Cyber Incidents and Intelligence: 2024

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

March 2025

kpmg.ca

Contents

01 Introduction

The cybersecurity landscape continues to evolve, with threats growing in complexity and attack methods constantly shifting. As adversaries refine their tactics, organizations need to adapt to defend against emerging vulnerabilities.

This report offers a deep dive into real-world threats Canadian organizations faced in 2024 and provides a forward-looking perspective of what's ahead in 2025. Developed by KPMG in Canada's Cyber Incident Response, Cyber Threat Intelligence, and Vulnerability Management teams, it delivers key insights, lessons learned, and informed perspectives to help organizations strengthen their defenses.

It should be noted that information contained in this report reflects real incidents and experiences throughout 2024. While descriptions of the events are accurate, victim details have been obfuscated.

02 Incident Response

IR SUMMARY

Overview of Cybersecurity Concerns

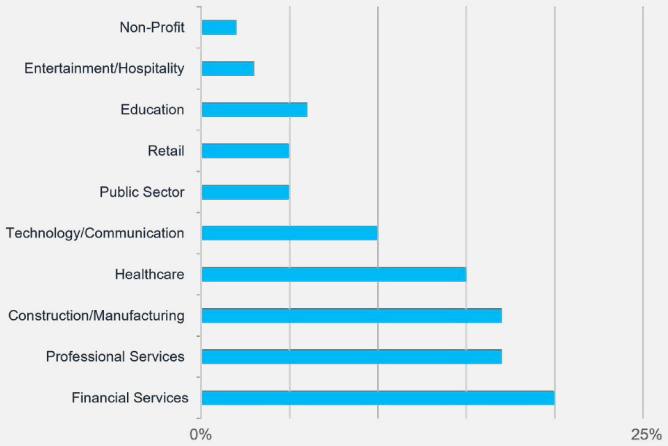
In 2024, Canadian organizations faced increased pressure from regulators, privacy commissioners, the public, and shareholders to strengthen their cybersecurity posture. However, the evolving threat landscape made this increasingly difficult, as attackers exploited vulnerabilities faster than organizations could patch them, targeting weak supply chain links, and bypassing defenses with sophisticated tactics.

KPMG observed a domino effect with ransomware incidents, where a single breach disrupted partners, service providers, and entire industry sectors. There was an increase in cyberattacks in the manufacturing and financial sectors, as threat actors took advantage of operational dependencies and data-rich environments to maximize their impact. However, with every cyber incident, there is a risk to identities. Cyber incidents and identity theft are deeply interwoven, as incidents often serves as a gateway for identity-based crimes.

TransUnion, a credit reporting agency offering monitoring in Canada, the US, UK, India, Hong Kong (SAR) China and South Africa, have shared some of the trends they are observing with respect to the Canadian threat landscape and subsequent identity theft.

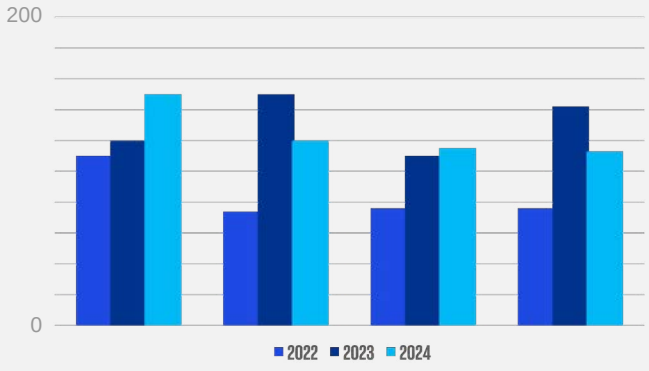
According to TransUnion, the most prevalent industry adopting identity protection services and monitoring is the Financial Services industry.

2024 Data Events by Industry



Source - TransUnion

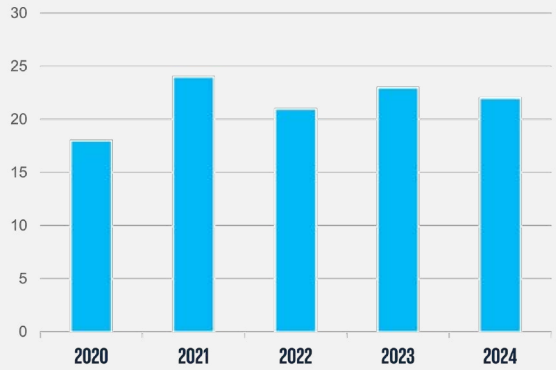
Number of Data Events by Quarter



As indicated in our Major Threat Statistics, TransUnion recorded increased breach events, with an overall reduction of breaches towards the end of 2024.

Source - TransUnion

Average Subscription Rate (in months) Year over Year Comparison



With the increasing number of breaches and subsequent threats to identities and personal information, TransUnion has observed average identity monitoring subscriptions between one to two years of coverage.

Source - TransUnion

Notable Observations

Increase in Firewall Exploitation

Since the beginning of 2024, KPMG's incident response and threat intelligence teams tracked vulnerabilities targeting various firewall products. KPMG identified that perimeter devices were often a preferred method for threat actors to gain access into an organization's environment. In 2024, there was a surge in the exploitation of firewalls, with threat actors racing to discover and take advantage of vulnerabilities before patches became available. The takeaway is clear: perimeter security alone is insufficient. As cybercriminals exploit vulnerabilities on a large scale, Canadian organizations need to pivot towards the adoption of proactive defense strategies, continuous monitoring, threat-intelligence-driven patching, and layered security controls to effectively combat the rapidly evolving threat landscape.

Ransomware Continues to Hit Hard at the Virtualization Layer

Threat actors increasingly targeted hypervisor environments, specifically ESXi and VMware hosts. This approach allowed threat actors to circumvent traditional endpoint defenses, enabling them to encrypt entire IT environments in one move. KPMG's frontline incident responders observed several ransomware incidents where threat actors successfully accessed hypervisor environments and encrypted Virtual Machines (VM). The shift in tactics enabled threat actors to maximize their impact with minimal effort, effectively crippling critical business operations by encrypting multiple VMs simultaneously.

Such tactics underscore the pressing need for stronger virtualization security measures. This challenge is pervasive, as current Endpoint Detection and Response (EDR) solutions are unable to secure the hypervisor level. Organizations relying on VMware and other hypervisors need to implement compensating controls to strengthen their infrastructure. These controls should include access management, privilege access management to safeguard root account credentials, network isolation for management, and robust back-up strategies to reduce the risk of total operational disruption. Security strategies need to evolve beyond endpoint protection to ensure the security of the foundational elements of IT infrastructure.

Malicious Use of Digital Forensics and Incident Response (DFIR) and Open-Source Tools

KPMG's frontline incident responders also observed that threat actors increasingly used readily available, free/open-source, and commercial digital forensics and incident response (DFIR) tools to evade detection, extract sensitive data, and maintain prolonged access within compromised environments. These open-source and publicly available forensic utilities were frequently misused for activities such as credential dumping, memory analysis, and establishing backdoor access, allowing attackers to operate discreetly while blending in with legitimate security operations.

This shift in tactics puts security teams in a difficult position when it comes to detecting the misuse of tools designed for detection. To effectively combat this issue, organizations need to move beyond traditional threat monitoring and begin to track the intent behind the use of these tools. It is not sufficient to merely know that these tools are being executed; understanding the context of when, how, and why they are being utilized is crucial.

Without implementing appropriate measures, threat actors will continue to exploit defenders' own tools against them, staying one step ahead in the cybersecurity chess game.

Brute Force Attacks, After-Hours Network Reconnaissance and VPN Masking

Threat actors persistently targeted IT environments through brute force attacks, often executing these attempts during late-night hours, early-mornings, or long weekends when security teams are less likely to detect suspicious activity in real time.

These campaigns bombard authentication portals with rapid password attempts, cycling through credential variations until a valid login is found. Similarly, network reconnaissance activities surged during off-hours, with adversaries scanning for open ports, misconfigured services, and exposed credentials, laying the groundwork for deeper compromise.

To further obfuscate their activities, threat actors have increasingly used Canadian VPN IP addresses to disguise their true origin and to appear as legitimate users. By leveraging commercial VPN services and compromised hosts within Canada, attackers are able to bypass geolocation-based security policies and blend in with regular traffic, making detection more challenging for security teams.

Key Learnings and Recommendations

Outlined below are key insights that some of our clients reflected upon following their experiences with cybersecurity breaches.

Log Retention: A Persistent Weakness

Log retention continues to be a significant gap, affecting approximately 50% of investigations conducted by KPMG in 2024. Critical logs—such as Windows Event Logs, network traffic logs, and security tool alerts —were often missing or overwritten, limiting visibility.

To address this, centralized logging solutions, such as Security Information and Event Management (SIEM) tools, are strongly recommended to ensure comprehensive log collection, long-term storage, and proactive monitoring, enabling more effective incident response and threat detection.

Threat Simulation Exercises

As cyber threats grow more sophisticated, organizations need to enhance their efforts and seek innovative strategies to stay ahead of these evolving risks while maintaining robust defenses against potential attacks.

KPMG's Cyber Threat Simulation is a structured exercise that replicates real-world cyber threats and attack scenarios. The primary goal is to assess and improve the effectiveness of an organization's security measures, processes, and incident response capabilities. This simulation employs methodologies similar to Red Teaming and Purple Teaming, while also incorporating unique features tailored to the specific goals and scope of each engagement. By emulating the tactics, techniques, and procedures (TTPs) of real adversaries, these simulations help organizations discover vulnerabilities, validate defenses, and improve readiness against cyber threats.

In 2024, KPMG hosted its inaugural Cyber Threat Simulation Challenge, attracting over 150 organizations to participate. This challenge provided a unique platform for organizations to test their cyber resilience in a competitive and collaborative environment. Explore the upcoming 2025 Cyber Threat Simulation Challenge to learn more about how leading organizations are preparing for the future of cyber defense.

Patch Management

Failing to keep hardware and software up-to-date continues to be a primary contributor to cyber incidents, with many investigations in 2024 originating from unpatched vulnerabilities in outdated systems. Threat actors continue to exploit known weaknesses that organizations fail to address, leaving critical systems exposed. To mitigate this risk, organizations need to implement proactive patch management strategies, which should include regular vulnerability assessments, prioritized updates for critical

systems, and automated patch deployment. Timely patching is one of the most effective defenses against preventable attacks.

Blind Spot in Asset Management

Ineffective asset management emerged as a significant vulnerability in around 30% of KPMG's incident response investigations conducted in 2024. Many organizations lacked visibility into their IT environments, with unknown accounts, unmanaged machines, and shadow IT systems going undetected. These blind spots provided threat actors with opportunities to infiltrate and maintain persistence without detection. To mitigate this issue, organizations need to adopt continuous asset discovery, centralized tracking, and conduct regular audits of all accounts, devices and systems.

EDR and SIEM Gaps

In 2024, KPMG's incident response investigations revealed that incomplete EDR coverage and the lack of SIEM tools were significant weaknesses in organizations' security postures. Many organizations had endpoints without EDR agents, which allowed threat actors to exploit vulnerabilities and move laterally within networks, escalating their attacks.

Similarly, a majority of ransomware victims did not have a SIEM tool in place, and where a SIEM was deployed, they often failed to ingest critical logs and/or had retention periods too short to support meaningful investigations. This left security teams blind to early indicators of an attack. In some cases, a SIEM was only deployed as log archive, but it was not fully configured to capture all relevant logs. These gaps do not just weaken defenses—they actively invite attackers to exploit unprotected systems.

Organizations need to prioritize the deployment of EDR across all machines to achieve complete coverage and ensure that SIEM tools are properly configured to ingest all necessary data while supporting long-term log retention. Anything less than this comprehensive approach leaves the door open for attackers to operate undetected.

For organizations that lack the resources to manage a SIEM deployment and a Security Operations Center (SOC), it is advisable to consider engaging a third-party for Managed Detection and Response (MDR) services. MDR services often come with Service Level Agreements (SLA) and provide organizations with peace of mind regarding their security posture.

Backups: Useless If You Can't Access Them

In most ransomware investigations conducted by KPMG, it was found that back-ups were either encrypted by attackers, deleted, or entangled in complications involving third-party IT services, leaving organizations with no means of recovery. Some organizations had offline backups but were unable to access them due to lost passwords, while others mistakenly assumed that their backups were intact—only to realize too late that they were not properly maintained or tested.

A back-up is only as effective as the organization's ability to restore it. Therefore, organizations need to establish a clear backup strategy that includes regular testing, effective credential management, and layered storage solutions (which should encompass online, offline, and immutable backups).

Security Awareness and Incident Preparedness

Cybersecurity is not just about technology—it is about how well your people, processes, and defenses hold up when an attack occurs. Organizations frequently operate under the false assumption of security until they find themselves in the midst of an incident, scrambling to respond. Security awareness needs to extend beyond training modules and phishing simulations. It is important for organizations to rigorously test their defenses through real-world tabletop exercises, red team assessments, and penetration tests to uncover weaknesses before attackers do.

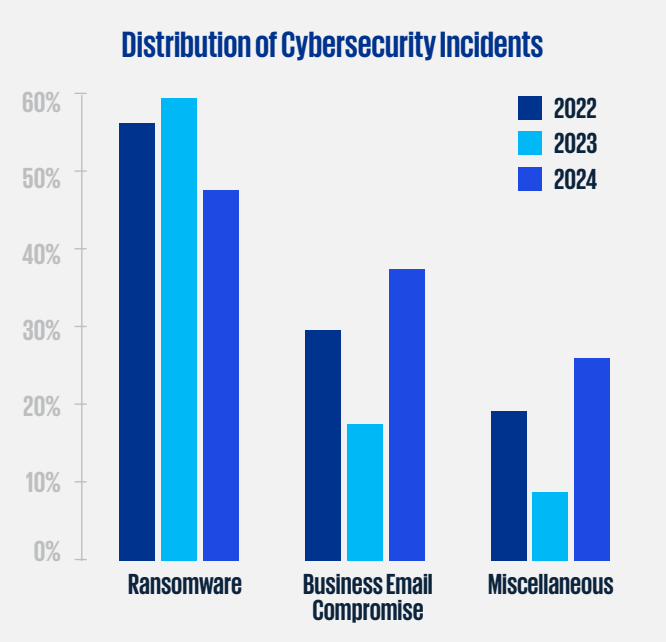
Regular threat hunting engagements should be a priority to proactively detect signs of a compromise, rather than waiting for alerts to trigger. Incident response should not be a reactive process; it requires rehearsal, refinement, and stress-testing. This preparation ensures that when a breach occurs, security teams are not responding blindly but are executing a well-practiced response plan. If your organization has not tested its defenses in a real-world scenario, it is already at a disadvantage compared to attackers who continuously assess and exploit weaknesses.

IR INCIDENTS

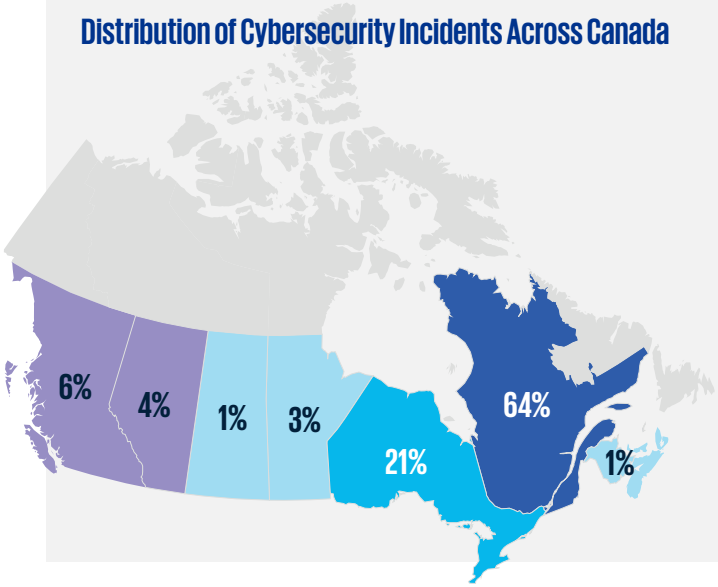
Major Threats and Statistics

Ransomware and Business Email Compromise (BEC) remain the most prevalent cyber threats facing Canadian organizations, with 46% of KPMG's investigations in 2024 involving ransomware attacks and 32% linked to BEC incidents.

While ransomware cases declined from 77% in 2023, attacks have grown more sophisticated, with threat actors increasingly targeting hypervisor environments to cripple organizations and bypass security controls. Meanwhile, BEC incidents surged from 15% in 2023 to 32% in 2024, with threat actors using multi-factor authentication (MFA) bypass techniques and Canadian VPNs to blend in with legitimate activity. These attacks were primarily targeted at executives, finance teams, and vendors, aiming to manipulate payments and steal credentials, often leading to significant financial losses and operational disruption. Other cyber threats, including unauthorized access and insider threats, rose to 22% from just 8% in 2023, indicating a broader diversification in attack methods.



Source: KPMG Incident Response



Additionally, cyberattacks in 2024 were heavily concentrated in Quebec and Ontario, reflecting the higher density of businesses and critical infrastructure in these provinces. In contrast, western provinces like British Columbia and Alberta experienced fewer incidents, with minimal activity reported in Northern and Atlantic Canada.

Source: KPMG Incident Response

Case Study #1

KPMG assisted a client during a ransomware attack in which the threat actor (TA) exploited an externally facing remote management tool. The TA gained access using a legitimate administrator account, which was made possible due to the absence of multi-factor authentication (MFA). Once inside the system, the TA established a covert backdoor by tunneling traffic through a trusted third-party service over port 443, ensuring persistent access even if the credentials were reset.

Following this, the TA exfiltrated data, mapped the network, and using DFIR tools, dumped memory to harvest credentials. To evade detection, the TA disguised a data exfiltration tool under a different filename before escalating the attack by accessing the client's ESXi environment via SSH and encrypting virtual machines. By the time it was detected, entire systems were locked down, crippling operations.

This case highlights how attackers leverage trusted third-party services for stealthy backdoor access and disguise malicious tools to evade detection. Without deep visibility into network traffic and process behavior, these threats can go unnoticed until it's too late.

Case Study #2

KPMG's frontline incident responders were called upon to investigate an incident in which a threat actor (TA) gained initial access to the organization's development (Dev) environment, which was not secured with the same controls as the production environment. With no Endpoint Detection and Response (EDR) coverage and a SIEM that only monitored production systems, the attacker moved undetected, laterally accessing domain controllers and VDI servers. The TA performed network reconnaissance, mapped key infrastructure, and exfiltrated approximately 65 GB of data using free, widely trusted cloud storage services such as Google Drive and SendSpace. Production data was in the Dev environment at the time of the attack. To further obfuscate their activities, the TA cleared event logs, erasing forensic evidence of their activities.

This incident underscores the often-overlooked security risks associated with development environments, particularly when production data is used in a non-production setting. Such environments can serve as a gateway to critical data and systems.

It also underscores how attackers abuse legitimate cloud services for covert data exfiltration and use log tampering to eliminate traces of their actions. Without full security coverage across all environments—including development—organizations face the risk of undetected attacks, often realizing the extent of the damage only after it has occurred.

Industry-Specific Analysis

Similar to our findings last year, KPMG observed that ransomware and Business Email Compromise (BEC) attacks affected organizations across multiple industries, with no single sector exclusively targeted. However, a significant trend emerged within the manufacturing sector, which experienced a higher frequency of attacks. This increase can be attributed to comparatively weaker cybersecurity postures in manufacturing businesses when contrasted to more technology-focused sectors. Many manufacturing organizations face challenges due to outdated infrastructure, limited security controls, and a prioritization of operational uptime over cyber resilience. This combination makes them appealing targets for financially motivated attackers.

In 2024, KPMG noted a significant increase in BEC and wire fraud attempts targeting small and medium-sized businesses within the financial services sector, marking a sharp increase from 2023. Threat actors concentrated their efforts on brokers and individual business owners in the financial and insurance industries, taking advantage of their frequent interactions with direct consumers and their reliance on email for exchanging key records, financial data, and, in some cases, banking information. These industry sectors have been particularly targeted by attackers seeking easier financial gains.

Trends

In 2024, KPMG observed a shift in ransomware tactics, with threat actors strategically lowering ransom demands to increase the likelihood of payment. Canadian organizations exhibited a greater propensity to pay a ransom demand when it was perceived as "manageable," resulting in an increase in payouts. Attackers often start with an inflated demand, subsequently lowering it to maximize profits through frequent, smaller payments rather than relying on substantial single payouts. This trend is particularly evident among less sophisticated threat actor groups that rely on social engineering and credential exploitation rather than advanced malware or zero-day vulnerabilities.

While ransomware continues to impact organizations across various sectors, threat actors have adopted different approaches towards the education and government sectors. In these cases, the focus has shifted from securing ransom payouts to generating media exposure to build their reputation. By ensuring high-profile incidents attract public attention, these groups increase fear, establish credibility, and exert pressure on future victims to comply more swiftly.

As ransomware tactics evolve, it is important for organizations to understand that negotiation strategies and media influence have become integral components of attackers negotiation strategies. KPMG's frontline responders observed ransomware payouts ranging from as low as USD $45,000 to as high as USD $1.75 million, in 2024.

IR IMPACTS

Ransomware-as-a-Service (RaaS): Supercharging the Ransomware Epidemic

Ransomware-as-a-Service (RaaS) continues to reshape the cyber threat landscape, making ransomware more accessible, efficient, and relentless than ever before. No longer limited to elite hackers, even low-skilled attackers could "subscribe" to ransomware operations, gaining access to pre-built malware, automated deployment tools, and negotiation playbooks.

This surge in RaaS affiliates flooded organizations with attacks, forcing IR teams to battle multiple ransomware variants, unpredictable attack patterns, and relentless encryption payloads—often within hours of initial compromise. The assembly-line efficiency of RaaS shortened response windows, leaving security teams scrambling to contain damage before data was exfiltrated or systems were locked down.

Extortion Techniques

Double extortion became the norm, and triple extortion turned up the pressure even further. Attackers no longer just encrypt systems—they first steal sensitive data, using it as blackmail to force payment. Even organizations with backups found themselves trapped—either paying the ransom or risking regulatory fines, lawsuits, and public exposure.

Many ransomware groups now operate leak sites, auctioning stolen data and publicly shaming victims who refuse to pay. But some took it even further with triple extortion, directly blackmailing customers, employees, and partners using stolen information.

IR Strategic Innovations

KPMG's Incident Response team undertook several innovative approaches to aid in immediate incident response and recovery activities, while also ensuring that victims were provided with a more stable and secure environment following an incident. One key innovation was the cyber threat hunting library.

Comprehensive Threat Hunting Library

KPMG developed a comprehensive threat hunting library by leveraging frameworks from MITRE ATT&CK, the current threat landscape, and use cases observed from indicators of compromise and tactics, techniques, and procedures (TTPs) from previous incidents. The results of each threat hunt allowed our clients to fine-tune alerts, customize blocking policies, and proactively strengthen detections ensuring a more secure posture before facing real threats.

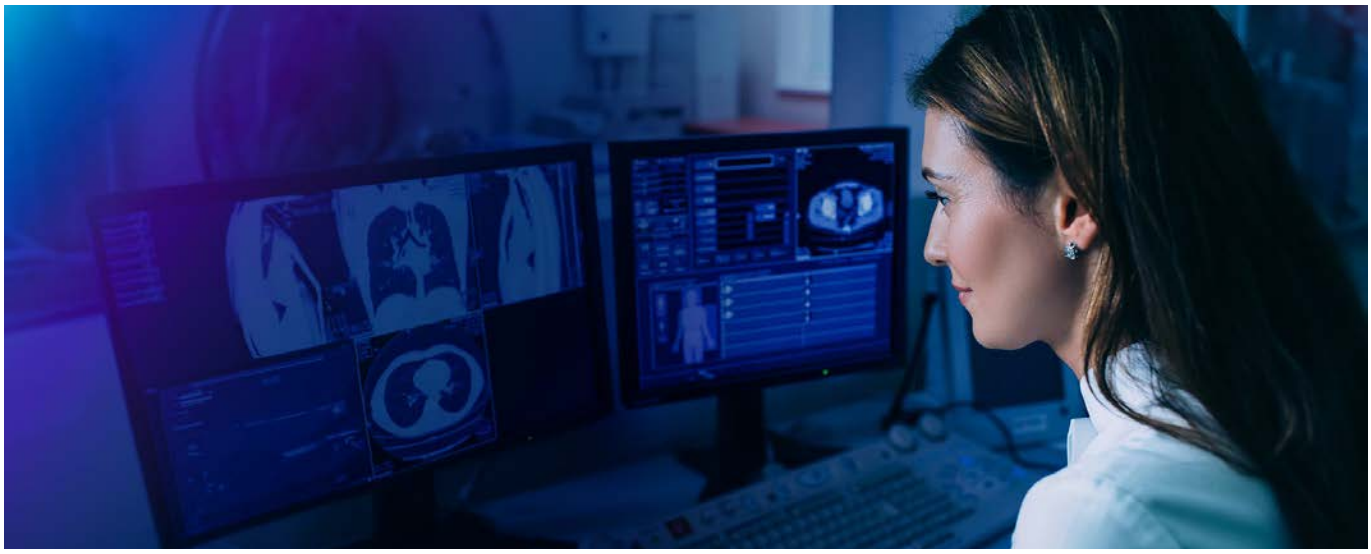
KPMG's Cyber Threat Simulation Challenge

During the summer of 2024, KPMG in Canada launched its first Cyber Threat Simulation Challenge to help organizations validate their cybersecurity capabilities. The challenge was free of charge and involved a small scale "purple team" exercise.

The initiative gave each participating organization the opportunity to assess their security posture in a controlled environment, and gain insights into their ability to detect and respond to cyber threats effectively.

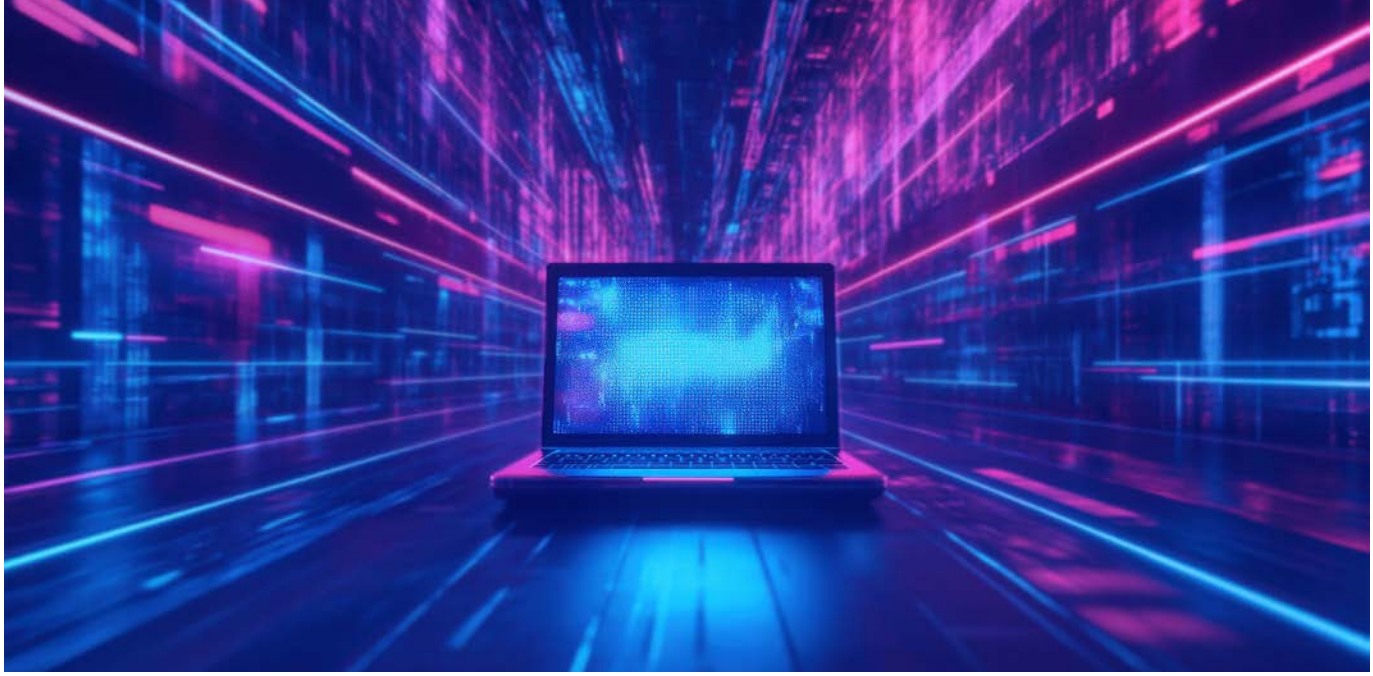
Over 150 companies from across Canada registered for the Challenge. We conducted a one-hour simulation for each participant, involving multiple attack scenarios (such as Command & Control, Discovery, Defense Evasion, Credential Access – Kerberoastable attack, Credential Access – Rubeus attack, Persistence, and Execution).

Please note that the findings from the Challenge are based on tests conducted with individuals who registered as part of the campaign. The results are limited to this specific group of participants.



Key Observations

- About 74% of the time, organizations failed to detect the attacks.
- There was a significant gap between logged events and alerts raised.
- The most frequently detected attack scenario was Execution.
- Defense and Persistence attack scenarios were detected the fewest number of times by participants.
- Smaller sized organizations faced higher detection failure rates, suggesting smaller sized organizations may face higher risks of undetected threats.
- Some organizations within specific industry sectors experienced more challenges in detecting threats, with Financial Services (primarily comprising small- to medium-sized financial institutions), Healthcare and Wellness, and Food and Beverage topping the list.
- Job roles of those who registered in our challenge varied, with a significant representation from IT Support, C-Suite and Executive Financial Leadership, indicating a strong interest in enhancing organizational security measures, highlighting the growing recognition of cybersecurity as a critical business priority, and an emerging need for leadership to address cyber threats within organizations.



Other key findings: Few organizations are well prepared

Each hour-long simulation tested 4 to 7 real-world tactics that threat actors frequently use in cyberattacks including Command & Control, Discovery, Defence Evasion, Credential Access – Kerberoastable, Credential Access - Rubeus, Persistence, and Execution. If the tests had been real intrusions, the attacks likely would have gone unnoticed for most participants.

Organizations that performed well during the simulations had strong technology in place to help detect and log cybersecurity incidents, as well as provide alerts to address them as effectively as possible.

Almost every participant indicated they hadn't tested their detection capabilities before. KPMG research indicates managed security service providers (MSSPs) don't conduct purple team exercises within their own environments frequently, so many organizations may be operating with ineffective detection use cases – and a false sense of security.

Simulation tests benefit companies of all sizes

One of the biggest misconceptions of purple team exercises is that they're only designed for large organizations. Purple team exercises are beneficial for companies of all sizes, especially when the scope and approach align with an organization's maturity, resources, and risk profile.

Small to medium-sized businesses (SMBs) often lack robust defenses, so cybercriminals increasingly target them. Purple team exercises help SMBs identify vulnerabilities, test defenses, and improve security processes cost-effectively. These exercises raise awareness and strengthen the security culture in organizations with limited resources.

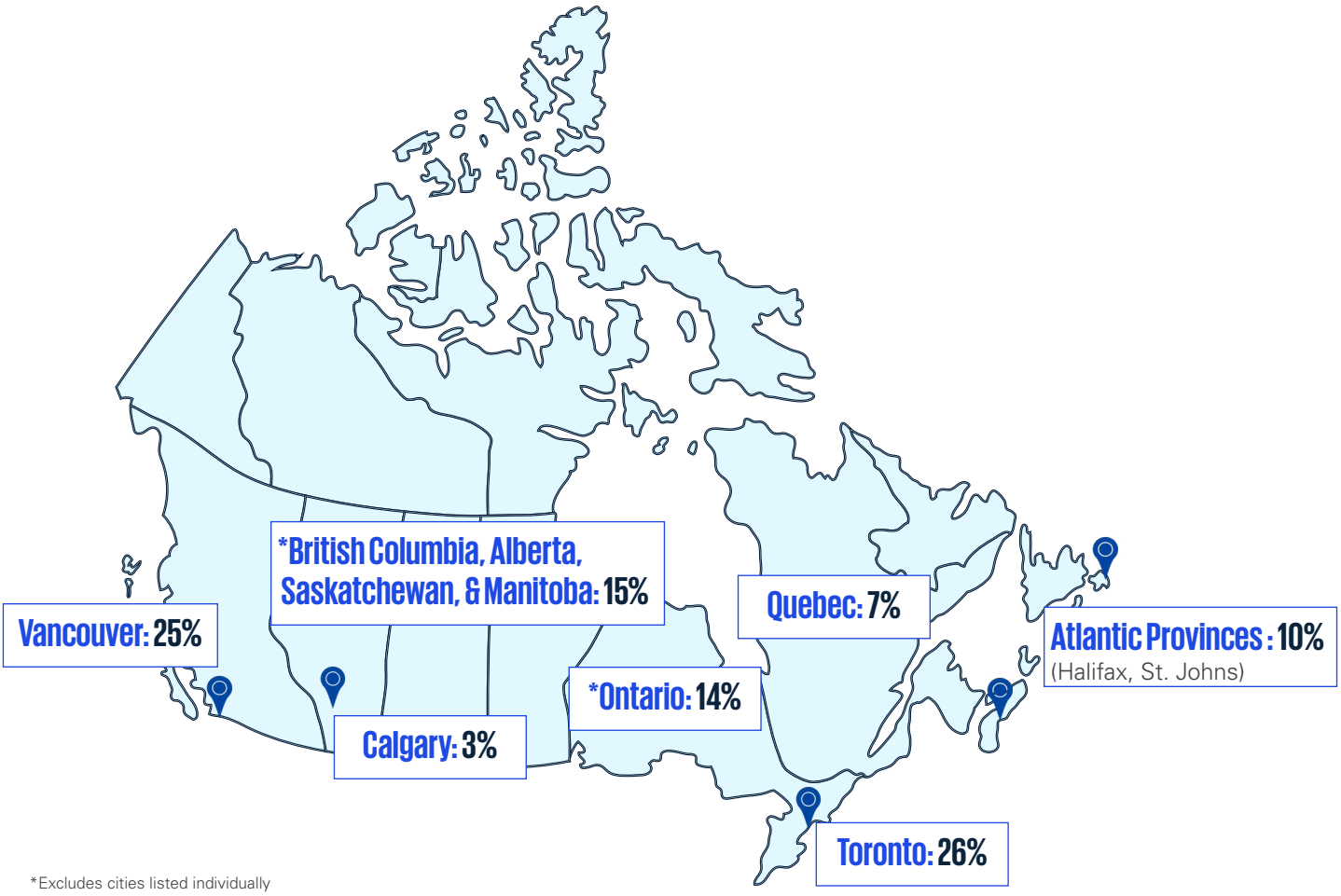
Mid-market companies manage growing complexities in IT environments (e.g., cloud, Internet of Things, etc.), but may still face resource constraints. Mid-market companies are often part of larger supply chains, making them attractive targets for attackers aiming at critical infrastructure or enterprise partners.

Large enterprises are high-value targets for advanced persistent threats (APTs), ransomware, and nation-state attacks. With complex IT ecosystems and distributed teams, purple team exercises ensure collaboration and coordination between their red and blue teams. They help validate security tools and strategies, refine incident response processes, and align with compliance requirements.

When downtime or breaches can have catastrophic consequences including security risks, financial and reputational losses, and even losses of life, purple team simulations can play a key role in your organization's cybersecurity operations, no matter the size or industry.

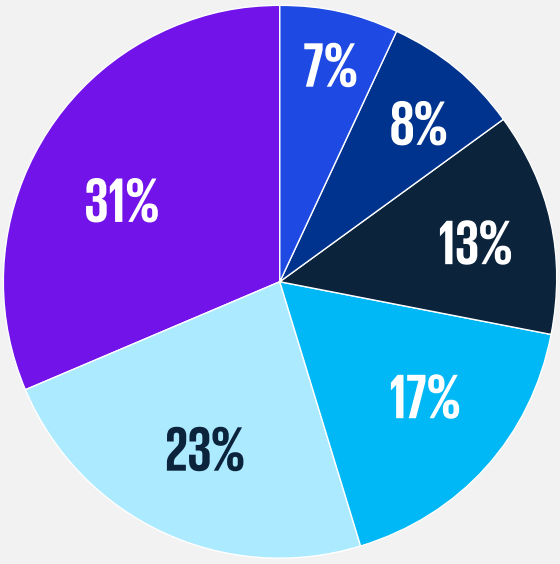
Participant Demographics

2024 Registrations by Province

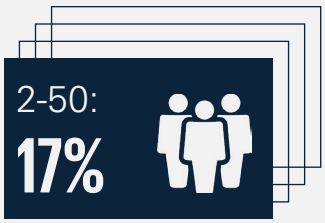


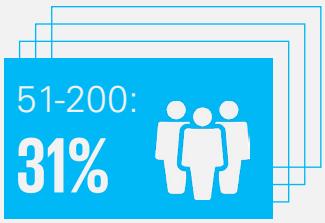
*Excludes cities listed individually

2024 Registrations by Company Size



2024 Top 3 Registrations by Company Size

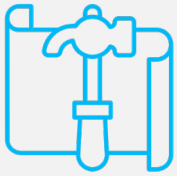




2024 Top 3 Registrations by Industry

Financial Services:
20%

Technology:
20%



Construction:
15%

2024 Registrations by Job Role

Information Technology Support	19%	Administration and General Counsel	10%
Directors and Senior Management	14%	Operational Management	7%
Executive Leadership	14%	Cybersecurity Leadership	5%
Financial Management	14%	Innovation and Technology Development	5%
Information Technology Leadership	10%	Sales and Marketing Leadership	2%

Looking Forward to 2025

As cyber threats continue to evolve, 2025 is poised to bring new challenges, more sophisticated attacks, and heightened pressure on organizations to adapt. Based on KPMG's investigations and industry trends, the following key areas are expected to shape the cybersecurity landscape in the coming year:

More Targeted Ransomware & Extortion Tactics

Ransomware groups will likely shift to more strategic targeting, prioritizing victims with a higher likelihood of payment while continuing double and triple extortion tactics to maximize impact. Expect shorter dwell times and more aggressive negotiation tactics.

Geopolitical Tensions Driving Cyber Activity

Global conflicts and economic shifts will fuel an increase in state-aligned cyber activity, targeting critical infrastructure, government entities, and high-value sectors. Espionage, data manipulation, and destructive attacks could become more frequent, impacting organizations caught in geopolitical crossfire. As a result, KPMG believes that there will be an increased scrutiny and potentially sanction of technology tools (software or hardware) built by Canadian state adversaries.

Growing Risks in the Cloud

As organizations expand their cloud footprint, attackers will increasingly exploit misconfigured cloud environments, weak API security, and overprivileged accounts to gain footholds in corporate infrastructure.

Continued Use of AI-Powered Attacks

As AI rapidly evolves, threat actors are increasingly leveraging large language models (LLMs) and automation to craft personalized phishing attacks, bypass security measures, and accelerate intrusions.

Zero-day Exploits Becoming More Accessible

The underground market for zero-day vulnerabilities will continue to grow, making weaponized exploits more accessible to cybercriminals.

03 Cyber Threat Intelligence

CTI Summary

The geopolitical and economic challenges of 2024 were underpinned by significant developments in the Cyber Threat Intelligence space, from states attempting to tackle the problem of ransomware, the proliferation of cyberwarfare and its fallout, exploitation of AI by attackers, and hacktivism to espionage and state actor threats. These developments cover the breadth of the cyber threat landscape, and should all be considered when conducting strategic planning for an organization's cyber security program in 2025 and beyond.

The State of Ransomware

In recent years, the ransomware-as-a-service (RaaS) model has become increasingly popular among threat actors, enabling them to target organizations worldwide. This surge in cyber-attacks has drawn the attention of law enforcement agencies, underscoring the urgency to counteract the malicious activities of ransomware gangs.

Since late 2022, the Federal Bureau of Investigation (FBI), in collaboration with other law enforcement organizations, have penetrated the networks of several ransomware groups. Though these actions may have rattled ransomware operators, the groups targeted by law enforcement have largely rebranded, rebuilt or reorganized, joining other ransomware groups, or forming new entities, providing significant challenges for law enforcement. Though the actions of law enforcement in 2024 were welcome, they may not have a major impact on the threat landscape.

To provide context, our team has summarized major developments with two threat actors in the ransomware space, ALPHV/BLACKCAT and LOCKBIT 3.0.

ALPHV/BlackCat Ransomware Group

In December 2023, law enforcement agencies executed a takedown of the ALPHV/BLACKCAT ransomware group, a rebrand of DARKSIDE and BLACKMATTER. The significant operation was aimed at disrupting the high profiles group's illicit activities, potentially propelled by the group's association to the high-profile cyber-attack against MGM earlier in 2023. Despite this initial success, the group quickly reestablished its operations, targeting many institutions, including hospitals—an area they had previously refrained from attacking.

Upon its return, ALPHV successfully infiltrated a hospital and demanded a ransom of $22 million. Following this incident, ALPHV affiliates alleged that the group had absconded with the ransom payment, indicating potential internal strife and a breakdown of trust within the organization.

The FBI's takedown operation may have catalyzed significant fallout among ALPHV's affiliates, leading to speculation that the group was contemplating an exit scam. While ALPHV/BLACKCAT has seemingly exited the ransomware landscape, many of its affiliates have likely migrated to other ransomware families, continuing the cycle of cybercrime. Furthermore, the remaining members of ALPHV are suspected to have rebranded themselves under new identities, perpetuating the threat posed by ransomware groups.

LOCKBIT 3.0 Attempted Takedown

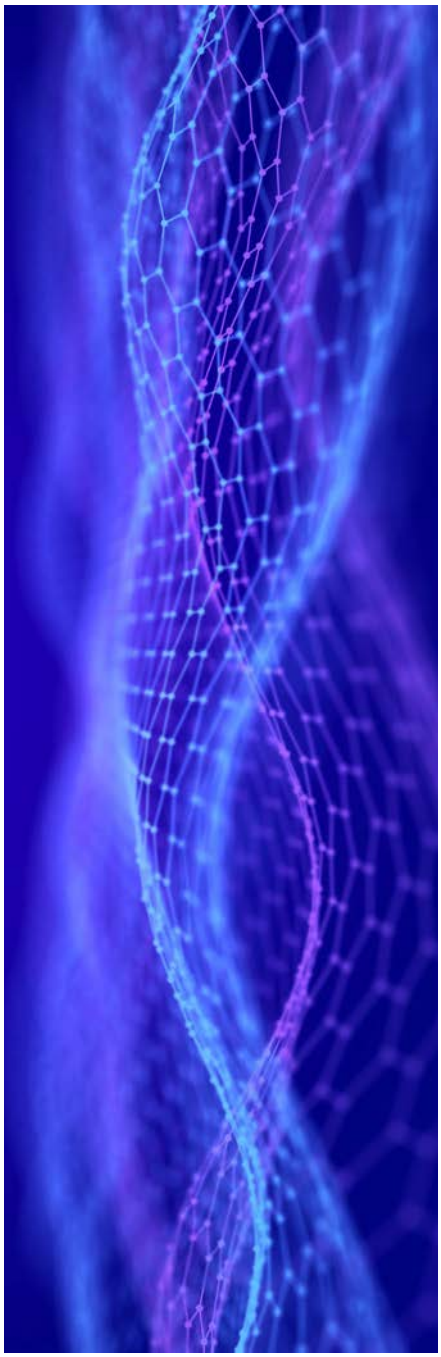
In February 2024, the FBI executed a significant operation against the notorious LOCKBIT 3.0 ransomware group by seizing control of their servers. This operation included utilizing the group's dark web site to disseminate updates regarding the FBI's takeover, signaling a strategic move to disrupt the group's operations.

However, within two days of this intervention, LOCKBIT 3.0 demonstrated its resilience by launching a new site. LOCKBIT 3.0 is recognized as one of the most active ransomware gangs in the cybercrime landscape. The group operates through a network of affiliates, which allows it to target a wide array of companies across the globe.

Sources: Security Week Cybersecurity News, Insights, and Analysis, Mar 6, 2024; Reuters, Feb 23, 2024; Infosecurity Magazine, Dec 19, 2023; CSO Online, Oct 6, 2023; Infosecurity Magazine, Feb 26, 2024; Resecurity, Mar 4, 2024

Prior to the FBI's intervention, LOCKBIT executed a high-profile attack on Fulton County, where they claimed to have accessed sensitive data files. The group demanded a ransom of $1.2 billion. The attack disrupted services, with restoration efforts extending over a two-month period.

Despite law enforcement efforts to dismantle LOCKBIT 3.0, the group maintained its status as a major player in the ransomware landscape throughout 2024. KPMG observations indicate that LOCKBIT claimed approximately 14 organizations in Canada alone during this period, illustrating the group's persistent threat and the challenges faced by law enforcement in curbing its activities.



Ransomware Threats on the Horizon

Ransomware operators have learned that to maximize their impact, their tools, tactics and techniques must be refined. Attacking a mature target in a highly monitored and defended environment is less likely to be successful with unproven tools, and as such, many of these threat actors are targeting developing countries to hone their craft.

The best examples of these efforts can be seen from the cyber-attacks carried out against Costa Rica and the Dominican Republic in 2022. In these attacks, the threat actors CONTI and QUANTUM RANSOMWARE executed significant operations against government entities. In the case of CONTI's attack, their stated intent was to overthrow the government through cyber warfare.

The Dominican Republic's Instituto Agrario Dominicano (equivalent to the Ministry of Agriculture) was specifically targeted, prompting a proactive investigation. This revealed CONTI had planted malware in the region ten months before the attacks. This discovery indicated a long-term strategy to infiltrate and exploit vulnerabilities in the victim's environment, demonstrating the patience and persistence which could be observed in planned attacks through 2024. The choice of targets, which were unlikely to afford ransom payments, suggests that these attacks served as dry runs for the threat actors, allowing them to refine their techniques and assess the effectiveness of their malware in less fortified environments.

Subsequent cyber incidents in other developing nations, including Senegal, Chile, Colombia, and Argentina, further support that these attacks are part of a broader strategy by threat actors to test their methods. The rapid digital transformation in many African countries, coupled with the ongoing challenges in maintaining robust cyber defences, make these regions particularly attractive targets. As organizations in these countries, including banks and government institutions, struggle to stay up to date with cyber defences, they inadvertently provide a fertile ground for testing attack methodologies.

By leveraging the vulnerabilities in developing countries, threat actors can refine their tactics and tools, ultimately gaining a competitive advantage when targeting more resilient systems in developed nations such as the United States, Canada, and the United Kingdom.

This cycle of exploitation not only endangers the immediate victims but also poses a broader threat to global cybersecurity, as successful attacks in developing countries can lead to more sophisticated and damaging operations in countries with stronger defences.

Sources: BleepingComputer.com, Aug 24, 2022; Financial Times, July 9, 2022

Cyber Warfare and its Implications

There have long been concerns over the use of cyberweapons in conventional conflict, and the subsequent fallout of those tools, tactics and techniques bleeding over from state use into the criminal sphere. 2024 has reenforced these concerns, with significant attacks taking place related to the Russia-Ukraine conflict, and the potential for devastating ICS targeting malware to find its way into the criminal realm.

Exposure of new Malware via CyberWeapons

The cyber-attack on Lvivteploenergo's network in Lviv, Ukraine, in January 2024 was a significant incident, occurring over winter. The attackers likely infiltrated the network nearly a year prior, on April 17, 2023, by exploiting an unidentified vulnerability in an Internet-exposed Mikrotik router. The absence of adequate network segmentation allowed the adversaries to manipulate hardcoded network routes, granting them control over the district's heating system controllers. Subsequently, they downgraded the firmware to versions lacking monitoring capabilities, thereby evading detection.

Months after the attack, FrostyGoop malware was discovered and linked to the incident. FrostyGoop malware specifically targets the Modbus protocol widely used in industrial settings. The malware is notable for being the ninth known instance of industrial control system (ICS) malware, following CosmicEnergy and Industroyer2, which were also associated with attempts by the SANDWORM group to compromise Ukrainian energy providers.

While the threat actor remains unknown, the attack exhibited connections to a Moscow-based IP address. These tactics and malware may serve as a blueprint for other threat actors aiming to execute financially motivated attacks on ICS infrastructure.

In March 2024, threats from Russia-backed SANDWORM increased, exposing newly undiscovered malware used in its attacks as the group attempted to disrupt 20 facilities across 10 regions in Ukraine. The attack targeted critical sectors including energy, water, and heating. These attacks were likely coordinated following attacks against Russia from Ukraine. The cyber-attack employed four (4) malware variants; BIASBOAT (Linux malware), LOADGRIP (Linux malware), GOSSIPFLOW (a Go-based malware), and Kapeka backdoor, a successor to SANDWORM's GreyEnergy malware, which was a new variant of BlackEnergy. BlackEnergy was used to attack the Ukrainian power grid in 2015.

Sources: Cybernews – Latest Cybersecurity and Tech News, Research & Analysis, Jul 23, 2024

SANDWORM-Linked Sub-Groups

Days before this widespread attack on Ukraine, four small Ukrainian internet providers suffered disruptions to their operations. The Russia-linked hacktivist group SOLNTSEPEK claimed responsibility for launching the attacks. It claimed to have obtained the ISPs' client databases and internal data. SOLNTSEPEK previously claimed responsibility for targeting Kyivstar, one of Ukraine's major telecommunications operators, in December 2023 in what was considered a highly impactful and disruptive cyber-attack. The attack impacted millions of customers who experienced service disruptions for several days. SOLNTSEPEK is thought to be an alias or cover identity for SANDWORM, potentially linking SANDWORM to these attacks.

Though SANDWORM's attacks have been focused on Ukraine, subgroups associated with the threat actor are alleged to be targeting facilities in the United States, Poland, and France. The SANDWORM-linked sub-group, Cyber Army of Russia Reborn (CARR) has claimed responsibility for attacks in Poland, France, and the U.S. The January 2024 attack on a Texas-based water facility led to a water tank overflowing with CARR showcasing its breach after launching a YouTube channel to demonstrate its manipulation of the facility's computer systems.

The continued targeting of industrial control systems (ICS) and operational technology (OT) demonstrates the value that adversaries place on critical infrastructure. State-sponsored actors aim to gain strategic advantages in geopolitical conflicts, while hacktivists continue to claim responsibility for attacks on critical infrastructure to elevate their messages and spread fear, uncertainty, and doubt. Ransomware actors will likely continue exploiting the growing convergence of IT and OT networks, capitalizing on poor security practices and network segmentation to access critical industrial systems.

As these threats evolve, organizations must proactively strengthen critical defenses, emphasizing layered security controls, continuous monitoring, and strict adherence to regulatory requirements to mitigate the heightened threat landscape facing ICS and OT environments.

Threat Actors Leveraging Artificial Intelligence

In February 2024, OpenAI, the artificial intelligence company responsible for ChatGPT, along with Microsoft, terminated accounts associated with five (5) nation-state groups. The threat actors from various countries were identified, with some of whom target critical infrastructure. In response to these threats, Microsoft has proactively issued guidelines to prevent misuse of its AI systems by state-backed threat actors.

Microsoft's guidelines emphasize several key areas:

- the identification and cessation of harmful use of AI technologies
- the importance of sharing findings with other AI providers to foster a collaborative approach to security
- the necessity of managing risks associated with AI deployment
- the documentation of activities related to threat actors to enhance understanding and response strategies
- the outlining of the company's countermeasures to mitigate potential threats.

These measures reflect a commitment to safeguarding AI technologies, particularly in the face of increasing threats from state-sponsored threat actors.

ChatGPT-4 Can Exploit Systems with Advisories Alone

Multiple observations through 2024 have demonstrated how ChatGPT-4 can be leveraged to exploit vulnerabilities, using only public security advisories as a source. The AI agent was used to test 15 known vulnerabilities in open-source software, which it successfully exploited 87% of the time. A threat actor leveraging tools like GPT-4, could automate the exploitation of vulnerabilities as soon as they are publicly disclosed.

As we look towards the future, the impacts of AI on the cyber threat landscape will be profound and multifaceted. The ability of AI tools like GPT-4 to exploit vulnerabilities not only accelerates the pace at which cyber threats can emerge but also raises significant concerns regarding the security of digital infrastructure. As AI continues to evolve, the race between attackers and defenders will intensify, making it imperative for all stakeholders to adapt and innovate in their approaches to cybersecurity.

Sources: WIRED, Apr 17, 2024; Cyber Security News, Apr 24, 2024; The Record Media, Mar 22, 2024; Restack, Feb 18, 2025; Microsoft Tech Community – Educator Developer Blog, Dec 11, 2024; Cyber Security News, Apr 22, 2024; The Hacker News, Feb 14, 2024

Hacktivism and Distributed Denial-Of-Service DDoS Threats in 2024

Hacktivism through distributed denial-of-service (DDoS) attacks has continued to pose a threat through 2024 and is likely to do so in 2025. Hacktivist groups are known for their politically motivated cyber activities, often targeting infrastructure related to states or organizations they perceive as adversaries or for political statements.

The operational impacts of many of these attacks were minimal, with some attacks unverified. However, we will likely see a continuation of this threat in 2025 as geopolitical tensions rise.

DDoS Threat on Canadian Entities

In May 2024, the hacktivist group NONAME057(16) claimed responsibility for multiple distributed denial-of-service (DDoS) attacks targeting various European organizations. In mid-June 2024, NONAME057(16) claimed it was targeting Canadian entities. The group claims to have DDoS attacked telecom provider TELUS and a financial company in Quebec.

In May 2024, a significant Distributed Denial of Service (DDoS) attack targeted Winnipeg Richardson International Airport, disrupting its online services and affecting passenger access. The attack was claimed by two hacktivist groups: HACKNET and the PEOPLE'S CYBER ARMY. These groups are known for their politically motivated cyber activities, often targeting infrastructure related to nations they perceive as adversaries or for political statements. While the specific motives behind the attack on Winnipeg Richardson International Airport were not extensively detailed, similar attacks by these groups often align with larger geopolitical tensions, including reactions against government policies or actions taken by states involved in international conflicts.

On November 22, 2024, the pro-Russian hacktivist group NONAME057(16) claimed responsibility for a series of Distributed Denial of Service (DDoS) attacks targeting several Canadian government and telecommunications websites. The affected organizations included government ministries, transportation customer service portals and others. NONAME057(16)'s claims are unverified, and the group has a history of false threats used for intimidation.

Nation State and Emerging National Security Threats

Activities attributed to state-sponsored actors typically involve strategic data collection against governments and private enterprise. State-Sponsored threat actors who may be engaging in espionage are often particularly interested in technology with potential economic or military applications, such as quantum computing, 6G networks, and aviation equipment.

The Communications Security Establishment (CSE) highlighted advanced persistent threats from China, Russia and Iran, but also named India as an emerging threat for the first time, citing its potential interest in espionage against Canadian government systems amid recent diplomatic tensions.

Nation State-Sponsored Threat Actors Target Canadian Provincial Government

A suspected state-sponsored cyberattack targeted 22 email inboxes within the British Columbia Government (BC), potentially compromising the sensitive information of 19 individuals. The Public Safety Minister confirmed on June 3, 2024, that only employee files were affected, and those individuals were notified. The BC government first detected the breach on April 10, 2024, and in response, officials told public service workers to change their passwords. The threat actor or nation-state behind this incident is unknown; however, a subsequent report warned Canadians about persistent outside interference in Canadian political affairs.

Midnight Blizzard Attack on Microsoft

In January, Microsoft verified they had suffered a breach following a password spray attack by state-sponsored hacking group linked to Russia's Foreign Intelligence Service (SVR) named BLUEBRAVO. The attack resulted in threat actors gaining access to a legacy non-production test tenant account that did not have multi-factor authentication enabled, granting the threat actors access to comprised systems.

Sources: X, Jun 13, 2024; Daily Dark Web, May 24, 2024; The Record Media, Jun 4, 2024; BleepingComputer.com, Mar 8, 2024; Microsoft Threat Intelligence, Jan 25, 2024

SALT TYPHOON Infiltrates Multiple US Broadband Providers

In 2024, the SALT TYPHOON nation-state threat group infiltrated approximately ten large enterprises within the U.S. telecommunications sector. There are reports that the adversaries gathered sensitive information regarding American citizens, including details about their communication patterns—specifically, who they communicate with, the timing of these interactions, and their geographical locations.

Notably, SALT TYPHOON reportedly eavesdropped on unencrypted communications from the mobile devices of numerous senior U.S. political figures. Initial assessments suggest that the attackers possess the capability to access data pertaining to all American citizens, indicating a broader interest from the nation-state group in monitoring American activities beyond high-profile individuals. In response to these developments, the U.S. government's Consumer Financial Protection Bureau (CFPB) issued guidance to its employees advising them to refrain from using personal cell phones for work-related communications. Instead, employees are directed to utilize secure platforms for meetings and discussions involving non-public data. This incident highlights the importance of utilizing encrypted communication channels to protect sensitive information from potential adversaries.

Canada's expanding digital footprint, coupled with aging cybersecurity measures, is creating exploitable opportunities for threat actors. The evolving threat landscape demands stronger collaboration between federal and provincial agencies, as well as private-sector partners. Intelligence-sharing platforms modeled on the U.K.'s i100 initiative, comprehensive incident response protocols, and significant investments in cybersecurity infrastructure can help mitigate the risks posed by advanced cyber threats.

Emerging National Security Threats

Insider Threats

North Korean Adversaries Act as IT Workers to Access International Jobs

On July 23, 2024, a US cybersecurity company reported that they had inadvertently hired a North Korean-affiliated IT worker for a remote engineering position. This event comes nearly three months after US law enforcement indicted multiple individuals in a wide-ranging hiring fraud scheme, claiming that North Korean-affiliated IT workers had defrauded 300 companies, earning "millions" for the regime.

The victim organization reported that they did not detect any anomalies in the new hire's background checks and other employment processing procedures, which included multiple video interviews. The individual sent in an AI-enhanced photo alongside information obtained from a stolen US-based identity as part of their application.

The victim organization first detected the fraudulent activity when the new hire attempted to download malware and other unauthorized programs onto their company-issued laptop. Since at least 2020, North Korean-sponsored cyber espionage groups have been observed attempting to place individuals in positions at Western-based companies in the information technology (IT), cryptocurrency, and software development industries.

Adversaries Leveraging Technology for Attacks

TP-Link Routers: A Potential National Security Threat

TP-Link, a global provider of WiFi networking and smart home devices, has been under scrutiny due to the unusually high degree of vulnerabilities in the routers. Attackers have exploited these vulnerabilities for various malicious activities, including the creation of powerful botnets. Notably, state-sponsored groups such as VOLT TYPHOON and CAMARO DRAGON have been implicated in these activities, with the former known for its hacking campaign against U.S. critical infrastructure and the latter for attacks on European foreign affairs entities using a firmware implant for TP-Link routers.

Regulatory concerns around China's requirement for security researchers to report vulnerabilities to the government before public disclosure, potentially enabling state-sponsored attackers to exploit these vulnerabilities, are a concern. This information is particularly relevant as many APT groups are known to target routers for initial access.

Sources: CNET, Oct 8, 2024; Dark Reading, Sept 25, 2024; Malicious Life by Cybereason, n.d.; Arstechnica, Jul 24, 2024; The Global Authority on PC Games, Aug 20, 2024; Cybernews, Aug 15, 2024

Chinese Lidar Technology May Pose National Security Threat

A 2024 report from the Foundation for Defense of Democracies raised questions regarding the implications of China's advanced remote sensing technology, particularly light detection and ranging (lidar), on critical infrastructure and national security. Lidar technology, which employs laser pulses to generate detailed three-dimensional maps, is increasingly being integrated into essential systems, including those related to public safety, transportation, and utilities.

The report indicates that Chinese companies are gaining a dominant position in the global lidar market, which may pose a substantial risk to U.S. and Western interests. The integration of Chinese-made lidar sensors into critical infrastructure raises alarms about potential espionage and sabotage, as these technologies could provide the Chinese government with access to sensitive data or the ability to disrupt vital operations. This situation draws parallels to previous concerns surrounding Huawei's communications technology, which faced similar allegations.

Considering these findings, U.S. lawmakers are responding with proposed legislation aimed at restricting the Chinese-made lidar technology and encouraging countries to consider developing and manufacturing lidar technology.

Sources: Foundation for Defense of Democracies, Dec 2, 2024; Reuters, Dec 2, 2024

Significant Vulnerabilities of 2024

Though much of this report deals with the strategic threats posed by state actors, ransomware, AI, hacktivists and others, the venerable vulnerability continues to present itself as a strong initial access vector, leading to significant attacks and disruptions.

With this in mind, the team has summarized notable vulnerabilities from 2024 which should be considered, both in a tactical sense for remediation, as well as a reminder that the fundamentals if vulnerability management are a cornerstone to an effective security program.

CVE-2024-45387: An SQL injection vulnerability in Traffic Ops in Apache Traffic Control 8.0.0 through 8.0.1, allows a privileged user with role "admin", "federation", "operations", "portal", or "steering" to execute arbitrary SQL against the database by sending a specially-crafted PUT request. A remote attacker could exploit this vulnerability and perform SQL Injection and Bypass Authentication on the targeted system

CVE-2024-52046: The ObjectSerializationDecoder in Apache MINA uses Java's native deserialization protocol to process incoming serialized data but lacks the necessary security checks and defenses. This critical vulnerability allows attackers to exploit the deserialization process by sending specially crafted malicious serialized data, potentially leading to remote code execution (RCE) attacks. This flaw affects multiple versions of the popular networking library, raising significant security concerns.

CVE ID	Severity	CVSS Score
CVE-2024-52046	Critical	10

Affected Products and Versions

- Apache MINA 2.0.0 through 2.0.26
- Apache MINA 2.1.0 through 2.1.9
- Apache MINA 2.2.0 through 2.2.3

CVE-2024-26633: Multiple NetApp products incorporate Linux kernel. Certain versions of the Linux Kernel are susceptible to a vulnerability which when successfully exploited could lead to disclosure sensitive information or Denial of Service (DoS). The impacted products are: FAS/AFF Baseboard Management Controller (BMC) - A900/9500 and FAS/AFF Baseboard Management Controller (BMC) - FAS2820.

CVE ID	Severity	CVSS Score
CVE-2024-26633	Critical	9.1

CVE-2024-3393: Palo Alto Networks revealed a high severity vulnerability, CVE-2024-3393, in its PAN-OS software for next-generation firewalls. This flaw lets unauthenticated attackers misuse the DNS Security feature by sending special DNS packets, leading to a Denial of Service (DoS) and causing firewalls to reboot and enter maintenance mode. The problem arises from poor handling of exceptional conditions in the DNS Security feature, allowing attackers to send harmful packets through the firewall's data plane, resulting in crashes and reboots.

CVE ID	Severity	CVSS Score
CVE-2024-3393	High	8.7

Affected Products and Versions

- PAN-OS 11.2: Affected versions are below 11.2.3.
- PAN-OS 11.1: Affected versions are below 11.1.5.
- PAN-OS 10.2: Versions below 10.2.8 are affected with additional fixes in maintenance releases.
- PAN-OS 10.1: Versions below 10.1.14 are affected.

CVE-2024-56145: A critical zero-day vulnerability has been discovered in Craft CMS, a widely used PHP-based content management system. This vulnerability allows unauthenticated attackers to execute arbitrary code remotely, posing a significant security risk to over 150,000 websites globally. The vulnerability arises from the register_argc_argv setting in PHP, which is enabled by default. This setting can be exploited to manipulate file paths and execute malicious code during Craft CMS's bootstrap process. The Craft CMS team has swiftly addressed this issue by releasing patched versions 5.5.2+ and 4.13.2+.

CVE ID	Severity	CVSS Score
CVE-2024-52046	NA	NA

Affected Products and Versions

- Craft CMS 3.9.14 and earlier
- Craft CMS 4.13.2 and earlier
- Craft CMS 5.5.2 and earlier

CVE-2024-38094 (SharePoint RCE Vulnerability Actively Exploited): Researchers discovered an unauthorized attacker who infiltrated a server, moving through the network and compromising the entire domain, remaining unnoticed for two weeks. The attackers gained initial access by exploiting CVE-2024-38094, a remote code execution (RCE) vulnerability in an on-premise SharePoint server. They used a series of GET and POST requests to deploy a webshell named "ghostfile93.aspx" on the target system. After using an initial breach stemming from a vulnerability in Microsoft SharePoint, threat actors then infiltrated further by compromising a Microsoft Exchange service account with administrative privileges. They utilized various tools and techniques to expand their foothold:

- **Impacket:** Attempted to install and execute this collection of Python scripts for network protocol interaction.
- **Horoung Antivirus:** Installed this Chinese AV software to disable existing security solutions.
- **Fast Reverse Proxy (FRP):** Deployed to maintain external access through firewalls.

The attackers demonstrated sophisticated knowledge of network penetration and evasion techniques:

- **Active Directory Exploitation:** Used tools like ADExplorer64.exe, NTDSUtil.exe, and nxc.exe to map the AD environment and gather credentials.
- **Credential Harvesting:** Employed Mimikatz (disguised as 66.exe) to extract login information.
- **Log Tampering:** Disabled system logging and cleared event logs to cover their tracks.
- **Persistence:** Established scheduled tasks on the domain controller for the FRP tool.

The threat actors tried to hide their actions by changing system logs and turning off logging on the compromised server. They also used Huorong AntiVirus to disable security products and operate more freely.

CVE ID	Severity	CVSS Score
CVE-2024-38094	High	7.2

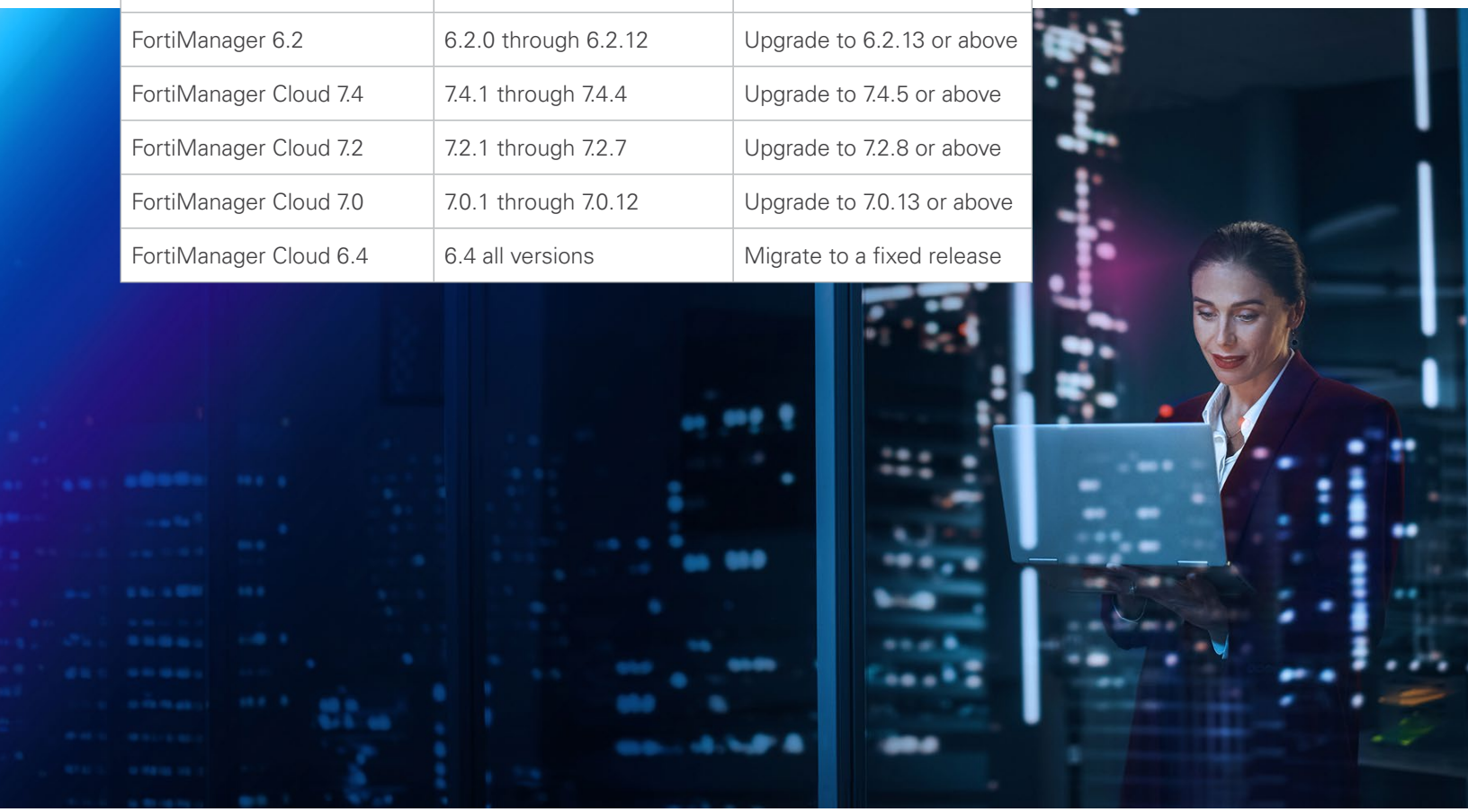
CVE-2024-47575: A missing authentication for critical function vulnerability in FortiManager fgfmd daemon may allow a remote unauthenticated attacker to execute arbitrary code or commands via specially crafted requests. It was observed that a new threat actor, UNC5820, was actively exploiting this FortiManager vulnerability as early as June 27, 2024. UNC5820 staged and exfiltrated the configuration data of the FortiGate devices managed by the exploited FortiManager. This data contains detailed configuration information of the managed appliances as well as the users and their FortiOS256-hashed passwords. This data could be used by UNC5820 or other cybercriminals to further compromise the FortiManager, move laterally to the managed Fortinet devices, and ultimately compromise enterprise environments.

In addition to updating to the latest versions, Fortinet has offered several workarounds for those unable to immediately upgrade. For example, users can enable the fgfm-deny-unknown setting to prevent unknown devices from attempting to register with FortiManager.

CVE ID	Severity	CVSS Score
CVE-2024-47575	Critical	9.8

Affected Products and Versions

Affected Product	Affected Version	Solution
FortiManager 7.6	7.6.0	Upgrade to 7.6.1 or above
FortiManager 7.4	7.4.0 through 7.4.4	Upgrade to 7.4.5 or above
FortiManager 7.2	7.2.0 through 7.2.7	Upgrade to 7.2.8 or above
FortiManager 7.0	7.0.0 through 7.0.12	Upgrade to 7.0.13 or above
FortiManager 6.4	6.4.0 through 6.4.14	Upgrade to 6.4.15 or above
FortiManager 6.2	6.2.0 through 6.2.12	Upgrade to 6.2.13 or above
FortiManager Cloud 7.4	7.4.1 through 7.4.4	Upgrade to 7.4.5 or above
FortiManager Cloud 7.2	7.2.1 through 7.2.7	Upgrade to 7.2.8 or above
FortiManager Cloud 7.0	7.0.1 through 7.0.12	Upgrade to 7.0.13 or above
FortiManager Cloud 6.4	6.4 all versions	Migrate to a fixed release



CVE-2024-28987: The vulnerability impacts SolarWinds Web Help Desk (WHD) software. This flaw involves hardcoded credentials within the Web Help Desk application. Attackers can remotely access the system without authentication, allowing them to modify help desk tickets and access sensitive data. This vulnerability is extremely severe, as it can expose sensitive data, such as passwords from reset requests and shared service account credentials. SolarWinds users are urged to update to version 12.8.3 Hotfix 2 to patch this vulnerability. The fix requires prior installation of Web Help Desk 12.8.3.1813 or 12.8.3 HF1.

Analysis:

CVE ID	Severity	CVSS Score
CVE-2024-28987	Critical	9.1

CVE ID	Affected Products
CVE-2024-9680	Firefox versions prior to 131.0.3
	Firefox ESR versions prior 115.16.1
	Firefox ESR versions prior 128.3.1
	Thunderbird versions prior to 115.16
	Thunderbird versions prior to 128.3.1
	Thunderbird versions prior to 131.0.1

Zero-Day Vulnerabilities in Palo Alto PAN-OS – CVE-2024-0012 and CVE-2024-9474

Palo Alto Networks has released security patches to address two actively exploited zero-day vulnerabilities in their Next-Generation Firewalls (NGFW). CVE-2024-0012 is a critical authentication bypass vulnerability in the PAN-OS management web interface. This flaw allows an unauthenticated attacker with network access to the management web interface to gain PAN-OS administrator privileges to perform administrative actions, tamper with the configuration, or exploit other authenticated privilege escalation vulnerabilities, like CVE-2024-9474. The second vulnerability, CVE-2024-9474, is a privilege escalation vulnerability that allows PAN-OS administrator to perform actions on the firewall with root privileges.

On November 14th, Palo Alto Networks confirmed an active threat campaign actively exploiting CVE-2024-0012. Although not explicitly linked to this campaign, CVE-2024-9474 may be exploited in conjunction with CVE-2024-0012. Reports indicate approximately 11, 000 IP addresses running PAN-OS management interfaces exposed to the Internet, with the most vulnerable devices located in the United States, India, Mexico, Thailand, and Indonesia. This zero-day vulnerability was first seen on November 8th, 2024, when Palo Alto released an advisory titled PAN-SA-2024-0015, following reports of an unknown threat actor selling access to this zero-day vulnerability on exploit forums. As of the latest updates, there is no publicly available proof-of-concept (PoC) exploit for these vulnerabilities.

Severity and CVSS Score:

CVE ID	Severity	CVSS Score
CVE-2024-0012	Critical	9.3
CVE-2024-9474	Medium	6.9

Affected Products and Versions:

Product Versions	CVE-2024-0012	CVE-2024-9474	Fixed Version
PAN-OS 10.1	Not Affected	10.1.14-h4 and below	10.1.14-h6 and above
PAN-OS 10.2	10.2.12-h1 and below	10.2.12-h1 and below	10.2.12-h2 and above
PAN-OS 11.0	11.0.5-h2 and below	11.0.5-h2 and below	11.0.6-h1 and above
PAN-OS 11.1	11.1.4-h7 and below	11.1.4-h7 and below	11.1.5-h1 and above
PAN-OS 11.2	11.2.3-h3 and below	11.2.3-h3 and below	11.2.4-h1 and above
Cloud NGFW	Not Affected	Not Affected	N/A
Prisma Access	Not Affected	Not Affected	N/A

18-Year-Old Browser Vulnerability Impacts MacOS and Linux Devices

A recently revealed long-standing vulnerability has been found to affect major web browsers, posing significant cybersecurity risks. This flaw, dubbed the "0.0.0.0 Day" vulnerability, enables hackers to manipulate requests directed at a specific IP address, rerouting them to private servers. The exploitation of this vulnerability involves deceiving users into visiting malicious websites that can access sensitive data and potentially infiltrate internal networks. It is crucial to note that this flaw specifically impacts Linux and macOS systems, leaving Windows unaffected. Both individuals and organizations operating web servers are at risk, underscoring the widespread threat this issue presents.

Researchers have identified multiple instances where the "0.0.0.0 Day" vulnerability is actively being exploited. One notable case is the ShadowRay campaign, documented by the same researchers last March. This campaign targets AI workloads running locally on developers' machines, specifically Ray clusters. The attack is initiated when a victim clicks on a link sent via email or found on a malicious site, which triggers JavaScript to send an HTTP request to 'http://0[.]0[.]0[.]0:8265', a port typically used by Ray. These requests reach the local Ray cluster, creating opportunities for arbitrary code execution, reverse shells, and configuration changes.

Another case involves a campaign targeting Selenium Grid. In this scenario, attackers utilize JavaScript on a public domain to send requests to 'http://0[.]0[.]0[.]0:4444.' These requests are directed to the Selenium Grid servers, allowing attackers to execute code or conduct network reconnaissance. Additionally, the "ShellTorch" vulnerability was reported by researchers in October 2023, where the TorchServe web panel was bound to the 0.0.0.0 IP address by default instead of localhost, making it vulnerable to malicious requests.

Despite the researchers' disclosure regarding these malicious activities, web browser developers are only beginning now to take action:

- Google Chrome, the most widely used web browser, has announced plans to block access to 0.0.0.0 through a gradual rollout starting with version 128 (upcoming) and continuing until version 133.
- Mozilla Firefox does not currently implement PNA (Private Network Access), but it is a high development priority. A temporary fix is being implemented until PNA is fully integrated, although no specific rollout dates have been provided.
- Apple has introduced additional IP checks on Safari through updates to WebKit, blocking access to 0.0.0.0 in version 18 (upcoming), which will be released alongside macOS Sequoia.

PHP Vulnerability Exploited to Spread Malware and Launch DDoS Attacks – CVE-2024-4577

A recently disclosed PHP vulnerability affecting installations running in CGI mode is being actively exploited just one day after its announcement. This vulnerability primarily targets Windows installations configured with Chinese and Japanese language locales, although it has the potential to impact a broader range of systems. Exploits associated with this vulnerability include command injection and the deployment of malware campaigns such as Gh0st RAT, RedTail cryptominers, and XMRig.

The critical vulnerability has been identified in PHP versions 8.1.* (prior to 8.1.29), 8.2.* (prior to 8.2.20), and 8.3.* (prior to 8.3.8). It allows attackers to achieve remote code execution (RCE) due to the manner in which PHP and CGI handlers parse specific Unicode characters. Various threat actors are actively exploiting this vulnerability to target susceptible devices.

Gh0st RAT is an open-source remote access tool that has been delivered as a UPX-packed Windows executable. In a sandbox environment, it dropped an additional executable named "Iqgqosc.exe," which enumerated connected drives and peripherals while querying the registry. The malware established a connection to a Germany-based command and control server at IP address 146[.]19[.]100[.]7 over port 8001. Another IP address, 147[.]50[.]253[.]109, was associated with several certificates bearing the Common Name (CN) "BangCloud," linked to a small server hosting provider in Thailand. Most IP addresses associated with this CN belonged to the same CIDR block as 147[.]50[.]253[.]109 and were flagged for connections to malicious files according to VirusTotal, sharing overlapping hashes and filenames.

The RedTail crypto mining operation exploited CVE-2024-4577 within days of its disclosure. The attacker utilized a request that took advantage of the flaw to execute a wget request for a shell script. This shell script subsequently made a network request to a Russia-based IP address to obtain an x86 version of the RedTail crypto mining malware. The script attempts to download the miner file using wget, curl, or a raw TCP connection as a fallback, searching for directories owned by the victim that have read, write, and execute permissions. It excludes directories mounted with the "noexec" option, as well as "/tmp" and "/proc." The script retrieves the system's architecture, tests for write permissions, and downloads and executes its payload based on the victim's architecture, renaming the file to "redtail."

Additionally, the shell script retrieves an ELF file named "pty3" from a different IP address, identified as a Muhstik malware sample. This malware is known for targeting Internet of Things (IoT) devices and Linux servers for crypto mining and distributed denial-of-service (DDoS) attacks.

Critical GeoServer GeoTools RCE PoC – CVE-2024-36401

CVE-2024-36401: GeoServer is an open-source server that allows users to share and edit geospatial data. Prior to versions 2.23.6, 2.24.4, and 2.25.2, multiple OGC request parameters allow Remote Code Execution (RCE) by unauthenticated users through specially crafted input against a default GeoServer installation due to unsafely evaluating property names as XPath expressions. The GeoTools library API that GeoServer calls evaluates property/attribute names for feature types in a way that unsafely passes them to the commons-jxpath library which can execute arbitrary code when evaluating XPath expressions. This XPath evaluation is intended to be used only by complex feature types (i.e., Application Schema data stores) but is incorrectly being applied to simple feature types as well which makes this vulnerability apply to **ALL** GeoServer instances.

CVE ID	Severity	CVSS Score
CVE-2024-36401	Critical	9.8

While the vulnerability was not being actively exploited at the time, researchers quickly released proof of concept exploits that demonstrated how to perform remote code execution on exposed servers and open reverse shells, make outbound connections, or create a file in the /tmp folder. The project maintainers patched the flaw in GeoServer versions 2.23.6, 2.24.4, and 2.25.2 and recommended that all users upgrade to these releases. The developers also offer workarounds but warn that they may break some GeoServer functionality. According to OSINT search engine, approximately 16,462 GeoServer servers are exposed online, most located in the US, China, Romania, Germany, and France.

Affected Products and Versions

Package	Affected Versions	Patched Versions
org.geoserver.web:gs-web-app (Maven)	>= 2.24.0, < 2.24.4	2.24.4
	>= 2.25.0, < 2.25.2	2.25.2
	< 2.23.6	2.23.6
org.geoserver:gs-wfs (Maven)	>= 2.24.0, < 2.24.4	2.24.4
	>= 2.25.0, < 2.25.2	2.25.2
	< 2.23.6	2.23.6
org.geoserver:gs-wms (Maven)	>= 2.24.0, < 2.24.4	2.24.4
	>=2.25.0, <2.25.2	2.25.2
	< 2.23.6	2.23.6

Looking Forward to 2025

2025 is likely to be a year of great change. With shifts in leadership across the globe, we are also likely to see a shift in priorities, investment and strategic outlook which will have a significant impact on cyber. These shifts will have a particularly strong impact on Canada, which sits at the intersection of pending elections, becoming a greater target for geopolitical foes and cyber criminals alike, and facing down the potential impacts of tariffs impacting security budgets and the ability of Canadian firms to attract top talent.

Some of the major security challenges which may present themselves are as follows:

Time-to-Attack

Ongoing exploitation of LLM and other AI systems by threat actors has the capacity to dramatically reduce the time required to generate and deploy custom malware, targeting specific vulnerabilities. This reduction in time-to-attack will increase the stress on security teams who will need to decrease the time required to develop detection rules and threat hunt packages to counter these threats.

Hand in hand with the decrease time to attack, is the lowering of the barrier to entry for customized malware. By leveraging these tools to generate exploits or malware targeting specific vulnerabilities, a less sophisticated threat actor who may previously have relied on malware-as-a-service providers may now gain the ability to carry out more significant attacks. Though their success rate may not be any higher, the reduced barrier to entry could lead to a significant increase in frequency of incidents which defenders must respond to.

Over time, the increase attack tempo, coupled with more specific attacks targeting vulnerabilities much more quickly after discovery, poses a significant risk to cyber defenders.

Social Engineering

Attackers levering AI will not be limited to exploiting vulnerabilities and lowering the technical barrier to entry for attackers, but also through an increase in sophistication of phish, vish and other social engineering attacks. As content generating LLMs become more sophisticated, an uptick in fraud exploiting this technology should be expected.

Many rudimentary examples of this type of exploit can be found across social networks, as malicious ads show trusted news sources claiming that celebrity X, organization Y or government Z has released a new product/program/benefit is now available to your target group. As these attacks increase in sophistication, they may be retargeted to collect credentials or sensitive details of target individuals at critical organizations.

Espionage and Penetration

As 2024 demonstrated, state actors are making concerted efforts to gain access to critical systems across industries, this trend is likely to continue through 2025 with a particular focus on critical infrastructure and defence targets. Attacks may be executed for the purpose of intelligence collection, technology theft, pre-position

access for later attacks, or to compromise targeted individuals. As a result of incidents in 2024, sensitive organizations should consider hardening both their cyber posture in terms of security solutions and hardware, as well as their communication plans.

Organizations should also consider their supply chains, not just in direct support of operations, but down to the manufacturers of equipment that is often taken for granted. This consideration may be useful both in planning for supply chain interruption, as well as identifying potential points of compromise within critical hardware.

Criminal Cyber Activity

In conjunction with the risk posed by AI exploitation, we are likely to see continued growth in ransomware incidents through 2025. It is unlikely that this threat is to subside in the near future, and organizations should consider the issues identified by our Incident Response team when considering their defensive posture and incident response plans.

Information Operations

In 2024, much of the focus of information operations (deliberate efforts to control narratives online, sew misinformation and shape public perception towards a specific policy) was targeted towards the US presidential election. That focus may now shift to Canada. With looming federal and provincial elections, international tensions between Canada and its trade partners, as well as greater geopolitical friction, Canadians will likely be the target of significant information operations.
Though information operations are often used to achieve a desired policy outcome, they may also be leveraged to recruit insiders at target organizations. Given this potential vector, organizations should consider their insider risk programs as well as their likelihood for being targeted by such an effort.

Tariffs

Though not a direct cyber threat, tariffs may pose a financial constraint to organizations and place pressure on security budgets. As Canadian organizations face this pressure, they may become more enticing targets as security cuts leave organizations vulnerable.

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

Cyber Threat Intelligence

Karan Ghoshal

Arvind Prabaharan

Mike Rosenlund

Aindrea Skelly

Incident Response

Mansoor Haqanee

Kyle Johnston

Anne Labbé

Jordan Michallet

Xavier Normand

Robin Penrat

Ganesh Ramakrishnan

Chris Walker

Contact Us

Incident Response

Alexander Rau
Partner
alexanderrau@kpmg.ca

Guillaume Clement
Partner
guillaumeclement@kpmg.ca

Ganesh Ramakrishnan
Senior Manager
gramakrishnan@kpmg.ca

Chris Walker
Senior Manager
chriswalker2@kpmg.ca

Anne Labbé
Senior Manager
alabbe@kpmg.ca

Xavier Normand
Senior Manager
xnormand@kpmg.ca

Cyber Threat Intelligence and Exploited Vulnerabilities

Robert Moerman
Partner
rmoerman@kpmg.ca

Mike Rosenlund
Senior Manager
mrosenlund@kpmg.ca