CTAC 2024
YEARLY REPORT







CTAC 2024
YEARLY REPORT

NATIONAL CYBER
SECURITY CENTRE

Table of Contents

LIST OF ABBREVIATIONS 4

CTAC YEAR 2024 IN REVIEW 5

1. SUMMARY 6

2. CYBER THREAT LANDSCAPE TRENDS IN 2024 7

3. REGIONAL THREAT ANALYSIS 9

- 3.1. Common Cyber Threats 9
- 3.2. Distinct Cyber Threats by Country 11
- 3.3. Conclusion 13

4. THREAT ACTORS AND CYBER THREATS 14

- 4.1. Most Exploited Vulnerabilities in 2024 14
- 4.2. Most Active Threat Actors 15
- 4.3. Different Types of Attacks 17
- 4.4. Targets of Cyber Attacks 19

5. THE MOST NOTORIOUS EVENTS OF 2024 20

6. 2024 TRENDS & 2025 PREDICTIONS 23

7. RECOMMENDATIONS 26

8. ENDNOTE 28

List of Abbreviations

Term/abbreviation	Meaning/explanation
AI	Artificial Intelligence
APT	Advanced Persistent Threat
ATT&CK	Adversarial Tactics, Techniques and Common Knowledge
CDN	Content Delivery Network
CERT	Computer Emergency Response Team
CISA	Cybersecurity & Infrastructure Agency
CTAC	Cyber Threat Analysis Cell
CVE	Common Vulnerabilities and Exposures
DDoS	Distributed Denial of Service
Disinformation	The term "disinformation" refers to false information that is intended to manipulate, cause damage, or misguide people, organisations, and countries.
ESG	Email Security Gateway
FBI	Federal Bureau of Investigation
FSB	Federal Security Service
FVEY	Five Eyes
GRU	The Main Directorate of the General Staff of the Armed Forces of the Russian Federation
ICS	Industrial Control System
IOC	Indicators of Compromise
LOTL	Living Off the Land
Malinformation	The term "malinformation" refers to information that stems from the truth but is often exaggerated in a way that misleads and causes potential harm.
MFA	Multi-factor Authentication
Misinformation	The term "misinformation" refers to false information that is not intended to cause harm.
NCSC	National Cyber Security Centre of Lithuania
OT	Operational Technology
RCDC	Regional Cyber Defence Centre, part of the NCSC
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
SSU	Security Service of Ukraine
SVR	The Foreign Intelligence Service of the Russian Federation
TTP	Tactics, Techniques and Procedures

CTAC Year 2024 in Review

- In 2024, CTAC continued enhancing its reporting capabilities, refining the structure and content of the reports released. In total, there were 51 Weekly, and 245 Daily reports published to stakeholders and other interested parties. A continuous report writing was established and the publication did not halt during the various cyber exercises CTAC participated in.
- 2024 marked another successful year for CTAC in terms of cyber exercises. Both Locked Shields 2024 and Amber Mist 2024 were great success for deepening knowledge in cyber security field and strengthening international connections and collaboration. Apart from these two exercises, CTAC had its presence in the US Department of Defence-organised cyber defence exercise Cyber Shield 2024.
- Last year was fruitful in terms of studies. CTAC completed, published and presented in various conferences across multiple nations two studies – *How to Recognize China Cyber Threats and Cyber Threats to Critical Infrastructure in the Baltic Sea Region*
- The Counter Ransomware Initiative (CRI) saw quite the growth in participants and interest. In June 2024, CTAC, together with colleagues from Belgium, organised a two-day training on Malware Information Sharing Platform (MISP) use in everyday CTI and defence operations, as well as shared experience alongside colleagues from different nations and organisations.
- CTAC continued the support to the Ukrainian cadet internship organised by the NCSC. Four Ukrainian cadet rotations took the month-long internship and learned from CTAC staff's expertise in the field of CTI.
- 2024 were election year with Presidential, Parliament and European Parliament elections taking place in Lithuania. Naturally, this is a very intense period in the cyber domain as disruption of the election process is a very attractive objective for adversaries. CTAC, alongside colleagues from the NCSC, formed a Working Group to safeguard through that challenging time.

01/ Summary

In 2024, the cyber threat ecosystem became more inventive and interconnected, with state-sponsored actors, cybercriminals, and hacktivists using cutting-edge tools to take advantage of different vulnerabilities. These advancements highlight how crucial resilience, intelligence-sharing, and cutting-edge technology are in defending against the ever more complex threats of the digital age. Adaptive cybersecurity strategies are urgently needed, as highlighted by the 2024 cyber threat landscape. The need for proactive defence measures was brought to light as a result of the growing integration of nation-state operations, hacktivism, and artificial intelligence. To reduce these changing risks, organizations are urged to invest in AI-driven threat detection systems, improve supply chain security, and promote global cooperation.

02/ Cyber threat landscape trends in 2024

The convergence of state-sponsored campaigns, AI-driven cybercrime, and the growing power of hacktivist groups made 2024 a turning point in the cyber domain. These events underscore the increasing complexity of cyber threats, their connection to geopolitical disputes, and their implications for global security.

State-sponsored cyber operations

The 2024 cyber landscape was significantly shaped by nation-state actors, who used sophisticated techniques to further their strategic goals. For instance, Taiwan reported that cyberattacks, which were mostly attributed to China, had increased by 100% year-over-year. To steal confidential information and interfere with business operations, these attacks targeted government organizations, vital infrastructure, and high-tech sectors. These campaigns' sophistication demonstrated the application of cutting-edge strategies like "Living off the Land" and zero-day exploits. [1]

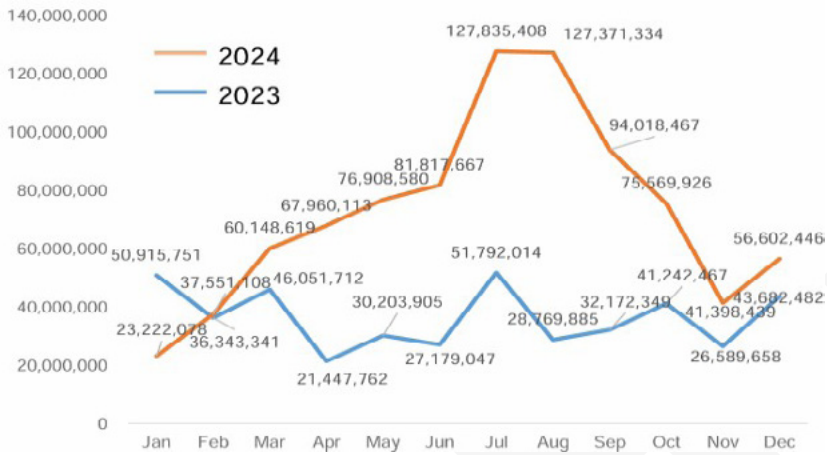


Figure 1. Comparison of cyber threat statistics between 2023 and 2024 (National Security Bereau of Taiwan)

[1] https://www.nsb.gov.tw/en/assets/documents/%E6%96%B0%E8%81%9E%E7%A8%BF/7d118bec-6a18-4e95-ad85-4055fc48cc31.pdf

AI-driven cyber crime

Artificial intelligence has been used by cybercriminals more and more to improve their operations, allowing for the widespread automation of ransomware, social engineering, and phishing campaigns. This trend was demonstrated by the rise of FunkSec, an AI-assisted ransomware-as-a-service organization. FunkSec used data theft and double extortion to target more than 85 organizations worldwide. Its operations were marked by the integration of innovative tools and strategic branding, underscoring the rising commercialization of advanced cybercrime. [2]

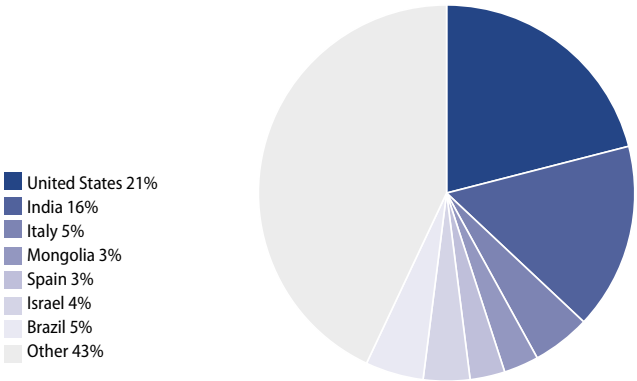


Figure 2. Distribution of FunkSec claimed victims by country according to DLS.(CheckPoint)

Hacktivism as a strategic tool

With politically motivated cyberattacks becoming more common and significant, hacktivist groups displayed previously unheard-of levels of activity in 2024. As an example, in reaction to ongoing military assistance for Ukraine, the pro-Russian hacker collective Killnet planned Distributed Denial of Service (DDoS) attacks against Western financial institutions and critical infrastructure. These attacks demonstrated a deliberate effort to erode public confidence and operational stability. Coordinated disinformation campaigns enhanced Killnet's activities, using social media to spread pro-Russian narratives and weaken the Western solidarity in favour of Ukraine.

[2] https://research.checkpoint.com/2025/funksec-alleged-top-ransomware-group-powered-by-ai

03/ Regional Threat Analysis

The cybersecurity landscapes of the United States, Poland, Lithuania, Sakartvelo, and Ukraine in 2024 demonstrated both shared challenges and distinct threats, underscoring the necessity of specialized defence tactics and the worldwide scope of cyberwarfare.

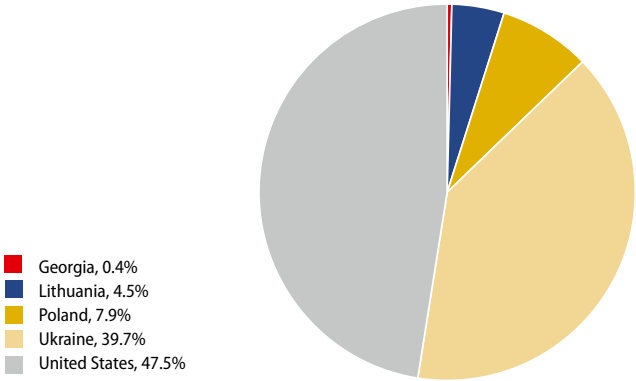


Figure 3. Percent of observed attacks against each RCDC-partner nation

Based on reporting done by CTAC, in 2024, the United States (47.5%) and Ukraine (39.7%) were the countries most targeted by cyberattacks, reflecting their roles as key geopolitical and strategic hubs, the US – because of its global influence, and Ukraine – because of the ongoing conflict-related cyber warfare. Poland (7.9%) and Lithuania (4.5%) were subjected to notable activity, likely related to their NATO roles and proximity to regional tensions. Georgia experienced minimal attacks (0.4%), possibly due to its less critical digital infrastructure. These trends highlight how geopolitical factors continue to shape the cyber threat landscape, with high-risk nations needing to prioritise robust cyber defences as we move towards 2025.

3.1/ Common cyber threats

State-sponsored cyberespionage, ransomware incidents, phishing campaigns, and distributed denial-of-service (DDoS) attacks were among the common cyberthreats observed in these countries. These threats are intended to cause havoc, steal confidential information, or disrupt critical infrastructure, systems of government buildings, educational institutions, and private companies. The employment of complex strategies, like malware distribution, social engineering, and software vulnerability exploitation, highlighted the adversaries' growing technological prowess and the dynamic character of cyberwarfare.

3.1.1 **Distributed Denial-of-Service Attacks:** These attacks were frequently detected as a threat in the US, Poland, Lithuania, Sakartvelo, and Ukraine. Adversaries used botnets and compromised devices to overload servers, networks, and target websites with traffic, disrupting access to authorized users. These attacks caused financial losses and reputational harm by interfering with essential services, such as financial institutions, government websites, and educational platforms.

3.1.2 **Phishing Campaigns:** phishing and spear-phishing attacks were directed towards individuals and organizations among RCDC partner nations. Cybercriminals trick people into disclosing sensitive information, like login credentials, bank account information, or personal information, by using false emails, messages, or websites. These attacks, which frequently posed as trustworthy sources or urgent communications, took advantage of people's weaknesses and trust relationships to gain unauthorized access to accounts or install malware.

3.1.3 **Ransomware Attacks:** ransomware has become a major cyber threat, impacting organizations in Poland, Lithuania, Ukraine, and the US. Ransomware was used by adversaries to encrypt important information or systems and then demand ransom payment for decryption keys. These attacks put victims through monetary strain, interrupted operations, and resulted in data loss. The indiscriminate nature of ransomware was brought to light by high-profile incidents that targeted critical infrastructure, governmental entities, healthcare organizations, and educational institutions.

3.1.4 **State-Sponsored Cyber Espionage:** In countries like Poland, Sakartvelo, and Ukraine, where cyber conflicts were fuelled by geopolitical tensions, state-sponsored cyber espionage operations were a common concern. Hacker groups with ties to Russia, including APT28, Sandworm, and Turla, carried out espionage operations aimed at critical infrastructure, government institutions, and military facilities. These adversaries aimed to undermine national security and deteriorate regional instability by stealing confidential data, obtaining intelligence, or interfering with operations to achieve their strategic goals.

3.1.5 **Hacktivist Activities:** As a form of political protest or activism, hacktivist groups targeted financial institutions, media outlets, and websites run by the government with DDoS attacks. Coordinated attacks were carried out by organizations such as Anonymous Russia, NoName057(16), and KillNet to express grievances, advance political agendas, or seek vengeance for perceived injustices. These attacks demonstrated the link between cybersecurity and socio-political dynamics by interfering with online services, obstructing communication, and escalating social tensions.

3.1.6 **Exploitation of Software Vulnerabilities:** Software Vulnerability Exploitation: Cyber adversaries from all over the world continue to use software and network infrastructure vulnerabilities as a common tactic. Threat actors used misconfigurations, zero-day exploits, and known vulnerabilities to obtain unauthorized access, increase privileges, or run malicious

code. Organizations were exposed to serious risks by vulnerabilities in web servers, industrial control systems, and widely used software applications. This underscores the significance of prompt patch management and vulnerability remediation efforts.

3.2/ Distinct Cyber Threats by Country



Lithuania: The cyber security situation in Lithuania remained stable in 2024, and the 63% increase in the number of incidents recorded by the NCSC is mainly attributable to the improving reporting habits of entities and citizens to the NCSC. Several external factors have a significant impact on Lithuania's cybersecurity posture. The geopolitical situation leads to an increased risk of cyber-attacks by state-sponsored groups linked to regional conflicts and tensions in the context of NATO and the EU. In 2024, the NCSC identified 6784 potentially vulnerable information systems and informed the affected organisations of the network and information system vulnerabilities found. Most of these identified vulnerabilities were related to authentication bypasses, remote code execution (RCE) and misconfigurations allowing access to sensitive information. As many as 59% of all cyber incidents recorded by the NCSC during the year involved social engineering techniques. Attacks such as fraudulent emails, artificial intelligence-generated voice calls (vishing) and QR code phishing have increased. In 2024, more than 46,000 people completed various NCSC training courses and more than 500 public sector and critical service organisations participated in the annual "Cyber Shield" exercise. Finally, the complexity of global supply chains increases the risk of cyber-attacks affecting Lithuanian companies through third parties, especially software or IT service providers.



Ukraine: The ongoing Russian-Ukrainian war has been accompanied by the active use of a cyber component. Compared to 2023, there were signs of an eventual escalation in the cyber impact of the Russian Federation against Ukraine and its partner countries in 2024. The primary objective of Russia's cyber actions in Ukraine remains unchanged: to facilitate the execution of the so-called "special military operation". The implementation of this is primarily done through utilisation of cyber units in subordination of special services, defence agencies and affiliated hacker groups (Sandworm, APT28, Bleeding Bear, Turla, Gamaredon, APT29, Ghostwriter, etc.), pro-Russian hacktivist groups (NoName057(16), Народная CyberАрмия, etc.) or individual IT specialists.

The priority targets for Russian threat actors remain information (information and communication) systems of the security and defence sector, state/local authorities, and critical infrastructure facilities.



Sakartvelo: Phishing and spear-phishing remain significant concerns for the Cyber Security Bureau (CSB) under the Ministry of Defence. Additionally, Sakartvelo experienced several DDoS attacks targeting the country, causing disruptions, while a major network provider

suffered a data breach that was resolved by the Ministry of Internal Affairs (MIA). The CSB actively monitors threats across the Ministry of Defence and implements countermeasures to strengthen national cybersecurity. By assessing incidents and deploying protective measures, the bureau works to mitigate risks and enhance resilience against cyber threats

Poland: In 2024, Poland experienced a dynamic year in cyber security, marked by major challenges, increased activity and significant achievements. As cyber threats became more sophisticated and frequent, entities within the National Cybersecurity System (NSS) prioritised strengthening resilience and enhancing the country's digital security. Their efforts were aimed at protecting the Republic of Poland from evolving cyber risks and strengthening national defence in the digital domain. In 2024, a total of 111,660 ICT security incidents were recorded at national level, an increase of 23% on the previous year. While some sectors saw a decrease, there was a significant increase in serious incidents (57%) and attacks against public sector organisations (58%) compared to the previous year.

National-level CSIRT	2023	2024	Percentage change
CSIRT NASK	80 267	103 449	+29%
CSIRT GOV	4 676	3 991	-15%
CSIRT MON	5 841	4 220	-28%
Total annual number of incidents	90 784	111 660	+23%

Table 1. Summary of umber of recorded incidents

	Types of incidents according to Article 2 para. 5-9 UKSC							
	Critical		Serious		Relevant		In public entities	
	2023	2024	2023	2024	2023	2024	2023	2024
CSIRT NASK	0	0	40	57	0	0	2 184	3 450
CSIRT GOV	0	0	0	6	0	0	0	3
CSIRT MON	0	0	0	0	0	0	0	0
Total:	0	0	40	63	0	0	2 184	3 453
Change:				+57%				+58%

Table 2. Summary of the number of incidents in the UKSC compliant classification

United States: In 2024, cybersecurity threats reached unprecedented levels, with major data breaches, ransomware attacks and AI-driven cybercrime reshaping the landscape. The cost of cyber incidents skyrocketed, prompting increased regulatory enforcement and new compliance measures. Ransomware emerged as a dominant threat, particularly in the healthcare sector, where attacks disrupted critical services and compromised the personal information of nearly 170 million Americans. In response, regulators introduced stricter security requirements, including encryption mandates and enhanced risk assess-

ments. AI has significantly accelerated cyberthreats, enabling criminals to automate phishing attacks, create deepfake fraud schemes and develop sophisticated malware. The rapid evolution of AI-driven cybercrime led to a surge in phishing-related ransomware incidents. The US government stepped up its cybersecurity enforcement, with the Department of Justice (DOJ) taking legal action against organisations that fail to meet federal cybersecurity standards. A landmark case against Georgia Tech underscored the government's commitment to holding contractors accountable for non-compliance. Tensions between the US and China escalated over cyber espionage campaigns targeting critical infrastructure and government communications. In response, the US introduced new data security measures to prevent foreign adversaries from accessing sensitive personal and government-related information. Finally, data breach litigation surged, with companies facing record settlements and regulatory fines. Lawsuits against companies for cybersecurity failures highlighted the growing legal and financial risks associated with inadequate data protection.

3.3/ Conclusion

2024 confirmed what was known for a long time - cyber threats are evolving at an alarming rate, and no sector or nation is safe. Ransomware attacks, AI-driven cybercrime and state-sponsored espionage defined the year, with critical infrastructure, healthcare and government systems relentlessly targeted. The scale of breaches and disruptions highlighted the growing sophistication of cyber adversaries, making it clear that traditional defences are no longer sufficient. Regulators have responded with stricter compliance measures, but the key takeaway is that cybersecurity must be proactive, not reactive. Going forward, organisations and governments must prioritise threat intelligence, rapid response capabilities and greater international collaboration to stay ahead of emerging threats.

04/ Threat Actors and Cyber Threats

4.1/ Most Exploited Vulnerabilities in 2024

In 2024, cyber threat actors heavily exploited vulnerabilities across various products and platforms, targeting critical infrastructure, enterprise systems, and cloud environments. Below are the key trends and associated vulnerabilities:

- **CVE-2024-21887:** Command injection vulnerability in Ivanti's Connect Secure and Policy Secure gateways was exploited by numerous groups, including Chinese-nexus actors (UTA0178, Flax Typhoon) and botnets like Raptor Train. Notably, GIFTEDVISITOR web shells and XMRig cryptocurrency miners were deployed to monetize unauthorized access. Critical sectors, like finance, healthcare, and government were heavily impacted due to their reliance on Ivanti's Connect Secure gateways for remote access. Exploitation of this vulnerability allowed threat actors to implant web shells and cryptocurrency miners, severely degrading system performance and compromising data security.
- **CVE-2024-1708 and CVE-2024-1709:** Path traversal and authentication bypass flaws in ConnectWise's ScreenConnect were widely used by ransomware groups, such as LockBit, Black Basta, and Bl00dy. North Korean-linked Kimsuky group and malware like ToddlerShark also leveraged these vulnerabilities for data exfiltration and lateral movement. Managed service providers (MSPs) were the primary target, as ConnectWise ScreenConnect is widely used for remote support and administration. Ransomware groups, like LockBit, exploited these flaws to gain initial access to MSP environments, allowing them to spread ransomware to client networks.
- **CVE-2024-3400:** A command injection vulnerability in Palo Alto Networks' PAN-OS was exploited by Iran-nexus Pioneer Kitten, alongside ransomware groups, like NoEscape and ALPHV. Threat actors deployed custom tools, including UPSTYLE Python backdoors, for persistence and data theft. Palo Alto Networks' PAN-OS is used in firewalls and other critical security devices. Exploitation of this flaw allowed attackers to deploy ransomware, disrupt corporate networks, and extract sensitive data. Industries like energy, telecommunications, and healthcare, heavily reliant on robust network security, were especially vulnerable.
- **CVE-2024-37085:** VMware ESXi faced exploitation due to an authentication bypass flaw. Actors such as Black Basta and Akira ransomware used this vulnerability to target virtualization environments, while Storm-0506 and Octo Tempest carried out espionage and disruption operations. Virtualization platforms are the backbone of modern data centres and cloud environments. This authentication bypass vulnerability was exploited by ransomware groups, like Akira and Black Basta, to target virtual machines, resulting in significant data loss and operational disruptions in industries, such as manufacturing, finance, and technology.

- **CVE-2024-34102:** Adobe products were impacted by XXE vulnerabilities, exploited by groups like Bobry, Surki, and Ondatry. These attacks focused on information disclosure, leveraging improperly restricted XML data for espionage campaigns. Adobe's multiple products, widely used in media, marketing, and content creation industries, were affected by this XXE vulnerability. Attackers leveraged it to extract sensitive information, disrupt workflows, and conduct espionage campaigns.

4.2 / Most Active Threat Actors



NoName057(16) – a pro-Russian hacker group well-known for its cyberattacks against the US, EU, and the Ukrainian Government's, media, and private company websites. It is thought of as a loosely affiliated, unrestrained pro-Russian activist group trying to gain notoriety in the West.
Origin: Russia.
Target countries: USA, Ukraine, and the European Union.
Target sectors: Government, Media, Finance, Telecommunications, Transport.
Tactics & Techniques: Distributed Denial of Service (DDoS)



People Cyber Army (Народная CyberАрмия) - The group is associated with a pro-Russian hacking group that emerged in 2022, following the start of the war in Ukraine. They claim responsibility for carrying out distributed denial-of-service (DDoS) attacks and website defacements against various targets, primarily in countries seen as supporting Ukraine. These targets have included government websites, critical infrastructure, and private companies.
Origin: Russia.
Target countries: Ukraine, USA, Lithuania, Latvia, Gibraltar, Turkey, Macedonia, Poland
Target sectors: Government, Media, Finance, Telecommunications.
Tactics & Techniques: Distributed Denial of Service (DDoS), website defacement, data breach.



Z-Pentest - is a relatively new Russian hacktivist group that has rapidly gained notoriety for targeting critical infrastructure, particularly in the energy and water sectors. Emerging around October 2024, the group has claimed responsibility for at least 10 breaches of operational technology (OT) control panels within a short span.
Origin: Russia.
Target countries: United States, Lithuania, Ukraine, Poland, Czech Republic, Austria, Netherlands, Romania, Croatia, Belgium, South Korea, Taiwan.
Target sectors: Water, Energy.
Tactics & Techniques: Exploiting Vulnerabilities, Remote Code Execution, ICS Protocol Exploitation, Malware Deployment, System Sabotage, Defacement.



OverFlame is a hacktivist group known for DDoS attacks and website defacements against government and corporate targets in Europe and North America. Aligned with pro-Russian groups, like NoName057 and the People's Cyber Army, their actions reflect anti-government and anti-corporate motives.
Origin: Russia.
Target countries: United States, Austria, Czech Republic, Estonia, France, Lithuania, Luxembourg, Poland, Portugal, Spain, Taiwan, Ukraine.
Target sectors: Aerospace and Transportation, Financial Services, Defence and Security, Public Services, Technology and Communications, Education, Nonprofit Organizations, Energy, Government.
Tactics & Techniques: Distributed Denial-of-Service (DDoS), Defacement.

4.3 / Different Types of Attacks

Understanding the motivations, methods, and outcomes associated with specific attack types is critical to mitigating threats effectively. In 2024, adversaries continued to leverage some of the most prolific and versatile attack methods, with phishing, ransomware, spyware, viruses, and malware remaining dominant due to their high success rates and adaptability. Next the reader can find an in-depth analysis of these attack types, explanation of their prevalence and what threat actors achieve through their use.

Phishing continues to be one of the most popular cyber-attack vectors due to its low cost, easy execution, and high success rate. Threat actors exploit human psychology, tapping into trust and sense of urgency to deceive victims. These attacks can target a broad audience or specific individuals, depending on the adversary's goals. Phishing often serves as a gateway for subsequent attacks, enabling adversaries to obtain login credentials, plant malware, or escalate privileges within a network. Many phishing campaigns specifically aim to steal usernames, passwords, and multi-factor authentication tokens, which can be sold on underground markets or used in follow-on attacks. By inducing employees to download malware, adversaries can cause significant disruptions to business processes.

Why it's effective:

- Phishing emails increasingly resemble legitimate communications, making detection difficult.
- AI tools allow attackers to craft highly tailored emails, mimicking specific writing styles or leveraging personal details from social media.
- Employees, even those trained in cybersecurity, remain susceptible to phishing due to stress, fatigue, or insufficient awareness.

Ransomware remained a cornerstone of the cybercriminal economy in 2024, with groups adopting Ransomware-as-a-Service (RaaS) models. The allure of significant financial gain and the relative anonymity offered by cryptocurrency make ransomware a preferred method. Threat actors demand ransom ranging from thousands to millions of dollars, payable in cryptocurrency to obscure their identities. In addition to encrypting files, attackers often exfiltrate data, threatening to leak it unless paid. Triple extortion includes targeting third parties (e.g., clients or partners) for additional payments. Businesses heavily reliant on digital systems may be forced to pay ransoms to restore operations quickly, especially when backups are unavailable or compromised.

Why it is effective:

- Financial rewards outweigh the operational risks for many attackers.
- Businesses' reliance on cloud infrastructure provides additional attack surfaces to ransomware groups.
- Despite increased awareness, many organizations remain underprepared for ransomware attacks, lacking proper backups or incident response plans.

Spyware is favoured by both cybercriminals and nation-state actors for its stealth and data-gathering capabilities. Unlike more destructive malware types, spyware operates silently, making it difficult to detect. Spyware often serves as a tool for maintaining long-term access to compromised systems, allowing adversaries to observe and act over time. Spyware enables attackers to monitor user activity, keystrokes, and communications, providing insights into sensitive information, like passwords and business plans. Confidential information, including trade secrets, financial records, and personal data, can be harvested and sold on dark web marketplaces or used for blackmail.

Why it is effective:

- Modern spyware can evade detection by antivirus programs and remain dormant until activated.
- Spyware can be delivered through phishing emails, infected websites, or even legitimate applications, expanding its reach.
- Increased reliance on personal devices and unsecured networks during remote work has made spyware more effective in infiltrating systems.

Viruses are one of the oldest forms of malware, yet they continue to pose significant threats due to their ability to self-replicate and spread across networks. Attackers use viruses to cause widespread damage, disrupt operations, and create opportunities for further exploitation. Viruses can cause system slowdowns, corrupt files, and crash critical infrastructure. Moreover, viruses often act as a delivery mechanism for other types of malware, including ransomware or spyware. A well-timed virus outbreak can erode trust in an organization's IT systems and brand reputation.

Why it's effective:

- Viruses can spread quickly through email attachments, shared files, and unpatched systems.
- As businesses and devices become more interconnected, viruses can move through systems more effectively than ever.
- Some modern viruses remain inactive for long periods, activating only when specific conditions are met, making them harder to detect.

Malware, as a broad category, includes various attack types that adversaries use to infiltrate and compromise systems. The adaptability of malware and its potential for customization make it a go-to tool for attackers with diverse objectives. Many malware types, like Trojans, provide attackers with remote control over infected systems, enabling data theft or further exploitation. Malware often focuses on stealing sensitive data, including financial records, personal information, and intellectual property. Some malware, like wipers, is designed to delete or corrupt data, leaving businesses unable to recover.

Why it is effective:

- Attackers use malware customized for specific industries or organizations, improving success rates.
- Malware has evolved to bypass traditional defences, using polymorphism and encryption to avoid detection.
- Proliferation of IoT devices, cloud services, and remote work tools provides more opportunities for malware infiltration.

The popularity of phishing, ransomware, spyware, viruses, and malware in general in 2024 stems from their proven effectiveness, adaptability, and ability to achieve diverse adversarial goals. Whether financially motivated cybercriminals or state-sponsored actors, these attack types offer scalable methods for stealing data, disrupting operations, or holding organizations hostage.

4.4 / Targets of Cyber Attacks

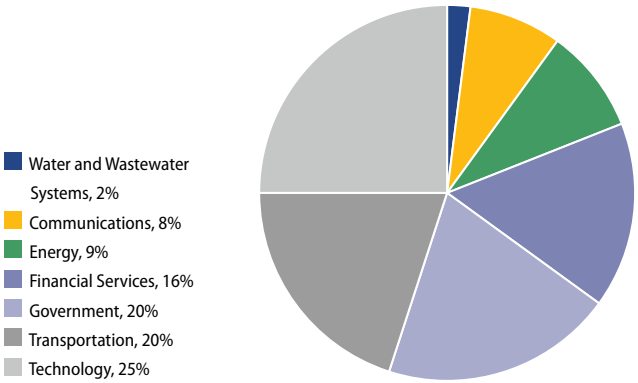


Figure 4. Most targeted sectors of 2024

In 2024, the technology sector emerges as the most targeted one, accounting for 25% of cyber-attacks based on CTAC reporting, a significant shift from previous years. This trend reflects the increasing reliance on digital infrastructure and the expanding attack surface created by rapid technological advances, including cloud computing, AI integration and interconnected platforms. The government and transport sectors, each accounting for 20% of the attacks, remain high-value targets due to their critical role in national security and public services. The financial sector, with 16% of incidents, continues to attract threat actors driven by financial gain, while the communications sector 8% faces persistent threats due to its role in data transmission and connectivity. Interestingly, water and wastewater systems accounted for only 2% of attacks, suggesting either improved security measures or a lower immediate value to cybercriminals. Looking ahead to 2025, this data suggests an increasing focus on technology-driven targets, highlighting the need for robust security practices in emerging technology environments. The high attack rates on the government and transportation sectors highlight ongoing geopolitical tensions, while the continued targeting of financial and communications infrastructure reflects the consistent appeal of data and financial assets to threat actors. Overall, these patterns underscore the need for adaptive cybersecurity strategies, proactive threat intelligence and cross-sector collaboration to mitigate evolving risks.

05/ The Most Notorious Events of 2024

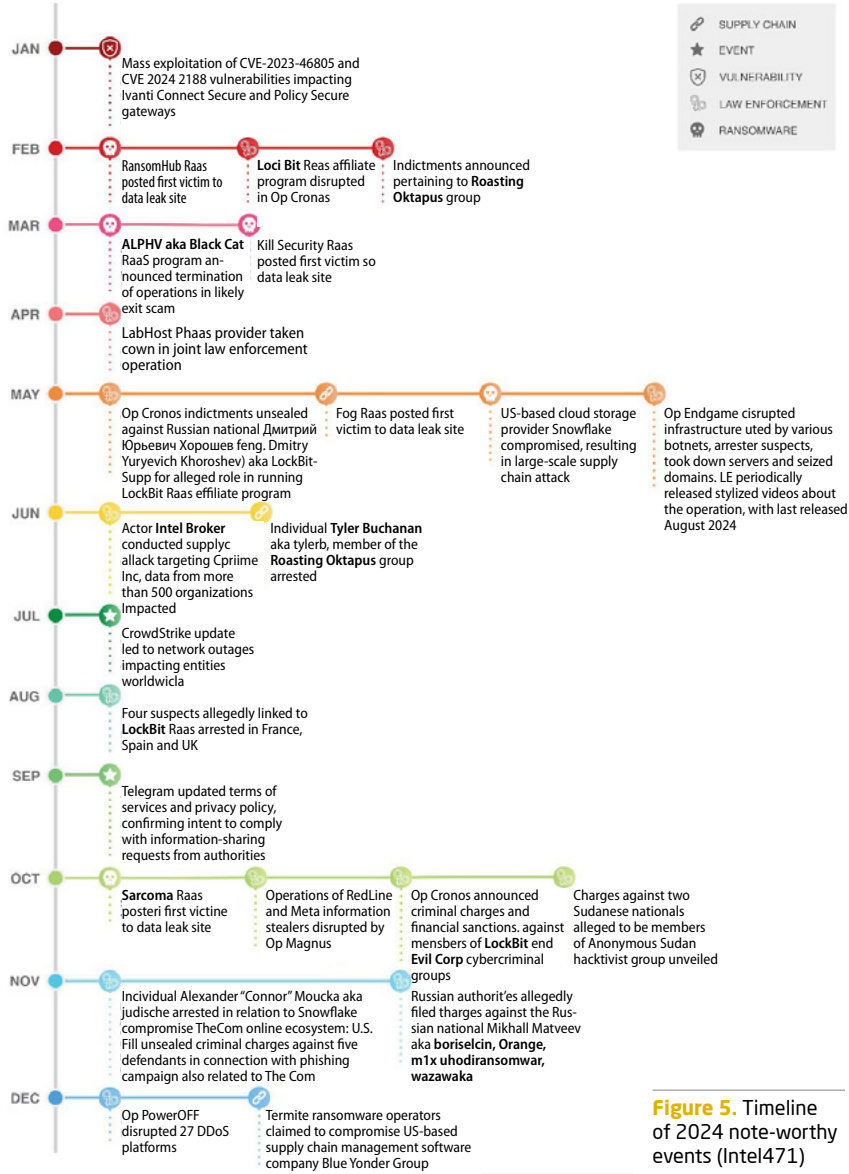


Figure 5. Timeline of 2024 note-worthy events (Intel471)

Significant cyber threats, such as ransomware dominance, large-scale supply chain attacks, and critical vulnerability exploitation, are highlighted in the 2024 timeline. Supply chain breaches, such as the Snowflake and Cprime breaches, highlighted systemic risks to interconnected systems, while ransomware-as-a-service (RaaS) operations persisted in targeting high-value organizations. Although law enforcement made significant progress on disrupting LabHost and apprehending important cybercriminals, adversaries continued to be persistent, changing their strategies and focusing on new vulnerabilities.

The increasing sophistication of attackers was demonstrated by the rise in hands-on keyboard techniques, social engineering, and exploitation of enterprise IT tools. The year highlighted the necessity for organizations to prioritize patch management, bolster supply chain security, and implement proactive threat detection and response to handle a constantly changing cyber threat landscape.

Salt Typhoon Telecom Breach

The Salt Typhoon cyberattack on U.S. telecommunications networks in early 2024 revealed an unprecedented level of sophistication in state-sponsored espionage. This incident leveraged a multi-vector attack strategy to exploit vulnerabilities in critical telecom systems. Salt Typhoon, a Chinese state-sponsored threat group, compromised leading telecom providers, including AT&T, Verizon, and T-Mobile, resulting in interception of sensitive communications and geolocation data for millions of Americans. One of the key tools employed by Salt Typhoon was SparrowDoor, a backdoor capable of bypassing authentication and establishing encrypted command-and-control channels. This malware exploited known vulnerabilities and zero-day flaws within telecom network equipment to escalate privileges and gain persistent administrative access. Salt Typhoon also utilized the Demodex rootkit, which enabled attackers to conceal their presence and evade forensic analysis. Combined with vulnerabilities in SS7 signaling protocols, these tools allowed the attackers to intercept calls, exfiltrate data, and monitor high-value targets, including President-elect Donald Trump and Vice President-elect JD Vance. Over several weeks, the attack rapidly escalated, with Salt Typhoon gaining access to critical infrastructure across the United States. The breach extended beyond large telecom providers to include smaller, regional systems, highlighting the vulnerability of less fortified networks. This campaign was part of a larger espionage strategy targeting sensitive communications globally, with particular focus on individuals of strategic interest to Chinese state intelligence.

The impact of the Salt Typhoon breach was felt worldwide, with significant geopolitical and national security ramifications. Federal agencies identified widespread compromises, ranging from data exfiltration to the potential manipulation of communications systems. This incident has since been labeled "the worst telecom hack in U.S. history." The attack underscored the critical vulnerabilities in supply chains and legacy telecom systems.

It highlighted the importance of zero-trust principles and robust SS7 protocol hardening.

The breach called for immediate upgrades to firmware and widespread deployment of AI-driven detection systems to preempt such sophisticated attacks.

Salt Typhoon's operation demonstrates the evolving capabilities of state-sponsored actors and the critical need for ongoing vigilance and innovation in cybersecurity defenses.

CrowdStrike Outage

In 2024, one of the most widespread and disruptive cybersecurity incidents was caused by faulty updates from CrowdStrike, a prominent endpoint security provider. A problematic update to CrowdStrike Falcon's Windows sensor on September 12, 2024, inadvertently caused 8.5 million Windows devices worldwide to experience severe operational issues. Affected systems ranged from blue screens of death (BSOD) to complete boot failures, effectively rendering critical infrastructure, enterprises, and government systems inoperable.

The incident stemmed from an error in the update's compatibility checks, which introduced a conflict between the CrowdStrike Falcon agent and a core Windows kernel module. This misconfiguration caused systems to crash during startup. Compounding the issue, automated deployment pipelines pushed the update to devices at scale, resulting in a cascade of failures. CrowdStrike initially attempted a rollback; however, the rapid propagation of the faulty update overwhelmed recovery processes and delayed mitigation efforts.

Organizations across multiple sectors, including healthcare, finance, and government, were affected, with critical systems going offline. Hospitals in Europe reported disruptions in patient care due to downed IT infrastructure, and several financial institutions in North America faced outages in trading platforms. The ripple effect underscored the dependency of modern operations on endpoint security solutions and the high stakes of software integrity.

CrowdStrike issued emergency patches within 48 hours and deployed a global support team to assist customers. Nevertheless, the damage to customer trust and operational continuity was profound. The incident serves as a stark reminder of the potential fallout from inadequate testing in software updates, especially for tools with expansive deployment footprints.

This event highlights the critical need for robust validation protocols in software update pipelines, especially for cybersecurity solutions with deep system integration. For organizations, it underscores the importance of comprehensive incident response plans to manage risks associated with third-party software dependencies. [3]

[3] https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/

06/ 2024 Trends & 2025 Predictions

Infostealers

The surge of infostealers in 2024 represents evolution in cybercrime tactics towards sophistication, with significant technical implications for both individuals and organizations. Infostealers have demonstrated enhanced capabilities to extract browser-stored credentials, session cookies, cryptocurrency wallets, and autofill data, often exploiting outdated software or unpatched vulnerabilities. These tools are now routinely deployed in phishing campaigns, malvertising, and even through compromised supply chains, reflecting their adaptability and low operational cost to threat actors. For instance, Redline Stealer[4] was implicated in campaigns targeting financial institutions in Europe, where attackers leveraged stolen credentials to bypass authentication and siphon funds. Similarly, Raccoon Stealer[5] played a pivotal role in large-scale cryptocurrency heists, utilizing browser session hijacking to access wallets without direct credential theft.

The technical impact is profound: once infostealers infiltrate a system, they exfiltrate data to command-and-control servers, enabling threat actors to analyse and weaponize the stolen information for lateral movement, privilege escalation, or secondary attacks, such as ransomware deployment. The use of advanced techniques. like encrypted communication channels and polymorphic code, further complicates detection by traditional antivirus tools.

The North Korean IT Worker Scheme

In 2024, persistence and sophistication of North Korean IT worker schemes have highlighted a critical and evolving cybersecurity threat. Since 2022, operations have been carried out by individuals sent by the Democratic People's Republic of Korea (DPRK) to secure remote IT roles in global organizations. The primary objectives of these schemes include generating revenue to evade sanctions, fund North Korea's weapons programs, and potentially establish long-term access to corporate networks for financial exploitation or espionage. Operatives, collectively tracked as UNC5267, rely on stolen identities, fabricated resumes, and front companies to infiltrate organizations.

UNC5267 operatives employ sophisticated methods, including leveraging compromised identities to gain employment and maintain remote access through corporate laptops shipped to facilitator-controlled "laptop farms." These facilitators use remote administration tools like AnyDesk and TeamViewer to obscure the true location of the operatives who are often based in China, Russia, or Southeast Asia. Once embedded, these workers access corporate systems, modify the code, and administer networks, posing significant risks of unauthorized data access and sabotage.

---

4 https://www.eurojust.europa.eu/news/malware-targeting-millions-people-taken-down-international-coalition

5 https://www.justice.gov/usao-wdtx/pr/ukrainian-national-sentenced-federal-prison-raccoon-infostealer-cybercrime-case

Despite primarily working within job responsibilities, these actors' elevated privileges enable them to exploit victim systems. For example, the use of a stolen identity to manage 60+ profiles led to over $6.8 million in revenue generated for North Korea between 2020 and 2023. Resumes tied to UNC5267 frequently feature incongruities, such as mismatched educational and employment histories, which raise red flags during thorough vetting processes.[6]

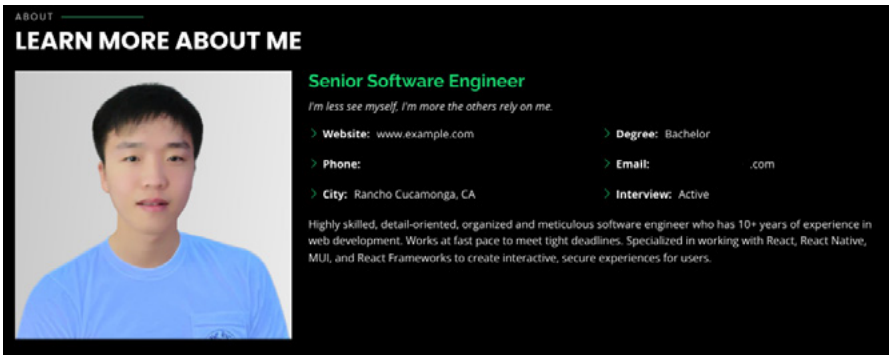


Figure 6. Example of adversary-generated resume (Mandiant)

Quantum Computing

In 2024, quantum computing reached a turning point that pushed cybersecurity into new heights as its ability to undermine conventional encryption techniques grew closer to reality. Widely used encryption algorithms, like RSA and ECC, which support secure communications, digital signatures, and financial transactions, are fundamentally threatened by the unmatched processing power of quantum computers. These systems solve mathematical problems exponentially faster than their classical counterparts. This threat is anticipated to increase in 2025 as quantum technology advances and the gap between theoretical and practical applications closes.

Quantum-resistant cryptography (QRC) must be implemented immediately by organizations to protect sensitive data and guarantee adherence to new legal requirements. By standardizing algorithms that can withstand quantum attacks, projects like the Post-Quantum Cryptography (PQC) project from the National Institute of Standards and Technology (NIST) are setting the path. Making the switch to QRC is difficult and calls for updating key management procedures, integrating new algorithms, and conducting thorough audits of cryptographic dependencies. Quantum key distribution (QKD), which uses the principles of quantum mechanics to create impenetrable communication channels, is another technique that businesses are increasingly investigating.

6 https://cloud.google.com/blog/topics/threat-intelligence/mitigating-dprk-it-worker-threat

Proactive steps will be essential to staying ahead of the threat curve as quantum technology develops. These include investing in infrastructure that is ready for quantum, educating cybersecurity teams, and keeping a close eye on market trends. The stakes are high: even current communications are at risk due to the rise of "store now, decrypt later" strategies, in which adversaries gather encrypted data now in preparation for upcoming quantum innovations. It is now essential to prepare for the quantum era in 2025 to protect data and systems in the long run.

More Complex Attack Vectors

Cybercriminals improved their strategies in 2024 to using more complex attack vectors that combine conventional techniques with state-of-the-art technology. Malware, social engineering, and phishing have developed into multi-layered attacks that frequently use artificial intelligence to take advantage of flaws in both systems and people. Threat actors now use deepfake technology to manipulate identities, polymorphic malware that changes to avoid detection, and AI-generated phishing emails that are almost identical to authentic communications. Organizations find it more and more challenging to recognize and eliminate threats before serious harm is done because of this increasing complexity.

As attackers hone their tactics and take advantage of the growing number of connected devices, cloud infrastructures, and hybrid work environments, the stakes will increase even more in 2025. Businesses must switch from reactive to proactive defence tactics, incorporating AI-powered security solutions that can spot irregularities instantly and adjust to new threats. To reduce risks, investments in threat intelligence sharing, user behaviour analytics, and strong zero-trust architectures will be essential.

07/ Recommendations

The widespread presence of infostealers highlights their function as a crucial catalyst of more extensive cyber threats. These tools, facilitating ransomware deployment, financial fraud, and credential theft, are now an essential part of multi-stage attacks rather than stand-alone malware. They are favoured for being inexpensive, simple to set up, and capable of taking advantage of common vulnerabilities, like out-of-date software and unpatched systems. Organizations should prioritize credential hygiene by implementing password managers, enforcing strict password policies, and encouraging the use of browser-independent authentication mechanisms, like hardware tokens or mobile-based MFA. Endpoint detection and response (EDR) solutions should be improved to detect infostealers' typical exfiltration patterns, such as encrypted outbound communications to command and control servers. From a strategic standpoint, organizations should limit the use of browser-stored credentials and autofill features, both of which are popular targets for infostealers. Additionally, educating users about phishing awareness and keeping systems up to date are critical. As threat actors continue to use infostealers in scalable attacks, proactive measures are required to mitigate the risks they pose to digital ecosystems.

The emergence of the North Korean IT worker schemes demonstrates a multifaceted threat that combines financial motivations and strategic espionage. These campaigns demonstrate advanced social engineering skills of using stolen identities and forged credentials to infiltrate global organizations as legitimate IT professionals. Once hired, they can steal funds, commit intellectual property theft, or lay the groundwork for future cyber-espionage operations. Organizations must improve their hiring processes to detect fraudulent applicants. This includes implementing strong identity verification systems, cross-referencing employment histories, and using open-source intelligence to identify suspicious patterns in applicant behaviour. Regular employee monitoring, especially in highly susceptible sectors, such as finance and technology, should be combined with anomaly detection tools to detect unusual activity indicative of insider threat. Furthermore, businesses should improve their third-party vendor due diligence, as DPRK operatives frequently infiltrate via subcontracting relationships. Organizations can detect and mitigate the risks posed by sophisticated schemes by incorporating advanced threat intelligence into their recruitment and vendor management processes.[7]

Emergence of quantum computing as a credible threat to traditional encryption emphasizes the critical need for organizations to future-proof their cryptographic infrastructure. The "harvest now, decrypt later" strategy used by threat actors heightens the urgency, as encrypted data intercepted today may be decrypted once quantum technology advances. This poses a significant risk to industries that rely on sensitive communications, such as finance, healthcare, and

[7] https://www.justice.gov/opa/pr/justice-department-disrupts-north-korean-remote-it-worker-fraud-schemes-through-charges-and

defence. To mitigate these threats, organizations should prioritize the immediate implementation of quantum-resistant cryptography (QRC). Transitioning to NIST-recommended[8] post-quantum algorithms necessitate a thorough examination of existing cryptographic dependencies, updates to key management protocols, and gradual integration into critical systems. Businesses should also consider using quantum key distribution (QKD), an approach the uses quantum mechanics principles to create impenetrable communication channels, to secure high-value communications. Organizations must handle this transition with urgency. Waiting for quantum computing to achieve widespread practical application is not an option. Data stolen and stored today is already at risk. Preparing today will protect future communications and ensure compliance with upcoming regulatory requirements in the quantum era.

Integration of artificial intelligence and advanced evasion techniques brought about a new era of cybercrime tactics. AI-generated phishing emails, deepfakes, and polymorphic malware increase attacker capabilities rendering traditional signature-based defences increasingly obsolete. These developments highlight the critical need for organizations to re-evaluate their cybersecurity posture. To limit attackers' lateral movement, organizations must implement zero-trust architecture (ZTA). Zero-trust principles, such as verifying every user and device before granting access and continuously monitoring all access requests, help to reduce credential theft and privilege escalation. Employment of user behaviour analytics enhances this approach by detecting deviations from baseline behaviours, which are frequently indicative of compromised accounts or insider threats. Sharing threat intelligence is another critical component of strengthening defences against these increasingly sophisticated attacks. Organizations that actively participate in information-sharing platforms can gain actionable insights into emerging threat actor techniques, such as the most recent uses of AI in cybercrime.

[8] https://www.nist.gov/cybersecurity/what-post-quantum-cryptography

08/ Endnote

In the past couple of years the cyber domain has shown that it goes hand-in-hand with the geopolitical trends. Rest assured that 2025 will see some of the highest tensions in the geopolitical field to date and it will have the ripple effect and transfer to the cyber domain. Trends like AI adaptation will greatly shape the cyber threat landscape in the upcoming years. Organisations must recognize and stay ahead of these trends to successfully counter these growing threats. The strengthening stance against AI-driven cyberattacks and growing sophistication of state-sponsored adversaries is a must heading into 2025. The ever-changing cyber threat landscape pushes organizations to adopt proactive security strategies, leveraging AI-driven threat detection and robust incident response capabilities. Fostering cross-sector collaboration and cyber threat sharing will be critical in mitigating the risks rising from both nation-state actor and organized crime groups. In this dynamic environment resilience, adaptability and strategic foresight will be key in maintaining security in an increasingly volatile cyber domain.





ISSUED BY THE REGIONAL CYBER DEFENCE CENTRE,
PART OF NATIONAL CYBER SECURITY CENTRE OF LITHUANIA

Layout by the Visual Information Division
of the General Affairs Department of the Ministry of National Defence,
Totorių g. 25, LT-01121 Vilnius



REGIONAL CYBER DEFENCE CENTRE

CTAC 2024 Yearly Report