REPORT

SpyCloud

THE IDENTITY SECURITY RECKONING: 2025 LESSONS, 2026 PREDICTIONS

A retrospective on identity threat trends from 2025 and projections for the year ahead

Connecting 2025's Dots to ***Forecast*** the Year Ahead

The threat landscape is fickle terrain that unendingly shifts and expands. At SpyCloud, our pulse-reading threat forecasters never rest, keeping constant eyes on the underground to inform the defense work taking place on the surface. For us, sourcing and supplying identity intelligence to defenders to effectively disrupt cybercrime is **our mission** – and our responsibility.

In this report, we're sharing our forecast projections for the year ahead, based on our observations of digital identity exposure trends from 2025 and the expert analysis of our team.

The major throughline? Why, it's identity misuse of course.

Teams will need to stretch and grow in new ways, sure. There's also wisdom in doubling-down on the evidence that lies before us today.

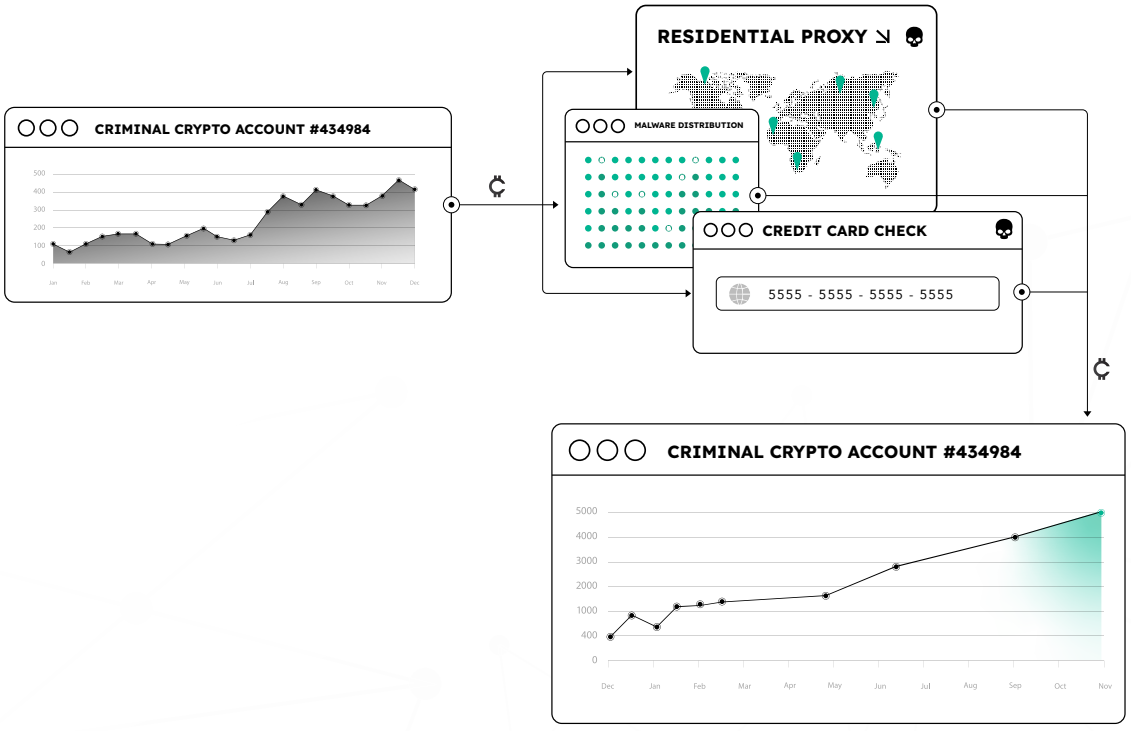
Without further ado, these are the trends and cyber-phenomena the SpyCloud team will be keeping a close eye on in 2026.

1 The Industrialization of Cybercrime Will Further Commoditize ***Plug-and-Play*** Identity Attacks

Cybercrime is a booming industry worldwide, and attack methods are being commercialized by and for threat actors much like corporate software models for traditional businesses (i.e. subscription models, multi-language support, etc.).

New capabilities especially in **"malware-as-a-service" (MaaS)** and "phishing-as-a-service" (PHaaS) kits are making it easy for bad actors to scale, and it's a complex, crowded space poised to keep growing. Popular infostealer malware like LummaC2 and its collaboration with **the GhostSocks residential proxy** led the charge in 2025, and a plethora of other packaged offerings, from crypting services, to install brokers and **plug-and-play panels**, are fueling criminal operations.

The scope and complexity of this dark industry may reach new heights in 2026, with competition breeding accelerated feature development and more affordable options for an even lower barrier to entry for sophisticated attacks. We will likely see an abundance of new offerings coming out of the woodwork, with increased segmentation into defined "roles" in the cybercrime economy – such as infrastructure providers, tool developers, access brokers, and even support services.



2 The Threat Actor Community Will Keep ***Splitting and Shifting*** Due to Youth Involvement, Platform Migrations, and Global Threat Expansion

The world of cybercrime does not sit still – rather it is a swirling and constantly moving system. SpyCloud is always watching closely to see where the activity is coming from and where it will go next. In 2025, we saw some significant shifting with notable darknet communities like BreachForums and XSS being disrupted or taken down by LEA, and Telegram changing their policies and effectively shutting out thousands of threat actor accounts after the **CEO was arrested in late 2024** for not complying with data requests from law enforcement.

Although there appears to be no slowdown for Telegram, the fallout of this drama is driving cybercriminals away from dark web forums to more mainstream communication platforms like **Threads**, X, and WhatsApp, where moderation of messaging is now deprioritized. We expect to see more of this in 2026.

Along with that, and the commoditized availability of attack tools, we expect to see:

- Younger demographics will continue getting more involved in malicious cyberactivity – **expanding on the foundation set by The Com, which incited a trend of experimentation based on easy access and the promise of financial payouts, status, and lesser consequences than non-minors** – and named cybercriminal groups or "gangs" will keep growing in popularity, such as Cl0p, Qilin, and **ShinyHunters**.
- While security teams **still count ransomware among the top two threats** they faced this year, we are also still seeing a shift away from traditional encryption ransomware attacks toward double extortion (encrypt and exfiltrate data), as well as plain data theft extortion, where actors threaten to leak stolen data they have exfiltrated.
- Regionally, **China** was a high-pressure system of threat activity in 2025, marking a shift from the historic concentration of focus on Western groups, and is poised to remain plenty relevant. Additionally we'll see threat actor activity swelling in many other areas of the globe, including Latin America where **fraud activity seems to be coalescing**.
- Geopolitics and world conflict will continue fueling hacktivist groups and pretenders. While the war in Ukraine rages on, other conflicts are starting up seemingly monthly between world powers which sets the stage for heightened cyberactivity and grassroots-type activism. Handala and **CyberToufan** are recent examples of groups like this.

3 Identity ***(And Non-Human Identity)*** Sprawl Will Be Tough to Wrangle In

The dark web in 2025 proved truly vast, littered with stolen information that has, can, and will be exploited for cyberattacks. The most striking observation we've made in our research is that, on average, corporate users have 12 times more exposed identity data – **so 146 exposed data records** tied to their digital identity – than previous tracking methods reported. This creates a trove of user data that can be used for targeted identity-based attacks like account takeover, session hijacking, ransomware, and fraud.

The identity sprawl of more accounts and more devices, paired with uneven security policies and authentication methods, means we will still be chasing this problem next year and beyond. It puts a greater urgency on security teams to understand and monitor for each user's "**holistic identity**," not just the specific accounts associated with the business, in order to catch and remediate any unseen exposures that can create pathways to business and customers data. New solutions are being introduced in the market to assist with mapping of identities across organizational and personal accounts, which will be a worthwhile investment to consider for your security program.

The challenge is further complicated by the fast-rising number of **non-human identities (NHIs)**, such as API tokens, OAuth keys, and service accounts. These are an added (and dangerous) thorn all their own, with privileged access to company systems minus the usual security controls of human users. As the explosive **year-over-year growth in NHIs** continues in 2026 – driven by cloud-native architecture adoption, DevOps acceleration, and AI/ML – security teams will need to ramp up privacy compliance and deletion protocols for every user's associated NHIs.

"In recent attacks, we've seen there be some kind of non-human identity stolen – like OAuth keys or GitHub personal access tokens – that then allows actors to pivot into those environments.

Non-human identifiers and secrets typically involve two computers or services talking to one another, without the need for a human. And by and large, enterprise protections like MFA are only in place on the more human-focused credentials. Businesses with engineering environments should prioritize **strong vetting for any vendor** they will allow to auth to their environments to make sure all their security controls are up to snuff."

Trevor Hilligoss | Head of Security Research and SVP of SpyCloud Labs

4 Insider Threats Will Become ***Mainstream***

Classifying insider threats in 2026 extends well beyond disgruntled employees; compromised users, negligent behavior, and emerging schemes like IT worker infiltration are making it a moving target that confuses normal behavior for legitimate security threats, and vice versa.

Things to watch out for?

- Existing employees or customers who have had their data compromised in a breach, malware exposure, or phishing campaign.
- Events like mergers and acquisitions, which can create risk by expanding attack surfaces with inherited users and systems, disrupting established security processes, creating temporary elevated access requirements, and potentially motivating malicious behavior among employees facing organizational uncertainty.
- Hiring, especially when hiring remote IT workers, where there are increased cases of fraudulent identities posing at workers and using the opportunity to funnel paychecks to regimes or crime groups, such as we saw with the widely-publicized **North Korean (DPRK) remote worker schemes** this year.

SpyCloud research found that

56%

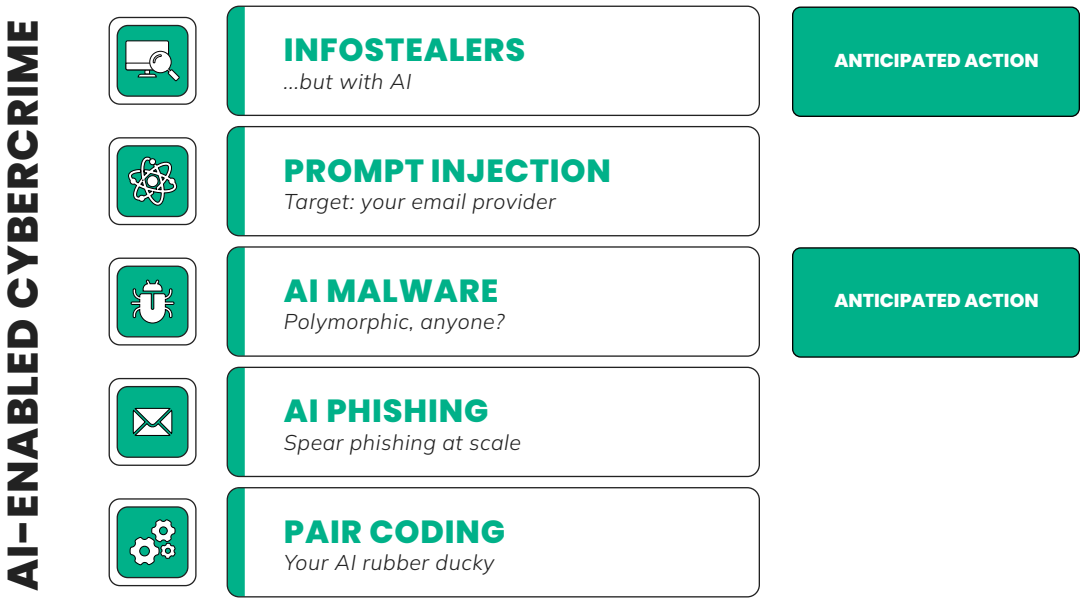
of organizations experienced an insider threat incident sometime in the past year.

"Malicious insiders are only getting better and more sophisticated at employment fraud schemes. And the tools that they're using are getting better, including artificial intelligence that allows them to leverage deepfakes and alter resumes in a way that's very convincing."

Aurora Johnson | Manager of Security Research Partnerships at SpyCloud

5 AI-Enabled Cybercrime & The AI Arms Race ***Will Play Out*** – For Bad or Good

AI talk was exhaustive in 2025, but its impact and implications certainly have some force behind them. So far, AI seems to mostly be exacerbating existing threats, but even as some promises of AI are overblown, its potential is still unrealized – including how it will be used in cybercrime.



While some of these have not yet been observed in the wild at the time of this report, this is SpyCloud analysts' hypothesis for AI use cases in cybercrime in 2026.

"Some threat areas AI is enhancing include phishing kits and social engineering. One of AI's more proven strengths so far is interpreting and recommending language trained on human communication, so it's likely to be used for **optimizing convincing copy on fraudulent emails and websites to mimic real brands or people** in order to deceive individuals into taking actions or giving sensitive information. It also helps threat actors bridge language barriers. Security teams should continually update their policies and training to help employees spot suspicious communications as they grow more advanced and believable."

Aurora Johnson | Manager of Security Research Partnerships at SpyCloud

Security concerns around AI usage are a major story this year and heading into next. Around **92% of organizations** feel that AI-powered cybercrime creates intensified risk. Security teams will need to stay up-to-date with the topic, as the nebula is a bit murky on the new ways it will be used and how effective they will be, but it will inevitably make headlines. AI-specific security roles will also likely become more common at the enterprise level, and 31% of teams surveyed by SpyCloud say that investing in AI-powered security tools is a top priority over the next 12-18 months.

AI usage in day-to-day work has also created a unique new vulnerability that will require security teams to keep org-wide AI use under a telescope.

In our 2025 Annual Identity Exposure Report, SpyCloud observed about

900,000

stolen credential records obtained from enterprise AI tools.

As business teams not only adopt AI usage in workflows, but allow employees to use AI tools, added layers of security are now essential and will be increasingly so in 2026.

6 Attackers Will Continue to ***Innovate to Bypass Defenses***

Over the past couple years, MFA bypass methods have become one of the most charged particles enabling successful ransomware events. Stolen session cookies from authenticated users allow for "session hijacking," which was **the third most common entry point for ransomware in 2025.** This is commonly powered by infostealer technology and phishing kits, such as **Tycoon 2FA**, which are surging in popularity and projected to keep spreading in 2026.

There are several other trending methods for bypassing MFA and other session defenses – covered in detail in our **MFA bypass guide**, and several other techniques and attack methods will continue to create new challenges in defense bypass next year. These include:

- Residential proxies used to bypass location authentication measures
- "Anonymity" or antidetect browsers (ex. Linken Sphere, MultiLogin) used to bypass device fingerprinting
- Mass notification services used for spam MFA approval messages
- Adversary-in-the-Middle (AitM) attacks used to phish credentials and steal valid cookies
- Malware crypting services used to evade antivirus software (ex. **Asgard Protector**)
  - An analysis of SpyCloud's recaptured database this year showed that **66%** of malware infections bypassed endpoint detection and response (EDR) or antivirus (AV) solutions.

> "When a malware infection goes undetected, or a valid session cookie ends up in criminal hands, the consequences can be catastrophic. We are in an arms race at the endpoint, where attackers are constantly evolving their tactics to skirt detection."
>
> **Damon Fleury** | SpyCloud's Chief Product Officer

In short, organizations cannot put their faith completely in these defense mechanisms no matter how many access management layers they're enforcing, and this will only become more apparent in 2026. Detection and remediation needs increased priority no matter the organization or perceived security strength, because attackers can and will find ways around every defense to carry out follow-on attacks.

7 *Pathways to* Supply Chain Compromise Will Multiply

It's of no surprise to anyone that the supply chain is a hotbed for security weaknesses that will present compounding challenges in the year ahead. According to Verizon research, third-party involvement was observed in **30% of all breaches in 2025** with year-over-year growth, and supply chain vendors and partners are a primary culprit for under-audited and monitored privileged access that becomes a massive entry point for attackers. Our 2025 Identity Threat Index found that the **IT, telecom, and software industries face 4-6x higher threat levels** than others with regard to possible identity exposures creating pathways into partner networks.

Heavily-regulated sectors like the federal government, financial services, and insurance industry are on the other end of the storm scale, with lower threat gravity due to their heavy investment in supply chain management measures – but not completely out of the woods.

A number of other factors will continue to create disturbances from the inside of business operations, including the rapidly expanding sea of non-human identities and outsourcing of contractors (supply chain, development, etc.). This fast-changing interconnectivity and sharing of access, even when seemingly limited, needs the same risk controls as full-time employees to prevent.

We see that placement continuing in 2026, and other industries can take notes with more substantial resources put into measures like:

- Vendor threat assessment and continuous monitoring
- Contractual safeguards
- Zero Trust access management for all third-party partners
- Joint incident response plans

"Contractors are often the way that larger organizations are breached. Businesses should **apply the same internal security controls and policies to remote vendors** they hire. For example, does your new overseas contractor for sure change their passwords at least once a year? Small details like this too often lead to the entire org getting compromised, so consistency for every type of worker is key."

Joe Roosen | Director of Security Research at SpyCloud

8 Synthetic Identity Fraud ***Will Gain More Momentum*** Using Stolen Data and AI

Another trend we are tracking is the increasing sophistication of the "synthetic identities" threat actors are building to use as crime tools, pieced together from fragments of stolen information. This is gaining steam as a challenge to address, with **56%** of banks naming synthetic identity fraud as their top fraud concern for the next two years. This is another area where AI will rear its head, as deepfakes and virtual characters are being used to pose as real people and the technology is growing more advanced by the day.

In 2026, teams will need to add some jet fuel to their verification and attribution abilities, and consider enhanced **fraud prevention measures** to help correlate new users with any exposures and flag suspicious accounts for additional investigation.

"Often when stolen credentials and PII end up on the darknet – including dates of birth, social security numbers, and sensitive data like that – that data can then be assembled to create other synthetic identities.

In security intelligence, it's helpful to work with long histories of data collections like ours, so when you see that a credential was leaked at some point, it can help you detect if that user info is more likely to be enabled for fraud or synthetic use in some way. By **analyzing historic exposure data**, you can try and predict the validity of individual users and detect fraud before it occurs."

Joe Roosen | Director of Security Research at SpyCloud

9 Distractions Like Megabreaches and Combolists Will Keep ***Popping Up***

Sensationalized events like megabreaches and **combolists** were headline-grabbers this year. Reports of "billions of records" found in several incidents made mainstream news and set off alarms for organizations scrambling to see if they were impacted. The truth is that criminal communities are assembling lists of already-exposed data to generate hype, fear, and clout – but most of the records are from old breaches or infostealer logs, sometimes dating back years.

Stories like megabreaches are a black hole for the attention and energy of organization leadership and security heads. They can also generate fatigue for teams when told to worry about something that they've already addressed, sometimes several times over.

> "That's the one thing that gets lost with the news buzz. What gets called a 'new breach' might actually just be a combolist containing data exposed from over the last decade, and now it's being recirculated. In most cases I've seen, the data usually dates back over at least five years. And it creates a headache for defenders who have already remediated the exposures."
>
> **Joe Roosen** | Director of Security Research at SpyCloud

Paired with the speed of social media dialogue that hits people over the head with hype stories and conversations, it's essential for businesses to – *ahem* – rely on continuous, proactive monitoring to avoid playing catch-up, and stay smart about what's a distraction and what their real security priorities should be.

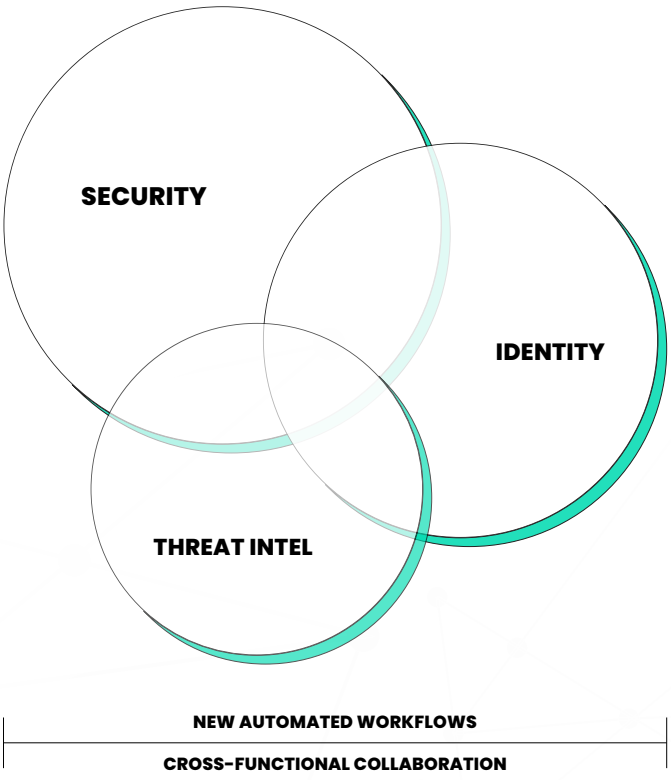
As we head into 2026, these trending topics and inevitably others will be a constant obstacle that require a sharp eye to stay focused where it matters, in some cases ignoring repeat news alerts or communicating with vendors, customers, and employees about the legitimacy of stories like this when they come up and how the business is or isn't affected.

10 Defenders, Teams, and Workflows ***Will Morph*** – and Unite

Just as the threat landscape evolves, so must security operations and best practices. The World Economic Forum reported a **12% increase in cybersecurity talent acquisition** in 2025, and it's likely to trend upward again in 2026 with only 14% of businesses reporting that they currently have the necessary talent to meet their cybersecurity objectives.

With identity as a unanimous focus as this year turns into next, we predict organizations will also prioritize more cross-functional workflows and consolidate some of the current roles to unify defenses, improve efficiency, and open budgets for more future-focused positions and skillsets.

Shared responsibilities across SOC, identity, and threat intel teams will be a key theme, along with the incorporation of automation and AI for security workflows, ticketing and coordination with HR, background checks, detection, remediation, and more. To help them do their jobs – and keep the company, employees, and customers safe – the identity and access management (IAM) stack is likely to be extended at many organizations to include more security tools and features. And along with consolidating some internal processes, vendor consolidation is also likely to continue increasing as a way to strengthen security posture.



Keep an Eye ***on the Horizon***

There's never a dull moment in cybersecurity, and we're sure to see one story after another next year that keeps us all on our toes and moving quickly to stay safe and minimize fallout where we can. We're banking on these stories as some of the major threads to follow and be proactive about where possible for business leaders and IT decision-makers. And when the newest threats emerge or security trends develop, we'll keep our customers informed and continue innovating to protect businesses and their customers.

"With the speed that technology moves, cybercrime evolves in lockstep and it is equal parts fascinating to watch and challenging to keep up with.

The commoditization and influence of the dark web will continue to complicate things, and will no doubt make 2026 another nonstop year for defenders. But can bet we'll be following along at every beat and working closely with our customers and partners to stay one step ahead, using **identity misuse as our North Star** for better protection and attack prevention."

Trevor Hilligoss | Head of Security Research and SVP of SpyCloud Labs

Continue reading about the recent threat landscape in our 2025 ***Identity Exposure Report*** *and* ***Identity Threat Report****, and then* ***Check Your Exposure*** *to help identify any current threats your business may be facing from past infections, exposures, and breaches.*

You can also stay up to date on security threats and prevention strategies on the ***SpyCloud blog*** *and via the* ***SpyCloud Labs*** *research team.*

Learn About SpyCloud's ***Identity Threat Protection*** Solutions

ENTERPRISE PROTECTION

Every user connected to your business – from employees to contractors to third parties – represents an entry point for cybercriminals.

SpyCloud Enterprise Protection closes identity exposure gaps before attackers can exploit them in ATO, session hijacking, and ransomware attacks.

SEE MORE ›

CONSUMER RISK PROTECTION

Cybercriminals exploit more than just passwords – they weaponize session cookies, stolen credentials, and PII from malware and breaches.

SpyCloud Consumer Risk Protection delivers deep, proactive intelligence to detect and stop identity threats before they lead to account takeover, fraud, or churn.

SEE MORE ›

INVESTIGATIONS

SpyCloud Investigations is the ultimate force multiplier for cybercrime and identity threat investigations.

Powered by dark web identity intelligence, analysts and investigators can surface hidden risks, uncover new investigative angles, and connect the dots for rapid response before cyber threats escalate.

SEE MORE ›

About SpyCloud

SpyCloud protects businesses from the stolen identity data criminals are using to target them now. Its automated identity threat protection solutions leverage advanced analytics and AI to proactively prevent ransomware and account takeover, detect insider threats, safeguard employee and consumer identities, and accelerate cybercrime investigations. To learn more about its holistic identity approach and see your company's exposed identity data, visit **spycloud.com**.

GET A DEMO OR REQUEST MORE INFO