REPORT

Cybersecurity and the AI Threat Landscape

Key insights, emerging tactics, and anticipated challenges for 2025

Executive Summary

In 2024, the cybersecurity landscape was marked by a dramatic surge in threats, driven by sophisticated tactics and emerging technologies. Infostealer malware led to significant breaches, such as the Snowflake incident, compromising sensitive personal and financial data. AI-generated phishing and social engineering attacks became more prevalent, successfully evading traditional defenses.

Non-Human Identities (NHIs) emerged as critical assets for automating workflows, yet most of them were not rotated within recommended timeframes, leaving them exposed to potential compromise. The financial sector faced a wave of deepfake fraud attempts, underscoring the growing menace of AI-assisted identity fraud. Meanwhile, Active Directory remained a prime target for ransomware attacks, causing widespread operational disruptions. Multi-factor Authentication (MFA) was implicated in nearly half of security incidents, often due to misconfigurations and fraudulent push notifications. Ransomware attacks, leveraging double extortion tactics and Ransomware-as-a-Service (RaaS), targeted sectors like technology, manufacturing, and construction, with advanced digital infrastructures in the US, UK, and Israel being prime targets.

We anticipate an even more challenging threat landscape in 2025. AI-driven ransomware and deepfake attacks are expected to become more frequent and sophisticated, amplifying the risk to businesses and critical infrastructure. Hyper-personalized phishing campaigns, fueled by AI's ability to synthesize vast amounts of public data, will make it increasingly difficult for users to distinguish legitimate communications from threats. Additionally, attackers are likely to intensify their exploitation of non-human identities and identity providers, taking advantage of inadequate lifecycle management and identity sprawl. These evolving attack vectors underscore the urgent need for organizations to strengthen their security postures, invest in advanced threat detection, and prioritize identity-first security strategies to stay resilient in the face of an ever-evolving threat landscape.

Preface

This report marks the inaugural publication from Delinea Labs, reflecting our commitment to advancing cybersecurity through cutting-edge research and industry collaboration. We aim to provide valuable insights into emerging attack techniques, helping organizations strengthen their security posture and stay ahead of evolving threats.

At Delinea Labs, our team consists of elite white-hat hackers, intelligence experts, and seasoned security leaders dedicated to understanding the ever-changing threat landscape. By studying post-exploit methods and analyzing attacker movement throughout the attack chain, we uncover critical vulnerabilities and share actionable intelligence to enhance defense strategies. Our research not only raises awareness of new and sophisticated threats but also fosters collaboration across the industry to drive continuous improvement in cybersecurity best practices.

We hope you find this report both informative and practical. If you have any feedback or would like to share suggestions for future research, we'd be grateful to hear from you. Your input helps us refine our work and better serve the security community.

Contents

Credential leaks

Credential leaks have become a major cybersecurity threat, fueled by various attack techniques and the increasing frequency of stolen credentials. These leaks, often caused by infostealer malware such as Redline and Raccoon, involve the theft of usernames, passwords, and session tokens, which are commonly sold on the Dark Web. With these stolen credentials, attackers can bypass traditional security defenses and gain unauthorized access to systems, resulting in significant breaches and financial losses. A notable example is the Snowflake breach that was disclosed in May 2024, which affected high-profile clients like Ticketmaster and Neiman Marcus, underscoring the widespread consequences of credential leaks.

According to Flare[1]:

90%

of breached companies had corporate credentials previously leaked in a stealer log

78%

of breached companies had corporate credentials leaked in a stealer log within 6 months before or after the incident

> Microsoft observed that password-based attacks make up over 99% of the 600 million daily identity attacks they tracked[2]

Identity attack trends

Phishing and social engineering

Phishing, particularly credential phishing and social engineering, continues to be a major cybersecurity threat. **According to SlashNext, there was a 202% increase in phishing messages and a 703% rise in credential phishing attacks in 2024**[3]. Delinea has observed a significant rise in credential phishing indicators, though more data is needed to validate the full scope of the trend.

Credential phishing involves tricking individuals into providing sensitive information, such as usernames and passwords, often through fake login pages that appear legitimate. These attacks often employ AI-generated, zero-day threats that bypass traditional security measures. For example, a recent campaign exploited DocuSign's legitimate infrastructure to send emails that appeared to be from DocuSign but contained links to malicious sites designed to harvest credentials.

Social engineering exploits human psychology to manipulate individuals into divulging confidential information or performing actions that compromise security. **These attacks increased by 141% in the latter half of 2024 and often involve tactics like posing as trusted colleagues or using urgent language to prompt immediate action.**

> According to SlashNext, in 2024, there was a 202% increase in phishing messages and a 703% rise in credential phishing attacks.[3]

Non-human identities

While human identities remain a primary attack target, non-human identities (NHI) have quietly become an equally critical — and often overlooked — security risk. NHIs are digital accounts used by applications, APIs, and services to authenticate and interact with each other. These identities — such as service accounts — hold permissions that allow access to resources. NHI credentials, like API keys and certificates, are used to authenticate to an NHI but do not carry permissions themselves. Distinguishing between the identity and its credential is crucial for security and access control.

> For every human identity, there are approximately 46 non-human identities according to a Delinea-created aggregated estimate using data from Delinea and Entro, Astrix, Natoma, Clutch, Oasis and Aembit.

Despite their importance, NHIs are often neglected in security practices. We understand that most vendors only see a limited view of the overall NHI landscape. By aggregating Delinea's data with publicly available figures from multiple NHI vendors — and applying weighted market share estimates — we've generated a weighted combined estimate of the ratio of NHI to human identities. **Our finding suggests that for every human identity, there are approximately 46 non-human identities,** illustrating their pervasive presence in modern infrastructures.

Alarmingly, according to EntroLabs, **over 70% of NHIs are not rotated within recommended timeframes, leaving them vulnerable to exploitation.** On average, these identities are rotated only once every 627 days, far exceeding security best practices. Furthermore, 97% of organizations expose their NHIs to third-party companies, significantly increasing the attack surface and the potential for misuse or unauthorized access. As attackers refine their techniques to target identity systems, the combination of unrotated credentials and widespread third-party access creates a growing and dangerous vulnerability.

Deepfakes

According to the 2025 Identity Fraud Report by Entrust, AI-assisted fraud has become increasingly sophisticated and frequent[10]. AI tools are being used to create sophisticated digital forgeries and deepfakes, posing significant threats to identity verification processes. Key findings include:

- **Deepfake attempts: Occurred every five minutes in 2024, highlighting the rise of hyper-realistic AI-generated fraud.** According to iProov's 2024 Threat Intelligence Report, face swap deepfake attacks surged by 704% from the first half to the second half of 2023, with deepfakes continuing to pose a growing threat to person-to-person identity verification in 2024[11].
- **Financial services:** The most targeted sector, with cryptocurrency platforms experiencing a 50% rise in fraud attempts.

These findings underscore the rapidly evolving threat landscape, where AI-powered attacks are not only more frequent but also increasingly difficult to detect. As deepfakes and identity fraud continue to rise, organizations must adopt advanced identity verification technologies, continuously monitor for anomalies, and implement robust identity security practices. Proactive defense strategies and industry collaboration will be essential to outpace adversaries and safeguard both human and non-human identities in an AI-driven threat environment.

Attacks targeting Active Directory

In 2024, Active Directory (AD) continues to be a vital infrastructure, often targeted by ransomware because of its essential role in business operations, centralized management of network resources, and the opportunity it provides attackers to gain extensive access and escalate privileges within the network. **According to a recent report by Semperis, AD is the target of 9 out of 10 attacks[12].** Despite having recovery processes in place, 87% of attacks caused significant disruption, including data loss and downtime.

These statistics highlight the critical need for organizations to prioritize Active Directory security, not just for prevention but also for rapid detection and resilient recovery. Given AD's central role in managing access and resources, even a single breach can have widespread consequences. Strengthening AD defenses with continuous monitoring, regular audits, and robust incident response strategies is essential to mitigate the risk of ransomware and minimize operational disruption.

> According to a recent report by Semperis, Active Directory is the target of 9 out of 10 attacks[12].

MFA's role in major attacks

According to Cisco Talos, in **Q1 2024, nearly 50% of security incidents involved multi-factor authentication (MFA), with 25% of these cases including fraudulent MFA push notifications[13].**

Configuration issues accounted for 21% of incidents, such as the ransomware attack on Change Healthcare where MFA was not set as default, and multiple attacks on Snowflake customers lacking MFA configuration.

Analysis of 15,000 push-based attacks from June 2023 to May 2024 revealed that attackers often targeted pre-work hours (8-9 a.m.) using methods like stealing authentication tokens and social engineering against IT departments. Additionally, 5% of sent push attacks were accepted by users, with most users who accepted fraudulent pushes receiving between one and five requests.

These findings underscore the importance of properly configuring and reinforcing multi-factor authentication to mitigate evolving attack techniques. As attackers refine their strategies — exploiting human behavior and timing attacks during vulnerable windows — organizations must adopt adaptive MFA policies, educate users on push fatigue, and implement stricter controls to prevent token theft and social engineering. Leveraging intelligent authorization solutions that assess risk signals, such as device health, geolocation, and user behavior, can further enhance security by dynamically adjusting access permissions in real time. Strengthening both these practices is crucial to reducing the risk of compromise and enhancing overall identity security.

Targeting IDPS

According to Delinea Labs data, 3.9% of all observed login attempts to Identity Provider (IDP) systems in 2024 were malicious attacks. These attacks primarily targeted IT roles, such as system administrators and engineers, as attackers sought elevated privileges to manipulate access controls, grant unauthorized access, or disable security measures. These trends reflect a broader strategy by threat actors to exploit identity systems as entry points to breach entire infrastructures.

> 3.9% of all observed login attempts to Identity Provider (IDP) systems in 2024 were malicious attacks
>
> *Delinea Labs*

Exploiting identity systems

The exploitation of identity systems has become a preferred tactic for cyber criminals and state-sponsored actors targeting sensitive government and corporate infrastructures. By leveraging vulnerabilities in identity management frameworks, attackers can gain persistent, unauthorized access to critical resources, often remaining undetected for extended periods. This growing threat is highlighted by incidents such as the US Treasury Department breach. Okta has also reported a surge in proxy-driven credential stuffing attacks, where reverse proxy tools are used to intercept and hijack authentication tokens, bypassing traditional defenses. Similarly, Microsoft's Midnight Blizzard attack demonstrated the risks of compromised identity systems, as threat actors exploited valid credentials to infiltrate cloud environments and access sensitive data.

These trends highlight the growing importance of securing identity systems as a frontline defense against modern cyber threats. Organizations must adopt a proactive approach, implementing continuous monitoring, identity threat detection, and robust access policies to mitigate evolving attack techniques. Strengthening identity security is not just a best practice — it's a necessity for protecting critical infrastructure in an increasingly hostile threat landscape.

Major identity attacks

The Midnight Blizzard attack

The Midnight Blizzard cyberattack, detected by Microsoft on January 12, 2024, was orchestrated by the Russian state-sponsored group APT29. The attackers exploited a legacy test tenant account lacking multi-factor authentication (MFA) through a password spraying attack. They gained unauthorized access, escalated privileges via OAuth applications, and exfiltrated sensitive emails and attachments, including cryptographic keys and credentials. The breach primarily affected Microsoft's corporate email systems, impacting senior leadership and various U.S. federal agencies.

Deepfake fraud: $25 million heist highlights growing cyber threats

In February 2024, a finance employee at **a multinational firm in Hong Kong was deceived into transferring $25 million to fraudsters who used deepfake technology** to impersonate the company's chief executive during a video call. This incident underscores the growing sophistication of cyberattacks employing deepfake technology.

Snowflake breach impacting multiple organizations

In April 2024, the Scattered Spider hacking group exploited compromised credentials from a Snowflake employee account to infiltrate the company's systems. This breach impacted several prominent clients, such as AT&T, and potentially compromised the data of 30 million Santander customers and 560 million Ticketmaster customers. The attackers utilized the stolen credentials to gain unauthorized access to sensitive information, including personal and financial records. The breach highlighted several security gaps, especially around the lack of robust MFA enforcement. Many of the accounts accessed did not have MFA enabled, making it easier for the attackers to use the compromised credentials without facing additional layers of security.

North Korean hackers linked to major cryptocurrency heists in 2024

In 2024, **North Korean hackers, specifically the Lazarus Group, were linked to several major cryptocurrency heists totaling $659 million**. Notable incidents included a $235 million theft from the Indian crypto exchange WazirX and a $308 million theft from Japan's DMM Bitcoin, which led to the exchange's closure. The hackers used sophisticated social engineering tactics, such as fake job offers and impersonations, to deploy malware like TraderTraitor and AppleJeus.

BlackCat ransomware attack on Citrix Systems

In September 2024, the BlackCat ransomware group, also known as ALPHV, utilized stolen credentials to breach a company's Citrix remote access service. **The attack resulted in the theft of 6 terabytes of data and the encryption of computers on the network, prompting the company to shut down IT systems** to prevent further spread.

The Internet Archive breach

In October 2024, the Internet Archive, famous for its Wayback Machine and massive digital archives, fell victim to a major data breach affecting 31 million user accounts. Unsecured authentication tokens, which are non-human identities typically used by systems and automation processes, were left accessible in their GitLab repository for almost two years, leading to this incident. These tokens, often associated with automated services or machine identities, were exploited by threat actors to gain access to critical systems, databases, and user data. The breach also involved the theft of sensitive support tickets, some of which contained personal identification details. Furthermore, attackers sent phishing emails and impersonated the company using the compromised Zendesk API token, another non-human identity used for automation and customer service interactions.

US Treasury Department attack

The US Treasury Department recently experienced a significant cybersecurity breach attributed to a China state-sponsored actor. This breach involved unauthorized remote access to Treasury workstations and unclassified documents using a stolen key. The incident was discovered in December by BeyondTrust, who lost an access key which led to the breach. In response, the compromised service has been taken offline, and the Treasury is collaborating with law enforcement and cybersecurity agencies. China's Foreign Ministry has denied the accusations. The Treasury is working with CISA, the FBI, US intelligence agencies, and third-party forensic investigators to fully understand the incident and its impact.

Ransomware

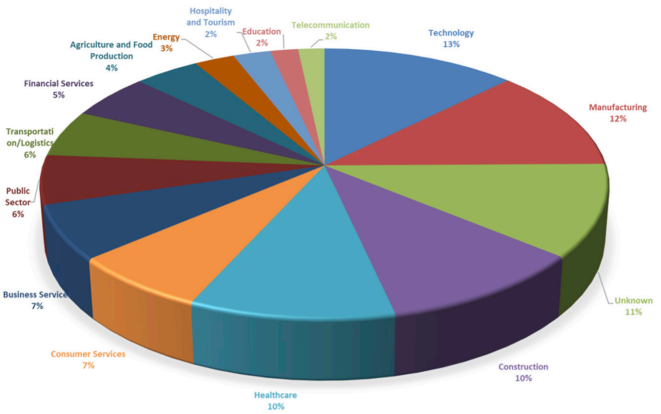
In 2024, ransomware attacks have evolved significantly, with trends showing a rise in double extortion tactics, where attackers not only encrypt data but also exfiltrate it and threaten to release it publicly. **The proliferation of Ransomware-as-a-Service (RaaS) has made it easier for less skilled attackers to launch sophisticated attacks.** Technology, manufacturing, and construction sectors are increasingly targeted due to their high value and likelihood of paying ransoms. Cyber criminals are leveraging AI to automate campaigns and identify vulnerabilities more precisely, while supply chain attacks and Living Off the Land (LotL) techniques are becoming more common, making detection and defense more challenging.

Most targeted industries

In 2024, sectors like technology, manufacturing, construction, and healthcare are highly vulnerable to ransomware due to valuable data, reliance on digital systems, and operational pressures.

Tech companies are targeted for their intellectual property, while manufacturers face risks from critical systems and supply chains. The construction sector's increasing digital reliance and tight timelines make it prone to delays, and healthcare is targeted for sensitive patient data and critical services.

RANSOMWARE INCIDENTS BY INDUSTRY

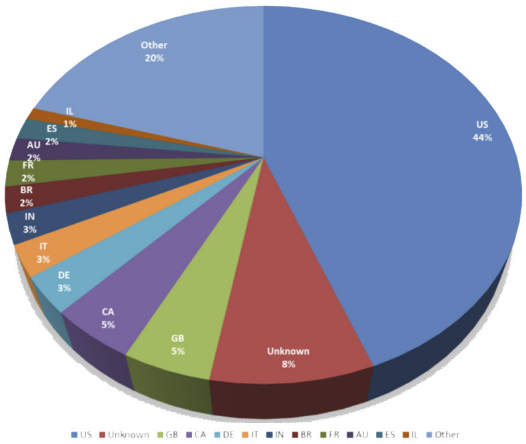


Source: Delinea Labs, Jan 2025

Outdated infrastructure, weak cybersecurity, and financial incentives further increase the appeal of these industries for ransomware groups.

Most targeted countries

RANSOMWARE INCIDENTS BY COUNTRY



Source: Delinea Labs, Jan 2025

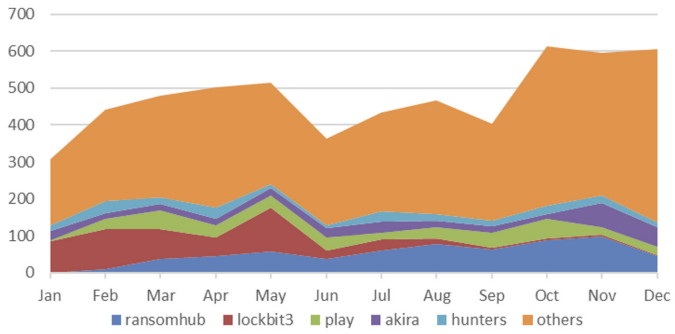
In 2024, countries like the US, UK, Canada, Germany, Italy, India, Brazil, France, Australia, Spain, and Israel were prime targets for ransomware due to their advanced digital infrastructures, large economies, and valuable data.

The widespread use of interconnected systems and sensitive data makes them attractive to cyber criminals, while some sectors suffer from inadequate cybersecurity.

From a geopolitical perspective, certain nations face heightened cyber threats due to regional conflicts, state-sponsored operations, and global influence. Israel and India are frequent targets of cyberattacks linked to geopolitical tensions, with threat actors exploiting vulnerabilities to disrupt critical infrastructure, gather intelligence, or destabilize political environments. Meanwhile, countries like the United States and United Kingdom remain prime targets for cyber espionage and sophisticated attacks, driven by their global influence, economic power, and strategic military assets. Adversaries often conduct prolonged, stealthy operations to infiltrate government agencies, defense networks, and key industries seeking to exfiltrate sensitive data or undermine national security. These threats reflect the evolving nature of cyber warfare, where digital domains have become an extension of geopolitical conflict, emphasizing the need for nations to strengthen their cyber defenses and foster international collaboration to combat cross-border cyber threats.

Monthly activity stats

RANSOMWARE INCIDENTS PER MONTH



Source: Delinea Labs, Jan 2025

Five ransomware groups — RansomHub, LockBit, Play, Akira and Hunters – were responsible for over 36% of all ransomware incidents in 2024, totaling over 5,700 attacks. For most of the year, LockBit was the most active ransomware group, but its dominance declined following a series of high-profile arrests and coordinated law enforcement actions.

The turning point was Operation Cronos in February 2024, an international effort led by Europol, the FBI, and several EU nations. The operation resulted in the seizure of critical servers and the arrest of key members. Law enforcement further weakened the group by arresting four more individuals; a developer in France, two affiliates in the UK, and an administrator of a bulletproof hosting service in Spain. More recently, an Israeli national linked to LockBit's technical operations was also arrested, further disrupting the groups infrastructure.

With Lockbit's decline, RansomHub has quickly risen to prominence, escalating its ransomware activities and claiming a larger share of attacks. Interestingly, ransomware incidents declined between July and September, possibly due to attackers taking time off for holidays. This temporary slowdown may explain the surge in activity observed in December, as ransomware operators return with renewed focus, pushing to meet end-of-year targets.

The top 5 ransomware groups

1 | RansomHub

A rebranded version of the old Knight ransomware operation, RansomHub emerged as a major RaaS group in 2024. It targets sectors such as healthcare, government services, and critical manufacturing, using phishing, exploiting known vulnerabilities, and sophisticated malware to gain access to networks. The group focuses on exfiltrating sensitive data for extortion, often encrypting files to increase pressure on victims.

2 | LockBit

Operating on a Ransomware-as-a-Service (RaaS) model since 2019, LockBit is one of the most prolific ransomware groups globally. It allows affiliates to use its tools in exchange for a share of the profits. LockBit is known for high-profile attacks across sectors like healthcare, education, and critical infrastructure, employing sophisticated encryption and double extortion tactics, threatening to leak stolen data if ransoms are not paid.

3 | Play

Also known as PlayCrypt, this group has been active since mid-2022. Play uses a double extortion model, encrypting data and threatening to leak it if ransoms are not paid. It targets businesses and critical infrastructure across North America, South America, and Europe. Play's ransomware is notable for its intermittent encryption technique, which speeds up the process and complicates data recovery without paying the ransom.

4 | Akira

Akira ransomware appeared in March 2023 and gained notoriety for its aggressive tactics and significant impact on businesses and critical infrastructure. It uses a double extortion strategy, stealing sensitive data before encrypting it and demanding ransoms for both decryption and non-disclosure. Akira is known for its retro-themed Tor leak site and its affiliation with the defunct Conti ransomware gang.

5 | Hunters International

Emerging in late 2023, Hunters is believed to be an offshoot of the dismantled Hive ransomware group. It quickly became a significant threat, using techniques and code similar to Hive. Hunters International operates on a RaaS model and has attacked various sectors, including healthcare, education, and financial services. The group is known for aggressive ransom negotiations and sophisticated malware.

Notable major ransomware attacks in 2024

Change Healthcare

In February 2024, Change Healthcare, a health care technology company owned by UnitedHealth Group, experienced a significant ransomware attack by the LockBit group. This breach is considered one of the largest in U.S. medical data history, affecting millions of patient records. The exposed data included personal information such as names, addresses, dates of birth, Social Security numbers, and medical records.

TEG (Ticketek)

In June 2024, TEG, the parent company of Ticketek, experienced a significant data breach. A hacker claimed to have stolen data from 30 million users, including full names, genders, dates of birth, usernames, hashed passwords, and email addresses. The breach affected Australian account holder information stored on a cloud-based platform hosted by a third-party supplier. TEG confirmed that no customer accounts were compromised due to their encryption methods.

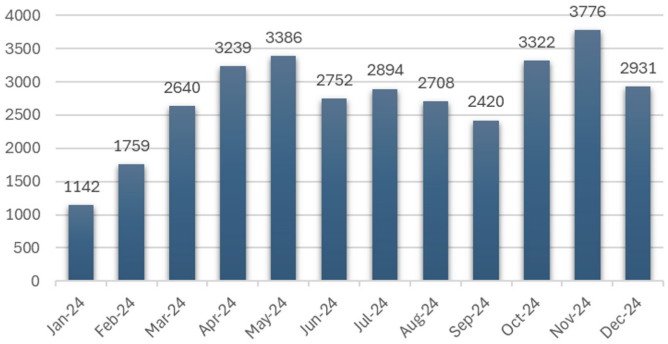
Blue Yonder

In November 2024, Blue Yonder, a SaaS provider, fell victim to a ransomware attack by the Termite gang, resulting in significant operational disruptions for major clients, including Starbucks and Morrisons, a prominent UK supermarket chain. The attackers claimed to have exfiltrated 680 GB of data, comprising database dumps and sensitive documents. The incident has had a particularly severe impact on the grocery and retail sectors, highlighting the cascading effects of supply chain attacks on critical industries.

Identity-related common vulnerabilities and exposures

Putting identity CVEs in context — an outlook on CVEs in 2024

TOTAL CVE



Source: Delinea Labs, Jan 2025

There was a significant increase of 39.4% in CVEs this year, from 23,686 in 2023 to 33,025 in 2024. This surge can be attributed to several factors:

- Firstly, the growing complexity of modern technology, including cloud services, IoT devices, and AI, has expanded the attack surface, leading to more vulnerabilities being discovered.
- Secondly, advancements in cyberattack techniques, such as zero-day exploits and supply chain attacks, have spurred the identification of more flaws.
- Thirdly, the rise of cybersecurity research, bug bounty programs, and automated tools has accelerated CVE discovery.
- Furthermore, the increasing use of open-source software has made vulnerabilities more visible. The weaponization of older CVEs has also played a role, with cyber criminals revisiting and refining past flaws for new exploits. Finally, heightened awareness of cybersecurity risks and the growing threat landscape has led organizations to seek and report vulnerabilities more actively.

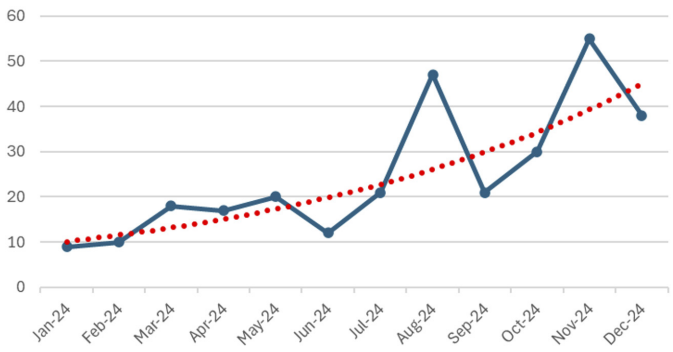
2024 CVE categorization

We focus on two kinds of CVE categories: vulnerabilities in identity products and identity-related vulnerabilities in all products. It is interesting to note that the observed decrease in CVEs during July-September and December could be attributed to seasonal factors, such as holiday periods, reduced workforce engagement, and attackers potentially postponing major campaigns to align with peak operational months.

CVEs in identity products

Although there are limited data points, they indicate a growth in the targeting of identity products. The increase in vulnerabilities in identity products can be attributed to several key factors:

VULNERABILITIES IN IDENTITY PRODUCTS



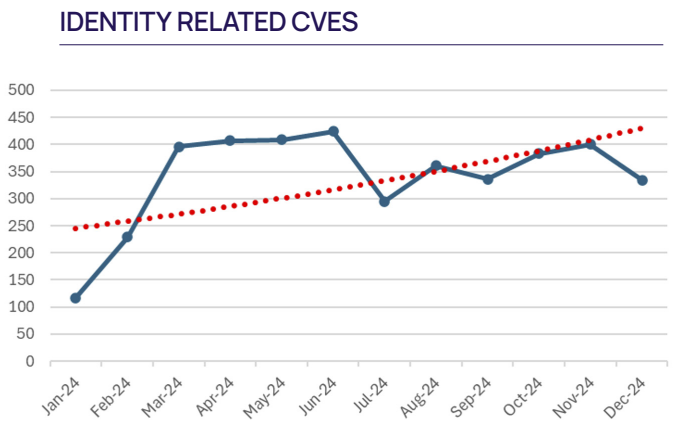
Source: Delinea Labs, Jan 2025

1. **Complexity of identity systems:** Modern identity products are becoming more complex to handle the growing number of Non-Human Identities and their interactions. This complexity can introduce new vulnerabilities
2. **Integration with multiple systems:** Identity products often need to integrate with various other systems and applications, which can create additional attack surfaces and potential vulnerabilities.
3. **Rapid technological advancements:** The fast pace of technological advancements means that identity products must constantly evolve. This rapid development can sometimes lead to insufficient testing and the introduction of new vulnerabilities.

4. **Increased targeting by attackers:** As identity products are critical for securing access to systems and data, they have become prime targets for attackers. This increased focus by cyber criminals can lead to the discovery and exploitation of more vulnerabilities.
5. **Insufficient security practices:** Some identity products may not implement the latest security best practices, such as strong encryption, regular security updates, secure storage of sensitive information (passwords, biometric data, and authentication tokens), and thorough vulnerability assessments.

> The targeting of identity systems has increased by more than 250% from Jan'24 to Dec'24. *Delinea Labs*

Identity-related CVEs



Source: Delinea Labs, Jan 2025

The increase in identity-related CVEs can be attributed to several key factors:

Wider adoption of identity products: As organizations continue to adopt and expand their use of Identity and Access Management (IAM) solutions, Single Sign-On (SSO), and Multi-Factor Authentication (MFA), the attack surface for identity-related vulnerabilities grows by creating more entry points for threat actors to exploit misconfigurations, unpatched vulnerabilities, and gaps in identity security.

1. **Complexity of hybrid and multi-cloud environments:** The integration of identity systems across on-premises, cloud, and hybrid environments introduces new complexities and potential misconfigurations, which attackers can exploit to gain unauthorized access.
2. **Evolving threat actors:** Cyber criminals are increasingly targeting identity systems as they are integral to securing access across an organization. Identity products have become high-value targets due to their ability to grant wide-reaching access to critical systems and sensitive data.
3. **Increased focus on Privileged Access:** With organizations increasingly recognizing the importance of securing privileged access, attackers are focused on finding vulnerabilities in Privileged Account Management (PAM) solutions and exploiting weaknesses to escalate their access.
4. **API exploitation:** The proliferation of APIs used to integrate identity products with other services has introduced new vulnerabilities, making these products more susceptible to attack.
5. **Faster vulnerability disclosure and research:** As the security community becomes more focused on identity-related threats, the pace of discovery and disclosure for identity-related CVEs has accelerated, increasing the number of reported vulnerabilities.

Predictions for identity threats in 2025 and beyond

The use of AI in ransomware attacks

This year saw a substantial rise in reported CVEs, reflecting the growing complexity of digital ecosystems and the increasing scrutiny of security vulnerabilities. Several factors have contributed to this surge, highlighting the evolving threat landscape.

- Advanced ransomware groups, including FunkSec-inspired collectives, are expected to increasingly harness AI to enhance and evolve their attack strategies. AI-powered capabilities will enable attackers to operate with greater precision, agility, and psychological sophistication, amplifying the impact of ransomware campaigns. Key areas of AI-driven advancements include: Automated Target Selection: Identifying high-value targets within an organization by analyzing internal communication patterns, shared files, or privileged accounts.
- **Adaptive encryption strategies:** Implementing algorithms that evade traditional decryption tools by continuously modifying encryption payloads during an attack.
- **Dynamic ransom messaging:** AI-generated ransom notes tailored to the victim's language, cultural context, or psychological triggers to increase payment likelihood.

Deepfakes as a tool for identity exploitation

As deepfake technology grows more sophisticated and widely available, attackers are poised to exploit it at scale to breach organizations and undermine trust. Cyber criminals and state-sponsored actors will increasingly use AI-powered impersonation tactics to manipulate human behavior, bypass security protocols, and compromise sensitive systems. These evolving threats will pressure organizations to rethink their approach to identity verification and adopt stronger, multi-layered defenses. We anticipate four key ways attackers will leverage deepfakes to escalate their tactics:

- **Credential theft through realistic impersonation:** Sophisticated deepfakes of C-suite executives, IT administrators, or HR personnel will be used to request sensitive credentials, manipulate workflows, or authorize large-scale transactions.
- **Targeted social engineering:** Attackers will use deepfake-powered video calls or audio impersonations to bypass identity verification protocols, gaining access to restricted systems.
- **Trust erosion:** The ubiquity of deepfake scams will lead to a decline in trust in digital communications, forcing organizations to adopt multi-layered verification processes.
- **Rising use of deepfakes in attacks:** The use of deepfakes in attacks will rise, with the goal of compromising identities and bypassing MFA systems. This includes simulating behavioral patterns to fool biometric systems or leveraging deepfake technology to bypass identity verification processes.

AI-driven phishing campaigns

We predicted that in 2025, AI-powered phishing attacks will evolve into even more advanced and automated threats, posing significant challenges to traditional cybersecurity defenses. **As attackers leverage AI to refine their strategies, we will see a surge in hyper-personalized, multi-channel campaigns that exploit human behavior and bypass existing security filters.** The ability to quickly scale these attacks across various communication channels will make detection increasingly difficult, resulting in higher success rates and broader impacts. Here's how we predict AI will reshape phishing tactics in the coming years:

- **Hyper-personalized attacks:** AI will enable attackers to analyze vast amounts of personal and professional data to craft phishing emails or messages that are highly tailored and convincing, aka as spear-phishing on steroids.
- **Natural Language Processing (NLP) exploitation:** AI-generated phishing messages will mimic human writing styles with flawless grammar and tone, making detection by traditional filters more challenging.
- **Omnichannel phishing:** Attackers will launch campaigns across email, social media, collaboration tools, and even voice channels, ensuring wider reach and higher success rates.
- **Automated phishing site creation:** Attackers will use AI to automate the creation and deployment of "personalized" phishing sites.

Emerging threats in identity systems

As identity systems become an increasingly integral part of organizational security, they are simultaneously evolving into high-value targets for cyber criminals and threat actors. In the coming years, we anticipate a surge in attacks specifically designed to exploit vulnerabilities within identity management platforms, authentication protocols, and multi-factor authentication (MFA) systems. **With the growing reliance on third-party integrations and cloud-based services, identity systems will face heightened risks from sophisticated, multi-faceted attacks that aim to bypass traditional security measures.** Here are the key emerging threats to watch for:

- **Compromising identity providers:** Attackers will increasingly target major identity management platforms (e.g., Okta, Microsoft Entra) to gain wide-reaching access to organizations' systems. This includes exploiting vulnerabilities in APIs used by these identity products to bypass authentication or escalate privileges.
- **Supply chain risks:** Third-party identity integrations will serve as an entry point for attackers, emphasizing the need for robust vendor security assessments. This risk is compounded by the exploitation of legacy on-premises Active Directory (AD) systems, where attackers can exploit misconfigurations, unpatched vulnerabilities, or over-permissioned accounts to move laterally within networks.
- **Advanced protocol attacks:** Sophisticated attacks on authentication protocols like Kerberos ticket forging ("Golden Tickets") or token hijacking in OAuth will rise. These attacks will be complemented by AI-augmented brute force methods, where AI is used to rapidly test password combinations, adapt strategies based on failed attempts, and evade detection.
- **Compromising MFA systems:** Attackers will employ AI to bypass multi-factor authentication (MFA) systems. This includes simulating behavioral patterns to fool biometric systems, automated creation of phishing sites, or leveraging deepfake technology to bypass identity verification processes.

Targeting non-human identities (NHI)

As organizations increasingly rely on non-human identities (NHIs) such as IoT devices, bots, service accounts, and AI agents, these digital entities are rapidly becoming prime targets for cyberattacks. **By the end of 2025, the number of NHIs is expected to exceed 45 billion, creating a massive and often overlooked attack surface.** With many of these identities being poorly secured or inadequately monitored, attackers will exploit vulnerabilities to gain unauthorized access, disrupt operations, and compromise critical infrastructure. The growing reliance on NHIs introduces significant risks that will need to be mitigated as part of future cybersecurity strategies. Here are the primary tactics attackers will leverage:

- **Weak authentication protocols:** Gaining unauthorized access due to inadequate identity protection.
- **Hardcoded credentials:** Leveraging default or static passwords embedded in device configurations.
- **Outdated firmware:** Exploiting unpatched vulnerabilities in legacy devices.

This growing attack vector will enable:

- **Lateral movement:** Expanding access across network environments to escalate attacks.
- **Data exfiltration:** Extracting sensitive information from compromised systems.
- **Critical infrastructure compromise:** Disrupting essential services and operations via insecure devices.

AI-driven exploitation and attack automation

As artificial intelligence (AI) and machine learning continue to advance, cyber criminals are expected to harness these technologies to automate and accelerate attacks across the entire cyberattack kill chain. **By 2026, AI-driven attacks are predicted to become faster, more sophisticated, and harder to detect.** These technologies will enable attackers to execute highly personalized, adaptive, and efficient campaigns, significantly reducing the time and resources required to compromise systems. The integration of AI into cyberattacks will lead to unprecedented levels of automation, amplifying the scale and effectiveness of both enterprise and individual-targeted threats. Below are key examples of how AI will reshape the attack landscape:

- **Phishing email generation:** Using ChatGPT-like models to craft highly convincing emails with near-perfect social engineering tactics.
- **AI-driven malware:** Adapting in real time to evade traditional detection mechanisms.

By 2026, studies predict:

- **Over 50% reduction in attack execution time** due to AI.
- **Increased sophistication in campaigns** targeting both enterprises and individuals.

References

1. Breached Identities and Infostealers: One of the Largest Ongoing Data Leaks in History - Flare | Cyber Threat Intel | Digital Risk Protection
2. Microsoft Digital Defense Report 2024
3. SlashNext-2024-Phishing-Intelligence-Report.pdf
4. Entro Labs
5. https://www.natoma.id/blog/what-are-non-human-identities
6. Clutch - Securing Non-Human Identities. Everywhere.
7. What are non-human identities
8. Non-Human Identities most common questions: What It Is, Why It Matters, and How to Manage It
9. A Human's Guide to Non-Human Identities (NHIs)
10. Entrust Official Website
11. The Top 5 Must-Read Analyst Reports of 2024 for Identity Verification and Cybersecurity Experts | iProov
12. Active Directory Forest Recovery - Semperis
13. How are attackers trying to bypass MFA?

Delinea

Securing identities at every interaction

Delinea is a pioneer in securing identities through centralized authorization, making organizations more secure by seamlessly governing their interactions across the modern enterprise. Delinea allows organizations to apply context and intelligence throughout the identity lifecycle across cloud and traditional infrastructure, data, and SaaS applications to eliminate identity-related threats. With intelligent authorization, Delinea provides the only platform that enables you to discover all identities, assign appropriate access levels, detect irregularities, and immediately respond to identity threats in real-time. Delinea accelerates your teams' adoption by deploying in weeks, not months, and makes them more productive by requiring 90% fewer resources to manage than the nearest competitor. With a guaranteed 99.99% uptime, the Delinea Platform is the most reliable identity security solution available. Learn more about Delinea on **Delinea.com**, **LinkedIn**, **X**, and **YouTube**.