Internet-facing assets.

Data Loss Prevention (DLP) and the Rise of Internal Security Incidents: Due to organizational downsizing and workforce layoffs, heightened concerns have emerged within organizations with respect to the potential theft of intellectual property when employees exit an organization. The current economic environment, characterized by frequent workforce reductions and turnover, has further aggravated this concern. In response to these challenges, organizations have renewed their focus on data loss prevention (DLP) strategies by implementing a multi-faceted approach to safeguard against the unauthorized exfiltration of valuable intellectual assets. Specifically, organizations are deploying enhanced monitoring of employee behaviour, stringent access controls, and DLP technology tools to safeguard against data theft.

Changes in Business Email Compromise (BEC) Tactics: In 2023, Business Email Compromise (BEC) attacks have increased despite heightened efforts by organizations and their email solutions to bolster security controls, such as the implementation of Multi-Factor Authentication (MFA). Further, we have observed a concerning trend in the adaptability of threat actors to existing defences. Threat actors are establishing fraudulent domains that closely emulate corporate identities and leveraging open-source intelligence to gain deeper insights into organizations to facilitate more sophisticated and successful fraud attempts. Furthermore, we have observed instances where successful BEC attacks have emboldened threat actors to launch repeated fraudulent assaults against an organization.

In response to these evolving threats, organizations are encouraged to move beyond relying solely on Multi-Factor Authentication (MFA). Instead, organizations should adopt a comprehensive approach which includes the enhancement of staff security training to effectively recognize and report phishing attempts. In addition, organizations should consider implementing supplementary accounting, such as requiring written and verbal approval when a request is made to modify banking information.

2.3 Key Learnings and Recommendations

Outlined below are key learnings that some of our clients reflected upon as a result of suffering a cybersecurity breach:

Logs, Logs, Logs: Organizations are encouraged to maintain logs, such as endpoint logs (i.e., Windows Event Logs), network logs (i.e., Firewall, Network Logs), and application logs (i.e., related to specific business applications) for a minimum of one year. In 2023, approximately 50% of KPMG's incident response clients identified a lack of logs available for analysis during the investigation associated with a cybersecurity incident. Further, KPMG recommends that organizations forward logs and events to a centralized repository such as a Security Information and Event Management (SIEM) solution.

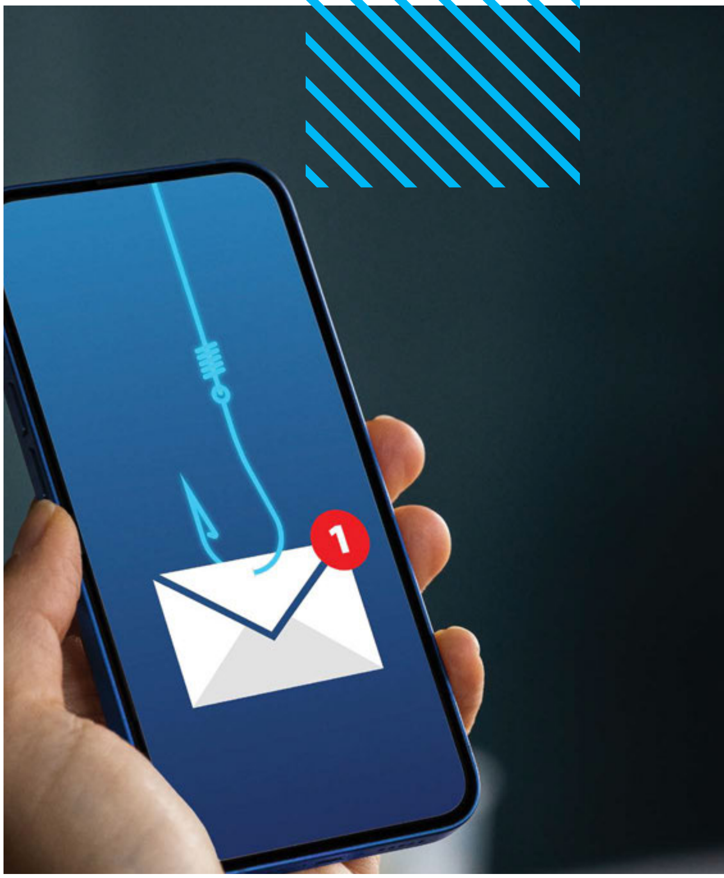
Active Directory Review and Maintenance: Active Directory (AD) remains a critical component of many organizations' IT infrastructure, serving as the backbone for authentication and authorization. It is also a common target for threat actors. Organizations should pay particular attention to service accounts, often granted elevated privileges to perform specific functions within an IT environment. Unfortunately, service accounts become lucrative targets for threat actors due to their broad access and typical lack of regular monitoring when not adequately managed. Organizations should periodically review and audit service accounts to ensure that unnecessary privileges are revoked, credentials are rotated regularly, and dormant accounts are decommissioned.

In addition to service accounts, organizations should review Group Policy Objects (GPOs). Misconfigured GPOs can unintentionally introduce vulnerabilities, grant undue permissions, or even be exploited by threat actors to propagate malware or enforce malicious settings across the domain. Regular audits and reviews of GPOs can identify and rectify these misconfigurations, ensuring that policies are secure and aligned with the organization's operational needs.

Optimal SIEM Indexing and Configuration: Security Information and Event Management (SIEM) solutions are pivotal in consolidating, analyzing, and responding to security events across an organization's network. However, the effectiveness of a SIEM solution could be improved by efficient indexing. Organizations should ensure that all logs are configured and indexed efficiently in their SIEM before security incidents occur rather than waiting to address indexing and performance issues post-incident when querying is most critical. This can involve normalizing log data (for example, converting firewall data to a format that can be easily parsed by the SIEM), removing redundant or irrelevant data, and focusing on high-priority event types as the index (for example, EventIDs in the Windows Event Logs). Periodic reviews of indexing strategies and logs ingested are crucial to ensure that the SIEM remains optimized as the organization's data and infrastructure evolve.

Remain Up to Date on Vulnerabilities: Organizations should maintain a comprehensive list of servers exposed to the Internet (including hosted applications) while closely monitoring vulnerability disclosures. Similarly, it is essential that organizations must establish a policy that considers the severity of a vulnerability and its significance to the business if the vulnerability is exploited. The policy should also define timelines for remediation. Regularly tracking progress related to patch management is critical, and in cases where patches cannot be promptly deployed, organizations should augment monitoring measures to maintain a vigilant cybersecurity posture.

Maintain Three Backups (Online, Offline and Offline-Offsite): Organizations should maintain three types of backups to prevent data loss associated with a cybersecurity incident. Online backups ensure quick accessibility during an accidental data loss or corruption, facilitating efficient recovery. Offline backups, being disconnected from the Internet or network, provide an added layer of security by reducing the risk of cyber-attacks compromising the back-up data. Additionally, offline-offsite backups offer a comprehensive strategy by protecting against cyber threats and mitigating the impact of physical disasters, ensuring data resilience and business continuity. This three-tiered approach significantly enhances the overall reliability and effectiveness of an organization's cybersecurity backup strategy.



Further, organizations should regularly test its backups to ensure data integrity and reliability. Without verification, organizations may not be aware that back-ups are corrupt or not restorable. By regular backup testing, organizations can identify potential issues early, ensuring that critical data and systems can be confidently and promptly restored in a critical security incident

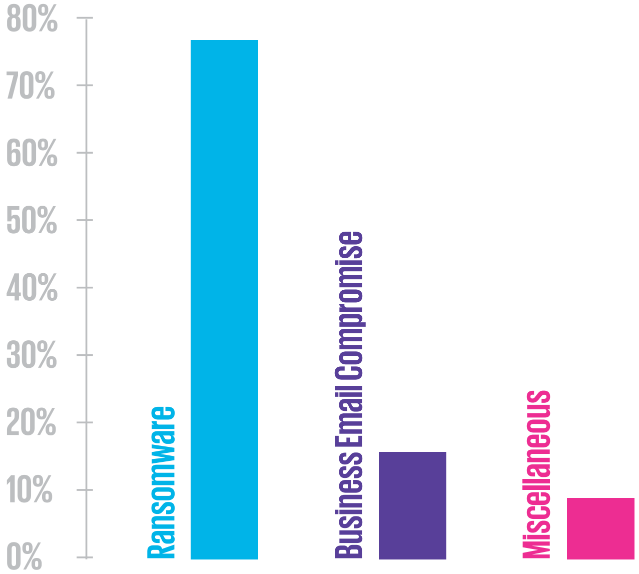
Conduct Regular Cyber Simulation (Tabletop) Exercises: As recommended by the National Institute of Standards and Technology (NIST), tabletop exercises simulate potential scenarios to assess an organization's response strategies. Tabletops offer a controlled environment to identify an organization's gaps and refine an organization's incident response plans. When facing real-world incidents, regularly practicing your response process ensures a swifter, coordinated and effective reaction.

IR Incidents

3.1 Major Threats and Statistics

Ransomware and Business Email Compromise (BEC) continue to be the top two threats impacting Canadian organizations and KPMG Cyber Incident Response clients. In 2023, KPMG observed that 77% of the incidents it responded to were related to Ransomware, and 15% of the incidents related to Business Email Compromise (the remaining incidents were related to miscellaneous security events). Compared to the previous year, ransomware incidents have increased by 20%, while BEC incidents have decreased by 11%.

Distribution of Cybersecurity Incidents



Case Study #1
A significant incident KPMG assisted with this year involved a client in the insurance sector. The attack resulted in the exfiltration of approximately 15,000 files. Investigations revealed that threat actors exploited a vulnerability in ManageEngine (a suite of enterprise IT management software), identified as CVE-2022-47966, which allowed the threat actors to execute malicious code within the client's IT environment. KPMG identified that the threat actors took advantage of the vulnerability only a couple of days after the CVE was made public. Despite the client's prompt response in patching the vulnerability, the client's actions were outpaced by the attackers who had already established a foothold in their IT environment. **This incident highlights the narrow window organizations have to deploy patches and underscores the intensifying struggle organizations have against cyber adversaries.**

Case Study #2
A significant incident KPMG assisted with this year involved a financial service company which acted as a service provider for Canadian banks. The company suffered a ransomware that resulted in approximately 220 GB of data being exfiltrated from the company's IT environment. Fortunately, KPMG's investigation determined that none of the data that was exfiltrated contained PII related to the bank's clients. This incident emphasizes the vulnerabilities that can exist in supply chains. KPMG's investigation revealed that the attackers gained initial access via a guest account on the VPN that lacked Multi-Factor Authentication (MFA) protection. **The breach underscores the importance of continuous security reviews for accounts with elevated privileges, regular audits to deactivate dormant accounts, and the indispensable role of MFA in fortifying security measures.**

3.2 Industry-specific Analysis

Similar to our 2022 findings, KPMG noted that the majority of Canadian organizations falling victim to ransomware attacks are spread across multiple industries rather than concentrating on a single sector. Nevertheless, there was an increase observed specifically within the manufacturing and financial services sectors.

3.3 Trends

Overall, KPMG noted an increasing number of clients acquiescing to ransom demands, not out of concern for encrypted data – as many clients maintained robust backup systems – but due to the potential release of exfiltrated data containing sensitive and/or personally identifiable information (PII). The release of such information poses significant risks to organizations, including potential legal repercussions and reputational damage. Payment of the ransom demand often becomes a strategy to mitigate these severe outcomes. This shift in ransomware dynamics

IR Impacts

AI: A Blessing and a Curse

Artificial Intelligence (AI) continues to transform various industries, offering advanced solutions and automation. However, its influence on the cybersecurity realm is twofold. On one hand, AI-driven tools are empowering organizations to detect and respond to threats with unprecedented speed and accuracy. Conversely, threat actors are leveraging AI to craft sophisticated attacks, automate their operations, and outpace traditional defense mechanisms. As AI technologies become more accessible, the balance of power in cybersecurity will hinge on who employs AI more adeptly - defenders or attackers.

The challenge presented by the illicity use of penetration tools

Recent collaborative efforts by law enforcement agencies, technology giants, and vendors of commercial penetration tools (designed to simulate advanced threat actors' tactics and techniques, the ability to deliver payloads, and command and control (C2) functionalities) have started clamping down on the illicit use of such tools which is reshaping the threat environment. With enhanced detection mechanisms for usage of commercial penetration testing tools, threat actors are feeling the heat. This pressure is nudging them towards seeking alternative tools and methods. As the dominance of commercial tools are being challenged, organizations will need to diversify their detection and response strategies, anticipating a broader range of attack tools.

IR Strategic Innovation

KPMG's Incident Response team undertook several innovative approaches to both aid in the immediate incident response and recovery as well as provide victims with a more stable, secure environment post incident. Key innovations that had positive impacts with victims include:

01

Automated Forensics Triage Package Collection: KPMG's Incident Response team developed an automated mechanism for swift forensics triage package collection, considerably reducing the traditionally lengthy image collection phase.

02

Advanced Data Recovery Techniques: In a specific ransomware case, KPMG's Incident Response team innovatively carved out files from slack space and initiated recovery procedures. Moreover, for images that were encrypted, a unique method was devised that enabled the recovery of partially encrypted files. This breakthrough offers an alternative solution to paying ransoms for data retrieval, especially for organizations that may not have maintained comprehensive backups.

Looking Forward

Strengthened Security Postures: Many organizations have taken strides to bolster their cybersecurity defenses. There has been a marked uptick in the adoption of robust security measures, with organizations investing heavily in state-of-the-art Endpoint Detection and Response (EDR) tools, refining their backup strategies, and undergoing rigorous cybersecurity training. Such proactive measures have significantly reduced the vulnerability surface for many entities.

The Double-Edged Sword of Interconnectedness: The intricate web of today's business world presents its own set of challenges. The interconnectedness of businesses, while fostering collaboration and growth, has also introduced potential chinks in the armor. Even if an organization has fortified its defenses, its exposure to third parties – be it through products, partnerships, or supply chains – can become an Achilles' heel. It would not be unexpected to observe a surge in compromises initiated through third-party channels. Organizations therefore should not just be focused on individual organizational security but on securing their entire ecosystem.

The Subtle Power of Non-Encryption Attacks: The cyber threat landscape has also seen evolutions that challenge conventional wisdom. The Cl0p ransomware group, for instance, has demonstrated that encryption is not the sole means to wreak havoc on an organization. Their campaigns, which often targeted products or services used by a plethora of organizations rather than going after individual entities, underline the potency of such an approach. By focusing on a single vulnerability in a widely used product or service, threat actors can magnify their impact.

The Looming Shadow of Zero-Days: Zero-day vulnerabilities remain a persistent and looming threat. Organizations must be particularly wary of products or services that, if compromised, could serve as gateways to multiple clients. Cl0p's success in exploiting such vulnerabilities underscores the urgency of this issue. The industry might see an uptick in zero-day exploits targeting popular and widely used services, given the amplified damage potential they present.

Adapting to the New Normal: In light of these emerging trends, organizations must rethink their defensive strategies. While strengthening individual defenses is crucial, there's an increasing need to evaluate and secure third-party interactions. Similarly, while encryption-based attacks are rampant, the industry must also prepare for subtler, yet equally devastating, non-encryption threats.

US Election Year: As 2024 is an election year in the United States, it is expected that the threat landscape will be more intense. Threat actors will be fully engaged in attempting to influence and shape the political landscape in the US. Additionally, with the ongoing geopolitical activities in Eastern Europe and the Middle East, threat actors from various backgrounds, including nation states will likely target different US and Canadian organizations that conduct business in the US.

AI-Driven Cyber Attacks: The use of artificial intelligence by threat actors could lead to more efficient and sophisticated attack methods. AI could be used to automate target selection, tailor phishing messages, or even find and exploit new vulnerabilities.

The journey ahead promises to be challenging, but with adaptability and foresight, organizations can navigate this intricate cyber maze.

03

Cyber Threat Intelligence

Cyber Threat Intelligence

2023 Observations

The Cyber Threat Intelligence landscape expanded greatly through 2023. Though in previous years many organizations found their adversaries to be criminal organizations with financial objectives, 2023 saw more and more cyber activity related to political objectives.

This increase in activity included observations around an increase in low-profile threat actors. These threat actors are not immediately or obviously connected to the more infamous ransomware or threat actors that make headlines like Lockbit 3.0, Cl0p or BlackCat.

In parallel to the increase of activity by low-profile threat actors were calls to action from threat actors to corporate insiders. While initial access markets continue to grow, purchased access is never as reliable or convenient as an insider actively assisting a threat actor.

When insiders and initial access markets fail, the tried-and-true methods of malware come into play. In 2023 we observed a shift in attacks to target operating systems that had previously been considered secondary targets, such as Linux. While it should be no surprise that threat actors would target such systems, the jump in volume is notable and should be considered when designing your security environment.

One of the great shifts of 2023 was the emergence of Large Language Learning Models (LLM). While these LLMs present a tremendous opportunity to enhance security, improve efficiency, these improvements are also being exploited by threat actors. The rise of LLM or AI enhanced malware and threat actors is very real and will be a major consideration in 2024.

This brings us to the elephant in the room for 2023, Nation State activities and hacktivism. While cyber actions by governments and activists alike is not a new development, in 2023 we observed significant activities in the space. Organizations which may not have considered themselves to be critical infrastructure, or the targets of state-actors suddenly found themselves in the crosshairs as the kinetic conflicts of our world spill into the cyber domain.

These trends are likely to continue into 2024 and should be examined carefully.

Many Low-Profile Threat Groups Observed in 2023

The collective impact of low-profile threat actors, although less publicized, can be a significant threat to businesses. Their targets span different sectors including those in critical industries. These emerging groups have leveraged the uncertainty surrounding recent global events to successfully compromise organizations. A lack of substantial historical data on these threat actors compared to more prominent ones, makes it harder to anticipate their tactics, techniques, and procedures (TTPs), further intensifying the risk they pose. Attribution to existing threat actors or nation-states is particularly challenging in the absence of a large sample size of TTPs.

- **UnSafe/Nsafe:** UnSafe/nSafe threat group quietly emerged in November 2022 posting leaks from various databases and breaches on their Telegram channel. This initial technique may have been to gather followers. They victimized entities from various industries and sizes suggesting motives are opportunistic rather than industry specific. They are known to advertise their operations on open-source platforms, then close intermediately following a breach, then in subsequent days reopen their site to announce a new victim, showcasing their attempts to remain out of the spotlight.

- **Phobos:** Active since 2018 and a rebrand of CrySiS Ransomware, Phobos ransomware continuously changes extensions and variants to stay inconspicuous. Phobos uses multiple email addresses to connect them with victims for ransom payments, another technique to help them evade detection. They target smaller organizations asking for lower-priced ransoms, likely because they are more inclined to pay. Although they do not make a lot of noise on social media or dark web sites, they still pose a significant threat to organizations as they continually generate new variants and engage with multiple partners, many of which have been observed utilizing their ransomware variant.

KPMG observed a few threat groups that displayed a negligible footprint before and after their attacks. They exploit vulnerabilities, successfully deploy ransomware, and disrupt business operations while showcasing minimal to zero footprints on the dark web. It is unclear if they were a rogue member from an established team or a low-tier cybercriminal looking to enter the threat landscape.

The escalating activities of new low-profile threat actors, and their ability to stay discreet, means no industry is immune from cyber-attacks. It highlights the need for organizations of all sizes to prioritize cybersecurity.

Insider Threats to Organizations

Insider threats are situations where individuals, either intentionally or inadvertently, misuse their organizational access or privileges, resulting in the compromise of sensitive data. Insider threat incidents represent a minority of cyber incidents on the whole; however, they can be among the costliest type of attacks to recover from.

Breaches attributed to insiders between 2018 and 2020 increased by 47%. The rise of cloud computing, which makes insider detection more difficult for employers, played a role in this spike. By 2022, 31% of all breaches were associated with insider threats, with costs topping $8.76 million globally. The rise of social media platforms, the use of mobile devices, and the trust already granted to insiders were all factors in this spike.

- **Intentional Actions:** Threat actors actively seek out dissatisfied employees, tempting them with offers like clicking on email links or divulging critical information to assist in a breach, often accompanied by monetary incentives. Employees with malicious intent may steal data for personal gain, either by selling it on the dark web or intentionally disclosing it to inflict harm on the organization. The data exfiltrated by an insider threat can include sensitive and valuable information. Threat actors frequent open-source platforms like the dark web, blogs, underground forums, and social media platforms where disgruntled employees sometimes vent their frustrations or discuss their employment dissatisfaction. Armed with this information, threat actors can lure and exploit these individuals with malicious motives.

- **Unintentional Actions:** Threat actors prey on individuals with privileged access using social engineering or exploitation of vulnerabilities to gain control over their accounts. Adversaries use social engineering campaigns to manipulate individuals into actions they did not intend, such as directing them to a fake webpage or clicking on an email link, inadvertently loading malware, and opening the door for an attack. An individual's carelessness can be using a weak password or overlooking a request, which could lead to a potentially nefarious event.

While overall business controls and role-based access controls can mitigate the potential damage from an unintentional insider, the risk posed by a malicious insider is greater. Threat actors have been observed recruiting or learning how to recruit corporate insiders through 2024. In many threat actor communities, the practice has become common enough to garner a shorthand – the "inny".

Threat actors have profiled potential inny targets and are employing social engineering and other exploitation methods to take advantage of disgruntled employees. Threat actors will often offer either a flat cash payment for access, or a percentage of the takings after a successful attack. They also go to lengths to try and ensure the anonymity of the inny working with them.

Linux Malware Threats

For a time, Linux enjoyed less attention from threat actors than other operating systems, despite Linux being crucial to many of our critical infrastructure enterprises, making up around 80% of Web servers and being the most employed system for IoT devices. The dependence on Linux in these areas, along with its use for virtualization in the enterprise environment, has led to a recent increase in new malware (including ransomware) targeting the OS.

In the past year, we have witnessed a surge in newly emerging malware, with a particular focus on Linux. Ransomware, among other threats, has begun introducing Linux variants, aiding in threats to a growing threat landscape for this operating system.

- **Rootkits:** By Mid-2022, we started to detect a wave of Linux-based malware with rootkit capabilities, and as the year progressed, their numbers grew. This marked the beginning of a new trend that continued its trajectory into the year 2023.

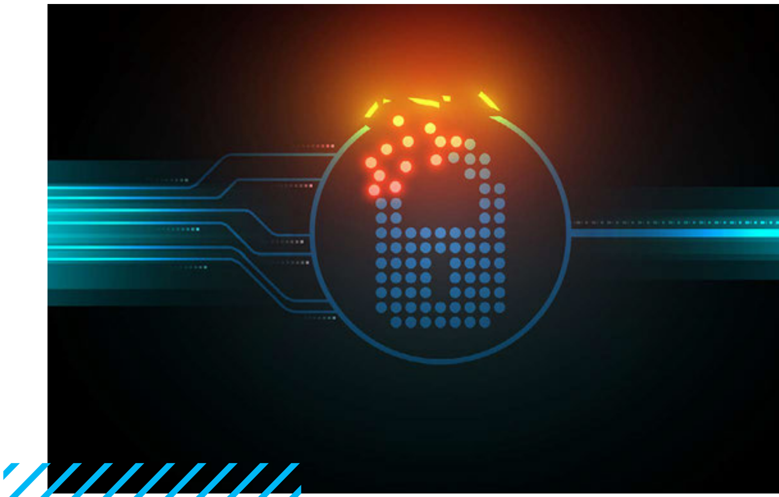
- **Ransomware:** By late 2022, a significant shift in the cybersecurity landscape. Ransomware groups, including many high-profile threat actors such as LockBit and Black Basta ransomware, began expanding their malware to include variants to attack Linux systems. As we reached mid-2023, Linux-specific variants associated with several high-profile and low-tier ransomware groups began to dominate the cyber ecosystem. These variants were tailored to infect Linux platforms, including VMware ESXi servers. Predominant groups like Akira, Royal, and ALPHV/BlackCat ransomware, threat groups known for targeting critical infrastructure, exhibited their Linux malware showcasing the gravity of the evolving threat landscape.

Threats from New AI Generated Tools

As AI continues to transform the global marketplace and cybersecurity, organizations must take proactive measures to mitigate AI-driven threats. The widespread adoption of tools, such as AI based chatbots, has made them a target for threat actors looking to exploit their popularity to deploy malware, posing significant risks to global businesses and supply chains.

Generative AI tools can be utilized to fight cybercrime. Companies began adopting these tools to better understand how and to secure environments. However, adversaries viewed them as a means to aid them in targeted attacks.

A few notable malicious tools made way into the cyber space this year:



ON_ID = CGI.ESCAPE("MY_APPLICATION_ID")
RD SHOULD BE SENT TO YOUR E-MAIL AFTER APPLICATION WAS CREATED
= CGI.ESCAPE("MY_PASSWORD")

FraudGPT: FraudGPT operates like ChatGPT but is tailored to facilitate cyber attacks. It is said to have the ability to create undetectable malware, composing malicious code, identifying vulnerabilities, designing phishing pages, and facilitating the learning of hacking techniques.

WormGP: WormGP is an AI module based off OpenAI's ChatGPT framework. It has been promoted on dark web platforms in 2023. Threat actors trained WormGPT on a range of data sources to automate the creation of sophisticated phishing emails personalized to recipients.

WolfGPT: WolfGPT is a Python-based tool that uses generative artificial intelligence (AI) technology to create hacking and unethical tools. It can create encrypted malware and draft sophisticated phishing messages. WolfGPT also offers confidentiality and privacy for AI sessions and generated content.

DarkBART & DarkBERT: DarkBERT was created with the intent to fight cybercrime. In the research stage, it is believed that hackers access the code and created a malicious version DarkBART. The author states it communicates in 27 different languages. DarkBERT is trained on a vast amount of text from the Dark Web, making it a powerful tool for cybercriminals. The malware is designed to enable various malicious activities, including advanced social engineering attacks, system exploitation, ransomware distribution, and phishing campaigns. It can also aid cybercriminals in finding zero-day vulnerabilities and searching for critical infrastructure weaknesses.

Currently, there are some doubts about these malicious tools; however, the entrance of generative AI tools and rise of AI malware and similar malicious chatbots, can encourage new threat actors to turn to nefarious cyber activities. These tools can create flawless phishing email, mimicking the language and culture of the targeted enterprise, improving the effectiveness a phishing email. We could see generative AI weaponized in future cyberattacks, posing significant challenges to the cybersecurity landscape.

Nation State Threats: Activity During Times of War

Nation-state threat groups are driven by government/geopolitical objectives rather than personal enrichment, leading to a greater focus on intellectual property theft, espionage, and critical infrastructure attacks. During times of significant geopolitical unrest, nation-state actors often work in conjunction with other threat actors, such as organized crime groups, hacktivists, or cyber extortionists, to intercept, influence, or disrupt relations between nations. Their ultimate objective may be to subvert, influence, or distract competing governments or, more directly, enable kinetic actions or the ability to defend against them.

- **Sandworm** – Known for their attacks on the Ukrainian power grid in December 2015 and December 2016, is recognized as one of the most destructive nation-state groups currently active.
  - Late 2022; Sandworm interrupted a Ukrainian power grid, causing a power outage in late 2022. This attack was in unison with missile strikes on critical infrastructure across Ukraine, aiding many to overlook the cyber-attack only discovered in November 2023.
  - May and September 2023; Sandworm targeted 11 telecommunications service providers in Ukraine, leading to service disruptions and potential data breaches.
  - May 2023: Sandworm targeted 22 critical infrastructure companies throughout Demark. It was the largest-ever cyber event to have threatened critical infrastructure in the country. The attack included 16 Danish energy companies, resulting in the comprise of 11 energy-related entities.

Hacktivist Activity in 2023

While hacktivism once conjured images of a Guy Fawkes mask and claims from Anonymous demanding document release, or other action in support of a de-centralized political goal, it has since evolved and expanded. Many hacktivist activities are now in support of nation-state objectives and may be tied into a great information campaign, or in some cases kinetic actions.

This expansion is an important development as hacktivists are often motivated by passion rather than finances. True believers may apply more effort, time and care with their attacks or attempts to gain access than criminals who are seeking quick and easy profits. The risk from these groups increased in 2023, included below are some examples of hacktivist groups supporting state actor positions.

Zarya

Zarya emerged in early 2022 and partnered with the threat group Killnet. The leader of Zarya suggested they were active before this merger using various names, including "0x000000" and "Quarantine". They were observed leaking files on compromised Ukrainian entities in 2022. In late 2022, they branched away from Killnet, forming a separate hacking brand.

- Documents were leaked in April 2023 referring to Zarya. In these documents, there were claims the group gained network access to the industrial control systems of an unnamed Canadian gas company in February 2023, giving them the ability to increase valve pressure, disable alarms, and force the shutdown of a gas distribution center. Is is still unclear whether the files were valid or doctors with the intent of a disinformation campaign, a common tactic used by hacktivists.

NoName057(16)

NoName057(16) is a hacktivist group active since March 2022. They predominantly conduct distributed denial-of-service (DDoS) attacks against government and critical infrastructure entities in Ukraine and nations supporting Ukraine.

- On April 10, 2023, NoName057(16) pointed their threats on Canadian entities, a used Denial-of-Service (DoS) campaign that lasted a week. NoName057(16) encouraged various threat groups to strike Canadian government-affiliated websites with the promise of a monetary reward.

Anonymous Sudan

Anonymous Sudan targets US companies, claiming attacks or in protest of the US involvement in Sudan affairs. However, the groups have associations with pro-Russian groups, suggesting the name is a decoy.

- In June 2023, Anonymous Sudan claimed an attack on Microsoft's Azure portal, slowing down service due to a DDoS attack.
- On November 2023, OpenAI experienced a distributed denial-of-service (DDoS) attack that targeted its API and ChatGPT services, resulting in service disruptions.

Indian Cyber Force

Indian Cyber Force (ICF) hacktivists target several countries. However, they have been observed specifically targeting nations they believe are anti-India or against India's political agenda.

- In Oct 2023 - Several Canadian government websites were inaccessible for 1 or 2 hours following a series of DDoS. These attacks followed the Canadian Prime Minister's allegations that the Indian government was involved in the assassination of a prominent Khalistan leader on Canadian soil. Indian Cyber Force took credit for these attacks, claiming the Canadian government "crossed the line."

SiegedSec

SiegedSec is a hacktivist group that has been observed compromising databases to steal personally identifiable information (PII)on large organizations, including many in the critical infrastructure industries. Following the Israeli/ Palestine conflict, SiegedSec and Anonymous Sudan stated they would be targeting Israeli critical infrastructure, industrial systems, and global navigation satellite systems (GNSS).In June 2023, Anonymous Sudan claimed an attack on Microsoft's Azure portal, slowing down service due to a DDoS attack.

- In October 2023, the group alleged to have stolen nearly 3,000 documents from an intergovernmental company.
- In November 2023, SiegedSec claimed to have breached and stolen personal data on employees from an American Laboratory. The laboratory and a cybersecurity firm recently announced a partnership to assist the laboratory with cyber-driven information to fight cyber threats on critical infrastructure.

Supply Chain Attacks in 2023 & SCATTERED SPIDER Case Study

In the fast-paced evolution of cybersecurity, the term "Supply Chain Attack" has emerged as a formidable threat vector. This method represents a departure from conventional cyberattacks, which typically hone in on exploiting weaknesses within the confines of a single organization's network. Unlike these traditional threats, a supply chain attack strategically navigates the intricate web of suppliers, vendors, and service providers that collectively form the backbone of the delivery of goods or services.

One of the distinguishing features of a supply chain attack is its strategic exploitation of trust. In traditional cyberattacks, threat actors often rely on technical vulnerabilities or weaknesses. In contrast, a supply chain attack capitalizes on the implicit trust that organizations place in their collaborators. As organizations forge partnerships with suppliers, vendors, and service providers, a level of trust is established, allowing for the seamless flow of goods and information. Cyber adversaries exploit this trust to introduce malicious elements into the supply chain, manipulating the very relationships that organizations rely on for their operations.

The network of an organization, when viewed in the context of a supply chain attack, extends far beyond its internal systems. It encompasses a complex and interwoven ecosystem that includes suppliers, vendors, service providers, and various other entities critical to the production and delivery of goods or services. Understanding the intricacies of this interconnected network is paramount for comprehending the potential vulnerabilities and risks associated with supply chain attacks.

According to news outlet Bleeping Computer one of the major incidents involving the supply chain compromise attack vector was the Kaseya Virtual System Administrator (VSA) cyberattack in 2021. The ransomware gang REvil seized an opportunity by exploiting a zero-day vulnerability in the widely adopted Kaseya VSA software, a preferred solution among managed service providers (MSPs). This software, instrumental in the remote monitoring and management of IT systems, became the unwitting conduit for cybercriminals to deploy the notorious ransomware. The ramifications of this insidious act extended beyond the MSPs themselves, reaching into the very fabric of their client base. REvil unleashed a wave of chaos by demanding an exorbitant $70 million ransom, for the decryption key which will decrypt all of the organizations affected by the ransomware attack.

In the aftermath, Kaseya navigated the complex landscape of cybersecurity hand-in-hand with experts and law enforcement agencies. Kaseya promptly released patches to address the vulnerabilities within its software, fortifying its defencses against potential exploits.

In a more recent case, Okta, a prominent U.S. access and identity management company, had reported that data from all its customers was compromised in a recent breach of its support systems. Initially, the company had indicated that only a small fraction of customers, approximately 1% or 134 organizations, were affected. The breach, which occurred in October 2023, involved a hacker utilizing stolen credentials to access Okta's support case management system and pilfer customer-uploaded session tokens, enabling potential unauthorized access to Okta customer networks.

In a blog post released later recapping the events, Okta's Chief Security Officer (CSO) revealed the extent of the breach encompassing more customers. Although an exact figure was not provided, Okta's CSO explained that on September 28, the hacker retrieved a report containing data pertaining to "all Okta customer support system users." For the majority (99.6%) of customers, the accessed information included full names and email addresses. In some instances, the hackers may have also obtained phone numbers, usernames, and certain employee role details.

According to Bleeping Computer and multiple other news outlets, the worst case of a supply chain attack came from a vulnerability in the file transfer application named MOVEIt. In late January 2023, the Cl0p ransomware group orchestrated a persistent campaign utilizing the zero-day vulnerability, to exploit the Managed File Transfer (MFT) platform. The campaign, spanning 10 days, resulted in the infiltration of approximately 130 victims. Notably, the Cl0p group themselves confirmed and asserted that they successfully exfiltrated data from the MFT platform during this period.

These cyberattacks underscores the increasing sophistication of ransomware groups and their ability to exploit zero-day vulnerabilities for targeted intrusions. As organizations grapple with evolving cyber threats, it becomes imperative to enhance cybersecurity measures, conduct thorough vulnerability assessments, and fortify systems to mitigate the risk of such incursions. These incidents serve as a stark reminder of the persistent challenges posed by cyber adversaries and the ongoing need for proactive cybersecurity strategies in the face of rapidly advancing threat landscapes.

In a recent investigation conducted by KPMG Canada's Cyber Threat Intelligence team, highlighted a supply chain attack campaign orchestrated by a threat actor known as "Scattered Spider". The victim company, with an extensive client base, provides various services to multiple entities. The discovery shed light on the intricate and evolving nature of cyber threats, showcasing the persistence of threat actors in breaching even well-established organizations.

SCATTERED SPIDER demonstrated a multifaceted approach, employing persistent attack vectors to compromise the security of the company and, consequently, its clients. Three prominent attack vectors were identified:

1

Two Factor Authentication (2FA) Spam
The threat actor targeted the two-factor authentication (2FA) mechanisms implemented by the victim organization. By specifically targeting the employees of the organization, the threat actor conducted a barrage of 2FA authentication requests. Eventually due to pressure/annoyance of the victim, they accept the malicious 2FA request, giving the threat actor complete access to their infrastructure. the malicious 2FA request, giving the threat actor complete access to their infrastructure.

2

Intimidation Tactics against Employees using SMS
SCATTERED SPIDER, along with 2FA spamming, engaged in direct SMS spamming. The threat actor threatened employees, either by bodily harm or violence to accept the malicious 2FA requests. This is congruent with recent intimidation tactics that have been demonstrated by the threat actor group. s, tactics and procedures to the SOC and other network defenders.

3

Bring Your Own Vulnerable Driver (BYOVD)
SCATTERED SPIDER also targeted the victim endpoints using drivers which were especially malicious. The group developed their own driver to defeat endpoint detection software & antiviruses. The threat actor would install the malicious driver and paired with an application, would suppress the defences of the endpoint.

The success of SCATTERED SPIDER's repeated attacks on the victim's infrastructure, resulted in severe consequences, extending beyond the immediate target. The company being a primary service provider, their employees had access to the internal infrastructure of multiple client organizations. The compromise of the victim company became a gateway for the threat actors to infiltrate the networks of these clients, leading to a domino effect of breaches across multiple companies.

The targeted attack illuminates the cascading impact of cyber threats within interconnected business ecosystems. The breach not only jeopardized the sensitive data and operations of the intended victim, but also paved the way for a chain reaction of compromises across other organizations. The incident underscores the critical importance of robust cybersecurity measures, constant vigilance, and collaborative efforts to mitigate the ever-evolving threats posed by adept and persistent threat actors like Scattered Spider. As organizations navigate the complex landscape of cybersecurity, it is imperative to recognize that the compromise of one entity can reverberate throughout the interconnected web of businesses, emphasizing the need for collective resilience and proactive defence strategies.

As evident, supply chain attacks have emerged as a prevalent and significant cybersecurity concern, influenced by various factors contributing to their occurrence. A primary contributor to this trend is the escalating complexity and interconnectivity inherent in global supply chains. The expansion of organizational networks, coupled with reliance on a diverse array of suppliers and service providers, creates an expansive attack surface, providing malicious actors with numerous potential entry points. Within the intricate web of dependencies characterizing supply chains, adversaries find opportunities to exploit vulnerabilities in specific components, thereby gaining access to the broader ecosystem.

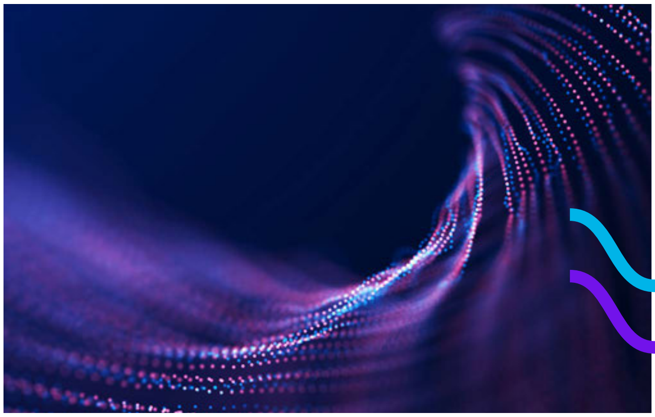
Another notable driver of supply chain attacks is the concept of amplification. The strategic targeting of a single supplier or service provider can yield far-reaching consequences as the compromise propagates through interconnected networks. Cybercriminals understand the ripple effect of infiltrating a pivotal link in the supply chain, allowing them to compromise numerous downstream entities. This amplification not only magnifies the scale of the attack but also poses a challenge for organizations attempting to accurately trace the origin and scope of the breach.

A third pivotal factor revolves around the trust placed in suppliers and service providers. Organizations often forge relationships with vendors based on trust, presuming that their partners uphold robust cybersecurity practices. Unfortunately, this trust can be misplaced, as suppliers may have weaker security postures or become victims of attacks themselves. Adversaries exploit this reliance, recognizing that breaching a trusted supplier can serve as a covert entry point into the targeted organization, evading conventional security measures.

Moreover, the financial incentives driving supply chain attacks should not be underestimated. Cybercriminals increasingly seek financial gain, and compromising the supply chain provides avenues for monetizing stolen data, intellectual property, or gaining leverage through ransomware. The potential for significant financial impact, coupled with the complexities of attribution in intricate supply chain environments, renders these attacks attractive to malicious actors seeking lucrative opportunities.

Cyber Threat Intelligence Impacts

The Cyber Threat Intelligence landscape is subject to the same impacts as Incident Response. The abuse of LLMs and AI technologies by threat actors is likely to continue, allowing them to evolve their attack methods and tools. This constant evolution will seriously degrade the effectiveness of indicators of compromised collected by forensic teams in a post-breach environment and are likely to frustrate efforts to attribute attacks to particular threat actors. As the environment becomes more dynamic CTI teams will need to adapt and revisit their models of attribution as well as their approach to supporting security programs to include more emphasis on behavioral indicators along with the technical to determine compromise and aid in attribution.



Intelligence as Strategic Innovation

KPMG in Canada prides itself on its Enterprise Intelligence as a Service offering. While it has always taken a business first approach to Intelligence, considering the second and third order impacts of an observation against its client's business operations, this has been further enhanced in 2023.

Fully integrating Threat Intelligence and Vulnerability Management teams allows both security teams to more fully understand the threat landscape and provider greater insights into threat actor tactics, techniques, and procedures (TTPs) as well as greater risk evaluation regarding vulnerabilities. Both teams are able to enrich each other's findings, delivering greater value from the timely, actionable and relevant intelligence they generate.

Cyber Threat Intelligence is the key connective tissue that that helps enable security teams to cross-silos and work together, providing maximum value and effectiveness.

Vulnerabilities Observed for the Year 2023

New scoring systems introduced for vulnerabilities: CVSS 4.0, the new Common Vulnerability Scoring System standard and the latest version of the Exploit Prediction Scoring System (EPSS).

CVSS 4.0: CVSS 4.0 is the new Common Vulnerability Scoring System standard. Some of the main updates and enhancements in the current version of Common Vulnerability Scoring System standard include increased simplicity and clarity by fine tuning the ideas of attack complexity and requirements making the score easier to understand.

The new CVSS 4.0 score also introduces new metrics and better structure allowing organizations to customize and tailor the scoring systems based on the needs and circumstances. The score is enriched by threat intelligence and risks associated by considering additional factors such as the possibility of potential attacks and consequence of exploitation leading to successful attacks.

Exploit Prediction Scoring System (EPSS): This scoring system is a data driven approach that aims to help organizations prioritize vulnerability remediation based on likelihood of exploitation in the wild. This is a great way to introduce a risk-based vulnerability management system. The EPSS probability score ranges between 0 to 100%, the greater the percentage the higher the likelihood of exploitation. The EPSS score is published for all CVEs in published state.

	CVSS	EPSS
Score range	0-10	0%-100%
Score meaning	Severity of a vulnerability	Likelihood of vulnerability being exploited in next 30 days
Data sources	Base, temporal, environmental and attack metrics calculated into score	Sources powered by machine learning, including present and historical data
Latest update	CVSS 4.0 (June 8, 2023)	Scores are updated daily

1. CVE-2023-27524 (Apache Superset RCE): This authentication bypass vulnerability is caused by insecure default configuration in the Apache Superset tool which is an open-source data exploration and visualization platform. Successful exploitation of this vulnerability leads to remote code execution, enabling threat actor(s) to gain administrative access on the targeted servers to compromise or steal user credentials.

This vulnerability is a result of a default Flask Secret Key, that has default predictable value at the time of installation, further causing session validation attacks and was seen exploiting by several malware families.

Impacted versions: all server instances that apply the default SECRET_KEY value as of version 1.4.1 and up to 2.0.1.

Although the evidence of widespread exploitation is not concrete, thousands of Apache Superset servers are vulnerable to this attack.

2. CVE-2023-2868 (Barracuda ESG): This OS Command Injection vulnerability in Barracuda Email Security Gateway appliance (ESG) exists due to improper input validation when processing .tar archives. The Barracuda Email Security Gateway is a hardware appliance designed to protect companies from various types of attacks such a spam, viruses, phishing, email threats and malware.

Successful exploitation of this vulnerability would allow threat actor(s) to send a maliciously crafted archive to the appliance and execute arbitrary perl commands on the targeted system, which may result in complete compromise on the vulnerable system. The vulnerability allows for the dropping and execution of a reverse shell on the Barracuda ESG appliance, establishing communication with the attacker's command and control server.

This vulnerability has been under active exploitation by various malware families such as SocGholish, DogeRAT, BlackByte Ransomware, LockBit Ransomware, Cl0p Ransomware, and more.

3. CVE-2023-27350 (PaperCut NG/MF): This improper access control vulnerability in PaperCut NG/MF software exists due to improper access restrictions within the SetupCompleted class. PaperCut NG/MF is a print management software that helps organizations with printing and copying tasks. This vulnerability allows threat actor(s) to bypass authentication to perform arbitrary code execution with system privileges.

Impacted versions: PaperCut NG/MF: before 22.0.9

This vulnerability was seen exploited in the wild and has been exploited by various malware families like Buhti Ransomware, Havoc C2 binary, Cobalt Strike, Lockbit 3.0 and Bl00Dy Ransomware.

4. CVE-2023-27351 (PaperCut NG/MF): This improper authentication in PaperCut NG/MF software exists due to an error within the SecurityRequestFilter class. This vulnerability allows threat actor(s) to bypass authentication to process and gain unauthorized access to the application.

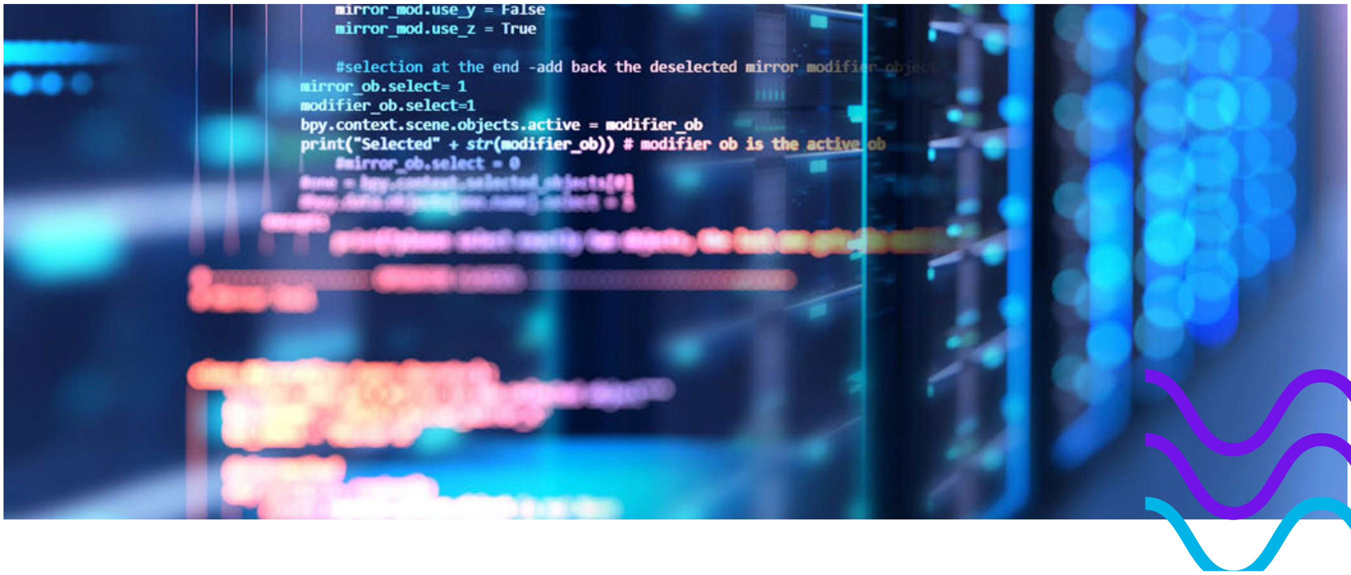
This vulnerability was seen exploited in the wild by various threat actor groups allowing the user to perform low complexity attacks with less user interaction (multiple malware families) such as including Ransom X, BlackByte Ransomware, LockBit Ransomware, Cl0p Ransomware, and Bl00Dy Ransomware.

Impacted versions: PaperCut NG/MF: before 22.0.9

5. CVE-2023-34362 (MOVEit Transfer and MOVEit Cloud): This SQL injection vulnerability exists due to insufficient sanitization of user supplied data. Threat actor(s) can send a specially crafted request to the impacted application and execute SQL commands within the application database.

This vulnerability was exploited by various malware families, the biggest one being Cl0p ransomware group which used the vulnerability to deploy a previously unseen web shell, LemurLoot to exfiltrate users' data and extort payments and the threat actor group released a public statement on their Tor data leak site. Exploit activity associated with this vulnerability has been observed on honeypots since June 2023.

6. CVE-2023-38035 (Ivanti): This vulnerability exists due to missing authentication on certain APIs. Threat actor(s) can send maliciously crafted HTTP requests to TCP port 8443 to bypass authentication and execute arbitrary code on the system.
This vulnerability was categorized as critical and has been observed by various malware families and threat actor(s) were seen exploiting this vulnerability with another Ivanti improper authentication vulnerability CVE-2023-35078.



```
    mirror_mod.use_y = False
    mirror_mod.use_z = True

    #selection at the end -add back the deselected mirror modifier object
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the active ob
    #mirror_ob.select = 0
```

7. Codesys vulnerabilities: Fifteen vulnerabilities were seen in Codesys' industrial control systems software that could potentially shut down power plants and gather sensitive information from critical infrastructures. The software development kit is used to configure and test programmable logic controllers (PLCs) for industrial systems.

CVE	CODESYS component	CVSS score	Impact
CVE-2022-47379	CMPapp	8.8	DoS, RCE
CVE-2022-47380	CMPapp	8.8	
CVE-2022-47381	CMPapp	8.8	
CVE-2022-47382	CmpTraceMgr	8.8	
CVE-2022-47383	CmpTraceMgr	8.8	
CVE-2022-47384	CmpTraceMgr	8.8	
CVE-2022-47385	CmpAppForce	8.8	
CVE-2022-47386	CmpTraceMgr	8.8	
CVE-2022-47387	CmpTraceMgr	8.8	
CVE-2022-47388	CmpTraceMgr	8.8	
CVE-2022-47389	CMPTraceMgr	8.8	
CVE-2022-47390	CMPTraceMgr	8.8	
CVE-2022-47391	CMPDevice	7.5	DoS
CVE-2022-47392	CmpApp/ CmpAppBP/ CmpAppForce	8.8	
CVE-2022-47393	CmpFiletransfer	8.8	

8. Microsoft Office and Windows HTML RCE (CVE-2023-36884): This vulnerability exists due to insufficient validation of user-supplied input impacting Microsoft Windows and Office products. Threat attacker(s) can trick the users to open a maliciously crafted file to perform remote code execution.

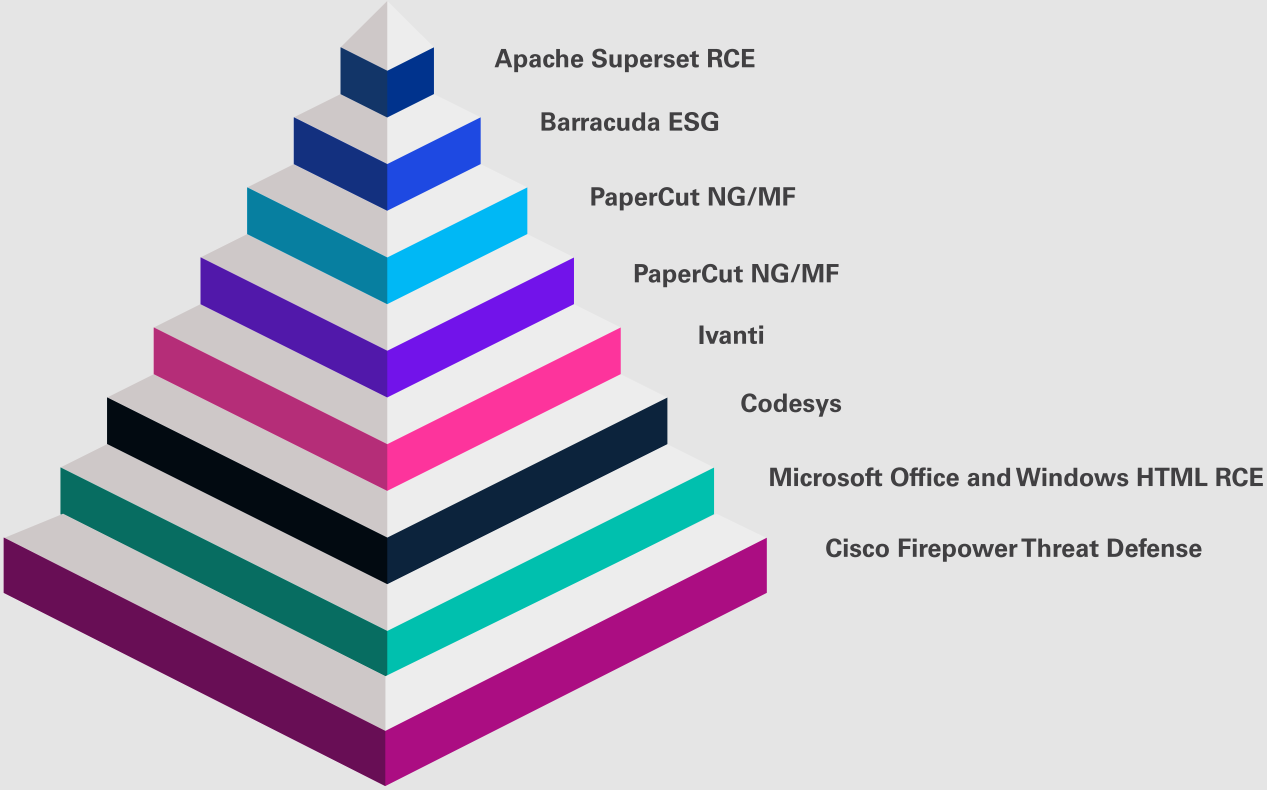
This vulnerability has been used by several malware groups, the prominent one being, the Storm-0978 group also known as the 'RomCom' (the name of the backdoor they distribute) is a cybercriminal group, popular for carrying extortion operations and targeted credential gathering campaigns to aid intelligence operations.

Historically, Storm-0978's targeted campaigns have impacted government and military organizations in Ukraine, as well as organizations in Europe and North America who are thought to be involved in Ukrainian affairs. These campaigns have impacted the telecommunications and finance industries among several others.

9. CVE-2023-20269 (Cisco Firepower Threat Defense): This authentication bypass vulnerability exists due to improper separation of authentication, authorization, and accounting (AAA) between the remote access VPN feature and the HTTPS management and site-to-site VPN features. Threat actor(s) can perform brute force attack to establish a clientless SSL VPN session with no authorization.

Among the various malware group such as LockBit Ransomware, Conti Ransomware, and Snatch Ransomware. Akira ransomware group was observed exploiting this vulnerability for financial motives and several reports have been observed selling this RCE exploit on a Russian forum for $100,000.

10. Top Exploited Vulnerabilities



In the coming year and beyond, collaboration and information sharing among industry peers, government agencies, and law enforcement will remain essential in the collective defense against cyber adversaries. As threats evolve, the collective intelligence and experience of the cybersecurity community will prove invaluable.

Looking Forward

The view ahead for 2024 is not dissimilar from 2023. State Cyber Activity, Criminal Cyber Activity, and Vulnerability Exploitation will continue to remain major forces impacting Cyber Security for the near future. With that in mind, 2024 does present some unique situational factors which will impact these forces.

State Cyber Activity

With the increase in volatility of global politics, an increase in information operations has followed. We have observed these operations meeting various degrees of success, however, more have been successful than not. As such with the looming 2024 United States Presidential Election, we anticipate a further increase in information operations carried out by states across the globe. These campaigns are likely to both target domestic mis-and-dis information within the United States, as well as campaigns regarding the actions of foreign states depending on the outcome of the election.

Depending on the outcome of that election we may also see campaigns from abroad encouraging insiders to take disruptive or destructive cyber action against employers or government entities.

Criminal Cyber Activity

2022 and 2023 witnessed an increase in efforts from threat actors to recruit corporate insiders, this is likely to continue into 2024. As threat actors see greater success across the landscape and have more resources at their disposal, it is possible that they will turn to buying insider access rather than the development custom tools and painstaking reconnaissance work against a target. While compromised tools are an effective means for threat actors to gain access, nothing is more effective than compromising an insider who is acting in bad faith.

Coupled with this is likely to be the continued rise of no-name or lesser-known threat actor groups and ransomware gangs. These no-name groups hope to avoid notoriety, in many cases to attempt to avoid the attention of state-level counter cyber operations and law enforcement.

Vulnerability Exploitation

2023 and 2024 will see further increases in interconnectedness and dependencies across providers. While this connectedness will help defenders via increased log sources and data, it also dramatically increases the risk of a third-party breach to most organizations. It is important to consider that Vulnerability Management programs are effective but cannot protect your organization from a lesser program at a critical vendor.

Leveraging CTI to monitor your critical third parties for compromise should be a standard feature of vulnerability management programs moving forward.

04

How KPMG can Help

KPMG in Canada's Cyber Security practice can assist with detecting, responding to and recovering from cyber breaches by providing immediate response services. Our professionals have experience in investigations, digital forensics, and recovery, which can help your organization secure evidence, understand what happened, mitigate risks and support internal, legal and law enforcement inquiries.

At KPMG, we help organizations effectively manage and protect their most valuable data across a broad spectrum of evolving threats and scenarios. We approach cyber security, not as a one-time project, but rather a holistic, adaptive strategy aligned to your business goals, focused on delivering long-term value for your business. So you can protect your future and expand possibilities.

KPMG Cyber Security Solutions include:

Incident response readiness and planning:
Assists you in improving incident readiness and response capabilities. So, in the event a security incident does occur, your organization is well-prepared to respond in a timely and effective manner.

Digital investigations and remediation:
Helps you efficiently respond to cyber incidents. When a breach occurs, we conduct forensic analysis and detailed investigations to determine what happened, how it happened, and, if applicable, who was involved.

Threat intelligence: Helps prioritize assets, identify possible threats and vulnerabilities, and determine organizational impact. This reduces the cost and complexity of proactively securing critical information assets and responding to attacks.

Data identification and remediation: Helps you efficiently leverage technology to securely manage confidential data, identify redundant, obsolete and trivial data (ROT) for remediation, and make it available in the business decision-making process.

Managed Detection and Response (MDR) Services:
MDR reduces the time to detect and respond by combining advanced threat technologies and 24/7 monitoring & analysis of an organization's security environment, allowing security analysts to identify and investigate potential threats in real-time. Our services are designed to help organizations identify and respond to cyber threats before they can cause significant damage or data loss by identifying the most actionable, timely and relevant information as alerts. Through automation and analyst driven guided response, the MDR service facilitates efficient and effective remediation and recovery of the assets.

05

Contributors

OT Security

Owen Key

Amir Rokinford

Cyber Threat Intelligence

Mike Rosenlund

Aindrea Skelly

Samanvitha Oruganti

Marie Eve Bergeron Tourangeau

Devin McDonald

Karan Ghoshal

Incident Response

Aleksandr Wagner

Yiwei Guo

Mohak Kamboj

Kyle Johnston

Chris Walker

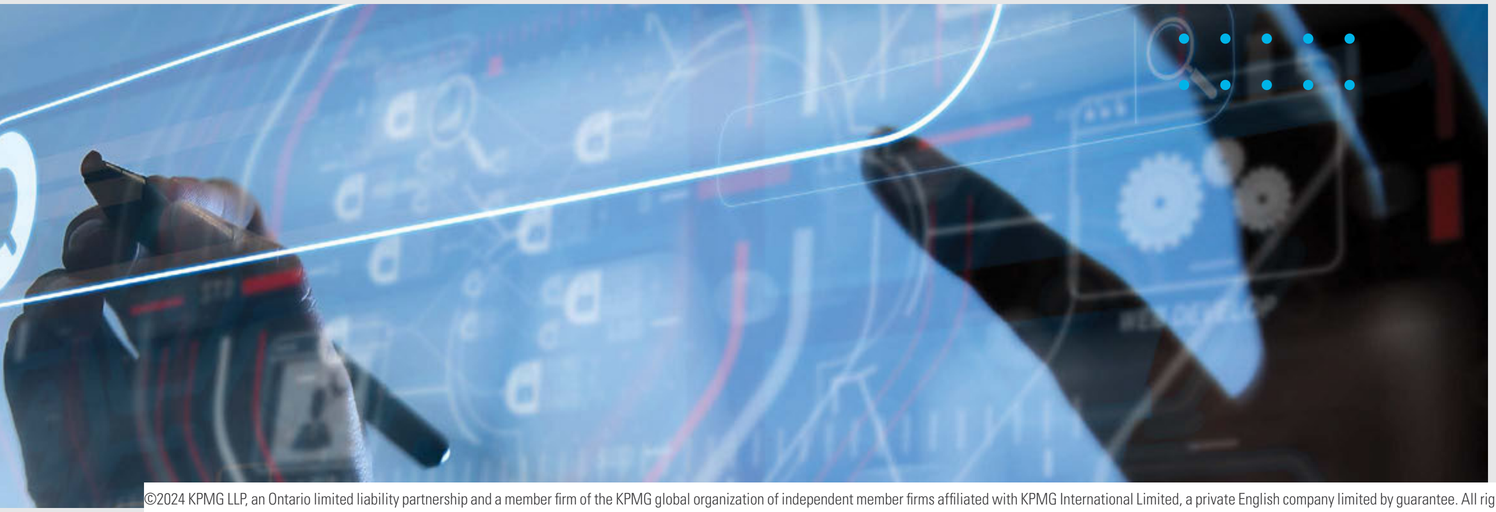
Ganesh Ramakrishnan

Xavier Normand

Robin Penrat

Jordan Michallet

Anne Labbé



Contact Us

Incident Response

Alexander Rau
Partner
alexanderrau@kpmg.ca

Ganesh Ramakrishnan
Senior Manager
gramakrishnan@kpmg.ca

Mansoor Haqanee
Manager
mhaqanee@kpmg.ca

Guillaume Clement
Partner
guillaumeclement@kpmg.ca

Valentin Bromont
Senior Manager
vbromont@kpmg.ca

Xavier Normand
Manager
xnormand@kpmg.ca

Cyber Threat Intelligence & Exploited Vulnerabilities

Robert Moerman
Partner
rmoerman@kpmg.ca

Mike Rosenlund
Manager
mrosenlund@kpmg.ca

Marie-Eve Bergeron-Tourangeau
Senior Manager
mbergerontourangeau@kpmg.ca

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

kpmg.ca