RELIAQUEST®

The Road Ahead: 2025 Cybersecurity Predictions

ReliaQuest
Threat Research

ReliaQuest's top five predictions for how the cyber threat landscape will evolve in 2025, featuring changes to the ransomware scene, increased threats posed by AI, an uptick in non-human identity-based attacks, shifts in hacktivist tactics, and continued use of successful initial access techniques.

Executive Summary

Ransomware Attacks

Ransomware attacks are set to surpass 2024 levels, with a notable increase starting January 2025. This surge is fueled by more English-speaking affiliates joining ransomware groups, breaking the usual Russian holiday lull. Victim numbers will peak in May, with "RansomHub" overtaking "LockBit" as the top threat, expanding its market share from 15% to 40% by mid-year. "Meow" will persist with single extortion tactics, targeting 30 victims monthly. The rise in native English-speaking affiliates is likely to boost helpdesk social engineering and voice phishing (vishing) attacks, exploiting low user vigilance.

Large Language Model (LLM) Abuse

In 2025, we anticipate that 8–10% of our investigations will involve threat actors exploiting target organizations' large language model (LLM) tools. As more companies embrace LLMs for efficiency, the risks of data breaches, insider threats, and ransomware attacks will grow. Adversaries will leverage these LLMs for swift data access and vulnerability exploitation. While LLMs offer versatility and integration benefits, they also enable rapid damage by threat actors, underscoring the need for Automated Response Plays (ARPs) to ensure speedy containment.

Non-Human Identity-Based Attacks

ReliaQuest forecasts a 10% rise in non-human identity (NHI)-based attacks, threatening overprivileged accounts essential for automation. In 2024, 85% of ReliaQuest customer incidents involved service account abuse, a common NHI attack. As automation accelerates and machine identities increase, this trend is set to grow. The professional, scientific, and technical (PSTS) sector is particularly vulnerable due to its heavy reliance on automation and access keys.

Geopolitics and Hacktivism

Hacktivist groups are shifting beyond traditional DDoS attacks, increasingly turning to ransomware and data exfiltration, fueled by geopolitical tensions and social justice causes. The pro-Russian group "KillSec" has launched a ransomware service, and we anticipate similar actions from pro-Palestinian groups as the conflict involving Israel, Hamas, Hezbollah, and Iran escalates. Hacktivism linked to social justice issues is expected to rise. While often driven by geopolitics, growing social unrest and responses to environmental protests may push activist groups to adopt hacktivist tactics, including DDoS attacks, mass email bombings, and data leaks.

Top Techniques

In 2025, spearphishing, exploiting public-facing applications, and targeting external remote services will remain the top cyber attack techniques. These methods continue to succeed as organizations face evolving challenges like rapid vulnerability exploitation, resource constraints, human error, increased exposed credentials, and the expanding threat surface due to new technologies.

Increased Need for Automating Containment

Threat actors are becoming faster and more effective, allowing them to swiftly navigate networks and cause significant damage. Trends like increased exposed credentials, overprivileged non-human identity accounts, and integrating data tools into LLMs make accessing networks and targeting data easier. To counter this, organizations should implement automated incident response to quickly contain threats and thwart malicious objectives.

Table of Contents

2024 Overview

2024 was marked by organizations across all industries rapidly embracing two particular types of technology:

- Artificial Intelligence (AI)
- Cloud Infrastructure

As a result, organizations' attack surfaces have also grown significantly, introducing new challenges to defenders. New technologies have introduced new opportunities for threat actors to compromise corporate networks more swiftly. Despite these developments, ReliaQuest observed little change in the tactics, techniques, and procedures (TTPs) used by threat actors.

Last year, we predicted that 2024 would usher in a wave of AI abuse by threat actors.

We predicted they would use AI to scale their campaigns, reducing turnaround times by using it to write scripts, facilitating malware deployment across different operating systems. This prediction held true, as we observed several cases of AI-generated phishing emails, AI-generated malware, and a rise in deepfake use for social engineering campaigns.[1]

However, our AI-Powered Cybercrime report highlighted that AI hasn't introduced entirely new techniques; rather, it has enabled cybercriminals to enhance, quicken, and expand their capabilities. We expect this threat to persist, compounded by the risk associated with organizations integrating tools into large language models (LLMs).

Another notable trend in 2024 has been the decline of major ransomware groups such as "LockBit" and "ALPHV." Contrary to our 2023 prediction that LockBit would expand its victim count in 2024, an international law enforcement operation known as "Operation Cronos" in February 2024 dismantled LockBit's operations. This involved a "three strikes" attack:

- Infiltrating LockBit's systems to obtain its data
- Taking control of the network
- Locking LockBit out[2]

This year's report explores the new groups expected to fill this void and examines how these groups are collaborating with English-speaking threat actors to boost their social engineering efforts.

Remarkably, the top five attack techniques used by threat actors remained unchanged in 2023 and 2024, indicating the continued success of tried-and-true techniques.

In this report, we give you visibility into why these traditional techniques remain effective, particularly as organizations manage new external and internal challenges to their security posture.

Cross-Border Alliances: Ransomware's New Frontier

We anticipate more ransomware activity than normal in January 2025, breaking the usual lull during Russian public holidays thanks to more English-speaking ransomware group affiliates. Victim numbers are expected to steadily rise and peak in May, with monthly averages topping 2024 levels.

As former powerhouses ALPHV and LockBit decline, groups like "RansomHub," "Black Basta," "Meow," and "Akira" are poised to compete for dominance. RansomHub saw an 800% increase in activity in Q3 2024, capturing 15% of the market share, and could dominate 40% by mid-2025. Meanwhile, Meow's single-extortion tactics are projected to hit 30 victims a month before slowing down later in the year.

In late 2024, Russian ransomware groups collaborated with native English speakers, boosting their social engineering capabilities. In 2025, we anticipate more voice phishing (vishing) and fake IT helpdesk scams targeting English-speaking firms. Law enforcement action is likely to intensify, as Anglophone hackers operate with less impunity in the West.[3]

New Groups Fill the Vacuum

The international law enforcement operation in February 2024 against the once-dominant LockBit, along with ALPHV's dramatic exit scam in March 2024, caused significant volatility in data-leak site activity. From January to May 2024, the number of affected organizations increased steadily, peaking at 535 in May, as LockBit rushed to publish victims before further law enforcement disruption. Subsequently, the number of affected organizations dropped by 40% as ransomware groups, likely feeling less secure, either ceased activities or became more selective with their targets. In Q3 2024, there was a small 2% uptick from the previous quarter, driven by emerging ransomware groups like "RansomHub" attracting new affiliates.

As new ransomware groups occupy the space left by ALPHV and LockBit, we expect the total number of ransomware incidents to return to pre-2024 levels. Typically, January is the quietest month for ransomware due to public holidays in many Russian-speaking countries lasting until around January 8. During this time, Russian-language threat activity and forum posts usually come to a near standstill. However, in 2024 we observed evidence of increased activity by English-speaking affiliates. These affiliates are mainly based in countries like the US and UK, where festivities end earlier for the majority of the population. As such, we expect January figures to be higher than in previous years, as ransomware activity is no longer exclusively dominated by Russian-speaking threat groups.

Unlikely Partners

Before 2024, Russian-language ransomware groups like LockBit and "Evil Corp" dominated the cybercriminal scene, with LockBit even becoming the first ransomware group to name over 1,000 victims in a single year on its data-leak site in 2023. Historically, Russian-speaking cybercriminals often expressed on forums their reluctance to work with English speakers, dismissing them as untrustworthy and incompetent.

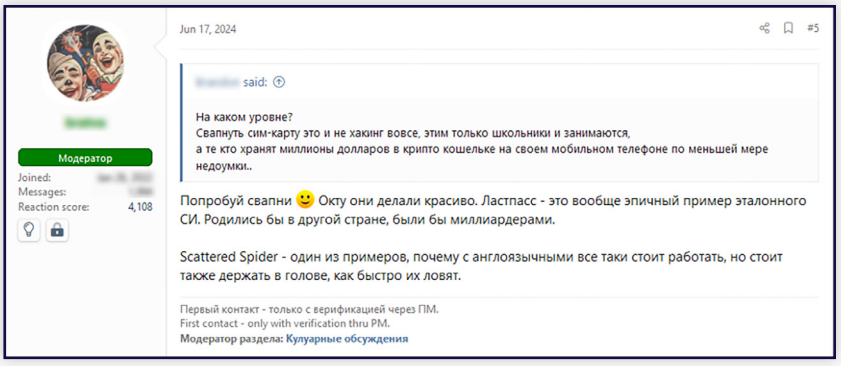


Figure 1: Forum user opines Scattered Spider shows why "it's still worth working with English speakers" although they get caught "quickly"

For example, one Russian-speaking forum user warned against collaborating with English-speakers, saying he found them "unreliable" and "difficult to establish communication" with. However, perspectives are starting to shift, with some Russian-speaking forum users pointing to "Scattered Spider" as an example of the potential benefits of partnering with English speakers.

This month alone we've investigated incidents that evidence this change in mindset. In October 2024, we observed a surprising collaboration:

The increasingly prominent ransomware group RansomHub—believed to have Russian-speaking affiliates who switched allegiances after the ALPHV exit scam—appeared to team up with the English-speaking Scattered Spider collective.

In this incident, the threat actor conducted a social engineering attack targeting an organization's help desk using vishing (voice phishing). Another notable incident involves the prolific threat group "Black Basta." It's highly likely that native English speakers were involved in their most recent social engineering campaign in which they debuted a new technique: using Microsoft Teams to communicate with targeted users.

Such attacks can only be pulled off with a high level of English fluency. Figure 2 shows a "job vacancy" posted on the prominent Russian-language cybercriminal forum XSS, where the poster is searching for English speakers to join a scam calling service. These services are designed to profit off English-speaking companies' lower levels of suspicion toward social engineering scams conducted by native speakers.

These incidents reveal a growing trend:

Russian-speaking threat actors are increasingly open to working alongside or hiring English-speaking cybercriminals. This willingness to collaborate with native English speakers is likely to result in increased leveraging of native-level English language skills in social engineering attacks.

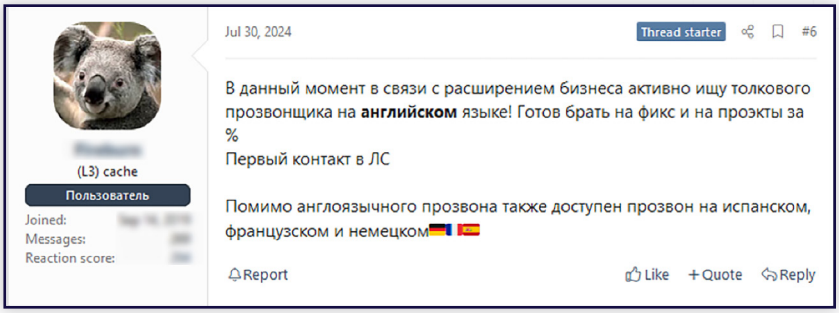


Figure 2: XSS user advertises vacancy for native English speaker to join scam call service

As a result, we expect to see more vishing and social engineering attacks targeting help desks. This would potentially allow ransomware groups to establish initial access and/or move laterally within networks, as observed in various customer incidents. However, these cross-border collaborations come with heightened risks of law enforcement crackdowns. This year, authorities in the UK, Spain, and the US have arrested members of Scattered Spider.[4] Now, ransomware groups must carefully consider the risks and rewards of partnering with English speakers.

Linux Under Fire

Another factor we anticipate will fuel increased ransomware activity in 2025 is a shift in operating system targets. In 2024, we observed more of a focus on Linux operating systems, enabling ransomware groups to successfully attack organizations previously beyond their technical reach.

> Over the past year, ReliaQuest has published almost 120% more intelligence on Linux-targeting malware compared to the previous year.

We've also seen ransomware groups like "Cicada," "Mallox," and "Play" expand their attacks to target VMware ESXi virtual machines (VMs) on Linux systems. It's realistically possible that this surge is driven by hackers using AI to tweak malware for different systems, some of which may have been beyond their technical capabilities until now, or by a strategic aim to maximize damage in enterprise environments.[5][6][7] The shift toward targeting Linux operating systems allows ransomware groups to attack more organizations, increasing their potential impact.

RansomHub's Meteoric Rise

Former affiliates of LockBit and ALPHV have moved over to emerging ransomware giants like RansomHub, which has also sought the skills of other affiliates like the Scattered Spider collective.

This influx of new talent and resources positions RansomHub as a formidable adversary in the cyberthreat landscape. RansomHub's rapid growth is expected to continue, as new affiliates show enthusiasm for their new group and are drawn to its appealing affiliate payment program, which offers a substantial 90% share of profits.

The number of organizations compromised by RansomHub surged by 800% in Q3 2024, making it realistically possible that the group will capture a 40% market share by mid-2025.

In October 2024, we investigated an intrusion for a customer in the manufacturing sector. We attributed the incident with high confidence to Scattered Spider, an English-speaking threat collective acting as an affiliate for RansomHub. Consistent with Scattered Spider's typical initial access method, the threat actor in this incident gained initial access by social engineering the organization's help desk. Initially the threat actor compromised the Chief Financial Office's (CFO) account by calling the helpdesk and requesting a password reset.

After realizing the account did not have access to Thycotic, a password vault, the threat actor requested a password reset for a domain administrator account with privileged access. Within six hours, the attacker began encrypting the organization's systems using a RansomHub encryptor.

This incident showcased the power of collaboration, which can even lead to the development of innovative social engineering techniques. It also confirmed suspicions that Scattered Spider had begun collaborating with RansomHub. We anticipate RansomHub will take the lead in 2025 as the most dominant ransomware group, particularly as it strengthens its capabilities by partnering with other threat groups.

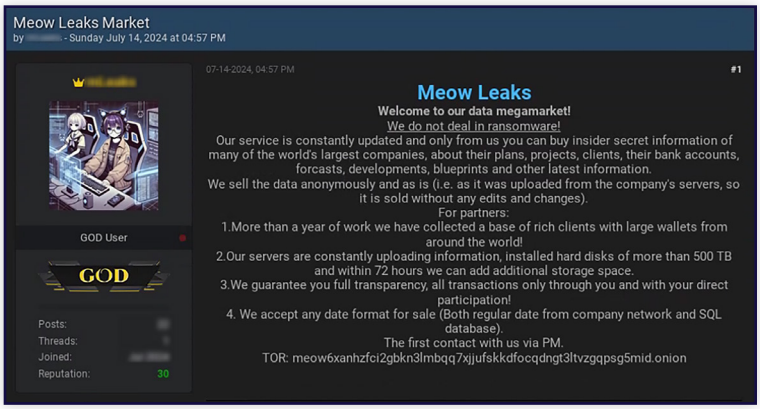


Figure 3: Meow Leaks Market advertises new "data megamarket" on prominent English-language cybercriminal forum BreachForums

Meow Scraps for Dominance

The rise of the "Meow" ransomware group in August 2022 marked a bold departure from the trend among ransomware groups of moving from single extortion to double- and even triple-extortion tactics. Initially, Meow focused on pure extortion, but by Q3 2024, the group pivoted its strategy away from encrypting data to selling exfiltrated information on its data-leak site, "Meow Leaks" and dark-web forums.

As illustrated in Figure 4, **Meow's activity has exponentially increased.** Given the group's momentum, it's likely its activity will continue to grow in the short-term.

However, this shift is likely to be short-lived due to the less lucrative nature of single extortion compared to double extortion. We previously predicted that single-extortion activity would increase. But, single-extortion groups typically do not last beyond one year, as affiliates and operators can earn more by disrupting operations via ransomware than via data theft alone.

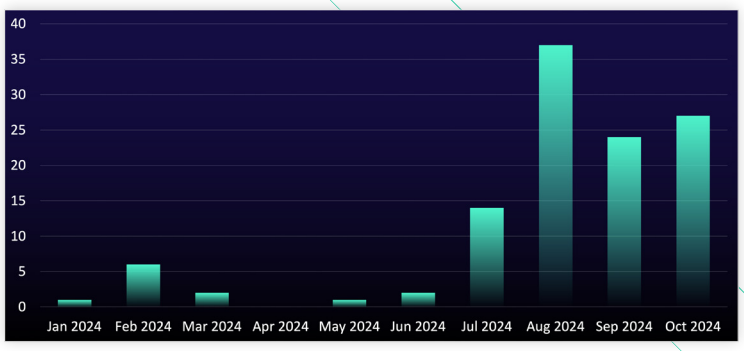


Figure 4: Meow activity rose dramatically, with numbers peaking at 36 organizations listed in August 2024

What's the Impact on Enterprises?

We anticipate that the changes in ransomware tactics that we detailed above will lead to more vishing attacks and fake IT help-desk scams. These techniques have only become prominent in the last year, so they are unlikely to arouse suspicion in targets, as user awareness is low. Employees are more likely to fall for phishing attacks, as a result. Meanwhile, threat actors are likely to capitalize on low user awareness and use this technique more frequently in 2025. To counter these novel threats, defenders will need to implement new detections and mitigations to ensure their systems stay safeguarded. The increased collaboration between Russian- and English-speaking threat actors will likely boost the effectiveness of social engineering campaigns, as targeted individuals may not be as vigilant when confronted with an English speaker. Our research shows that ransomware groups such as "Black Basta" and RansomHub have had success in using these techniques to gain initial access, ultimately significantly increasing the likelihood of ransomware deployment. By targeting help desks, ransomware groups can infiltrate highly privileged accounts and gain access to sensitive data and systems. The impact of such ransomware attacks is considerably more damaging to organizations than if less privileged accounts were compromised.

As prominent ransomware groups compete for notoriety, they will likely engage in "big game hunting," targeting large, well-known corporations. Groups like Black Basta, which typically targets major organizations in the professional, scientific, and technical services (PSTS) and manufacturing sectors in the US, are leading the charge. Critical infrastructure, like VMware ESXi VMs, is at risk, threatening significant business disruptions to the operational technology (OT) the manufacturing sector relies on. The PSTS sector is an appealing target because of its vast stores of sensitive data, making it especially susceptible to supply-chain vulnerabilities. Targeting these weaknesses gives ransomware operators more leverage during negotiations. However, the impacts extend beyond this sector: All sectors must remain vigilant against third-party compromises stemming from vendors within the PSTS industry. Thoroughly vetting vendor security and ensuring solid third-party insurance coverage are essential steps in mitigating these risks.

Countering the Threat with ReliaQuest

Our security operations platform GreyMatter provides behavioral analytics, which, in a volatile threat landscape, is more effective at detecting threat activity. Threat groups—whether mature or emerging—typically follow specific behavioral patterns when conducting attacks. Deploying behavior-based detection methods will enhance the ability to identify and respond to malicious activities because they detect malicious activity, rather than artifacts belonging to specific threat groups. This facilitates the detection of new and lesser-known threat groups when suspicious behavior is identified in networks. Additionally, GreyMatter's threat feeds ingest the latest indicators of compromise (IoCs) associated with different threat actors, ensuring our signature-based alerting is always up to date.

Fortify Your Security Posture By:

Blocking JavaScript Execution via wscript.exe: Malware strains like "SocGholish" or "GootLoader," used to download further payloads, often precede ransomware attacks. Simply and effectively stop JavaScript-based malware from executing by setting .JS files to open with notepad.exe instead of wscript.exe, deterring user execution.

Hardening JML and Role-Based Access Control Policies: Implement strong joiners, movers, and leavers (JML) policies to promptly update or revoke access rights when employees change roles or leave the organization. Use role-based access control (RBAC) to ensure users have only the access necessary for their roles, especially concerning Windows Command Shell or PowerShell. This approach minimizes the risk of attackers exploiting outdated or overly privileged accounts, thereby limiting their ability to locate and encrypt sensitive data.

Defending Against Phishing via Teams: Organizations can protect against phishing attacks conducted via Microsoft Teams by disabling communication from external users to prevent unwanted messages. When external communication is necessary, only specific trusted domains should be allowlisted. Additionally, implementing aggressive anti-spam policies and ensuring logging is enabled for Teams, especially for the "ChatCreated" event, will help detect and investigate suspicious activities.

LLMs: Balancing Innovation with Risk

In 2025, we expect 8-10% of our investigations to involve threat actors abusing internal large language model (LLM) tools. As more companies adopt LLMs for efficiency, the risks of data breaches, insider threats, and ransomware attacks will intensify. Adversaries will use these LLMs to access data faster and exploit vulnerabilities.

AI Arms Race

By late 2024, market analysts were labeling AI as a "bubble," predicting its imminent "pop."[8] Nevertheless, organizations—especially those with existing LLM subscriptions—continue to seek increased productivity and efficiency through AI.

63% Surveys indicate that 63% of organizations with annual revenues exceeding $50 million regard generative AI as a top priority.

Yet **91%** admit they don't feel "very prepared" to implement it responsibly.[9] As a result, it's realistically possible that organizations rush implementation, inadvertently leaving themselves exposed to new cybersecurity risks.

The Risk of Easy AI Data Access

Organizations are integrating tools like cloud storage and databases into LLMs, enabling natural language queries. This consolidates access to multiple tools into one searchable platform, simplifying the process for employees—and threat actors—to find sensitive data. While this streamlined data querying allows for improved convenience, it also shortens the time a threat actor needs to go from initial access to impact.

In the past, adversaries needed prior knowledge or discovery efforts to locate sensitive data. Now, with access to a misconfigured LLM or a privileged user's account, a ransomware actor, for example, can simply use plain English queries to locate and access sensitive data. Consequently, LLMs are likely to become threat actors' first port of call when searching for sensitive information, leading to more incidents involving this technique. It's also important to consider that LLMs significantly heighten insider risk. Users might inadvertently access unauthorized data or accidentally expose sensitive information to the LLM vendor. Such breaches can expose critical data that threat actors could exploit in their attacks.

AI Weak Spots: The Vulnerabilities of LLMs

LLMs have weaknesses beyond misconfigurations. OpenAI's "Memories" feature in ChatGPT, which allows the model to remember information across chats, has been exploited for prompt injection and data exfiltration, even after patches.[10] Other vulnerabilities like CVE-2024-7475 allow hackers to tweak Security Assertion Markup Language (SAML) configurations and log in as unauthorized users.[11] These critical flaws reveal the serious risks tied to using LLMs.

Despite efforts by LLM vendors to patch vulnerabilities and create safeguards, LLMs continue to be vulnerable to prompt injections, in particular. "Do Anything Now" (DAN) prompts are designed to exploit AI filtering weaknesses by using manipulative language and taking advantage of contextual loopholes. Disguised as games or stories, they embed commands in broader contexts to evade detection, much like social engineering. By appealing to AI's curiosity or desire to help, they bypass safeguards and "trick" the LLM into giving a response which contradicts the vendor's security policies. Cybercriminals frequently share DAN prompts on cybercriminal forums (see Figure 5) and platforms like GitHub, making them easily accessible to threat actors who wish to abuse LLMs as part of their attacks.

Both researchers and threat actors have found ways to trick LLMs by modifying prompt spellings (for instance, asking for an "3xploit" instead of an "exploit") or by encrypting malicious instructions to create vulnerability exploits.[12] The natural language querying that LLMs are designed to process increases the complexity of creating safeguards, as developers must anticipate the countless ways threat actors might manipulate a chatbot.

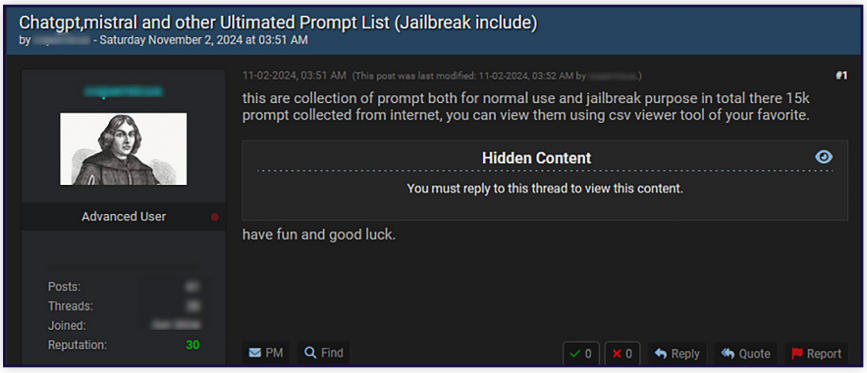


Figure 5: A BreachForums user shares jailbreaking prompts for several LLMs

Organizations using outdated versions of LLMs risk their tool being abused by threat actors familiar with known vulnerabilities. For instance, if a threat actor gains access to a device running an older version of ChatGPT, they may be able to execute malicious code directly from the LLM.

Data Risks in LLM Fine-Tuning and Vendor Exposure

During fine-tuning, developers may inadvertently expose sensitive data by including it in training data, making it an accessible part of the LLM's memory.

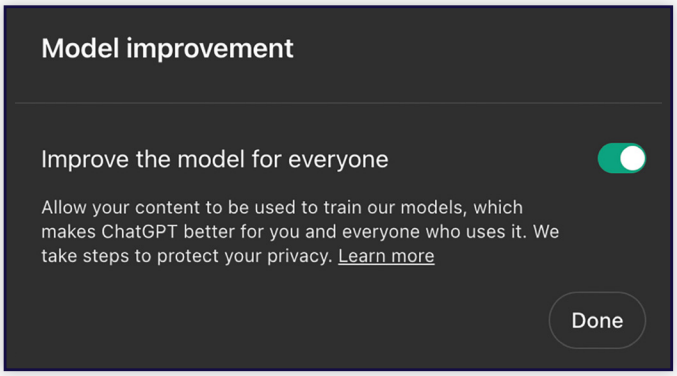


Figure 6: ChatGPT toggle to "opt out" of allowing a user's content to be used to train models

This risk is greater for technically mature businesses using custom LLMs, as custom models demand extensive internal training data. Additionally, there's a risk with LLMs when sending sensitive data to vendors.

By default, inputs are processed and stored on vendor servers unless users "opt out" (see Figure 6). Organizations that share sensitive data with LLM vendors risk their data becoming part of the LLM's "memory," potentially exposing it to other users accidentally or through breaches if the LLM vendor is targeted by cyber attacks and lack proper data encryption measures.

What's the Impact on Enterprises?

The repercussions of data exposure—whether through insider risks or misconfigurations—are well-known but worth repeating. Financially, breaches can lead to hefty fines, recovery costs, and lost revenue. Legally, companies may face lawsuits and regulatory penalties for failing to safeguard sensitive data. Reputationally, a breach undermines trust with customers and partners, potentially causing long-term damage to brand image and customer loyalty. In addition, LLM vendors issue API keys, but this comes with risks.

An API key being exposed could be costly:

LLM vendors charge customers per token, with one query typically equaling one token, and prices varying by vendor. If a company's LLM API key is leaked, hackers could flood the API with automated requests, causing outages and sky-high costs. This simple attack is immensely effective and could be exploited by hacktivists or insider threats aiming to financially harm a company.

LLM flaws can help threat actors execute malware, establish persistence, and exfiltrate data. Malicious commands could be stored in an LLM's long-term memory, allowing continuous data exfiltration to an external server via a command-and-control (C2) connection.[13] When organizations integrate multiple tools into an LLM, adversaries can move faster within a network once a vulnerability has been successfully exploited, reducing the time from initial access to impact. This speed highlights the importance of logging all LLM-accessed tools and implementing automated incident response to quickly contain threats and reduce damage.

As employees embrace the productivity benefits of generative AI, the risk of data leaks increases if companies don't ensure safe access to LLMs. **A survey by the US National Cybersecurity Alliance (NCA) found that:**

38% of organizations with annual revenues exceeding $50 million regard generative AI as a top priority.

52% lack training in safe AI practices.[14]

Such negligence could result in major data breaches, particularly since prompts in LLMs like ChatGPT cannot be deleted from chat history.[15] To avoid costly breaches, businesses are investing in secure LLM access, seeing it as a cheaper alternative to handling a significant data breach. However, due to the risk of data exposure to vendors, organizations should keep LLM vendors' data-sharing policies top of mind during the procurement process.

Countering the Threat with ReliaQuest

While LLMs offer versatility and the benefits of tool integration, they also enable threat actors to rapidly inflict damage, far outpacing the capabilities of an average security operations center (SOC). To effectively counter this threat, organizations should adopt automated incident response by implementing GreyMatter Automated Response Playbooks. These Playbooks considerably reduce the mean time to contain (MTTC) threats by automating containment actions, halting threat actors in their tracks as they attempt suspicious activities.

By doing so, organizations can drive their MTTC down to as low as five minutes. A short MTTC is crucial for preventing threat actors from maintaining access or further infiltrating a network and achieving their objectives. To guard against API abuse, GreyMatter Digital Risk Protection (DRP) detects API key exposure, allowing you to rotate keys before they can be exploited by threat actors.

Fortify Your Security Posture By:

Managing Training Data Wisely: Treat training data as the "memory" of an LLM. Ensure it only includes information accessible to users, and avoid using sensitive data to prevent unauthorized access. Limit what data LLM vendors can collect by opting out of vendor data training use, and ensure LLM application logs are visible to security tools.

Implementing Two-Factor Authentication and Individual User Accounts: Enforce two-factor authentication (2FA) for LLM access and queries to prevent unauthorized entry with stolen credentials. To prevent insider threats, assign individual user accounts tailored to specific roles and regularly update privileges to reflect role changes, avoiding over-privileged access.

Preventing Prompt Injection: Implement hard-coded defenses like input/output filtering to block prompt injections and reduce hallucinations. For instance, ensure hard-code instructions execute Python code in isolated containers to avoid malicious or faulty code execution.

Aliens Among Us: The Dangers of Non-Human Identities

We anticipate a 10% increase in non-human identity (NHI)-based attacks resulting from organizations' expanding use of automation, APIs, and cloud infrastructure. In 2024, service account abuse—one of the most prevalent forms of NHI attack—was a factor in 85% of ReliaQuest customer incidents. This trend will likely intensify as the pace of automation accelerates and machine identities proliferate.

What Are NHIs?

As organizations advance in their use of API integrations, automation, and cloud infrastructure, they become more susceptible to non-human identity (NHI)-related breaches. Unlike traditional attacks that exploit human identities (think business email compromise [BEC]), **NHI attacks target machine identities like API keys, Secure Shell (SSH) keys, service accounts, and digital certificates.**

These NHI credentials can be exposed online in several ways. Developers might inadvertently include them in public repositories like GitHub because of oversight or improper version control. Hardcoding credentials in application source code heightens exposure risk, especially if the code is shared or leaked. Misconfigured access controls on cloud services or databases can also lead to unauthorized access.

Additionally, information-stealing malware (infostealer) attacks or compromised development environments may result in credential theft. Once exposed, malicious actors can locate and exploit these credentials to gain unauthorized access to systems and data, risking security breaches and data loss.

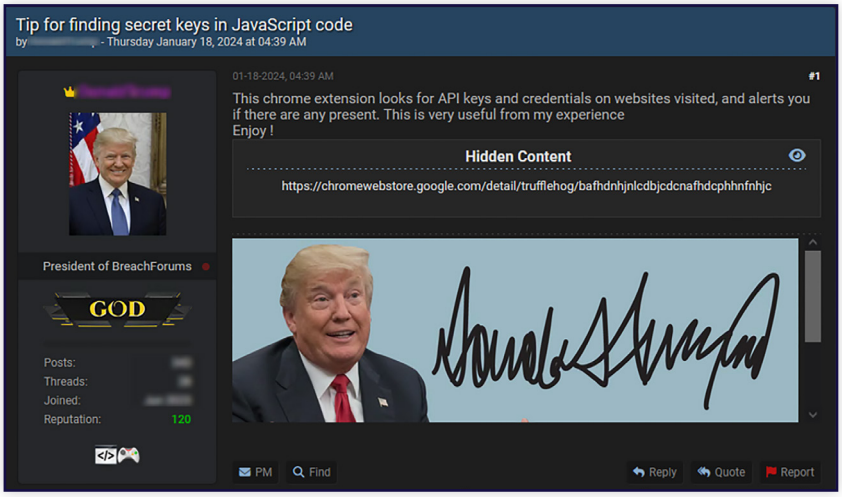


Figure 7: BreachForums user shares Chrome extension which searches for API keys and credentials

Pivoting from NHI

In an NHI attack, a cybercriminal can target a network by exploiting vulnerabilities in NHIs, such as Internet of Things (IoT) devices. These devices, such as smart thermostats or security cameras, have assigned machine identities to authenticate and communicate within a network. The attacker gains unauthorized access by intercepting weak or default credentials, allowing them to impersonate the device and blend in seamlessly within the network. Once inside, the attacker can move laterally across the network, accessing sensitive data and potentially causing widespread disruption.

NHIs Run Wild

The growing number of NHIs and reliance on manual management practices create serious operational and security risks. For instance, manually updating identity credentials or permissions can lead to inconsistencies, leaving some identities with outdated security settings. Since NHIs are essential for automated tasks and processes, organizations often prioritize business continuity over security. This means NHI credentials aren't always handled as carefully as human ones—they're often poorly stored, shared without proper security, and rarely rotated. To complicate matters, multifactor authentication (MFA) can't be enforced for NHI accounts, as they're used for processes requiring no human intervention, leaving them vulnerable to direct account takeovers.

NHI-based attacks are tough to detect because these identities usually have high privileges and perform routine tasks that look legitimate. This predictable activity can mask malicious actions, making it hard for traditional security tools to tell the difference. As a result, NHI breaches can remain under the radar for hours or days, giving attackers plenty of time to move laterally, establish persistence, and maximize attack impact.

In Demand: Service Accounts

Service accounts are an example of an NHI that's frequently targeted by threat actors due to their versatility and extensive access privileges. To avoid access issues, organizations often grant service accounts excessive privileges, bypassing the need for separate accounts for different tasks.

However, this also makes them a single point of failure. If one service account is compromised, hackers can quickly take over the whole system, instantly enjoying top-level access without needing to escalate privileges. At present, around 85% of incidents investigated by ReliaQuest involve service account compromise.

We predict that the overall number of incidents involving NHI-based attacks, including service account abuse, will increase to 95% in 2025. This trend underscores the critical need for robust security measures to protect these high-value targets.

In April 2024, we identified a Kerberoasting attack in a customer's environment, marking the onset of a "BlackSuit" ransomware incident. Kerberoasting exemplifies an NHI attack technique, as it specifically targets service accounts. A Kerberoasting attack is a cybersecurity technique where attackers use legitimate user credentials to request and extract encrypted Kerberos service tickets from a Key Distribution Center (KDC) to crack offline and obtain service account passwords.

The attack encrypted critical systems and exfiltrated sensitive data. Active since May 2023, BlackSuit has targeted US-based companies across key sectors using a variety of methods. Our investigation revealed that BlackSuit used PsExec for lateral movement, Kerberoasting for credential access, and file transfer protocol for data exfiltration.

This incident revealed key vulnerabilities exploited by the attackers. The "admin1" account had a service principal name (SPN), making it vulnerable to Kerberoasting, where attackers extract service account credentials. The quick compromise of this account highlights the need for strong encryption and passwords. Plus, its excessive domain admin privileges gave attackers full control.

What's the Impact on Enterprises?

NHIs are vital for scaling business operations, driving efficiency through automation, cloud storage, and tool integration. They're particularly important for software-as-a-service (SaaS) vendors and organizations using IoT devices or operational technology (OT).

However, a compromised NHI can lead to major financial losses. With highly privileged accounts like service and system accounts at risk, attackers can initiate unauthorized processes, escalate privileges, disable logging, and more. These actions, coupled with the difficulty of detecting NHI compromise, enable adversaries to deploy ransomware, steal or erase data, and install backdoors—resulting in steep remediation costs, fines, and damages. Organizations also face reputational damage, higher insurance premiums, and operational downtime.

NHIs encompass IoT devices, virtual machines, and service accounts, forming the backbone of OT. Disabling these can halt essential automated processes and sensor functions, incurring high costs and physical risks. **For example:**

Compromising factory temperature sensors could significantly increase fire risks.

Sector at Risk: PSTS

PSTS organizations rely on thousands of NHIs for automation, APIs, and cloud services. These identities include service accounts, API keys, and scripts. The volume of NHIs significantly increases organizations' attack surface, making it easier for attackers to find vulnerabilities. The heavy use of cloud services by PSTS organizations for data storage, processing, and collaboration, as well as the scalability, also introduces risks like misconfigured resources, exposed access keys, and insecure APIs, which can be exploited.

These organizations are prime targets for threat actors due to their vast repositories of sensitive data. Between January and October 2024, we noted a 19% rise in NHI-related alerts in the PSTS sector compared with the previous ten months (see Figure 8). These alerts highlighted exposed access keys and expired certificates, posing a risk of unauthorized access to infrastructure or data.

For example, an exposed RSA private key could grant third parties entry to a private network, while a MySQL connection string might expose an internal database, revealing sensitive information like account credentials, which can be exploited in future attacks.

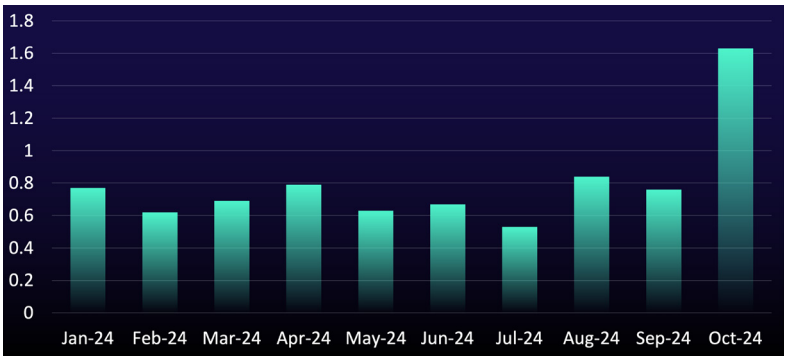


Figure 8: Percentage of NHI-related alerts for the PSTS sector

Countering the Threat with ReliaQuest

GreyMatter DRP detects exposed API keys and credentials across both the clear and dark web, swiftly alerting customers for rapid action. This proactive detection allows organizations to preemptively rotate credentials and identify data leaks, effectively preventing the abuse of valid credentials by threat actors. In addition, GreyMatter DRP monitors data leaks, brand impersonation, and threat actor activities, delivering comprehensive insights to help mitigate digital threats.

Fortify Your Security Posture By:

Using API Gateways: Prevent unauthorized API calls by implementing API gateways. In Amazon Web Services (AWS), generate Secure Sockets Layer (SSL) certificates to verify that HTTP requests originate from the API Gateway, ensuring only authorized users can access API keys.

Implementing Robust Secrets Management: Securely store and manage API keys, SSH keys, tokens, and other credentials using tools like HashiCorp Vault, AWS Secrets Manager, or Azure Key Vault. Regularly rotate keys and enforce strict access- and role-based controls to prevent unauthorized access and limit credential validity.

Auditing Service Accounts: Maintain an accurate inventory by identifying and documenting all service accounts in your environment. Additionally, catalog current service account permissions to identify and adjust over-privileged accounts, granting only necessary access. Deregister accounts with service principal names (SPNs) if they are no longer needed to reduce potential attack surface, as accounts with registered SPNs are vulnerable to Kerberoasting attacks.

Geopolitics and Hacktivism

In 2025, hacktivist groups are expected to rely less on distributed denial of service (DDoS) attacks, favoring tactics like ransomware and data exfiltration. This aligns the growing trend of using tools like the leaked "LockBit 3.0" builder for ransomware attacks or teaming up with established ransomware groups.[16] The pro-Russian hacktivist group "KillSec" has launched its own ransomware service, and we anticipate similar moves from pro-Palestinian groups as the conflict between Israel and Hamas, Hezbollah, and Iran continues to escalate.

We forecast an increase in hacktivism driven by social justice issues. While often tied to geopolitic events, rising social unrest and police crackdowns on environmental protests may push activist groups to adopt hacktivist tactics. These could include DDoS attacks, mass email bombings, and data leaks.

Ransomware—Hacktivists' Silver Bullet?

The open-source availability of ransomware builders and other offensive tools has made ransomware-as-a-service (RaaS) more accessible than ever.

As a result, hacktivist groups have begun launching their own ransomware services. The pro-Russian hacktivist group "KillSec," which first became active in 2021 originally as a loosely affiliated member of the Anonymous movement, initially focused its activities on website defacements and data breaches.

However, in June 2024, KillSec diversified its operations by introducing a RaaS program. This initiative allows even less technically skilled cybercriminals to participate in cyber extortion using customizable ransomware variants (see Figure 9).

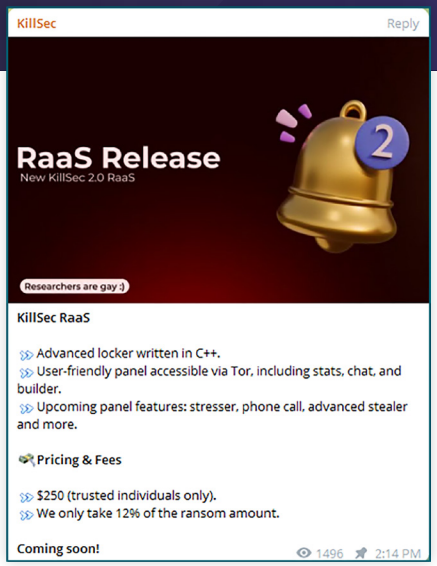


Figure 9: KillSec advertises second version of a RaaS platform on Telegram

We predict that in 2025, more hacktivist groups, including pro-Palestinian groups, will begin to engage in financially motivated cybercrime. Ransomware attacks serve hacktivist groups' dual objectives of attracting attention and causing damage to their targets' infrastructure and wealth sources, while also funding their campaigns by raising cryptocurrency. This shift will likely increase hacktivist activity by providing hacktivists with a means to earn a living while advocating for their causes, rather than engaging in hacktivism solely on a voluntary basis. Moreover, ransomware and data exfiltration attacks will likely gain more attention than DDoS attacks, which have become commonplace and, therefore, attract less media attention after several years of intense hacktivism.

Hacktivism in the Middle East

Cyber attacks play a major role in the ongoing Middle East conflict. High-profile incidents like the detonation of Hezbollah's telecom devices in Lebanon show the physical dangers of cyber compromises. Hacktivist groups on both sides of the conflict, including "Cyber Toufan," "Anonymous Sudan," and "CyberAv3ngers" are actively targeting each other, ramping up regional cyber warfare. As the conflict escalates in Lebanon, we can expect more cyber attacks and the emergence of new hacktivist groups opposing Israel. This escalation will likely push hacktivist groups toward more destructive tactics, including ransomware attacks.

Even with efforts to resolve the conflict, hacktivist activity is unlikely to waver. The region's complex geopolitics mean these groups are unlikely to be satisfied with resolutions and will highly likely continue cyber warfare, viewing any ceasefire or peace agreement as unjust. Staying informed about geopolitical changes and related cyber threats is crucial for organizations to effectively manage these risks.

Impact of New US Presidency

With Donald Trump serving as US president, we anticipate a surge in cyber attacks from pro-Palestine hacktivists and Iranian advanced persistent threat (APT) groups, fueled by his pro-Israel stance and, therefore, the US government's stance on the conflict in the Middle East. Western and Israel-linked targets could face increased threats from pro-Palestinian hacktivist groups aiming to inflict damage on opposition networks and raise awareness for their cause.

In the context of Russian-Ukrainian cyberwarfare, we also expect to see disruptions. Trump's less supportive stance on Ukraine will likely lead to a decrease in Russian APT attacks on the US, while pro-Russian hacktivists will highly likely ramp up attacks on Ukraine and NATO.

President Trump has expressed a desire to enter into negotiations with Russia to end the war in Ukraine, which could further spur hacktivists on both sides.[17] Financially motivated Russian cybercriminals primarily targeting the US are likely continue their activities as usual, as their motivations are not directly tied to geopolitics.

Rising Social Unrest

In 2025, social unrest is expected to escalate due to the Israel-Hamas-Hezbollah conflict, disinformation, and anti-immigration sentiment. These issues, along with economic worries from a cost-of-living crisis and fears about AI-induced job displacement, have fueled protests worldwide. As traditional protest methods often face police intervention, social justice protesters may increasingly turn to hacktivist methods to amplify their impact.

Figure 10: Extinction Rebellion launches "Digital Rebellion" campaign targeting the insurance industry for their involvement with fossil fuels

In the US, Trump's proposed crackdown on pro-Palestinian campus protests[18] and his hardline stance on protest movements could lead to more arrests. As a result, domestic activists, including climate change groups, may turn to hacktivism tactics for anonymous protest and disruption against perceived harmful businesses.

Groups like Extinction Rebellion have already launched Digital Rebellions—a digital campaign against the insurance industry for its role in insuring fossil fuels—using email spamming, mass phone calls, and social media storms. These disruptive methods, which require minimal technical skill, could gain wider traction among climate activists.

Additional strategies may include DDoS attacks, website defacement, and data theft, similar to a breach on Disney in July 2024 where attackers, aided by an insider, exfiltrated 1.1TB of confidential information from the messaging app Slack to protest Disney's use of AI-generated art.

What's the Impact on Enterprises?

Israeli government and military bodies, along with key industries like finance and insurance, utilities, telecommunications, and PSTS are prime targets for cyber attacks aimed at destabilizing Israel's economy and global reputation. In the broader region, sectors such as utilities, health care, and transportation will likely face DDoS or ransomware attacks to amplify the effects of military strikes, not only causing operational disruptions but also financial damage.

Organizations with business ties to Israel, including those buying or selling Israeli products, maintaining offices there, or providing financial services to Israeli companies, are at high risk of hacktivist attacks from pro-Palestinian threat actors. Similar threats exist for connections to Iran, although these are less prevalent in the US and Europe. Even without direct links to Israel, organizations face a significant risk of supply-chain compromise if their partners are targeted, potentially leading to data breaches and reputational and financial harm.

Environmental hacktivism will highly likely affect the mining, quarrying, and oil and gas sectors, which have historically been frequent protest targets, though mainly through physical demonstrations. The finance and insurance sector has attracted increased protester attention in 2024 for insuring oil and gas companies.[19] These sectors are all highly probable targets for DDoS and data exfiltration attacks, as protesters seek to disrupt operations and tarnish reputations. Additionally, organizations facing protests and hacktivism by environmental groups will likely incur increased physical security and cyber insurance costs.

Organizations running high-profile events, such as those in the arts, entertainment, and recreation sector, are likely to be targeted by website defacement attacks and DDoS attacks, particularly from environmental protest groups aiming to raise awareness. Such attacks could lead to operational downtime and reputational damage, often coinciding with physical protests that introduce additional risks.

Countering the Threat with ReliaQuest

By continuously monitoring network activity, GreyMatter can detect unusual patterns that point toward a ransomware attack, enabling immediate intervention to prevent encryption of critical data. GreyMatter's Automated Response Playbooks help to rapidly isolate affected systems and block malicious IP addresses, mitigating the attack's impact. Additionally, the GreyMatter Intel feature helps your organization stay up to date on hacktivist and ransomware activities, allowing you to filter by sector and geography to access relevant intelligence updates.

Fortify Your Security Posture By:

Implementing DDoS Defenses: Employ a multi-layered security approach to guard against DDoS attacks. Use network tools like firewalls and intrusion prevention systems, along with services like Content Delivery Networks (CDNs) and DDoS protection, to absorb and filter malicious traffic.

Employing Rate Limiting and Throttling: Configure email servers to limit the number of emails accepted from a single source within a specific timeframe. This will help mitigate the impact of mass email campaigns, which are often used by environmental groups, by slowing down their delivery rate.

Deploying DRP for Company Mentions: Establish an effective DRP strategy to continuously monitor your organization's assets online. GreyMatter DRP scans the dark web, Telegram, and other sources to detect mentions of your organization or its supply-chain partners by hacktivist groups. This allows you to proactively react to oncoming threats by taking additional steps to strengthen ransomware or DDoS protections, for instance.

Initial Access: Same Techniques, Different Challenges

Spearphishing with links and attachments, exploiting public-facing applications, and abusing external remote services will remain the most common initial access techniques in 2025.

Threat actors will continue to find success using these tactics as organizations grapple with new external and internal challenges that limit their network defenses.

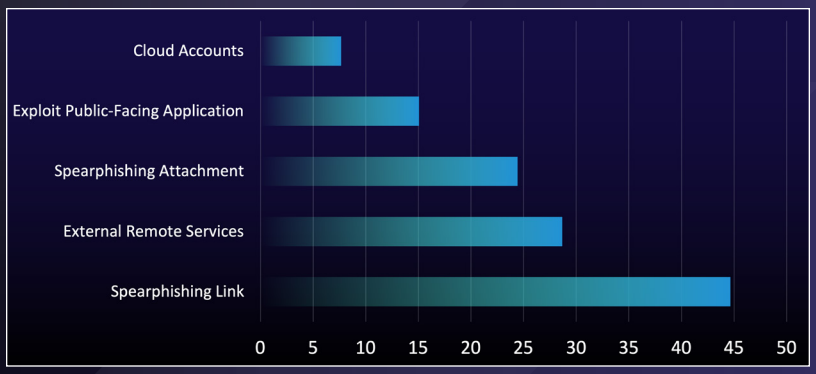


Figure 11: Percentage of initial access techniques used in customer incidents in 2024

Little Change in Initial Access

This year, threat actors stuck with tried-and-tested initial access techniques, such as spearphishing with links or attachments, exploiting public-facing applications, and abusing external remote services, as shown in Figure 11. These techniques have consistently ranked among the top five methods since 2023, proving that well-known strategies can still be highly effective. However, the real game-changer in cybersecurity is an organization's ability to defend against these threats. Despite technological advancements, human error, budget constraints, and an ever-expanding attack surface driven by innovation keep threat actors from needing to make drastic changes. While organizations continue to struggle with effective network protection, threat actors adapt to evolving technologies with ease.

Breakneck Vulnerability Exploitation

In 2024, we noted a 14.3% increase in the average monthly number of published vulnerabilities compared to 2023, as illustrated in Figure 12. This spike allows threat actors to exploit a growing array of applications for initial access, lateral movement, or further exploitation.

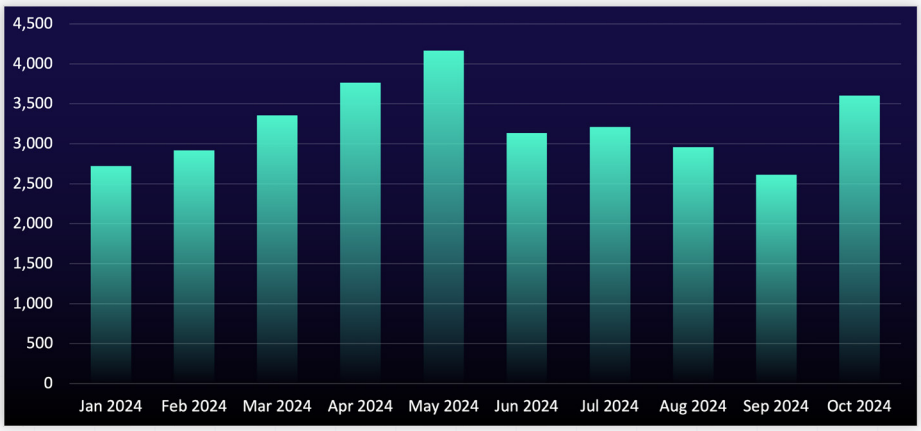


Figure 12: Number of published vulnerabilities is gradually increasing since January 2023

We've also seen the average time to exploit vulnerabilities plummet from 40 days in 2023 to just 18 days in 2024—a 45% decrease.

This trend puts defenders under immense pressure to patch vulnerabilities quickly, which is already complicated by limited resources and the risk of operational downtime. Consequently, many organizations are forced to prioritize certain patches, leaving some vulnerabilities unaddressed and open to exploitation.

Human Fumbles and Resource Demands

Despite technological advancements, human mistakes and resource constraints remain big hurdles. Many organizations struggle with under-resourced cybersecurity teams and rising costs related to data breaches and cyber insurance. CISOs often find themselves frustrated as boards of directors may assume that a lack of breaches equates to sufficient protection, leading to inadequate resources for cybersecurity.

Insufficient budgets for the necessary tools impact an organizations' ability to detect, investigate, and respond to cybersecurity incidents, giving threat actors more time to operate within a network undetected. Crucially, this lack of resources also weakens an organization's defenses against initial access techniques, enabling threat actors to continue exploiting the same techniques effectively.

New Technologies

New technologies, such as cloud infrastructure, Single Sign-On (SSO), and generative AI, have significantly broadened the attack surface. Keeping up with patches and updates is a constant challenge, often leaving security gaps for attackers to exploit. Techniques like exploiting public-facing applications and external remote services will likely remain prevalent, as vulnerabilities in Virtual Private Networks (VPNs) and remote monitoring and management (RMM) tools are exploited, allowing attackers initial access and persistence.

Leaked Creds Kill Street Cred

Infostealer malware poses a major risk by harvesting sensitive information.

101% In 2024, the average monthly alerts for "Credential Exposure" and "Evidence of Credential Access" among clients skyrocketed by an impressive 101% compared to 2023.

This number is expected to increase in 2025, as infostealer malware becomes more widespread. Stolen data sold on dark-web markets provides attackers with easy initial access.

Infostealers infiltrate systems and harvest credentials, which are then shared or sold cheaply online, making corporate credentials available for as little as $10. Without strict MFA, organizations face the risk of attackers gaining direct network access using these exposed credentials. This is particularly damaging if the exposed credentials pertain to an external remote service, such as a VPN. Exposed VPN credentials can grant unauthorized users access to a corporate network, enabling them to move laterally and deploy malware.

What's the Impact on Enterprises?

The growing number of vulnerabilities increases the risk of cyber attacks, leading to data breaches and financial losses. Exploiting critical vulnerabilities enables attackers to execute malware, escalate privileges, exfiltrate data, or conduct Man-in-the-Middle (MitM) attacks, which can disrupt operations and damage reputations.

Addressing these gaps requires substantial cybersecurity investments, straining budgets and diverting focus from core business goals. In regulated industries, unpatched vulnerabilities can result in non-compliance with data protection laws, triggering legal penalties and further damage. In 2025, managing and monitoring numerous cybersecurity tools will continue to challenge organizations, contributing to the enduring success of traditional initial access techniques.

The costs associated with multiple security tools, combined with the overwhelming volume of alerts generated from the tools, place significant demand on resources and lead to "alert fatigue" among analysts, who must juggle multiple platforms at once. This complexity makes incident investigations cumbersome for analysts, as they are required to constantly switch between tools to gain full event visibility. This highlights the importance of streamlining security operations. Without investing in integrated solutions, organizations risk a slow MTTC, which would allow attackers more time to infiltrate networks and cause damage.

As organizations adopt more tools and technologies, the risk of commercial applications used for malicious operations (CAMO) increases. CAMO involves exploiting the legitimate functionality of software for malicious aims. From January to August 2024, 60% of our critical hands-on-keyboard incidents involved legitimate tools—a 16% increase from 2023. Adversaries will likely continue to use commonly abused legitimate tools like AnyDesk and PDQ Deploy, while also exploring new IT tools such as RMM, software deployment, and network scanners. Using CAMO tools allows attackers to remain undetected, because these tools often serve legitimate purposes and come with valid code-signing certificates, enabling them to bypass security measures.

Many organizations lack comprehensive tool inventories, leading to confusion between malicious and benign activities, complicating detection and response. This oversight then increases dwell time and risks data exfiltration or encryption.

Countering the Threat with ReliaQuest

GreyMatter integrates various security functions into a unified ecosystem, eliminating the need for disparate solutions. This consolidation enhances threat detection and response, streamlines operations, and reduces complexity. With comprehensive visibility and control, along with Automated Response Playbooks, GreyMatter enables the detection, investigation, response, and containment of threats in under five minutes.

As phishing remains a primary attack vector, effective phishing protection programs are crucial. Organizations must keep these programs up to date to reflect the latest phishing campaigns. GreyMatter Phishing Analyzer automates the entire abuse mailbox management process. It analyzes reported messages, sends follow-up notifications to reporters, and takes remediation action across multiple technologies—all within minutes of the initial report.

GreyMatter DRP protects against exposed credentials by continuously monitoring sources like the dark web and paste sites for compromised corporate credentials. This proactive approach ensures early detection, allowing for swift remediation actions such as password resets and user notifications, effectively mitigating potential threats. By providing comprehensive coverage and insights, GreyMatter DRP helps organizations refine security policies to prevent future exposures, maintaining robust credential security.

Fortify Your Security Posture By:

Developing RMM Policies: Conduct a thorough audit to identify all remote-access software currently in use within the environment. Create comprehensive policies that list approved RMM tools and provide detailed guidelines for their proper usage. Subsequently, perform regular audits to ensure no unauthorized software is being used, maintaining a secure and compliant environment.

Disabling Password Saving: Enforce stringent network policies or Group Policy Objects (GPOs) to prevent passwords from being saved in web browsers. This security measure is crucial because many information-stealing malware target stored credentials to exfiltrate sensitive data. Conduct regular audits to ensure compliance and assess the ongoing effectiveness of this policy, ensuring robust protection.

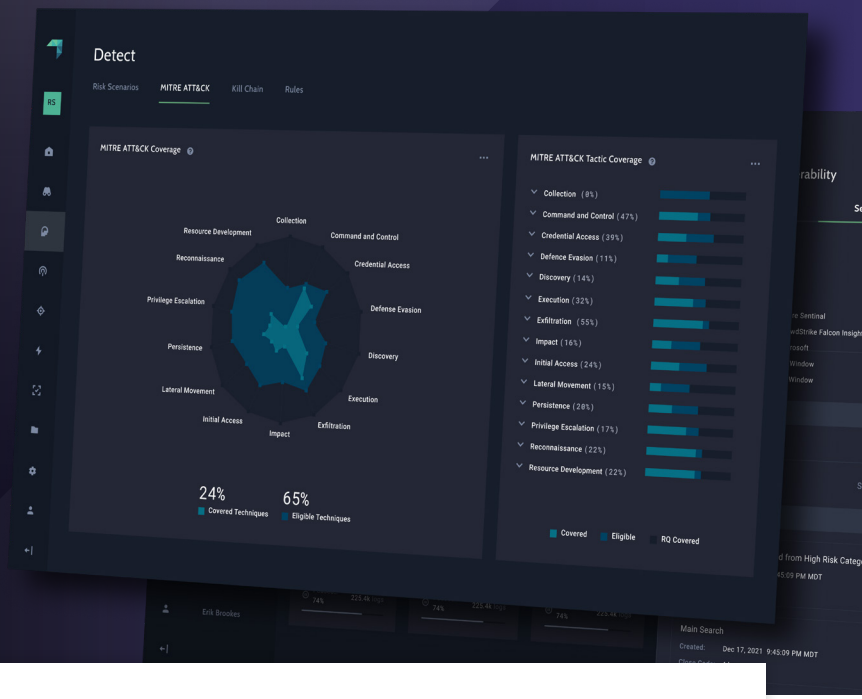
Enforcing Access Controls: Implement robust security measures to ensure that only authorized personnel can access critical resources. This can be achieved by utilizing tools such as RBAC to assign access rights based on an individual's role within the organization, and MFA for an additional layer of security. Regularly review and update access permissions to adapt to personnel changes and promptly revoke access when no longer needed.

Conclusion

The cybersecurity landscape of 2025 presents both challenges and opportunities for organizations as they navigate an evolving threat environment.

The new landscape is marked by the increased use of AI, the emergence of new ransomware groups, and the continued reliance on established, tried-and-true attack techniques, underscoring the complexities ahead.

However, integrating advanced technologies like GreyMatter provides a promising path to enhance threat detection, streamline operations, and maintain a robust security posture.



Many of the threats described in this report involve threat actors becoming faster and more efficient. Trends in LLM use, exposed credentials, and NHI breaches hand threat actors easy access to sensitive data and systems, giving them more time to focus on causing maximum impact.

This highlights the importance of organizations using Automated Response Plays to contain threats and reduce MTTC, as immediately containing an adversary prevents them from causing further damage to the network. Automation also boosts security teams' productivity by reducing alert noise and false positives, removing low-brain, high-time tasks.

In 2024, we saw organizations' attack surface expand because of more use of:

Machine Identities | **LLMs** | **Cloud Technologies**

As organizations adopt innovative solutions, they must carefully balance the risks associated with new technologies and geopolitical tensions.

A proactive approach—characterized by vigilant monitoring, comprehensive threat intelligence, and responsive mitigation strategies—will be essential for safeguarding operations and maintaining resilience against emerging threats.

Appendix: Endnotes

1. hxxps://www.securityweek[.]com/ai-generated-malware-found-in-the-wild/
2. hxxps://www.nationalcrimeagency.gov[.]uk/the-nca-announces-the-disruption-of-lockbit-with-operation-cronos
3. hxxps://www.bleepingcomputer[.]com/news/security/uk-arrests-suspected-scattered-spider-hacker-linked-to-mgm-attack/
4. hxxps://www.darkreading[.]com/cybersecurity-operations/teenage-scattered-spider-suspect-arrested-in-global-cybercrime-sting
5. hxxps://www.bleepingcomputer[.]com/news/security/linux-version-of-new-cicada-ransomware-targets-vmware-esxi-servers/
6. hxxp://securityonline[.]info/mallox-expands-arsenal-targets-linux-with-modified-kryptina-ransomware
7. hxxps://www.bleepingcomputer[.]com/news/security/new-play-ransomware-linux-version-targets-vmware-esxi-vms/
8. hxxps://www.theguardian[.]com/commentisfree/article/2024/aug/07/the-guardian-view-on-a-tech-bubble-going-pop-ai-pays-the-price-for-inflated-expectations
9. hxxps://www.mckinsey[.]com/capabilities/risk-and-resilience/our-insights/implementing-generative-ai-with-speed-and-safety
10. hxxps://thehackernews[.]com/2024/09/chatgpt-macos-flaw-couldve-enabled-long.html
11. hxxps://thehackernews[.]com/2024/10/researchers-uncover-vulnerabilities-in.html
12. hxxps://www.darkreading[.]com/application-security/chatgpt-manipulated-hex-code
13. hxxps://thehackernews[.]com/2024/09/chatgpt-macos-flaw-couldve-enabled-long.html
14. hxxps://staysafeonline[.]org/resources/oh-behave-the-annual-cybersecurity-attitudes-and-behaviors-report-2024/
15. hxxps://www.darkreading[.]com/cyber-risk/shadow-ai-sensitive-data-exposure-workplace-chatbot-use
16. hxxps://thecyberexpress[.]com/killsec-launches-raas-program/
17. hxxps://www.politico[.]com/news/2024/09/27/trump-zelenskyy-meeting-new-york-russia-war-00181429
18. hxxps://www.aljazeera[.]com/news/2024/5/28/trump-promises-crackdown-on-pro-palestinian-protests-if-elected
19. hxxps://digitalrebellion[.]uk/actions/insure-our-survival