2025 IDENTITY THREAT RESEARCH REPORT

Identity-Centric Threats: The New Reality

Breaking Down the Rapid Growth of Identity-based Cyberattacks

eSENTIRE
THREAT RESPONSE UNIT

Introduction

In recent years, the cybersecurity threat landscape has transformed significantly with identity-based attacks emerging as one of the most dominant threat vectors.

Where traditional attacks focused on exploiting technical vulnerabilities in systems and applications, modern threat actors recognize that compromising user identities provides direct access to the most valuable organizational assets with significantly less technical complexity.

According to threat research conducted specifically on identity-related security incidents by eSentire's Threat Response Unit (TRU), there has been a dramatic shift in adversarial tactics, moving from traditional asset-focused cyberattacks to sophisticated identity-centric campaigns that can bypass traditional security controls.

TRU's threat data presents a stark reality: **identity-driven threats have increased by 156% between 2023 and 2025, now representing 59% of all confirmed threat cases during Q1 2025**. This shift reflects not merely an evolution in attack techniques, but a fundamental change in how cybercriminals approach organizational targets.

The driving force behind this shift is the rise of Cybercrime-as-a-Service ecosystems, which promise immense returns for any threat actor willing to pay a subscription fee. The economic model is compelling for threat actors: low barrier to entry with exceptionally high return potential, particularly when targeting business email accounts for fraud operations.

For instance, Phishing-as-a-Service platforms like Tycoon2FA, which account for 58% of observed account compromise cases, can be rented for as little as $200-300 USD per month. These services provide enterprise-grade credential harvesting capabilities, complete with Adversary-in-the-Middle functionalities that bypass traditional multi-factor authentication.

Moreover, information stealer malware has evolved beyond simple credential theft to become comprehensive identity harvesting platforms.

These malware campaigns now represent 33% of all disrupted malware incidents, with sophisticated capabilities for extracting browser-stored credentials, password manager databases, VPN configurations, and application-specific authentication tokens.

The stolen credentials are immediately monetized through underground marketplaces that operate with the efficiency of legitimate e-commerce platforms, allowing threat actors to filter and purchase specific organizational credentials within hours of theft.

Perhaps most concerning is the exploitation of monitoring blind spots within organizational security architectures. Unmanaged devices, shadow IT infrastructure, and third-party supply chain partnerships create an attack surface that is nearly invisible to traditional security controls.

The implications for organizational security strategies are profound. Traditional security models built around perimeter defense and endpoint protection are fundamentally insufficient against adversaries who possess valid credentials.

Organizations must architect their security posture around the assumption that identities will be compromised, implementing continuous authentication verification, comprehensive credential monitoring, and rapid response capabilities for identity-based threats.

The Identity Revolution: Current Threat Landscape Analysis

Identity-based attacks have evolved from opportunistic attacks to systematic, service-driven operations that target the foundation of an organization's security architecture. TRU's analysis of threat case data spanning 2023 through Q1 2025 reveals the scope and sophistication of this transformation.

Identity-based attacks have evolved from opportunistic attacks to systematic, service-driven operations that target the foundation of an organization's security architecture. TRU's analysis of threat case data spanning 2023 through Q1 2025 reveals the scope and sophistication of this transformation.

Pure identity attacks, defined as threats that directly target user credentials and authentication mechanisms, have **more than doubled from 23% of all threat cases in 2023 to 59% in 2025 year-to-date**.

When expanding the definition to include **identity-enabled attacks** such as infostealer malware, the percentage increases dramatically. This growth represents how threat actors have shifted their attack strategies and methodologies toward the most efficient attack vectors available.

Email account compromise cases specifically have increased by 60% year-over-year, with 41% of all 2025 cases involving some form of business email compromise or account takeover.

These attacks follow predictable patterns: threat actors harvest initial credential through Phishing-as-a-Service platforms, followed by immediate monetization through business email compromise fraud.

Moreover, the timeline between initial compromise and malicious activity has decreased significantly, with threat actors moving from credential theft to active fraud within hours rather than days or weeks.

When considering geographic distribution, **78% of identified phishing-as-a-service operations originate from the United States**. However, this reflects the use of legitimate hosting providers and content delivery networks rather than the actual location of threat actors.

Subsequent authentication attempts using stolen credentials show a much broader geographic distribution, with threat actors leveraging VPN services and proxy networks to mask their true locations while maintaining the appearance of legitimate access from expected geographic regions.

Cybercrime-as-a-Service: Democratizing Advanced Attacks

The emergence of Cybercrime-as-a-Service platforms represents one of the most significant developments in the threat landscape since the introduction of the Ransomware-as-a-Service model. These platforms have altered the economics of cybercrime by lowering the barrier to entry and providing specialized services that enable threat actors to focus on specific aspects of a cyberattack campaign while outsourcing complex technical components.

This is especially the case with Phishing-as-a-Service (PhaaS) platforms, which may cost threat actors anywhere from $100 to $1,000 per month on average. For example, Tycoon2FA provides comprehensive credential harvesting capabilities ranging from $200 to $300 USD.

These platforms include sophisticated Adversary-in-the-Middle (AitM) functionality that can intercept and replay authentication tokens, effectively bypassing traditional multi-factor authentication implementations. The technical sophistication of these services rivals that of legitimate security tools, complete with user interfaces, customer support, and regular updates to counter defensive measures (Figure 1).

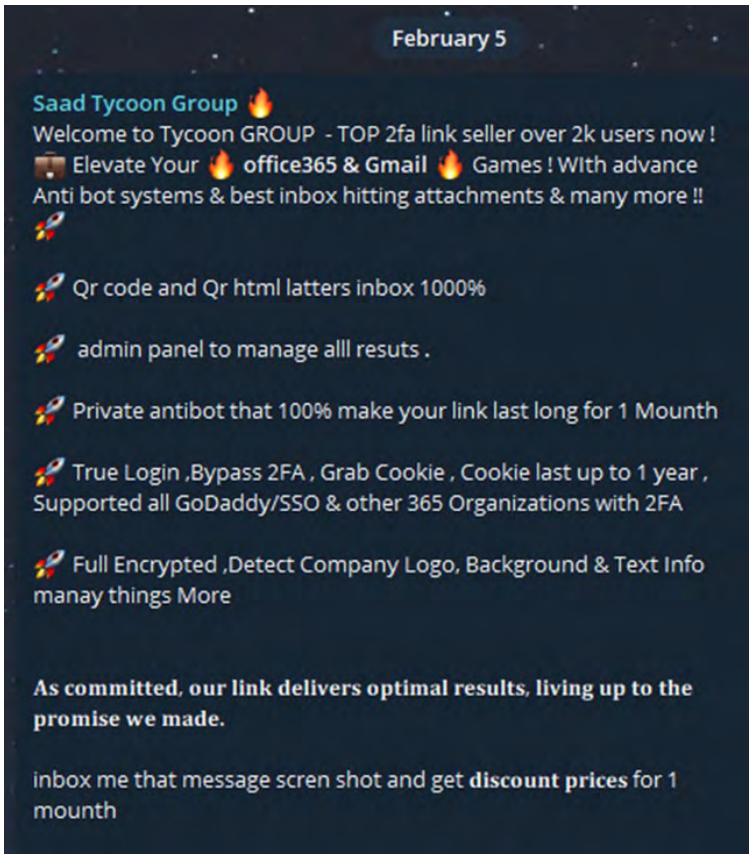


Figure 1: The operators of Tycoon2FA brag that their Phishing -as-a-Service offering can grab cookies, bypass 2-factor authentication protections, and defend against anti-bot software, among having other capabilities.

TRU's analysis of PhaaS AitM campaigns reveals the scale and sophistication of these operations. The infrastructure used by these services and their customers/affiliates was tied to 229 distinct Autonomous System Numbers (ASNs) and 668 distinct networks, providing geographic distribution across 240 source locations:

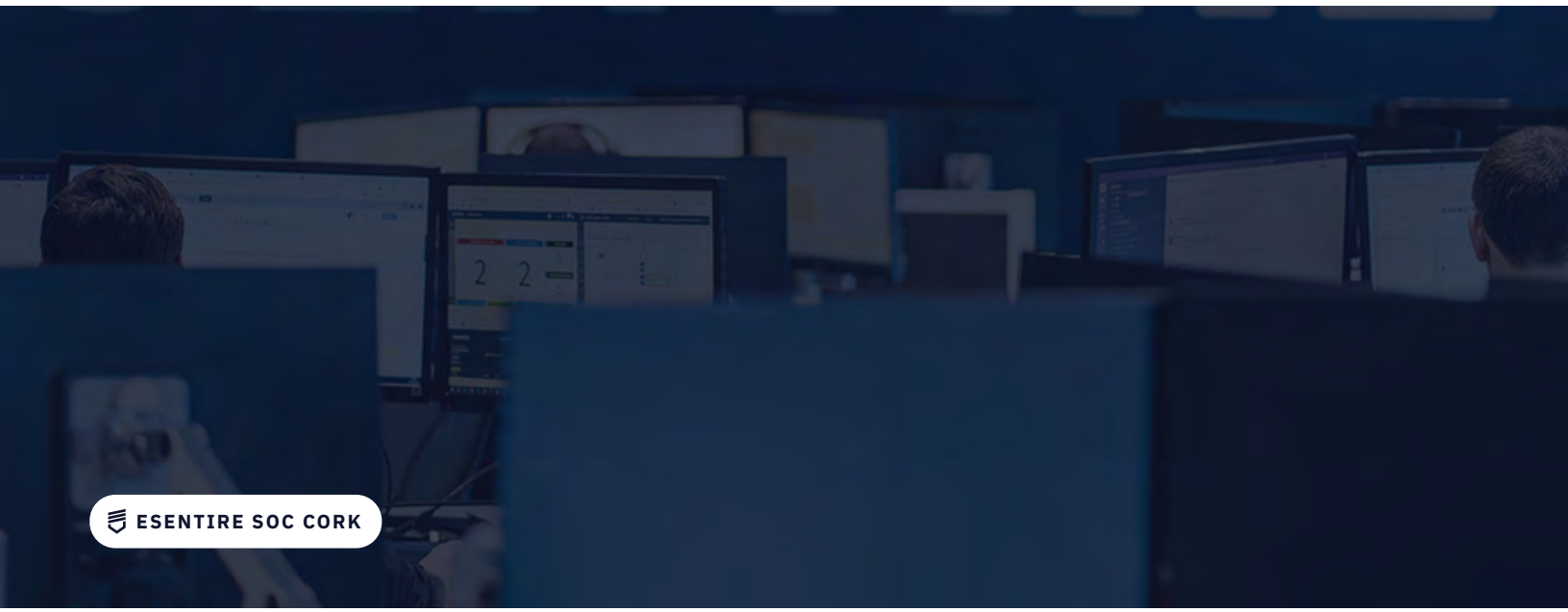
Top PhaaS Threats (% of Account Compromise Cases)	Threat Actor Infrastructure	Top Source Countries
• Tycoon2FA **(58%)** • Mamba2FA **(<2%)** • Sneaky2FA **(<2%)** • EvilProxy **(<1 %)** • Gabagool **(<0.5%)** • Others **(38%)**	• Distinct ASNs: **229** • Distinct Networks: **668** • Distinct Source Locations: **240** • Distinct Privacy Services: **32**	• United States **(78%)** • Great Britain **(4%)** • Netherlands **(3%)** • Germany **(3%)** • Nigeria **(2%)**

This infrastructure diversity serves multiple purposes:

1. Evading geographic-based security controls, providing redundancy against takedown efforts
2. Maintaining the appearance of legitimate traffic patterns

The customer base for these services extends far beyond traditional cybercriminal organizations. The low barrier to entry and high potential return on investment have attracted a broader range of threat actors, including those with limited technical capabilities who can now execute sophisticated identity theft campaigns.

This democratization has significantly expanded the threat actor ecosystem, making credential theft attacks more frequent and geographically diverse.

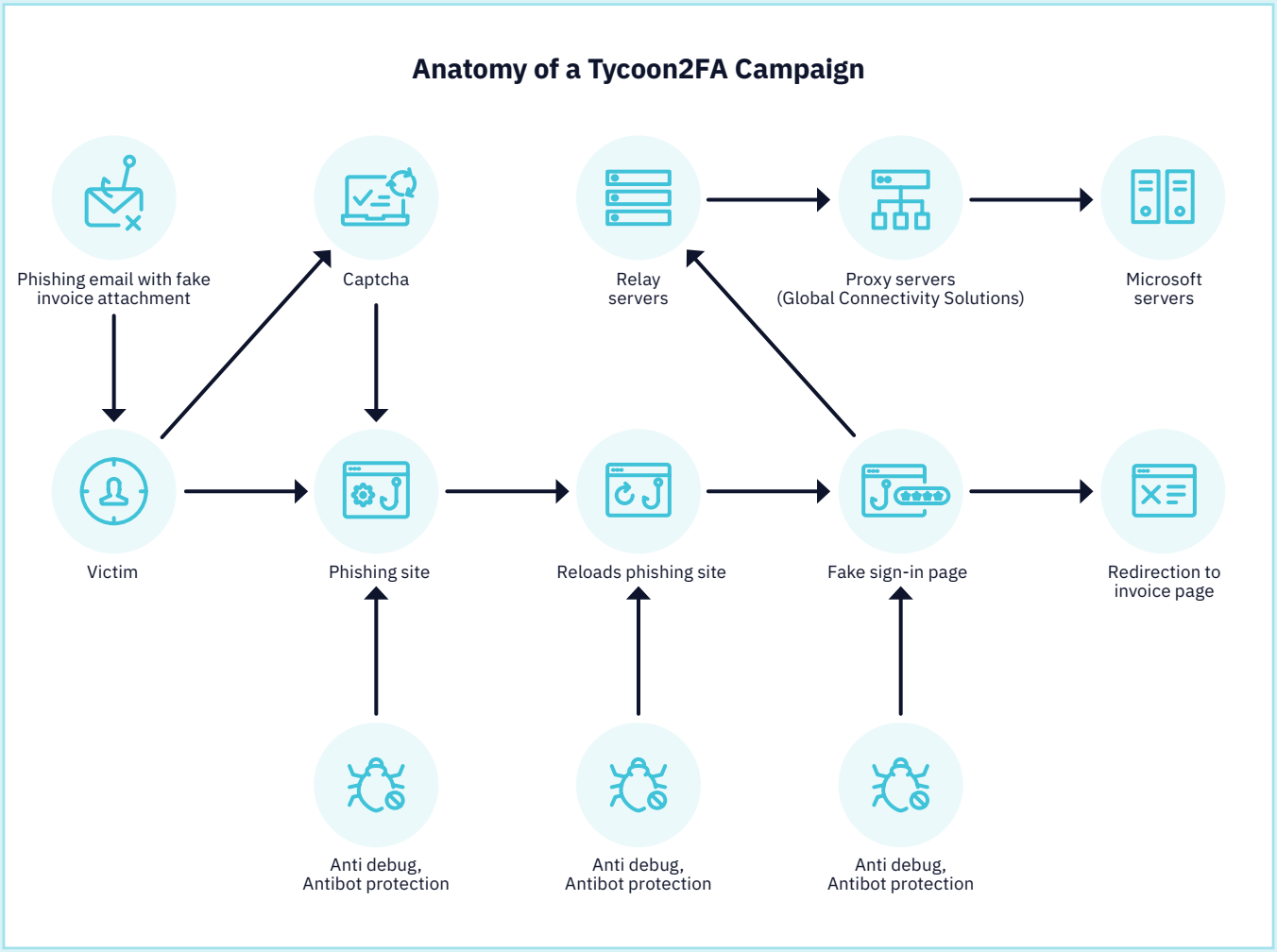


Spotlight on Tycoon2FA Phishing-as-a-Service

Tycoon 2FA is a sophisticated phishing-as-a-service (PhaaS) platform that emerged in August 2023, designed to bypass multi-factor authentication (MFA) and steal session cookies from Microsoft 365 and Gmail accounts.

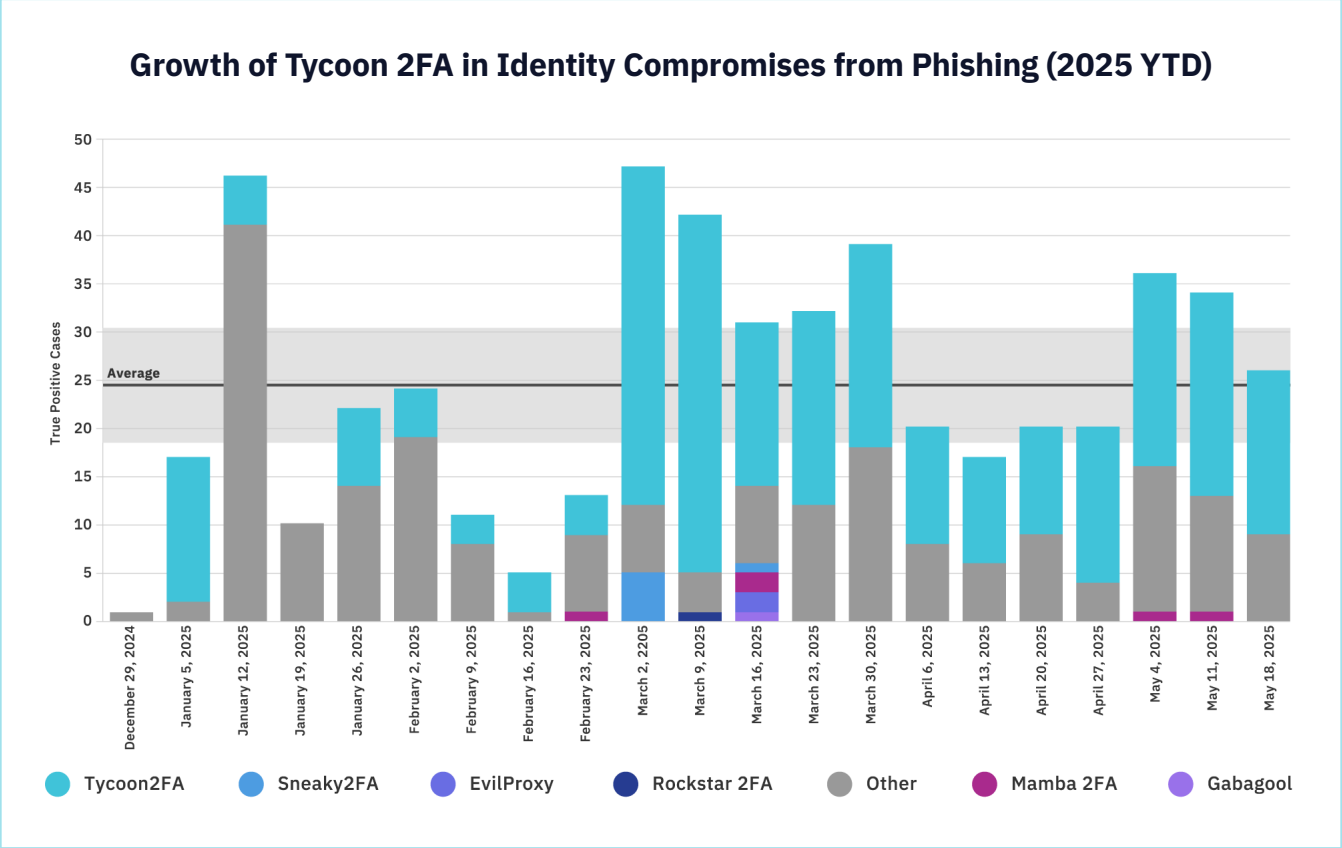
It uses advanced evasion techniques and is continuously updated, making it a significant threat to users and organizations. In recent campaigns, TRU has observed a shift away from using Cloudflare Turnstile captchas to the implementation of a custom algorithm to generate captchas.

The figure below highlights a **Tycoon2FA phishing campaign**, breaking down each stage of the attack chain:



While investigating the incident, TRU observed the initial phishing email, the sophisticated evasion techniques employed, including custom CAPTCHA implementation, anti-debugging mechanisms, and traffic filtering methods. The analysis also covers the credential harvesting process, focusing on how the phishing kit handles user authentication, encrypts communications, and exfiltrates stolen credentials.

According to TRU's research, Tycoon2FA has dominated as the primary PhaaS platform used by threat actors in 2025, as seen in the figure below:



Tycoon2FA has historically leveraged geographically-varied infrastructure tied to Global Connectivity Solutions LLP, a known bullet proof hosting (BPH) provider, which may be a front for several BPH services marketed on underground forums under names such as 4VPS.

In 2025, Tycoon2FA transitioned to Hivelocity Inc. IP addresses for it's final hop when relaying credentials to Entra ID. This suggests centralized management despite the distributed appearance.

Unlike Global Connectivity Solutions, TRU considers Hivelocity is a legitimate provider of cloud hosting services. It's common for legitimate service providers to be co-opted by threat actors for hosting malicious infrastructure as a means to subvert reputation based controls.

To mitigate cyber threats like Tycoon2FA, TRU recommends implementing a **24/7 Managed Detection and Response (MDR) service** that includes identity threat detection and response capabilities so organizations can revoke session tokens and terminate active sessions.

In addition, regularly conduct proactive threat hunting for sign-ins from unusual autonomous system labels (ASLs)/user agents/applications, modifications to MFA methods, auto-forwarding of emails to external accounts via forwarding rules, extraction of sensitive emails/contacts, access to single-sign-on (SSO) applications, email redirection, and audit log deletion.

Advanced Phishing: Beyond Traditional Email Attacks

Modern phishing campaigns have evolved far beyond simple credential collection forms that mimic legitimate login pages. Contemporary Phishing-as-a-Service platforms implement sophisticated Adversary-in-the-Middle (AitM) architectures that provide real-time credential interception and authentication token capture.

These systems operate as transparent proxies between victims and legitimate authentication services, capturing not only legitimate usernames and passwords but also multi-factor authentication tokens, session cookies, and device fingerprints.

The technical implementation of these attacks highlights just how adversarial capabilities have evolved. When a victim visits a phishing site, their browser communicates with the legitimate identity authentication service (e.g., Microsoft Entra ID) through the attacker's infrastructure.

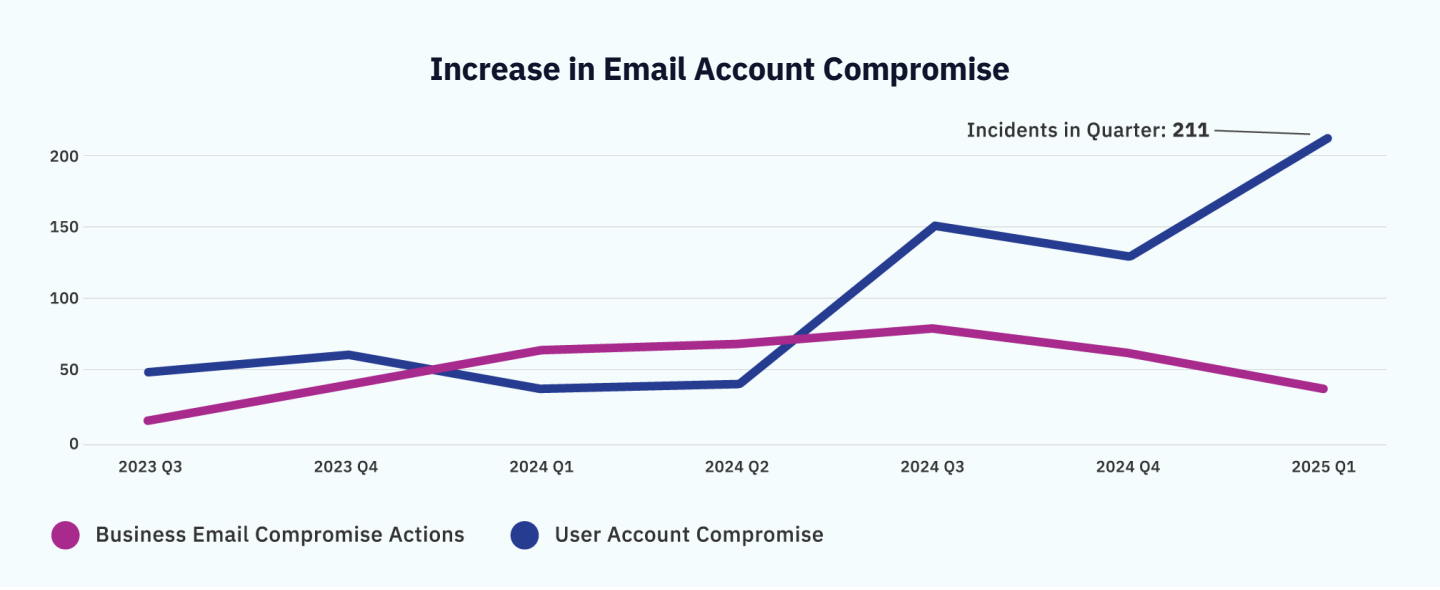
The phishing platform captures all authentication credentials and session tokens, which can be replayed at a later point with the target service. This approach allows threat actors to bypass multi-factor authentication by replaying captured tokens within their validity periods, often within minutes of the initial theft.

Business Email Compromise campaigns have become increasingly sophisticated in their execution timelines and social engineering techniques, costing domestic and international organizations billions of dollars.

According to FBI's IC3 data, between 2013 – 2023, there had been 300K+ domestic and international incidents reported, costing upwards of $55B USD.

Based on threat data observed by TRU across our global customer base, **email account compromises and business email compromises make up 41% of total cases in Q1 2025, up from 25.6% of cases in 2024**. It's important to note that this figure looks at not just phishing attempts (e.g. a user received a malicious email in their inbox) but confirmed cases where a user's identity was compromised.

While both email account takeovers and business email compromises declined in late 2024, TRU has seen a sharp increase in email account compromises, which peaked in early 2025. In comparison, business email compromise cases peaked at 78 in late 2024, followed by a decline:



When looking at the industry breakdown, TRU's analysis highlights that organizations in the **Construction**, **Manufacturing**, Business Services, and Software sectors saw elevated exposure to email-based threats. However, it should be noted that all industries saw some degree of exposure:

Phishing and BEC by Industry

Phishing and BEC	2023	2024	2025
Agriculture			
Construction			
Education			
Entertainment			
Financial			
Government			
Healthcare			
Legal			
Manufacturing			
Retail			
Business Services			
Software			
Transportation			
Utilities			

TRU's analysis also reveals that threat actors are moving from initial account access to active fraud attempts within increasingly compressed timeframes. The figure below shows the timeline from a recent account compromise case where user credentials acquired from a PhaaS kit were used by a threat actor to access the account and immediately begin business email compromise:

10:44 AM	**Tycoon2FA Relay** **Global Connectivity Solutions** Axios/1.7.9
11:10 AM	**Threat Actor Login** **PIA VPN** Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
10:12 AM	**BEC Actions** **Susp. Forwarding Rules** **Inbox Recon**

The typical pattern involves immediate reconnaissance of the compromised account to identify high-value targets, followed by carefully crafted fraudulent communications that leverage legitimate business relationships and communication patterns.

The use of anonymization services has become standard practice among threat actors. Approximately 44% of business email compromise cases involve the use of commercial VPN services or proxy networks to mask the true geographic location of fraudulent activities.

Threat actors frequently select VPN exit points that align with the victim's expected geographic region, making the fraudulent access appear legitimate to basic geographic anomaly detection systems.

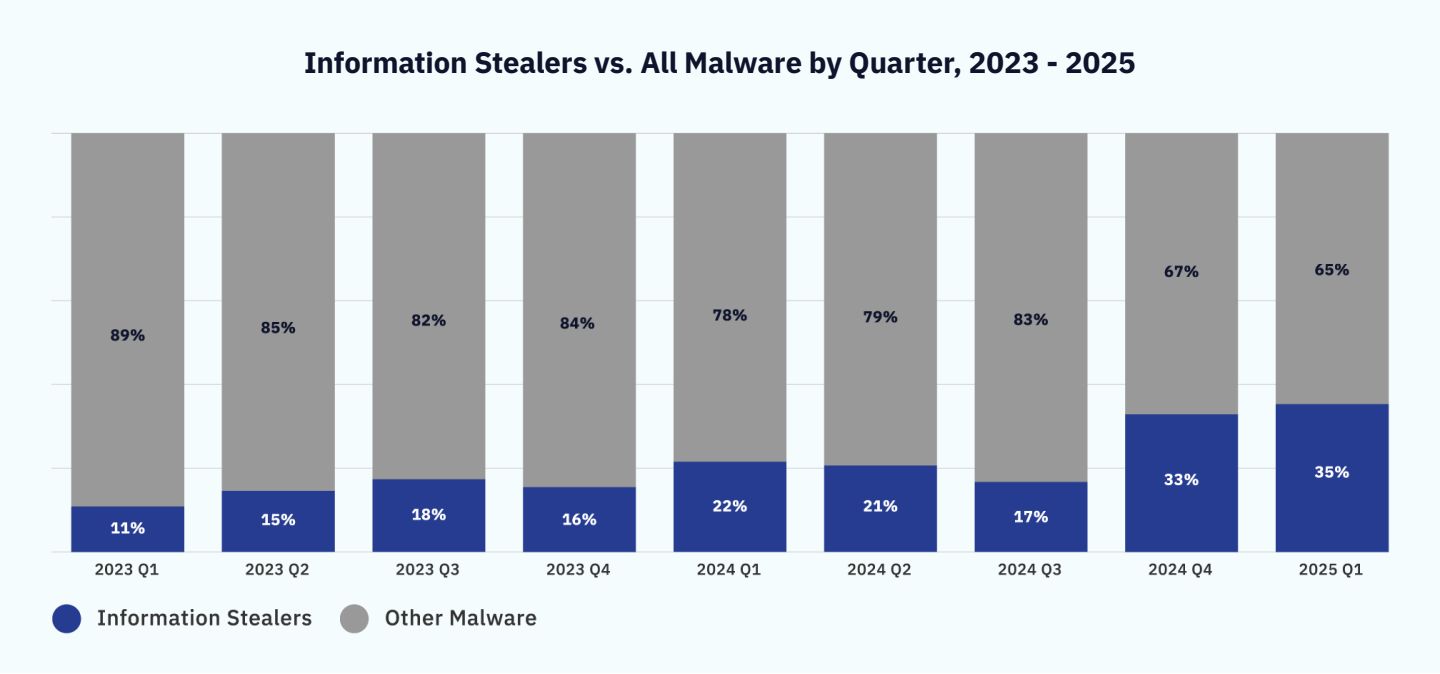
The infrastructure supporting these campaigns demonstrates remarkable persistence and adaptability. Phishing-as-a-Service platforms maintain consistent infrastructure patterns over extended periods, suggesting professional management and operational security practices.

When the infrastructure is disrupted through takedown efforts or defensive measures, these services typically migrate to alternative providers within days, maintaining service continuity for their customer base.

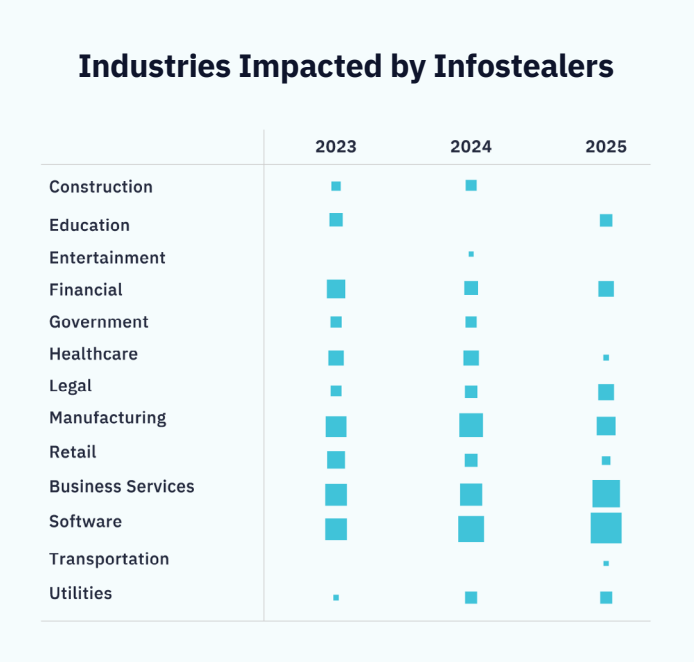
Information Stealers: Comprehensive Identity Harvesting

Infostealers represent another critical component of the Cybercrime-as-a-Service ecosystem. They have evolved from simple keyloggers to comprehensive identity harvesting platforms capable of extracting stored credentials or authentication tokens from infected systems.

Infostealers represent 35% of all disrupted malware threats in 2025, reflecting both their popularity among threat actors and their effectiveness in generating monetizable intelligence. The figure below breaks down the quarter-over-quarter view from 2023 to 2025:



When breaking down by industry, TRU's research has shown that organizations in the Business Services and Software industries have been consistently impacted by infostealers between 2023 – 2025. This is likely due to the increasing reliance on drive-by social engineering tactics observed by TRU.



Modern infostealers target an extensive range of credentials often stored in SaaS applications, identity services, and more.

However, browser-stored passwords, which many users rely on for convenience, are primary targets. These malware families can extract saved passwords from all major browsers, including credentials for business applications, personal services, and admin accounts.

In addition, password manager databases, once considered secure credential storage solutions, are increasingly targeted through memory injection techniques and database extraction methods.

The scope of credential theft extends beyond traditional web-based authentication. VPN client configurations, remote desktop connection files, SSH keys, and application-specific authentication tokens are systematically harvested and prepared for sale.

Cryptocurrency wallet files and browser extension data provide additional monetization opportunities, creating multiple revenue streams from each successful infection.

Of course, the primary concern with credentials stolen by infostealers is that these identities are sold on underground marketplaces through underground forums, markets, and chat rooms. In fact, the infrastructure for these underground marketplaces has become quite sophisticated so threat actors can easily find the type of credentials they want.

Stolen credentials are automatically categorized, filtered, and priced based on perceived value. High-value targets such as business email accounts, administrative credentials, and financial service access command premium pricing.

The marketplaces even provide search and filtering capabilities that allow purchasers to identify specific organizational targets or credential types, dramatically reducing the time between credential theft and exploitation.

The deployment patterns for information stealers reveal the integration of these tools into broader attack campaigns.

Rather than operating as standalone threats, infostealers are frequently deployed alongside Remote Access Trojans and Remote Monitoring and Management tools.

This combination provides threat actors with both immediate credential monetization opportunities and persistent access to compromised systems for follow-on activities.

One of the more recent infostealers to come onto the hacker scene is the so-called Acreed Infostealer. It first emerged in February 2025 and since then, it has been competing to become the number one infostealer on the Dark Markets, especially since law enforcement took action against the Lumma Stealer infrastructure in May 2025 (Figure 2).

Figure 2: A threat actor promoting stolen logs from various online accounts on Russian Market. The infostealer used to steal the logs is listed as the Acreed malware. The threat actor is advertising logs for the online banking websites Capital One bank and Chase bank, Amazon, the Internal Revenue Service, AT&T, and many others.

Spotlight on Lumma Stealer Malware

Lumma Stealer, identified by TRU as the most disrupted malware family in 2024 and 2025, demonstrates the evolution of these tools toward service-oriented architectures.

Also known as LummaC2, this malware is developed in C language and has been operating as a Malware-as-a-Service in Russian-speaking forums since August 2022. The malware targets browser-stored credentials, password manager databases, cryptocurrency wallets, VPN configurations, and application-specific authentication tokens (Figures 3-4).

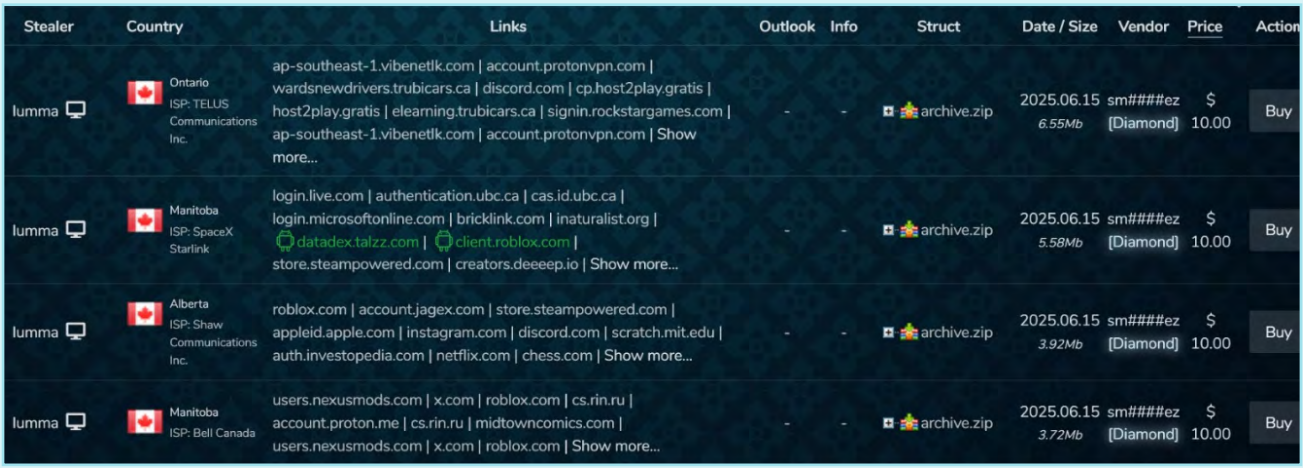


Figure 3. A variety of logs, from various Canadian-based victims, are listed for sale on Russian Market. Each victim has a log archive, and each archive is $10 to purchase. Lumma Stealer targets credentials stored in the victims' browsers, password manager databases, cryptocurrency wallets, VPN configurations, and application-specific authentication tokens.

Extensions:

MetaMask | 1Password | Braavos | Agrent X | Coinhub | Leap Wallet | Safepal | LastPass | Ronin Wallet | Evernote | MultiversX Wallet | ForniterWallet | Fluvi Wallet | Glass Wallet | Morphis Wallet | XVerse Wallet | Compas Wallet | Havah Wallet | Sui Wallet | Venom Wallet | Trust Wallet | TronLink | OKX | Binance Chain Wallet | Yoroi | Nifty | Math | Coinbase | Guarda | EQUA | Jaxx Liberty | BitApp | iWlt | EnKrypt | Wombat | MEW CX | Guild | Saturn | NeoLine | Clover | Rabby | Martian | Bitwarden | Nami | Petra | ExodusWeb3 | Sub | PolkadotJS | Talisman | CryptoCom | Liquality | Terra Station | Keplr | Sollet | Auro | Polymesh | ICONex | Nabox | KHC | Temple | TezBox | DAppPlay | BitClip | Steem Keychain | Nash Extension | Hycon Lite Client | ZilPay | Coin98 | Authenticator | Cyano | Byone | OneKey | Leaf | Solflare | Magic Eden | Backpack | Authy | EOS Authenticator | GAuth Authenticator | Trezor Password Manager | Phantom | UniSat | Rainbow | Bitget Wallet | MetaMask Mozilla

Cold Wallets:

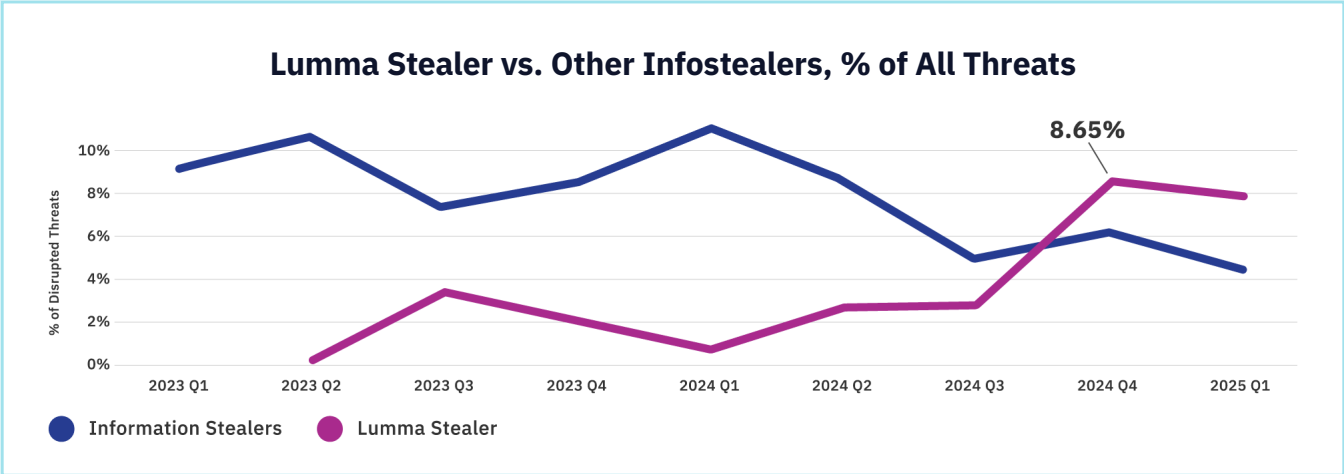
Ethereum | Exodus | Ledger Live | Atomic | Coinomi | Bitcoin core | Binance | JAXX New Version | Electrum-LTC | ElectronCash | Guarda | DashCore | Wasabi | Daedalus | Chrome | Chrome Beta | Opera | Opera Neon | Opera GX Stable | Edge | Brave | EpicPrivacyBrowser | Vivaldi | Maxthon | Iridium | AVG Secure Browser | QQBrowser | 360Browser | ZiNiao Browser | CentBrowser | Chedot | CocCoc | Mozilla Firefox | Waterfox | Pale Moon

Applications:

KeePass | 1Password | Bitwarden | NordPass | Telegram | FileZilla | TotalCommander | AnyClient | 3D-FTP | SmartFTP | FTPGetter | FTPbox | FTPInfo | FTPRush | FTP Commander Deluxe | FTP Manager Lite | Auto FTP Manager | OpenVPN | NordVPN | ProtonVPN | AnyDesk | Azure | Notes | Notezilla | TheBat | Pegasus | Mailbird | EmClient

Figure 4. An online posting from the operators of Lumma Stealer, outlining the various applications, crypto wallets, and extensions that it targets for users' credentials.

However, it wasn't until late 2024 that Lumma Stealer surpassed all other infostealers in terms of the top disrupted threats by TRU:



The stolen data is automatically formatted and prepared for sale on underground marketplaces, creating an efficient pipeline from initial infection to credential monetization by way of facilitating fraudulent bank transfers and cryptocurrency theft.

The malware includes built-in filtering capabilities that allow threat actors to prioritize high-value credentials directly within the control panel interface. This eliminates the need for manual credential review and accelerates the monetization process.

The recent law enforcement disruption of Lumma Stealer infrastructure in May 2025 provides insight into the scale of these operations, with thousands of active customers and millions of stolen credential records.

Exploitation of Monitoring Blind Spots to Deploy Ransomware

One of the most concerning trends in the current threat landscape is the exploitation of "out-of-scope" endpoints (i.e., an organization's unmonitored blind spots) by sophisticated threat actors.

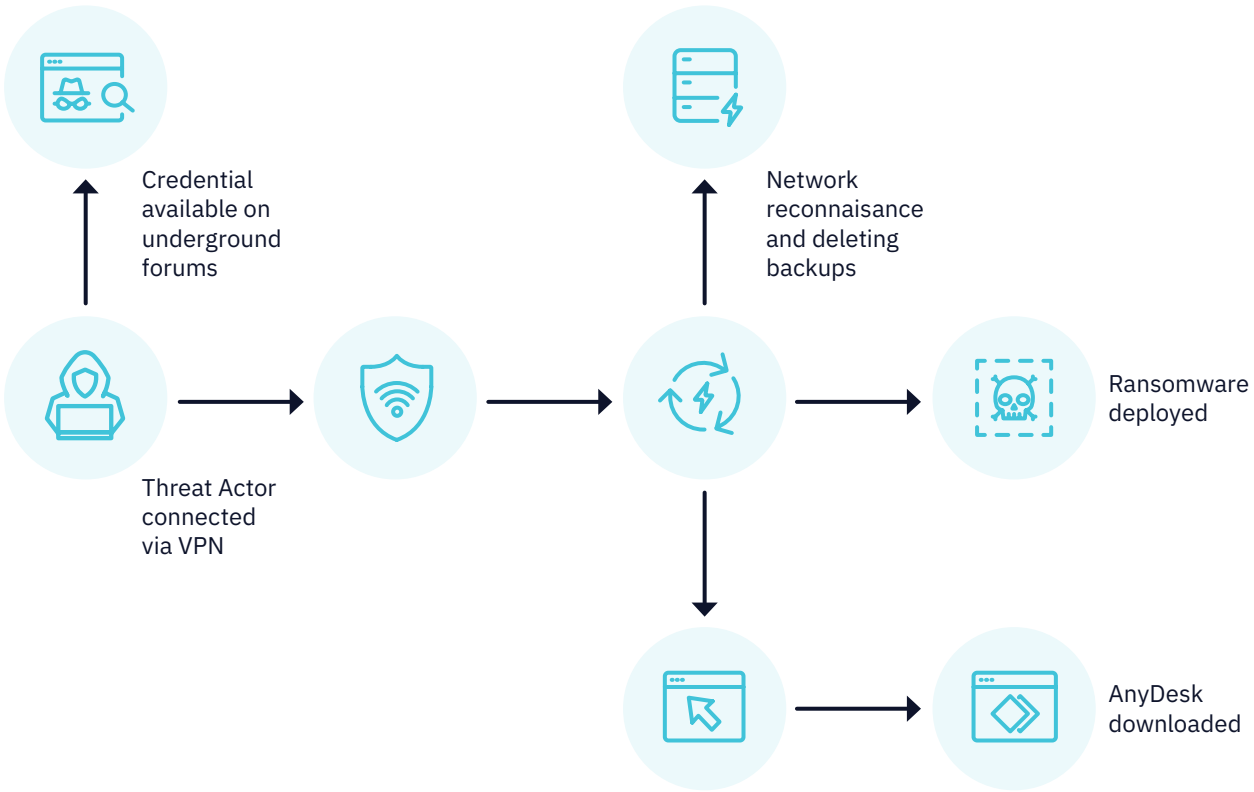
These gaps in security visibility create opportunities for adversaries to establish persistent access while remaining undetected for extended periods. TRU's research reveals multiple attack patterns that specifically target these visibility gaps.

Unmanaged devices represent the most significant blind spot in most organizational security architectures. Personal devices used for business purposes, legacy systems outside formal asset management, and shadow IT infrastructure create attack surfaces that remain invisible to traditional security controls.

When infostealers compromise these devices and extract corporate credentials, the initial infection often goes undetected while the stolen credentials provide authenticated access to corporate resources.

In one incident observed by TRU, stolen credentials that were then purchased from an underground market were used to access the network using the corporate VPN service. The threat actor was able to establish a foothold within the internal network before deploying ransomware.

Valid Credentials Used to Deploy Ransomware



The organization's first indication of compromise occurred during the ransomware deployment phase, well after the initial credential theft and network access. Our team of 24/7 SOC Analysts discovered the intrusion mid-exploitation and traced the infection to an unmanaged device.

Unfortunately, it turned out that the organization was not monitoring their VPN logs, creating a blind spot that the threat actor had exploited.

This pattern represents a fundamental challenge for organizations that lack visibility into the security posture of devices that have access to corporate credentials.

Furthermore, third-party relationships create additional blind spots that sophisticated threat actors actively exploit. For example, Managed Service Provider (MSP) compromises have become particularly impactful, since MSP credentials often provide privileged access to multiple downstream customer environments.

TRU has identified multiple cases where Remote Monitoring and Management (RMM) platforms that were managed by an MSP were compromised by threat actors, providing them with legitimate admin access to customer networks.

The supply chain implications of these attacks extend beyond direct compromise. When MSP environments are compromised, the threat actors inherit the trust relationships and access privileges that the MSP has established with its customers.

This creates a force multiplication effect where a single compromise can impact dozens or hundreds of downstream organizations. The legitimate nature of MSP access makes these attacks particularly difficult to detect through traditional monitoring approaches.

Shadow IT infrastructure presents another significant challenge for organizational security visibility. Development systems, test environments, and forgotten infrastructure often lack the security controls and monitoring capabilities deployed in production environments.

Our case analysis includes multiple instances where exposed development systems with weak authentication were successfully brute-forced, providing threat actors with legitimate credentials for production systems.

These attacks succeed because the compromised systems exist outside normal security monitoring and lack the defensive measures that would prevent or detect brute force attempts.

Strategic Recommendations to Defend Against Identity-based Threats

Transforming the Identity Security Architecture

Given that traditional authentication mechanisms are insufficient against modern threats, organizations must fundamentally restructure their security architecture. To effectively mitigate these risks, organizations must rethink their identity security architecture by shifting from reactive defenses to proactive, risk-aware strategies.

We strongly recommend taking a modernized approach centered around phish-resistant authentication, Zero Trust principles, and real-time access to threat intelligence to protect against credential compromise and unauthorized access:

Prioritize Phish-Resistant Authentication:

- Traditional MFA can be bypassed through Adversary-in-the-Middle attacks so replace traditional MFA with phish-resistant methods such as FIDO2/ WebAuthn and passkeys, which use cryptographic authentication that cannot be intercepted or replayed by adversaries.
- Deploy phish-resistant MFA policies first for high-value targets, including privileged administrative accounts, executive identities, and critical business applications that contain access to sensitive data.
- Develop a phased rollout strategy, applying immediate protection to privileged users and gradually transitioning standard users.

Adopt Zero Trust Identity Principles:

- Move away from static, one-time authentication models in favor of real-time access validation that treats each access request as potentially risky.
- Enforce continuous identity verification that evaluates a combination of dynamic risk signals, such as:
  - **User identity verification** – Authenticate the legitimacy of the user beyond initial login, factoring in context like session behavior and historical access patterns.
  - **Device compliance status** – Confirm that the connecting device meets baseline security requirements (e.g., corporate-managed, updated software).
  - **Geographic location** – Identify geographic anomalies, such as logins from unfamiliar or high-risk regions, that may indicate credential misuse.
  - **Behavioural anomolies** – Monitor for irregular activity like access at odd hours or attempts to use unauthorized applications, which may signal an active threat.

Integrate Device Compliance into Access Decisions:

- Treat the device as a critical factor in trust decisions by requiring real-time evaluation of its security posture before granting access to applications or data.
- Make sure to assess:
  - **Patch and update status** – Ensure the device is running the latest OS and software versions to close known vulnerabilities.
  - **Endpoint protection presence** – Verify that next-gen anti-virus, **endpoint detection and response (EDR) solutions**, or other security controls are active and up-to-date.
  - **Configuration compliance** – Check that devices meet internal security policies, such as full-disk encryption, secure boot, and restricted admin privileges.
- Block access from devices that fail to meet security baselines, even if valid credentials are used, reducing the risk posed by compromised or unmanaged endpoints.

Implement Risk-Based Conditional Access Policies:

- Move beyond simple role- or group-based access controls by applying adaptive policies that change based on assessed risk at the time of access.
- Use contextual signals such as:
  - **Unusual login geographies** – For example, a sudden login from a foreign country immediately after a domestic session.
  - **Behavioral deviations** – Detect unexpected usage patterns such as a finance user accessing HR tools or downloading excessive data.
  - **Irregular application access activity** – Identify attempts to access sensitive applications that fall outside the user's normal behavior profile.
- When risk signals are detected, enforce step-up authentication, session termination, or access blocks until further verification is completed.
- Regularly review and refine these policies using internal data, incident trends, and external threat intelligence to ensure they remain aligned with current risks.

Advanced Detection and Monitoring Capabilities

Detecting identity-based threats early is critical to preventing lateral movement, privilege abuse, and data exfiltration. As adversaries increasingly exploit stolen credentials and evade traditional perimeter defenses, organizations must adopt advanced monitoring strategies that go beyond static rule-based detection.

Therefore, we recommend implementing sophisticated monitoring capabilities that can identify identity-based attacks in their early stages, before significant damage occurs:

Centralized Authentication Log Analysis as a Foundational Layer:

- Establish **comprehensive logging** for all authentication activity across cloud platforms, on-premises applications, and remote access services.
- Ensure logs are centralized into a SIEM or security data lake for correlation and real-time analysis.
- Analyze logs for early indicators of identity compromise, including repeated failed login attempts, login anomalies (e.g., time-based irregularities or unexpected user-agent strings), and lateral movement between cloud services using shared tokens or OAuth abuse.
- Integrate logs with behavioral baselining tools to differentiate between legitimate and anomalous activity.

Autonomous System Number (ASN)-Based Threat Intelligence Integration:

- Use ASN-based monitoring to identify authentication traffic originating from malicious hosting infrastructure, often tied to Phishing-as-a-Service (PhaaS) operations.
- Maintain **updated threat intelligence feeds** that track ASN/IP ranges known for credential phishing campaigns, brute-force and password-spraying attacks, botnet-driven login activity, and more.
- Automatically flag or block authentication attempts from suspicious ASNs, reducing the attack surface from known malicious infrastructure.

Enhanced Impossible Travel Detection Using Contextual Signals:

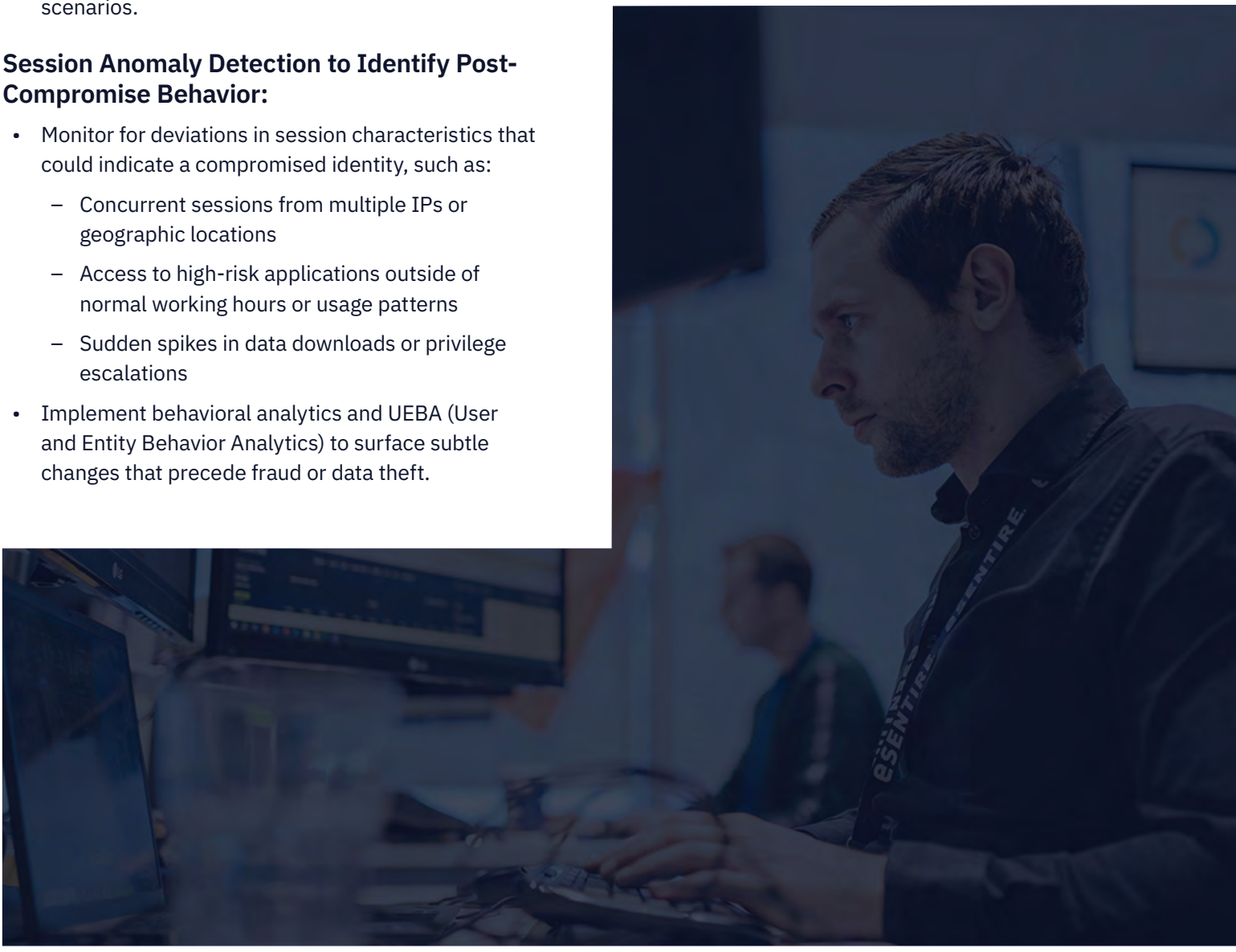
- Move beyond basic geo-velocity calculations by incorporating:
  - **Device fingerprinting** – Match device types and OS across sessions to confirm consistency.
  - **Historical access patterns** – Consider a user's normal travel, VPN usage, and cloud-based login behavior.
  - **Application context** – Flag anomalies where logins from different geographies are used to access unrelated or restricted apps.
- Adjust detection thresholds to minimize false positives from legitimate business travel or split-tunneling VPN scenarios.

Session Anomaly Detection to Identify Post-Compromise Behavior:

- Monitor for deviations in session characteristics that could indicate a compromised identity, such as:
  - Concurrent sessions from multiple IPs or geographic locations
  - Access to high-risk applications outside of normal working hours or usage patterns
  - Sudden spikes in data downloads or privilege escalations
- Implement behavioral analytics and UEBA (User and Entity Behavior Analytics) to surface subtle changes that precede fraud or data theft.

Credential Exposure Monitoring Across Underground Markets and Threat Intel Sources:

- **Continuously scan dark web** marketplaces, paste sites, and underground forums for leaked or stolen organizational credentials.
- Upon detection, trigger automated response protocols, including immediate password resets, targeted monitoring for affected accounts, and account audit and activity review to assess compromise scope.
- Integrate this intelligence into identity lifecycle management workflows to ensure compromised identities are contained before abuse.



Operational Response Framework Enhancement

The accelerated pace of identity-based attacks demands a shift from traditional, reactive incident response toward agile, identity-centric frameworks capable of executing containment measures within hours.

Stolen credentials can be weaponized in minutes, allowing attackers to escalate privileges, exfiltrate data, or establish persistence long before conventional response teams can mobilize.

To effectively mitigate identity-related threats, organizations must evolve their response playbooks to include rapid identity isolation, automated containment triggers, and integrated legal and third-party coordination procedures:

Implement Dual-Track Response Protocols for Identity and Asset Containment:

- When identity compromise is detected, initiate parallel containment workflows:
- Identity-focused actions (e.g., password reset, token revocation, MFA re-enrollment).
- Asset-focused investigation, examining all systems accessed by the compromised account for signs of malware, lateral movement, or data access.
- Ensure incident response playbooks include identity compromise scenarios with coordinated roles across IAM, SOC, and endpoint teams.

Accelerate Response Timelines to Reflect Modern Threat Speed:

- Redefine incident SLAs for identity-related threats to mandate containment actions within one hour of detection.
- Automate critical response steps including session termination, password reset and credential revocation, and elevated logging and real-time monitoring.
- Base urgency on the fact that credential misuse often begins within minutes of compromise, limiting the effectiveness of traditional response windows.

Establish Escalation Triggers Based on High-Confidence Indicators:

- Define automated escalation rules that combine multiple telemetry sources to validate probable compromise (e.g., logins from known malicious ASNs, geographic or behavioral anomalies, and unusual access to sensitive applications).
- Calibrate these triggers regularly to balance speed with accuracy, minimizing false positives while ensuring high-risk events receive immediate attention.

Codify Legal and Regulatory Response for Credential Exposure:

- Prepare pre-approved communication templates for notifying internal stakeholders, affected users, and external regulators.
- Establish jurisdiction-aware decision trees to handle varying notification requirements based on data residency, industry compliance requirements (e.g., GDPR, HIPAA, SEC rules), and severity and scope of the identity compromise
- Involve legal and compliance teams early in incident workflows to accelerate disclosure timelines without missteps.

Enforce Identity Security Requirements in Third-Party Risk Management:

- Require phish-resistant authentication, activity logging, and incident response capabilities from vendors and partners with access to internal systems.
- Conduct regular security assessments to validate controls and identify identity-related gaps.
- Include identity security clauses in contracts, specifying requirements for identity verification practices, notification obligations for identity-related breaches, and alignment with internal response expectations.

A 90-Day Implementation Roadmap for Securing Identities

Organizations should implement identity security improvements through a phased approach that addresses the most critical vulnerabilities first while building toward comprehensive identity security architecture.

DAYS 0-30

Immediate actions to focus on high-impact, low-complexity improvements that provide immediate risk reduction.

- The initial assessment phase should evaluate current MFA implementations for vulnerability to Adversary-in-the-Middle attacks. Inventory current authentication methods and prioritize replacement of vulnerable implementations with phish-resistant alternatives.
- Authentication monitoring for known PhaaS infrastructure should be implemented immediately using existing SIEM capabilities.
- Threat intelligence feeds that identify known malicious ASNs and IP ranges can be integrated into existing monitoring platforms to provide immediate alerting for authentication attempts from suspicious sources.
  - This capability can be implemented within days and provides immediate protection against known threats.
- Third-party security assessments should be conducted within the first 30 days to identify potential blind spots in organizational security posture.
  - These assessments should focus specifically on authentication security, credential management practices, and incident response capabilities.
  - Any identified deficiencies should be addressed through contract modifications or alternative service arrangements.

DAYS 31-90

Short-term initiatives that focus on implementing foundational identity security capabilities.

- Phase one deployment of phish-resistant multi-factor authentication should prioritize privileged accounts and critical business applications. This deployment should include managed phishing and security awareness training and support procedures to ensure successful adoption while maintaining operational continuity.
- Enhanced logging and monitoring capabilities for authentication anomalies should be implemented during this phase. Organizations should deploy centralized authentication logging, implement real-time analysis capabilities, and establish baseline behavioral patterns for users and applications.
  - These capabilities provide the foundation for advanced threat detection and response procedures.
- Organizations should implement network scanning, asset discovery, and device compliance monitoring to identify systems that have access to corporate resources but lack appropriate security controls. This assessment should include personal devices used for business purposes, legacy systems, and shadow IT infrastructure.

BEYOND 90 DAYS

Long-term strategic transformation initiatives that focus on comprehensive zero trust identity architecture implementation.

- Organizations should implement advanced threat hunting capabilities specifically designed for identity-based attacks, comprehensive third-party risk management programs, and continuous security awareness and simulation programs.
- The complete zero trust identity architecture should implement continuous authentication verification, device compliance integration, and risk-based access controls across all organizational resources.

Timeline	Key Initiatives	Objectives
DAYS 0-30	→ Assess existing MFA for phish resistance → Monitor authentication via threat intelligence (ASN/IP feeds) → Conduct third-party identity security assessments	✓ Identify and mitigate high-risk vulnerabilities ✓ Deploy quick wins with immediate protection ✓ Reduce third-party blind spots
DAYS 31-90	→ Begin phish-resistant MFA rollout (privileged accounts/apps) → Deploy centralized auth logging and anomaly detection → Launch unmanaged device discovery and risk analysis	✓ Establish foundational monitoring and access controls ✓ Support secure adoption with training ✓ Identify hidden attack vectors
BEYOND 90 DAYS	→ Architect full Zero Trust identity stack (continuous auth, device compliance, risk-based access) → Implement identity-focused threat hunting- Expand third-party risk governance → Launch ongoing user awareness and simulation programs	✓ Achieve long-term resilience against identity-based threats ✓ Operationalize identity security as part of business processes ✓ Mature vendor oversight and user education programs

Conclusion

The cybersecurity landscape has undergone a fundamental transformation that requires organizations to completely rethink their approach to security architecture and threat response.

Identity-based attacks are not an emerging threat that should simply be monitored; they are the current dominant attack vector that require organizations to have a strong 24/7 threat detection and response defense strategy in place to prevent business disruption.

TRU's threat data of over 19,000 identity-related security investigations, since 2024, across our global customer base provides clear-cut evidence of this shift.

The 156% increase in identity-driven threats between 2023 and 2025 reflects how adversarial attack patterns have shifted toward the most efficient and effective attack methods available.

Traditional security models built around perimeter defense and endpoint protection are fundamentally insufficient against adversaries who possess valid organizational credentials.

Compounding this shift are the economic drivers behind this transformation that ensure its persistence and continued evolution. Cybercrime-as-a-Service platforms have democratized access to sophisticated attack capabilities, enabling threat actors with limited technical skills to execute enterprise-grade credential theft campaigns.

The ROI for identity-based attacks far exceeds that of traditional malware or vulnerability exploitation, creating strong incentives for continued adversarial focus on authentication systems and credential theft.

Organizations that fail to adapt their security architectures to address identity-centric threats face significant business risks that extend beyond traditional cybersecurity concerns.

Business Email Compromise attacks result in direct financial losses, regulatory compliance violations, and reputational damage that can impact customer relationships and market position. Moreover, the compressed timeline of modern identity attacks leaves little margin for error in threat detection and response capabilities.

It's clear that the path forward requires immediate action across multiple dimensions of organizational security:

- **Phish-resistant authentication** must be implemented for all high-value accounts and critical business applications.
- **Comprehensive monitoring capabilities** must be deployed to detect identity-based attacks in their early stages.
- **Rapid incident response procedures** must be established to contain threats within hours of detection rather than the days or weeks typical of traditional incident response timelines.

Of course, technical implementations can only take organizations so far; IT/Security leaders must educate executive teams and board members about the fundamental nature of identity-based business risks.

IT leadership must allocate budget and resources to identity security initiatives that may require significant upfront investment but provide essential protection against the dominant threat vector in the current landscape.

To adapt to the evolving threat landscape, organizations must prepare for continued development in identity-based attack techniques. The organizations that invest in comprehensive identity security architectures today will be best positioned to adapt to these future developments while maintaining effective protection against current threats.

Organizations can either proactively transform their security architectures to address identity-centric threats, or they can continue operating with obsolete security programs until a successful attack forces reactive changes under crisis conditions.

Why Choose eSentire MDR for Identity to Protect Against Identity-based Threats

As the number of attacks transition from on-premises to the cloud, organizations need seamless extension of security measures.

eSentire MDR for Identity investigates and responds to compromised identities and insider threats across your hybrid cloud environments. We go beyond just controlling and provisioning identity access. With eSentire, you can unify and strengthen your security posture at the identity attack vector by detecting credential misuse, privilege escalation and lateral movement.

How We Help	Your Outcomes
• Monitor users, entity behavior, and activities with learning-based analytics for authentication and authorization • 24/7 monitoring and investigation of identities • Identify unused accounts, unused permissions, scenarios of over-permissions, and unnecessarily large, compromised identity blast radius • Disable suspicious or compromised users • Force a password reset • Detects potential malicious insider activity	• Visibility into advanced persistent and malicious insider threat activities • Correlate identity-related events with broader security incidents from various sources including logs, network, and endpoint • Reduced alert noise • Reduced Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) • Improvement of overall security posture • Mitigation of potential business disruption • Complete response to identity and insider threats with elite threat hunting and remediation support

Ready to get started?

Get in touch to discuss how eSentire MDR can help you build a more resilient security operation today.

CONTACT US

eSentire

eSentire, Inc., the Authority in Managed Detection and Response (MDR), protects the critical data and applications of 2000+ organizations in 80+ countries, across 35 industries from known and unknown cyber threats by providing Exposure Management, Managed Detection and Response and Incident Response services designed to build an organization's cyber resilience & prevent business disruption. Founded in 2001, eSentire protects the world's most targeted organizations with 65% of its global base recognized as critical infrastructure, vital to economic health and stability. By combining open XDR platform technology, 24/7 threat hunting, and proven security operations leadership, eSentire's award-winning MDR services and team of experts help organizations anticipate, withstand and recover from cyberattacks. For more information, visit **www.esentire.com** and follow **@eSentire**.