CyberProof®
A UST Company

# 2025 GLOBAL THREAT INTELLIGENCE REPORT

## Mapping Threats and Trends

**cyberproof.com**

# TABLE OF CONTENTS

**EXECUTIVE SUMMARY** 3

**GEOPOLITICAL CONFLICTS AND CYBER WARFARE** 4

Russia-Ukraine Conflict 5

Israel-Hamas Conflict 6

China-Taiwan Conflict 7

North Korea-South Korea Conflict 8

Olympics and Geopolitical Conflicts 9

Elections and APT Interference 10

**THE RISE OF RANSOMWARE ALLIANCES AND SECTOR-SPECIFIC TARGETING** 12

Trend: Healthcare Sector Under Siege 12

Trend: Collaboration Between APT and Ransomware Groups 14

Trend: Evolution of Extortion Tactics 15

**THE RISE OF SUPPLY CHAIN CYBER THREAT** 18

Trend: Targeting Widely Used Software Libraries 18

Trend: Exploiting Cloud-Based Systems and Hybrid Environments 19

Trend: Third-Party Vendor Risks in Critical Infrastructure 20

**PREDICTIONS FOR CYBERSECURITY IN 2025 BASED ON 2024 TRENDS** 21

**OUR RECOMMENDATIONS** 22

**ABOUT CYBERPROOF** 23

# EXECUTIVE SUMMARY

In 2024, the evolving cyber threat landscape was shaped by geopolitical tensions, advancing ransomware tactics, and the rise of supply chain attacks. This report maps the defining cyber trends of the past year, offering a detailed overview of how state-sponsored actors, cybercriminals, and hacktivists reshaped the global security environment. From critical infrastructure disruptions to advanced ransomware campaigns, the data reflects a year marked by escalating cyber risks and widespread operational disruptions.

State-sponsored groups and hacktivists leveraged ongoing global conflicts to intensify their operations, targeting sectors such as healthcare, utilities, and defense. The Russia-Ukraine conflict remained a focal point for cyber warfare, with Russian Advanced Persistent Threat (APT) groups conducting operations that disrupted essential services and imposed economic strain on Ukraine and its allies. Simultaneously, Iran and North Korea executed targeted campaigns against U.S., Israel, and South Korean infrastructure, reflecting the expanding role of cyber operations in geopolitical rivalries.

The data in this report will shine a light on critical trends, including the increase in supply chain attacks compared to the previous year, exposing significant weaknesses in software, cloud environments, and operational technology. Incidents such as the Polyfill.io JavaScript compromise and Volt Typhoon's infiltration of U.S. infrastructure through third-party vendors revealed the fragility of digital dependencies across industries. These attacks highlighted vulnerabilities in vendor security and demonstrated the cascading risks that can ripple throughout entire networks.

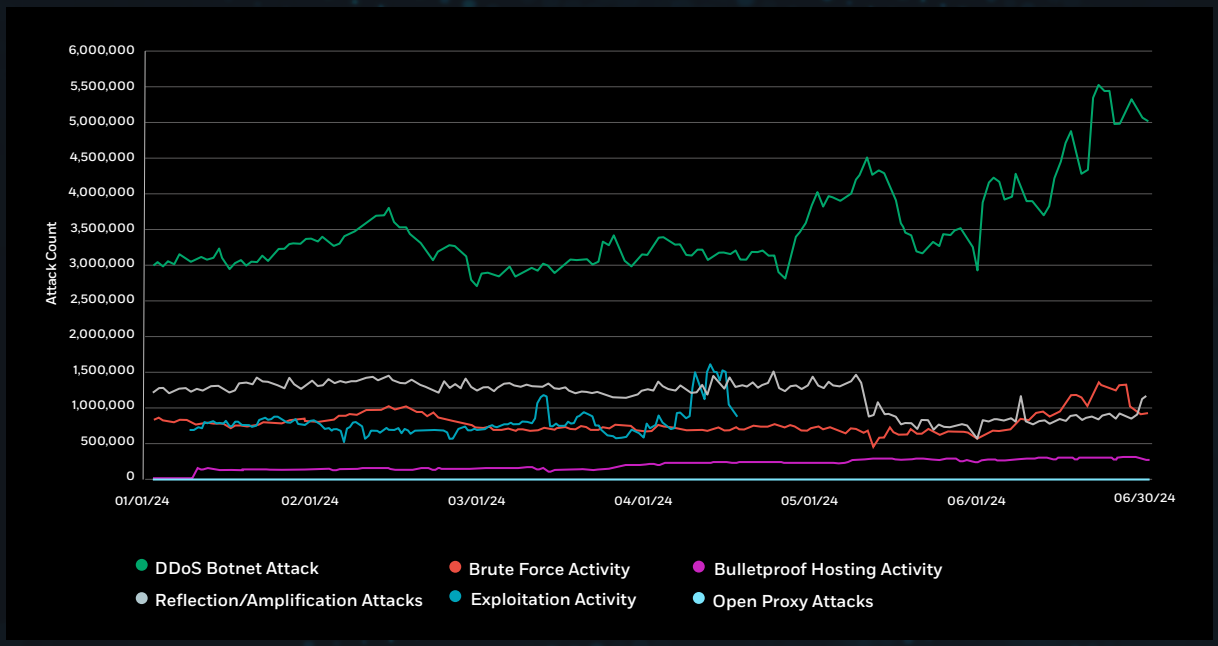
We will share examples of how ransomware attacks remained a dominant threat in 2024, with healthcare emerging as a primary target, and uncover how the sector experienced a year-over-year increase in confirmed ransomware incidents, disrupting operations and resulting in record-breaking payouts to attackers. The collaboration between APT groups and ransomware groups blurred the lines between state-sponsored activity and financially motivated cybercrime, intensifying the reach and impact of ransomware across industries. The adoption of double and triple extortion tactics further amplified the financial and reputational risks faced by organizations globally.

As cyber threats evolve, the trends from 2024 highlight the complex risks facing governments and enterprises. This report serves as a guide to understanding the shifting threat landscape, providing insights to help organizations anticipate and address emerging challenges in the year ahead.

# GEOPOLITICAL CONFLICTS AND CYBER WARFARE

In 2024, geopolitical tensions significantly shaped the global cyber threat landscape, with state-sponsored groups and hacktivists increasingly targeting critical infrastructure sectors such as energy, telecommunications, and healthcare. These cyber operations, whether focused on espionage, disruption, or influence, have become indispensable tools in broader geopolitical conflicts. While this trend is not new, the scale and sophistication of attacks in 2024 represent a marked escalation compared to previous years.

Such attacks incorporate various tactics and take on different forms, ranging from espionage campaigns to Distributed Denial of Service (DDoS) attacks. Driven by APT groups and ideologically motivated hacktivists, these campaigns aim to disrupt essential services, instill fear, destabilize economies, and exert political pressure. Moreover, the ripple effects of these operations extend beyond the immediate parties involved in a conflict. Countries aligned with each side—whether through economic ties, military alliances, or political support—are frequently targeted. These allies often suffer from significant cyberattacks on critical infrastructure, as adversaries seek to weaken their support and create broader instability.




Increase in DDoS attacks against critical infrastructure 2024 (Data source: Netscout)

The following section explores key geopolitical conflicts where cyber warfare played a pivotal role in 2024. Through detailed examples, we examine the strategies, motivations, and impacts of state-sponsored and hacktivist attacks, highlighting how the interconnected nature of the modern world makes these threats increasingly global.

**Over the past four years, there has been a 55% increase in DDoS attacks against critical infrastructure.** [1]

[1] Netscout Threat Report 2024, https://www.netscout.com/threatreport.


## RUSSIA-UKRAINE CONFLICT

The Russia-Ukraine conflict, which escalated with Russia's full-scale invasion of Ukraine in February 2022, remains one of the most cyber-active battlegrounds globally. Russian-linked APT groups have focused on disrupting Ukraine's critical infrastructure while extending their reach to Ukraine's allies in Europe and the U.S. Approximately 75% of Russian cyber operations have targeted Ukraine or NATO member states, as Moscow seeks to collect intelligence on Western policies regarding the war.[2]

**Attack on Ukrainian Energy Infrastructure:** In early 2024, Ukraine's energy sector faced a series of cyberattacks attributed to Russian APT groups. The attackers deployed malware designed to infiltrate and manipulate SCADA (Supervisory Control and Data Acquisition) systems, causing temporary blackouts in key urban areas. These attacks leveraged vulnerabilities in outdated operational technology, demonstrating the significant risks posed by legacy systems. This campaign highlights Russia's strategic focus on undermining essential services to destabilize Ukraine.[3]

**DDoS Attacks on European NATO and Governmental Institutions:** In mid-2024, European organizations, including NATO member states and governmental entities supporting Ukraine, experienced a surge in DDoS attacks. Pro-Russian hacktivist groups, such as NoName057(16), used platforms like "DDoSia" to overwhelm networks with high traffic volumes, causing intermittent service outages. These attacks aimed to disrupt critical operations and send a message of deterrence to countries providing support to Ukraine.[4]

### SPOTLIGHT: **NoName057(6)**

Active from March 2022, NoName057(16) is a pro-Russian hacktivist group that emerged as a prominent player in the ongoing Russia-Ukraine conflict. Known for conducting DDoS attacks, the group primarily targets organizations aligned with Ukraine and its allies, including NATO member states and European government institutions. Operating through a platform called "DDoSia," the group incentivizes participants by offering rewards for executing successful attacks, effectively crowdsourcing their operations. Their campaigns aim to disrupt critical services, create political and economic instability, and amplify pro-Russian narratives. NoName057(16) blends state-aligned hacktivism with sophisticated cyber tactics, marking a significant evolution in hybrid warfare.

[2] https://blogs.microsoft.com/on-the-issues/2024/10/15/escalating-cyber-threats-demand-stronger-global-defense-and-cooperation/
[3] https://news.ucsc.edu/2024/05/ukraine-cybersecurity.html
[4] https://www.bleepingcomputer.com/news/security/spain-arrests-three-for-using-ddosia-hacktivist-platform/


## ISRAEL-HAMAS CONFLICT

The Israel-Hamas conflict, which escalated dramatically with Hamas's attack on Israel in October 2023, has increasingly manifested in the digital realm. Cyber actors, including state-sponsored groups and hacktivists, have targeted Israeli critical infrastructure and Western entities supporting Israel, reflecting the growing intersection of geopolitical tensions and cyber warfare.

**Attempt to Disrupt Israeli Flight Communications:** On February 18, 2024, hackers attempted to interfere with the communications networks of two Israeli flights over the Middle East. The pilots received suspicious instructions potentially aimed at diverting the planes, but safely continued to their destinations after disregarding the instructions. The incident occurred in an area where Iran-backed Houthi militants operate, though the threat remains unattributed to any specific actor. [5]

**Targeted Iranian Cyberattacks on U.S. Critical Infrastructure:** In 2024, Iranian state-sponsored hackers engaged in a year-long cyber campaign targeting U.S. critical infrastructure, including healthcare and energy sectors, as well as allies of the United States. This campaign, uncovered in October 2024, utilized brute force techniques and advanced credential harvesting to infiltrate sensitive systems.

Analysts tied these activities to Iran's geopolitical strategy of targeting nations allied with Israel, aiming to disrupt their stability and weaken their alliances. By exploiting vulnerabilities in interlinked infrastructure, the attackers amplified the operational impact of their actions, demonstrating a sophisticated approach to cyber warfare. [6]

Analysts tied these activities to Iran's geopolitical strategy of targeting nations allied with Israel, aiming to disrupt their stability and weaken their alliances. By exploiting vulnerabilities in interlinked infrastructure, the attackers amplified the operational impact of their actions, demonstrating a sophisticated approach to cyber warfare. [6]

[5] World Cybercrime Index, https://www.infosecurity-magazine.com/news/russia-ukraine-world-cybercrime/
[6] https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-290a

China/Taiwan

## CHINA-TAIWAN CONFLICT

Rising tensions between China and Taiwan have been reflected in an uptick in cyber activity, with Chinese APT groups targeting strategic Taiwan industries and U.S. critical infrastructure organizations aligned with Taiwan's interests. Such activities are seen as a strategy to deter the U.S. from defending Taiwan should China attempt to blockade or invade the island, which it views as part of its "One China" policy.

**Attacks on U.S. Defense Contractors:** In August 2024, Chinese cyber operatives conducted a sophisticated campaign targeting U.S. defense contractors connected to military support for Taiwan. Employing spear-phishing techniques and exploiting zero-day vulnerabilities, the attackers infiltrated sensitive networks to exfiltrate defense-related data. These breaches illustrate China's ongoing strategy to weaken U.S.-Taiwan defense alliances, with cyber incidents against U.S. defense contractors rising sharply in 2024. [7]

**Volt Typhoon Botnet Campaign:** In September 2024, the Chinese state-sponsored group Volt Typhoon launched a renewed campaign utilizing a newly constructed botnet. This operation targeted U.S. critical infrastructure, specifically exploiting vulnerabilities in the edge devices of three leading U.S. broadband providers, such as outdated routers. The botnet, which emerged nearly 10 months after a previous takedown by U.S. authorities, demonstrated Volt Typhoon's ability to rapidly rebuild and adapt. The campaign primarily focused on reconnaissance, data theft, and disruption capabilities, with research suggesting it was part of a broader effort to undermine U.S. support for Taiwan amid escalating tensions in the Taiwan Strait. [8] [9]

### SPOTLIGHT: **Volt Typhoon**

Volt Typhoon is a Chinese state-sponsored APT group active since at least mid-2021. The group is known for its stealthy operations, employing living-off-the-land (LOTL) techniques to blend into legitimate system activity and evade detection. Volt Typhoon primarily targets critical infrastructure sectors, including telecommunications, energy, and transportation, with a focus on intelligence gathering and maintaining persistence for potential disruptive operations. In May 2023, the group was implicated in a widespread campaign that infiltrated U.S. critical infrastructure, including power and water systems, as part of efforts to prepare for potential conflicts in the Taiwan Strait. By 2024, Volt Typhoon's campaigns had evolved, utilizing advanced botnets to target vulnerabilities in broadband networks, highlighting their continued sophistication and strategic intent to undermine U.S. and allied critical infrastructure.

[7] https://breakingdefense.com/2024/06/china-actively-targeting-us-industrial-base-warns-cybercom-chief/
[8] https://www.csoonline.com/article/3604173/volt-typhoon-returns-with-fresh-botnet-attacks-on-critical-us-infrastructure.html
[9] https://www.csoonline.com/article/3605085/us-says-china-conducted-massive-espionage-through-breached-telcos.html

North Korea/South Korea

## NORTH KOREA-SOUTH KOREA CONFLICT

The decades-long conflict between North and South Korea has extended well into the digital realm, with North Korea adopting an aggressive cyber strategy to target South Korean interests and its allies. Beyond espionage, North Korea's campaigns frequently aim to disrupt essential services and exfiltrate sensitive data, leveraging cyberattacks as a cost-effective tool to exert geopolitical influence.

**Attacks on U.S. and U.K. Strategic Sectors:** In July 2024, North Korean state-sponsored hackers executed a targeted campaign against critical sectors in the U.S. and U.K., both key allies of South Korea. These operations concentrated on defense, nuclear energy, and power systems, using spear-phishing and supply chain compromise to infiltrate sensitive networks. The goal was to extract classified military and nuclear data while pre-positioning malware for potential sabotage.[10]

**Ransomware Campaign on Healthcare Systems:** In early 2024, North Korean hackers launched a widespread ransomware campaign targeting U.S. healthcare facilities. The attackers deployed encryption malware to lock patient records, demanding ransom payments to restore access. The attacks caused significant disruption to hospital operations, including emergency services, and threatened the safety of patients. U.S. cybersecurity agencies intervened, recovering over $500,000 in ransom payments, and mitigating further impact. This campaign underscored North Korea's willingness to exploit the vulnerabilities of vital sectors like healthcare to further its economic and strategic goals.[11]

**North Korea's campaigns frequently aim to disrupt essential services and exfiltrate sensitive data, leveraging cyberattacks as a cost-effective tool to exert geopolitical influence.**

[10] https://www.ncsc.gov.uk/news/ncsc-partners-vigilant-dprk-sponsored-cyber-campaign
[11] https://apnews.com/article/technology-health-crime-lisa-monaco-government-and-politics-1c8384b8ea7a4cbe7fc1550c2f2eb110

## THE OLYMPIC GAMES AND GEOPOLITICAL CONFLICTS

The Olympic Games gather participants and stakeholders from around the world, including nations embroiled in geopolitical conflicts. This makes them attractive to threat actors aiming for maximum visibility and impact. The 2024 Paris Olympic Games demonstrated how global events are not immune to geopolitical tensions but instead serve as another venue for threat actors to exploit. International sporting events, with their high-profile nature and complex organizational structures, have increasingly become targets of cyberattacks. These incidents reflect how geopolitical conflicts extend into seemingly neutral arenas, using them as platforms to disrupt, intimidate, or make political statements.

**DDoS Attacks on French Government Websites and Olympic Organizers:** Leading up to the Paris Olympic Games, pro-Russian hacktivist group "Anonymous Sudan" launched DDoS attacks targeting French government websites and Olympic organizers, motivated by France's support for Ukraine. These attacks aimed to disrupt event preparations and create public doubt about the security of the Olympic Games. [12] [13]


Anonymous Sudan Telegram page stating they have attacked numerous French Government network infrastructure [14]

[12] https://www.politico.eu/article/french-government-hit-with-cyberattacks-of-unprecedented-intensity/
[13] https://www.lemonde.fr/en/france/article/2024/03/11/french-state-services-hit-by-intense-cyberattack_6608727_7.html#
[14] https://cybernews.com/news/france-government-cyberattack-anonymous-sudan/

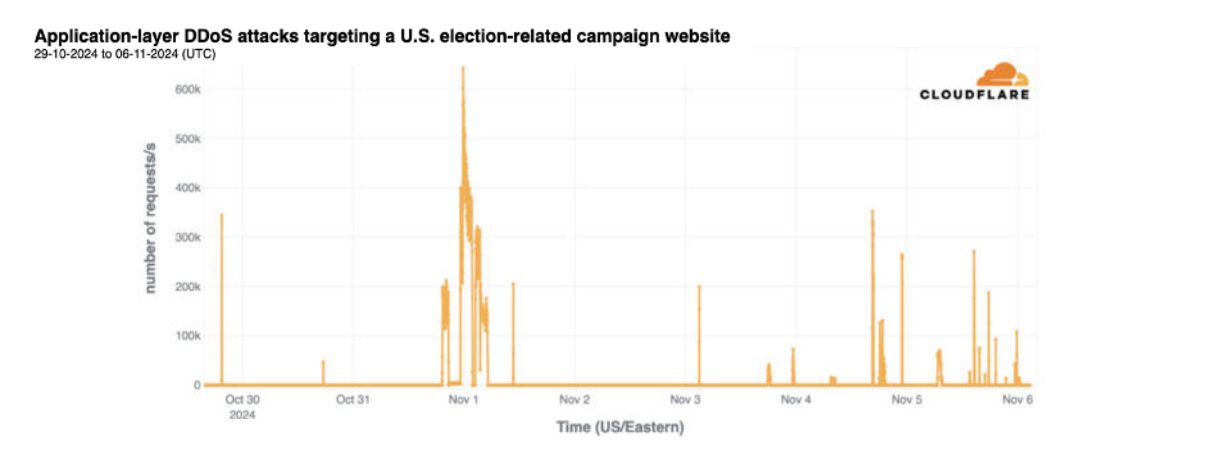
**Data Leak Targeting Israeli Athletes:** Shortly before the Olympic Games began, a cyber group named "Zeus" leaked sensitive information pertaining to Israeli athletes, including military IDs, home addresses, and other personal details. This politically driven attack appeared intended to raise security concerns for Israeli participants. The incident highlighted the cybersecurity challenges associated with hosting international events that draw participants from politically contentious regions. [15]

## APT INTERFERENCE DURING ELECTIONS

In 2024, election periods remained critical targets for cyber interference, with state-sponsored APT groups exploiting these events to influence public sentiment, disrupt democratic processes, and sway political outcomes. This trend persisted globally, fueled by geopolitical tensions and ongoing worldwide conflicts that motivated adversaries to expand their influence operations. Significant campaigns targeted various elections, underscoring the persistent interest of foreign actors in leveraging cyber tools to undermine trust in electoral systems and manipulate democratic institutions.

**U.S. Presidential Election 2024:** Leading up to the 2024 U.S. presidential election, state-sponsored groups from Russia, China, and Iran orchestrated extensive cyber campaigns aimed at influencing voter perceptions and eroding confidence in the electoral process. Election-related cyber incidents rose by 15% compared to previous cycles, highlighting a consistent and evolving focus on shaping U.S. political outcomes through cyber means. These efforts included spear-phishing attacks targeting election infrastructure, campaign websites, and media outlets. Beyond traditional tactics, adversaries also leveraged large-language models (LLMs) to craft sophisticated disinformation campaigns, creating fake news sites and impersonating activists to amplify divisive narratives. In October 2024, reports highlighted how Iranian hackers intensified their efforts, specifically targeting swing states to manipulate voter sentiment. [16] [17]

**In the United States, over 6 billion malicious requests tied to DDoS attacks were blocked between November 1-6, ahead Election Day 2024 [18]**




DDoS activity between October 30th 2024 and November 6th 2024 (Source: Cloudflare)

[15] https://www.cyberproof.com/blog/racing-against-cyber-threats-at-the-2024-paris-olympic-games/
[16] https://www.darkreading.com/vulnerabilities-threats/russia-china-iran-targeting-us-election
[17] https://blogs.microsoft.com/on-the-issues/2024/10/23/as-the-u-s-election-nears-russia-iran-and-china-step-up-influence-efforts/
[18] Cloudflare, Elections and Cyberattacks, 2024 https://blog.cloudflare.com/elections-2024-internet/

## SPOTLIGHT: Storm-1516

Storm-1516 is a threat actor believed to be state-sponsored, active primarily in influence operations since late 2022. The group specializes in crafting and amplifying disinformation campaigns, leveraging advanced tools such as large-language models and deepfake technologies to create realistic fake videos and news articles. Storm-1516 frequently targets political events and high-profile elections, aiming to undermine trust in democratic institutions and sway public opinion. In 2024, the group focused heavily on the U.S. presidential election, producing fabricated scandals involving false allegations against political figures and U.S. intelligence agencies. These operations often included laundering narratives through fake journalists and non-existent whistleblowers, distributed via inauthentic news websites. Storm-1516 exemplifies the evolution of cyber influence tactics, blending technical sophistication with strategic messaging to achieve geopolitical objectives.


Fabricated documentary "Olympics Has Fallen" made by Storm-1679 to distribute disinformation at the 2024 Olympics [19]

**European Parliament Elections:** During the 2024 European Parliament elections, pro-Russian hacktivist group "NoName057(16)" launched cyberattacks aimed at disrupting the electoral process and signaling opposition to EU policies. The group claimed responsibility for DDoS attacks targeting European Union infrastructure on the first day of voting, affecting access to various government websites.[20]

The cyber threat landscape of 2024 has been significantly shaped by geopolitical unrest, with a notable surge in targeted cyber operations against critical infrastructures worldwide. These activities reflect the strategic deployment of cyberattacks by state-sponsored groups and hacktivists aiming to influence global politics and exert pressure on adversaries and their allies. The diversity and sophistication of the attacks, as examined in the preceding examples, reveal a complex and escalating threat environment. This trend highlights the importance of understanding the nexus between geopolitical conflicts and cyber threats, as it is increasingly clear that such cyber operations have become integral to the strategies of nation-states and political actors in the modern arena of international relations.

[19] https://cybernews.com/news/fake-tom-cruise-undermining-paris-olympics/
[20] https://www.euronews.com/my-europe/2024/06/06/pro-russia-group-claims-responsibility-for-cyber-attacks-on-first-day-of-eu-election

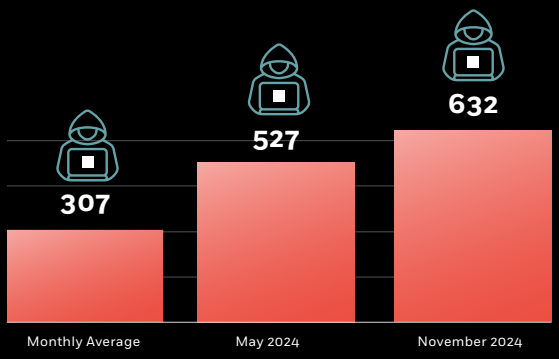
# THE GLOBAL RISE OF RANSOMWARE ALLIANCES AND SECTOR-SPECIFIC TARGETING

Ransomware proved to be one of the most disruptive cyber threats in 2024, inflicting widespread damage across industries and organizations globally. In the first half of the year, ransomware attacks generated a record-breaking $450 million in revenue for cybercriminals, reflecting a 10% year-over-year increase in confirmed attacks.[21] The year-end revenue is projected to surpass 2023, highlighting the escalating financial and operational toll of these campaigns. Below, we explore key trends and major incidents that defined the ransomware landscape in 2024.

## TREND: HEALTHCARE SECTOR UNDER SIEGE

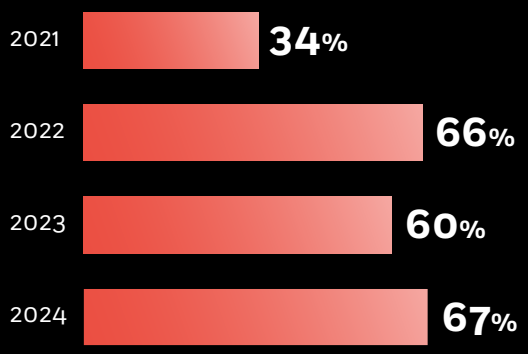
The healthcare industry faced a significant surge in ransomware attacks in 2024, as cybercriminals exploited the sector's critical role, reliance on interconnected systems, and often outdated cybersecurity measures. The sensitive nature of patient data and the need for uninterrupted medical services made hospitals, medical research centers, and healthcare providers worldwide prime targets for attackers seeking substantial payouts and operational leverage.

*Global ransomware activity reached unprecedented levels in November 2024, with 632 victims reported on data leak sites—more than double the usual monthly average of 307 and surpassing the previous record of 527 in May, reflecting a sharp and ongoing rise in ransomware incidents.* [22] [23]




Ransomware activity levels - a sharp and ongoing rise in ransomware incidents

*67% of healthcare organizations were impacted by ransomware attacks in the past year, marking a four-year high since 2021.* [24]

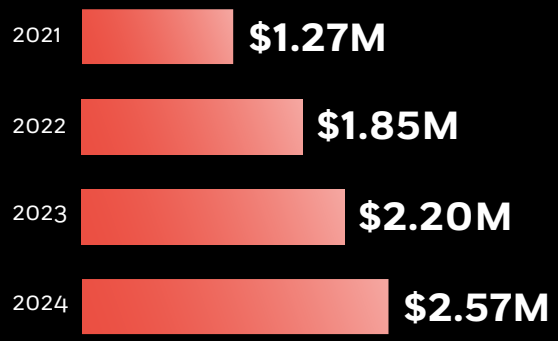



The percentage of healthcare organizations impacted by ransomware 2021-2024 (Source: Sophos)

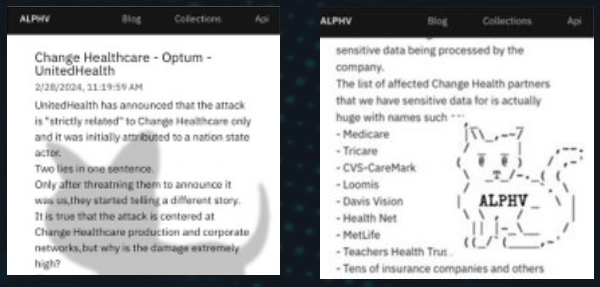
[21] https://www.bleepingcomputer.com/news/security/ransomware-rakes-in-record-breaking-450-million-in-first-half-of-2024/
[22] https://www.infosecurity-magazine.com/news/akira-ransomhub-ransomware-claims/
[23] Corvus Insurance, Q3 2024 Cyber Threat Report, https://www.corvusinsurance.com/blog/q3-2024-cyber-threat-report?utm_campaign=FY-24-Q4-Q3%20Cyber%20Threat%20Report&utm_source=featurednav&utm_medium=website
[24] Sophos, The State of Ransomware in Healthcare 2024, https://www.sophos.com/en-us/whitepaper/state-of-ransomware-in-healthcare

**Change Healthcare Breach:** The ransomware attack against Change Healthcare, carried out by the BlackCat/ALPHV group, was characterized by healthcare officials as one of the most impactful cybersecurity incidents in U.S. healthcare history. This breach disrupted the operations of over 200 hospitals across the United States, crippling billing and payment systems, delaying claims processing, and jeopardizing patient care. The attackers exploited vulnerabilities within the organization's IT infrastructure, gaining initial access through compromised remote desktop protocol (RDP) credentials. Once inside, they used lateral movement techniques to escalate privileges and deploy ransomware across critical systems. Exfiltrating 6TB of sensitive patient and financial data, the attackers accessed medical records and payment information linked to over 100 million individuals. [26]

*The mean cost for a healthcare organization to recover from a ransomware attack has risen to $2.57 million in 2024, up from $2.20 million in 2023.* [25]



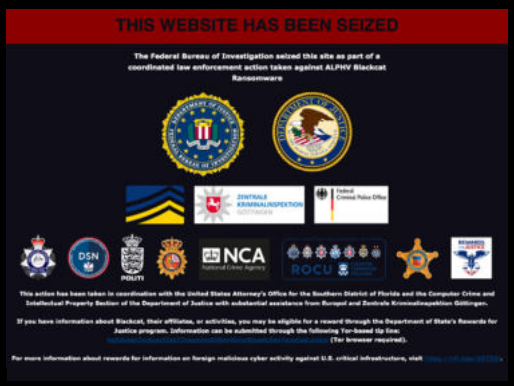

Cost to recover from a ransomware attack in healthcare 2021-2024. (Source: Sophos)




Message on ALPHV/BlackCat's leak site confirming listing Change Healthcare as their victim [27]

## SPOTLIGHT: **ALPHV/BlackCat**

BlackCat, also known as ALPHV, is a notorious ransomware group active since late 2021, operating through Ransomware-as-a-Service (RaaS). Infamous for targeting high-profile organizations across multiple sectors, the group is particularly known for its sophisticated double and triple extortion tactics, which intensify pressure on victims. In December 2023, the group was reportedly taken down following increased law enforcement efforts, only to resurface in 2024 with the high-profile attack on Change Healthcare. Shortly after, BlackCat allegedly ceased operations, fueled by speculation of a significant payout from the victim. Despite claims of their shutdown, it is believed BlackCat has rebranded, potentially aligning with, or evolving into other threat actors such as RansomHub or Cicada3301.




Fake takedown notice published on ALPHV/BlackCat's leak site [28]

[25] Sophos, the State of Ransomware in Healthcare 2024, 2024. https://www.sophos.com/en-us/press/press-releases/2024/09/two-thirds-healthcare-organizations-hit-ransomware-four-year-high
[26] https://techcrunch.com/2024/10/24/how-the-ransomware-attack-at-change-healthcare-went-down-a-timeline/
[27] https://dig.watch/updates/alphv-blackcat-ransomware-gang-claims-cyberattack-on-change-healthcare
[28] https://cyberscoop.com/ransomware-group-behind-change-healthcare-attack-goes-dark/

**Synnovis Ransomware Incident:** The ransomware attack on Synnovis, a key diagnostic services provider in the UK, caused significant disruption across London's healthcare system, resulting in over 800 canceled surgeries within a week. Attackers exploited vulnerabilities in third-party vendor integrations, initially accessing the network through a compromised software update mechanism. Once inside, they deployed ransomware that encrypted critical files in diagnostic and laboratory systems, halting operations and rendering essential medical diagnostics inaccessible. The attack forced hospitals to divert patients, delay treatments, and revert to manual processes, creating widespread operational chaos. [29]

These incidents reveal the devastating impact ransomware can have on healthcare systems, disrupting operations and compromising patient safety on a significant scale. The ripple effects of such attacks expose critical vulnerabilities within connected healthcare infrastructures, where disruptions in one area can paralyze entire networks.

## TREND: COLLABORATION BETWEEN APT AND RANSOMWARE GROUPS

In 2024, state-aligned APT groups increasingly collaborated with ransomware operators, merging the technical expertise of APTs with the financial motivations of ransomware actors. These partnerships have blurred the lines between politically driven cyberattacks and traditional cybercrime, creating more complex and multifaceted threats. with APT groups leveraging ransomware as a tool for both disruption and fundraising.

**Andariel's Play Ransomware Campaign:** North Korea's Andariel group launched a ransomware campaign in mid-2024, using the "Play" ransomware variant (one of the most prolific ransomware examples of 2024) to target healthcare facilities and transportation systems in the United States and South Korea. Attackers infiltrated systems by exploiting unpatched vulnerabilities in operational technology networks and used lateral movement techniques to access and encrypt critical data. This campaign disrupted hospital operations in South Korea and delayed logistics in the U.S., demonstrating how APTs weaponize ransomware to achieve dual objectives of disruption and revenue generation.

**Chinese APT Groups Leveraging CatB Ransomware for Espionage:** In 2024, Chinese state-sponsored APT groups, including ChamelGang, deployed ransomware to obscure their espionage operations. One notable campaign involved the use of the CatB ransomware variant, which encrypted systems while simultaneously exfiltrating sensitive data from targeted industries. By disguising their activities as financially motivated attacks, these groups misdirected investigators and delayed attribution, allowing them to achieve their intelligence-gathering objectives.

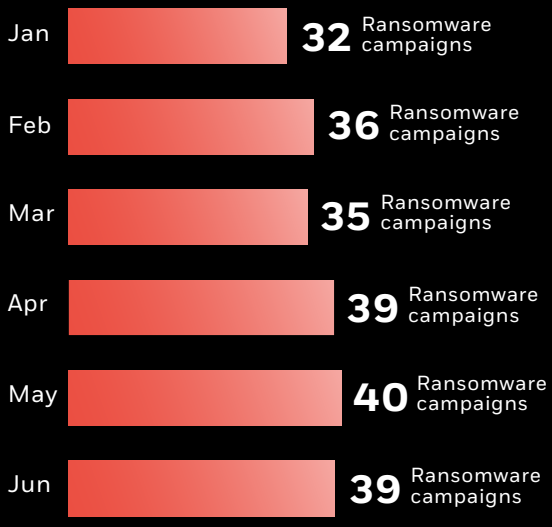
The collaboration of APT groups and ransomware operators allows threat actors to use ransomware not only for financial gain but also as a tool for disruption and espionage, complicating attribution, and response efforts. These evolving alliances have amplified the impact of cyber campaigns, highlighting the growing sophistication of modern threats.

[28] https://cyberscoop.com/ransomware-group-behind-change-healthcare-attack-goes-dark/
[29] https://securityaffairs.com/164541/cyber-crime/londol-hospitals-canceled-800-operations-ransomware.html

## TREND: EVOLUTION OF EXTORTION TACTICS

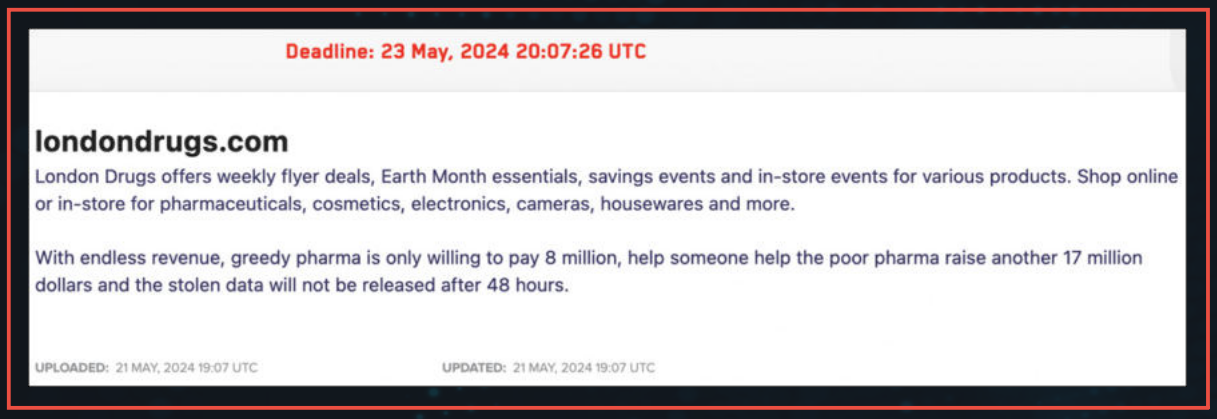
In 2024, ransomware groups expanded and intensified their use of double and triple extortion methods, evolving the strategies that were employed in previous years. These tactics now appear with greater frequency, involving not only locking victims out of their systems but also stealing sensitive information and threatening to sell or publicly expose it. By combining encryption with data exfiltration, attackers have amplified pressure on victims, leveraging both operational disruptions and the reputational risks of leaked information. This escalation reflects the growing reliance on multifaceted extortion campaigns to maximize impact and financial gain. [31]

*In May 2024, the number of name-and shame ransomware campaigns reached an all-time high, with 40 active listings of victims on dedicated leak sites.* [30]




Number of ransomware listing victims on leak sites per month. (Source: Secureworks)

**Attack on Canadian Pharmacy Chain:** In April 2024, Canadian retail pharmacy chain London Drugs became the target of a sophisticated ransomware attack carried out by the notorious LockBit group. Exploiting vulnerabilities in the company's IT infrastructure, the attackers infiltrated networks and encrypted critical operational systems, severely disrupting business functions. Over 79 stores across Western Canada were forced to close for more than a week, creating widespread risk for customers dependent on essential medications. LockBit exfiltrated sensitive customer and operational data and demanded a $25 million ransom, threatening to publish the stolen information. When London Drugs refused to comply, the group began leaking the exfiltrated data on its dark web leak site, exposing private customer information and internal corporate records. [32]




London Drugs listed on LockBit's leak site [33]

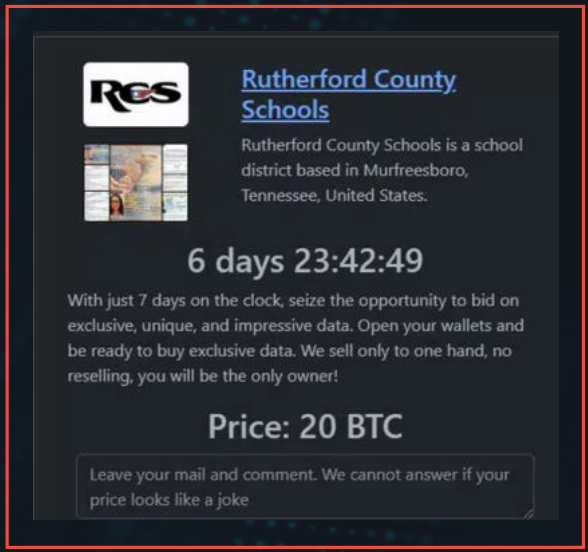
[30] Secure Works, State of the Threat 2024, 2024. https://www.secureworks.com/resources/rp-state-of-the-threat-2024
[31] https://www.forbes.com/sites/heatherwishartsmith/2024/12/09/the-persistent-ransomware-threat-2024-trends-and-high-profile-attacks/
[32] https://www.cbc.ca/news/canada/british-columbia/london-drugs-closure-western-canada-1.7187615
[33] https://www.bleepingcomputer.com/news/security/lockbit-says-they-stole-data-in-london-drugs-ransomware-attack/

SPOTLIGHT:

## LockBit

LockBit is a prolific and highly sophisticated ransomware group that has been active since 2019, known for its Ransomware-as-a-Service model. The group targets a wide range of industries globally, focusing on high-value organizations with critical operations, including healthcare, finance, and retail. LockBit is well known for its fast encryption methods and the use of double extortion tactics. Despite its dominance, the group faced increased pressure from law enforcement, with reports of successful takedown operations disrupting parts of its infrastructure. However, LockBit has demonstrated resilience, with evidence suggesting it may have shifted operations, rebranded to evade further scrutiny, or paused operations to reorganize and strengthen its tactics.

**Rhysida Ransomware Targeting of Schools:** Educational institutions have increasingly become prime targets for ransomware attacks, with the Rhysida ransomware group targeting Rutherford County Schools in Tennessee in November 2024. The attackers infiltrated the district's network, encrypting critical data and exfiltrating sensitive information. They demanded a ransom of 20 Bitcoin (over $2 million at the time), threatening to sell the stolen data to the highest bidder and refusing to restore infected systems if the ransom was not paid. This double extortion tactic not only disrupted the district's operations but also jeopardized the personal information of employees, highlighting the severe impact such attacks can have on educational institutions. [34]




Rhysida leak site listing Rutherford County Schools as their victim [35]

**Higher education organizations reported a $4.02M mean cost to recover from a ransomware attack in 2024, which is almost four times higher than the $1.06M reported in 2023.[36]**

[34] https://www.wkrn.com/news/local-news/hackers-appear-to-sell-data-stolen-from-rutherford-county-tn-schools/
[35] https://x.com/H4ckManac/status/1866799185661473101
[36] Sophos, State of Ransomware in Education

Ransomware attacks employing double and triple extortion techniques caused widespread disruption across various sectors, targeting sensitive data, and threatening public trust. These tactics, now more frequent and sophisticated, leverage operational downtime and data exposure to maximize impact.

Ransomware activity in 2024 demonstrated the increasing sophistication and adaptability of cybercriminals, who aggressively targeted critical sectors, with the healthcare industry experiencing a significant surge in attacks - the highest in four years. Other key targets included utilities, education, and organizations with hybrid cloud environments. Geopolitical dynamics further fueled ransomware operations, as state-sponsored APT's collaborated with ransomware groups to expand their reach, intertwining financial motivations with geopolitical agendas. In the first half of 2024, ransomware attacks generated a record-breaking $450 million in revenue for cybercriminals. These developments reflect an alarming trajectory for ransomware threats, cementing their position as one of the most disruptive forces in the modern cyber landscape.

**In the first half of the year, ransomware attacks generated a record-breaking $450 million in revenue for cybercriminals, reflecting a 10% YoY increase in confirmed attacks.**

# THE RISE OF SUPPLY CHAIN CYBER THREATS

Supply chain cyberattacks have continued to rise in both frequency and impact in 2024, emerging as one of the most significant threats to global cybersecurity. These attacks exploit the interconnected nature of modern digital ecosystems, leveraging trusted relationships between vendors, suppliers, and their customers to infiltrate downstream systems. Recent statistics indicate that supply chain breaches increased by 68% compared to 2023.[37] This surge reflects the growing sophistication of attackers and their ability to exploit systemic vulnerabilities in software, cloud environments, and operational technology.

Unlike traditional attacks, supply chain threats capitalize on the ripple effects of trust relationships, allowing attackers to amplify their reach and disrupt multiple organizations with a single breach. The operational and financial repercussions are significant, with recovery times stretching to months for some impacted organizations. In this section, we examine three key trends that shaped supply chain cyberattacks in 2024 and analyze major incidents to highlight these evolving threats.

## TREND: TARGETING WIDELY USED SOFTWARE LIBRARIES

The exploitation of widely adopted software libraries remained a dominant tactic for attackers in 2024. These libraries often serve as critical building blocks for applications, making them high-value targets for adversaries seeking to compromise a broad user base.

**The Polyfill.io Breach:** In 2024, attackers compromised the popular Polyfill.io JavaScript library, injecting malicious code into its updates. Polyfill.io is used by developers to ensure browser compatibility, and its compromise impacted over 380,000 hosts globally, including major corporations such as Hulu, Mercedes-Benz, and Warner Bros. The malicious code created backdoors in client systems, enabling attackers to escalate privileges and exfiltrate sensitive information. The attack disrupted operations across multiple industries, as organizations scrambled to patch vulnerabilities and assess the extent of the damage. [38]

The Polyfill breach highlighted the risks of relying on third-party software without rigorous security checks. Attackers are increasingly targeting the development pipeline, embedding malware into open-source libraries that developers and enterprises consider trustworthy. This tactic demonstrates how attackers exploit the software supply chain to achieve widespread impact with minimal effort.

**The global cost of software supply chain attacks is expected to rise from $46 Billion in 2023 to $138 Billion by 2031.[39]**

[37] https://www.verizon.com/business/resources/reports/dbir/
[38] https://thehackernews.com/2024/07/polyfillio-attack-impacts-over-380000.html

## TREND: EXPLOITING CLOUD-BASED SYSTEMS AND HYBRID ENVIRONMENTS

The growing reliance on cloud services has introduced new vulnerabilities, particularly in hybrid environments where on-premises systems connect with cloud infrastructure. Misconfigurations and weak integrations have become primary entry points for attackers, allowing them to infiltrate sensitive systems.

**Snowflake Breach by UNC5537:** UNC5537, a sophisticated threat actor, launched a targeted attack on Snowflake in 2024, exploiting misconfigured cloud integration settings. The group gained unauthorized access to sensitive customer data, leading to data theft and extortion. The attackers deployed advanced credential-harvesting malware to breach multiple enterprise accounts like Ticketmaster and AT&T, successfully extorting over $2.7 million from affected organizations.[40]

The Snowflake incident highlights the critical need for securing cloud integrations. Hybrid environments, while offering flexibility, create new attack surfaces that are challenging to monitor and defend. The trend reflects a shift in attacker priorities, focusing on vulnerabilities that enable lateral movement across interconnected systems.

### SPOTLIGHT: UNC5537

UNC5537 is a sophisticated and financially motivated cyber threat actor known for targeting high-value organizations. Active since at least April 2024, the group demonstrates advanced techniques and persistence, frequently leveraging zero-day vulnerabilities and exploiting compromised credentials to infiltrate systems. Their operations primarily focus on espionage, data theft, and extortion. By exploiting accounts lacking strong authentication measures, UNC5537 gains unauthorized access to sensitive information, which they use to extort victims, often threatening to sell or publicly release stolen data.

[39] Sophos, State of Ransomware in Education
[40] https://cyberscoop.com/as-many-as-165-companies-potentially-exposed-in-snowflake-related-attacks-mandiant-says/

## TREND: THIRD-PARTY VENDOR RISKS IN CRITICAL INFRASTRUCTURE

Critical infrastructure sectors, including energy, transportation, and utilities, have become prime targets for supply chain attacks due to their reliance on third-party vendors to manage operational technology (OT) systems. These dependencies create vulnerabilities that adversaries are quick to exploit, as many vendors lack the resources or expertise to implement strong cybersecurity measures, making them attractive entry points for attackers.

**Volt Typhoon Supply Chain Campaign:** As discussed as part of the spike in attacks during election periods, in 2024, the Chinese state-sponsored group Volt Typhoon launched a campaign targeting U.S. critical infrastructure, leveraging the supply chain as an entry point to infiltrate utilities, manufacturing, and transportation sectors. The group employed living-off-the-land techniques, exploiting trusted tools within third-party vendors' networks to blend into normal operations and avoid detection. Their activities aimed to establish persistent access in critical systems, positioning themselves to disrupt communications and infrastructure during potential conflicts in the Taiwan Strait.

A significant aspect of this campaign was Volt Typhoon's use of vulnerabilities in supply chain dependencies to compromise OT environments. By targeting third-party vendors managing OT systems, the group disrupted key communication networks and exposed vulnerabilities in energy grids.

The surge in supply chain attacks in 2024 reflects the evolving tactics of adversaries and the growing dependence of digital ecosystems. These attacks exploit the inherent trust between vendors and customers, targeting software libraries, cloud environments, and critical infrastructure sectors. A notable trend this year has been the phenomenon of more customers impacted by fewer software supply-chain breaches, highlighting the disproportionate reach and efficiency of these attacks. Organizations must adapt to these challenges by securing their supply chains and addressing vulnerabilities in both technical and operational processes.

# PREDICTIONS FOR CYBERSECURITY IN 2025 BASED ON 2024 TRENDS

### Increased Targeting of Critical Sectors

Ransomware actors will continue prioritizing sectors like healthcare, emergency services, and utilities, where downtime is intolerable. These industries' operational dependencies and critical nature make them lucrative targets. In 2024, we observed a shift toward precision attacks, emphasizing sectors where disruption can yield the greatest financial and operational impact, a trend expected to intensify in 2025.

### Adoption of Advanced Ransomware Tactics

Threat actors are continuously evolving their approaches, with double and triple extortion now standard practice. These tactics not only threaten data leaks but extend to targeting third parties, such as customers and partners, intensifying pressure on victims. In 2025, ransomware groups are expected to adopt new strategies, including the use of AI to enhance attack precision and the exploitation of interconnected systems for greater disruption. Increasingly, attackers may bypass the encryption stage altogether, opting to exfiltrate sensitive data and demand payment for its return, reflecting a shift toward faster and more aggressive extortion methods.

### Enhanced Regulation and Cybersecurity Standards

The expansion of global cybersecurity regulations in 2025 is expected to reshape the threat landscape, potentially forcing ransomware groups and cybercriminals to adapt their strategies. As governments impose stricter data protection laws and mandate incident response protocols, larger organizations are likely to bolster their defenses, which may drive attackers to shift focus toward smaller, less-regulated entities and third-party vendors. This could result in a rise in supply chain attacks and ransomware campaigns aimed at disrupting operations rather than stealing data, allowing attackers to bypass regulatory scrutiny. While these regulations may lower the frequency of successful attacks on critical infrastructure, they could create a more selective, high-impact threat environment where adversaries prioritize targets with weaker defenses and greater operational dependencies.

### Lines Between Hacktivists, APTs, and Cybercriminals Will Continue to Blur

The lines between hacktivists, APT groups, and cybercriminals are expected to blur even further in 2025, as these actors increasingly collaborate or adopt each other's tactics to achieve overlapping objectives. Nation-states will continue to leverage ransomware groups and hacktivists to carry out politically motivated attacks while maintaining plausible deniability, turning financial cybercrime into a tool for espionage and disruption. Likewise, ransomware operators are already aligning with APT groups to enhance their capabilities, using nation-state resources to bypass defenses and conduct more destructive attacks. This convergence will continue to complicate attribution in 2025, making it harder for defenders to distinguish between ideologically driven attacks and financially motivated cybercrime, ultimately increasing the complexity of response and mitigation efforts.

### Erosion of Trust in Supply Chain Relationship

The dependency on third-party vendors remains a critical vulnerability. In 2025, we expect organizations to demand greater transparency and stricter security measures from vendors. Supply chain attacks in 2024 demonstrated how attackers exploit interconnected ecosystems, requiring a reevaluation of trust across industries.

# CYBERPROOF'S RECOMMENDATIONS

**The following proactive steps are recommended to reduce threat impact:**

### AI TO FIGHT AI

Implement AI-based security solutions that can detect and respond to AI-implemented attacks in real-time, including: (1) Develop or use Machine Learning countermeasures and Natural Language Processing (NLP) to detect advanced stealthy threats, such as regular Domain Generation Algorithm (DGA) domains, polymorphic malware, and granular malware behavior. (2) Create a baseline of the network traffic to look for anomalous activity, such as unexpected data transfers or incoming connections from unknown sources.

### KEEP UP TO DATE WITH THE GEOPOLITICAL THREAT LANDSCAPE

Ensure your defense tools track threat actors associated with countries that may target your industry. Keep up to date with industry-specific geopolitical developments and plan your cyber defense accordingly.

### IMPLEMENT BACKUP AND DISASTER RECOVERY PLANS

Have a comprehensive backup and disaster recovery plan in place to ensure the availability of critical systems in the event of a security breach or natural disaster.

### REGULARLY SCAN FOR VULNERABILITIES

Conduct regular vulnerability scanning to identify and address vulnerabilities – especially those on external-facing devices – to limit the attack surface.

### CREATE DETECTION RULES AND PLAYBOOKS

Implement detection rules and playbooks, keeping them up to date with current sophisticated ransomware attacks and system malfunction scenarios to deploy mitigation techniques.

### SEGMENT YOUR NETWORKS

Apply zero-trust principles to further segment your networks, minimizing the risk of lateral compromise. Implement separate networks for IT and OT systems to prevent potential breaches from spreading between environments.

### USE ENCRYPTION

Encrypt sensitive data and communications to protect against unauthorized access or data being intercepted or harvested.

### TRAIN EMPLOYEES ON SOCIAL ENGINEERING TECHNIQUES

Run phishing simulations using in-the-wild campaigns, so that employees get into the habit of recognizing and reporting phishing attempts and other suspicious activity.

CyberProof®, a UST company, delivers better security operations and drives superior experiences for enterprise customers. Our cloud-first, AI-powered approach to security, delivers industry-leading security services to drive real business results. We believe that working closely with our customers and partners through a "better security, together" services model, jointly empowers us to defend against the greatest of threats.

For more information, visit **cyberproof.com**.