



The Infostealer-Driven Surge in Account Takeovers and BEC Attacks



WHITEPAPER

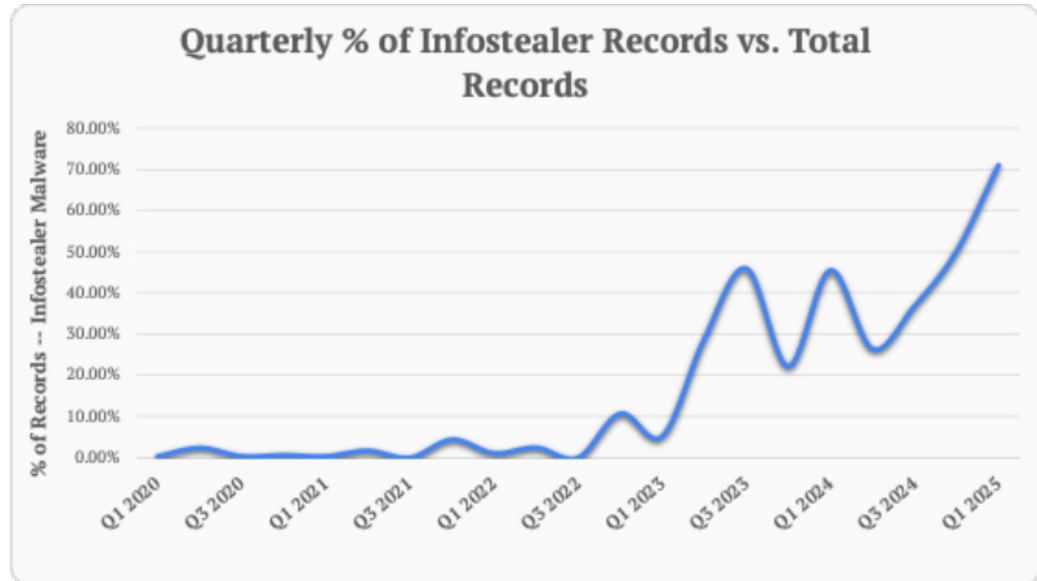




Executive Summary

Account Takeover (ATO) and Business Email Compromise (BEC) attacks continue to plague enterprises, now supercharged by an abundance of stolen data available to cybercriminals. In the past 1–3 years, information-stealing malware (“infostealers”) have enabled a massive underground supply of credentials, session tokens, cookies, and other sensitive data. Threat actors leverage this data to hijack accounts at scale – bypassing multi-factor authentication (MFA) and launching fraud or breaches with alarming ease. For example, over **6 billion** account credentials were stolen by infostealer malware in 2024 alone, accounting for nearly two-thirds of all credentials stolen that year. Enormous infostealer data dumps circulate on the dark web and Telegram; one recent 1.5 TB cache contained **284 million** account credentials lifted from infostealer logs on a single Telegram channel. This glut of stolen login data is directly fueling a rise in ATO and BEC campaigns. Enterprise security teams face a heightened risk environment where even “secured” accounts can be silently compromised using valid credentials or session cookies.

This whitepaper examines the persistent identity and access threats of ATO and BEC in the context of infostealer-driven data breaches. We define ATO and BEC and explain why they remain so pervasive. We then explore the surge in infostealer malware and the types of data they siphon, along with trends in dark web and Telegram marketplaces where this data is traded. Real-world cases illustrate how infostealer-derived data is exploited by attackers. We discuss the cybersecurity risks for organizations and individuals – particularly how stolen cookies and credentials enable attackers to bypass MFA and infiltrate environments undetected. Finally, we provide recommendations for security teams to detect and mitigate these threats.




(Figure 1: Percentage of total dark web records attributed to infostealer malware, by quarter — HackNotice Threat Monitoring Data, 2020–2025.)

Understanding ATO and BEC: Persistent Threats

Account Takeover (ATO) refers to an attack where a malicious actor gains unauthorized access to a user's account – be it an employee's corporate login or a customer's online account. Once in control, the attacker can steal data, initiate fraudulent transactions, or escalate their access. Business Email Compromise (BEC) is a related threat in which an attacker compromises a business email account (or convincingly impersonates one) to trick employees or partners into executing unauthorized payments or divulging sensitive information. BEC scams typically involve fraudulent emails from what appears to be a trusted executive, supplier, or partner, and they frequently lead to large financial losses or data exposures.

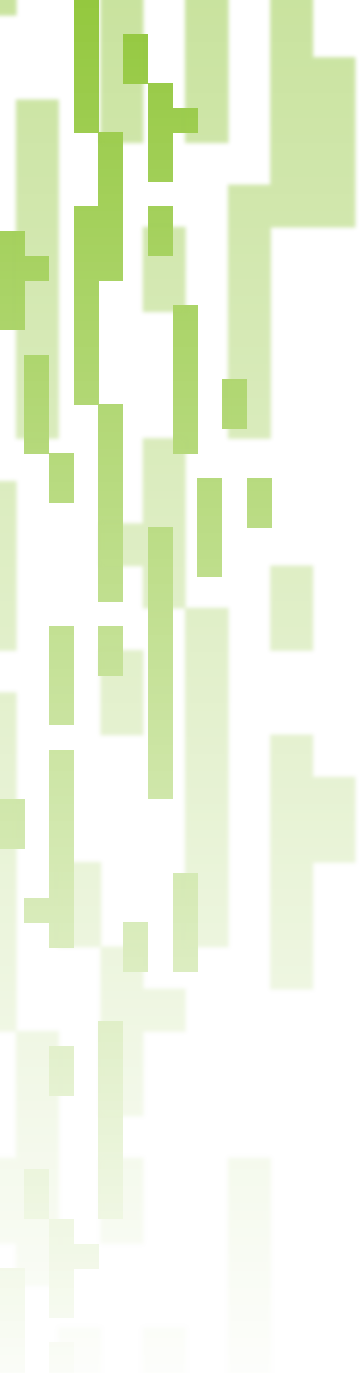
Both ATO and BEC have proven to be persistent, costly threats. More than 75% of security leaders globally rank account takeovers among their top concerns, and with good reason – one industry report found that account takeover fraud resulted in nearly \$13



billion in losses in 2023 alone. Likewise, BEC continues to be one of the most financially damaging cybercrimes each year. In 2023, the FBI's Internet Crime Complaint Center received over 21,000 BEC reports totaling \$2.9 billion in reported losses.¹ Attacks in both categories have risen steadily. ATO incidents increased 24% year-over-year in 2024, and 83% of organizations surveyed experienced at least one account takeover in the past year. BEC also remains rampant globally, as cybercriminals find ever more creative ways to deceive organizations via compromised email channels. In short, virtually every enterprise today is at risk from account hijacking and email fraud attempts, despite widespread awareness of these attack types. The lucrative payouts and the relative ease of executing ATO/BEC (especially with a ready supply of stolen logins) ensure that threat actors will keep exploiting these tactics.

The Surge of Infostealer Malware and Data Theft

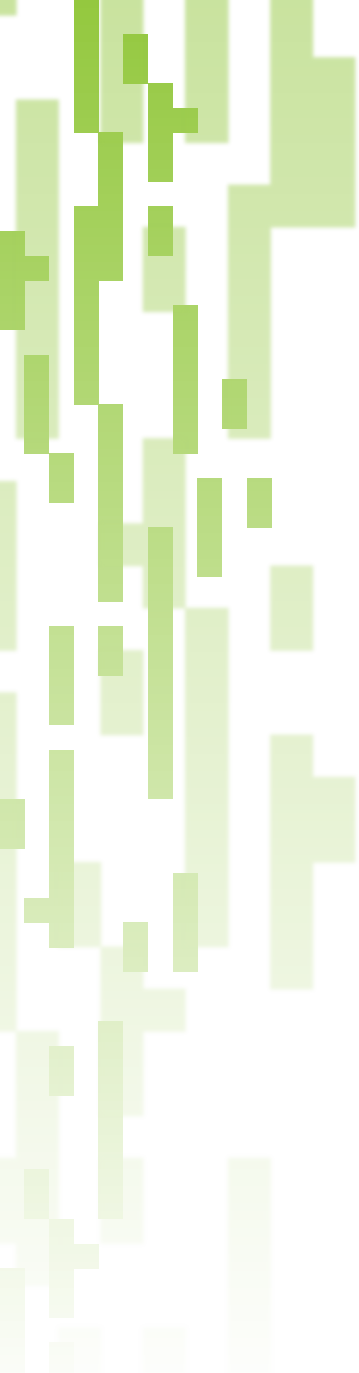
Fueling the ATO and BEC epidemic is a parallel infostealer malware boom. Infostealers are a class of malware designed to surreptitiously harvest sensitive information from infected systems – most importantly, saved login credentials and session data. Once an infostealer infects a victim's device (often via phishing emails, malicious downloads, or software cracks), it quickly extracts data such as browser-stored usernames and passwords, cookies and session tokens, auto-fill data, cryptographic wallet keys, system information, and more. The malware then transmits this bounty back to the attacker or to a drop server. The collected package – containing all the victim's captured credentials and digital fingerprints – is commonly referred to by cybercriminals as a “log.” Infostealer logs from a single machine can be astonishingly comprehensive; on average, one infostealer log contains



credentials for 26 different business applications or accounts. In other words, a single infected employee can inadvertently hand over the keys to dozens of corporate services.

Over the last few years, infostealer malware usage has exploded. IBM's security analysts observed a 266% increase in infostealer activity in 2023 compared to the prior year.² By 2024, infostealers had become one of the most pervasive tools in the cybercrime arsenal – responsible for stealing the majority of credentials that end up for sale. HackNotice's threat intelligence report revealed that infostealers were used to steal over 6 billion credentials in 2024, nearly two-thirds of all credentials stolen that year. This represented a 36% jump in the total volume of stolen credentials compared to 2023, highlighting just how rapidly infostealer-driven theft is growing. Multiple commodity infostealer strains (such as RedLine, Raccoon, Vidar, Lumma, and others) are readily available “malware-as-a-service” kits on criminal forums. Many are inexpensive and easy to use – some sold for as little as ~\$200 per month subscription in 2024 – which has lowered the barrier of entry for aspiring cybercriminals. Would-be attackers can rent an infostealer, infect victims to collect credentials, and immediately monetize that data without needing advanced skills. This democratization of credential theft has led to a widespread infostealer epidemic affecting organizations and individuals globally. By one estimate, over 4.3 million machines were infected by infostealers in 2024, yielding more than 330 million harvested credentials that year ³. Notably, nearly 40% of the infected machines in that study contained credentials for sensitive corporate systems (email, VPN, internal platforms, etc.) – underscoring that infostealers are not only an opportunistic consumer threat but a serious enterprise security issue.³

Compounding this threat is the growing trend of malware authors embedding infostealer code directly into open-source software

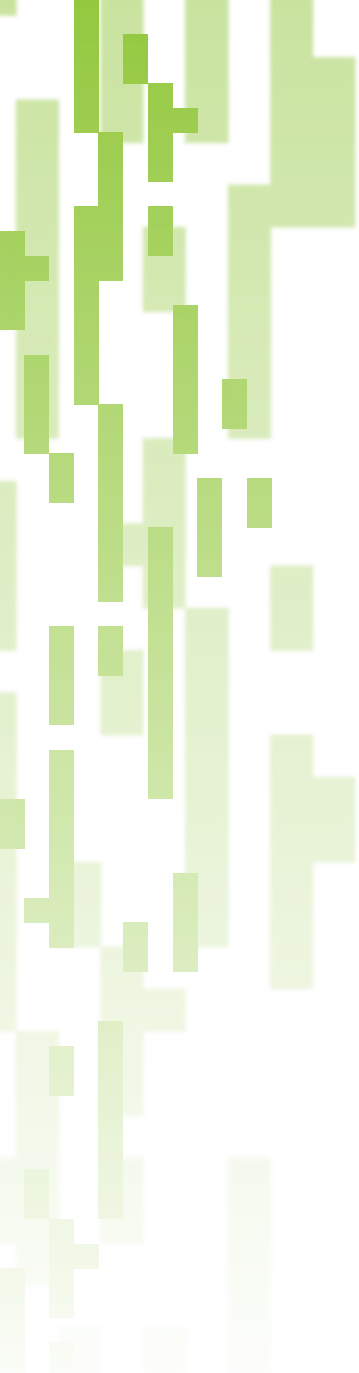


projects. In some cases, threat actors subtly inject malicious functionality into public repositories – often under the guise of a benign code update or feature contribution. Once merged, the compromised code becomes part of the official project and is unknowingly distributed across the software supply chain. Organizations that rely on these projects may inadvertently import malware into their environments simply by updating their dependencies. These supply chain attacks are particularly dangerous because they often bypass traditional security controls and exploit the implicit trust developers place in open-source libraries. As a result, a single malicious commit can silently propagate infostealer malware to thousands of downstream systems, greatly amplifying its reach and impact.

Dark Web and Telegram Marketplaces: Stolen Data Trafficking Trends

Stolen credentials and session data from infostealers are the fuel driving many modern ATO and BEC attacks – and this fuel is abundantly traded in underground communities. In the past 1–3 years, cybercriminal marketplaces on the **dark web**, as well as channels on encrypted messaging platforms like **Telegram**, have seen a surge in activity trafficking infostealer-derived data.

Traditional dark web forums have long sold stolen login dumps, but more recently they have been augmented or replaced by **automated log markets**. These are illicit marketplaces where criminals upload infostealer logs daily, and buyers can search and purchase specific compromised accounts (often for just a few dollars or less per log). The now-defunct **Genesis Market** was a prime example of this model – before being shut down by law enforcement in 2023, Genesis Market listed over 450,000

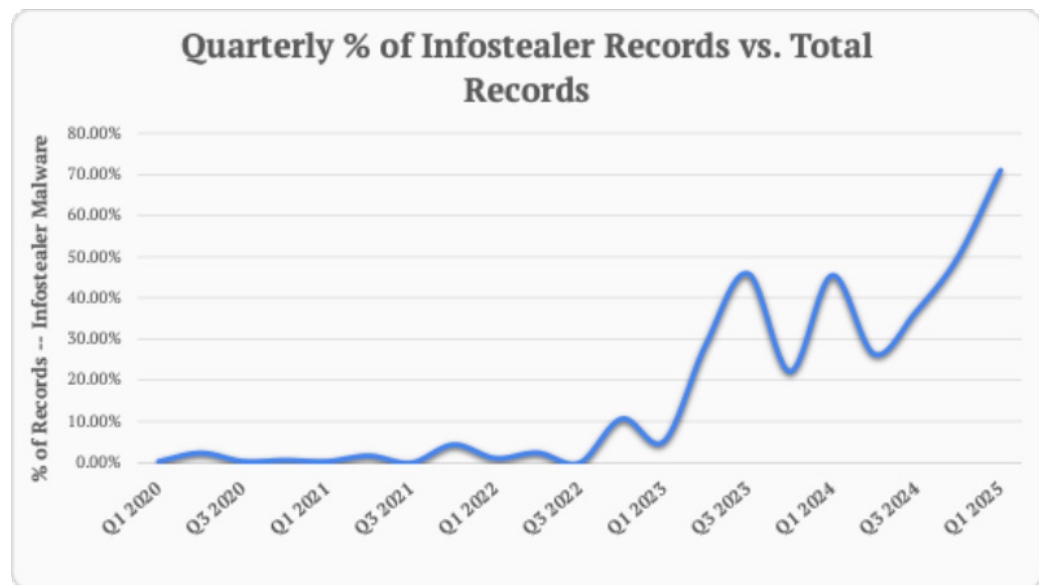


stolen “bots” (infected devices), and authorities estimated its total inventory included data from about **1.5 million** compromised machines.⁴ Genesis not only sold passwords but also session cookies and device fingerprint profiles, allowing attackers to impersonate victims’ browsers with one click. Its success spawned numerous copycats and drove demand for more stolen logs; in fact, Genesis began actively recruiting more infostealer log suppliers in 2023 to keep up with user demand ⁴. Although Genesis Market was taken down (in an international operation aptly codenamed “Cookie Monster”), many other marketplaces and private channels have continued the trade. Markets like RussianMarket, 2Easy, and various Tor sites offer tens of thousands of fresh logs from infostealer infections, indexed and sold to the highest bidder.

At the same time, **Telegram** has emerged as a key platform in the cybercrime ecosystem for distributing stolen data. Its encrypted, semi-anonymous nature and ease of use make it attractive for sellers and buyers of illicit data. Some infostealer operators use Telegram bots to automatically exfiltrate stolen logs from infected machines directly to a private channel. Others use Telegram groups to advertise and sell bundles of logs. In recent years, HackNotice has observed a significant uptick in infostealer activity on Telegram. In early 2025, a dramatic example came to light: security researchers discovered a Telegram channel (dubbed “ALIEN TXTBASE”) sharing a trove of infostealer logs amounting to **1.5 terabytes** of data. Analysis showed this single cache contained over **284 million unique account credentials** (spanning nearly 500 million email/website pairs) stolen via various infostealers. This illustrates the massive scale at which stolen data is being circulated in the cyber underground.

Such trends make it clear that the underground supply of compromised credentials has ballooned. HackNotice’s own threat monitoring data reflects this evolution. Figure 1 (below) shows

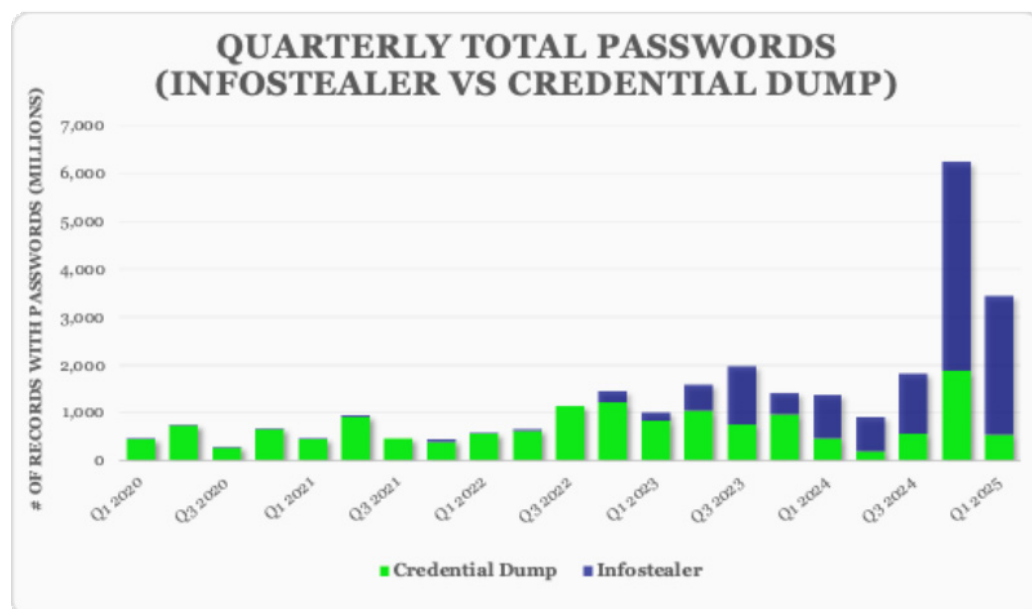
the percentage of total dark web records each quarter that were sourced from infostealer malware. The data reveals a sharp and accelerating rise in the dominance of infostealer-derived records, particularly beginning in early 2023. By Q1 2025, nearly 70% of all dark web records captured by HackNotice originated from infostealer malware. This shift underscores how infostealers have become the primary engine behind leaked credentials, enabling persistent waves of account takeover attempts, business email compromise (BEC), and other forms of cyber-enabled fraud.



(Figure 1: Percentage of total dark web records attributed to infostealer malware, by quarter — HackNotice Threat Monitoring Data, 2020–2025.)

Credential Dump vs Infostealer: The Changing Composition of Password Leaks

While traditional credential dumps have long been a staple of dark web markets, their dominance is rapidly declining in favor of infostealer-derived data. Figure 2 (below) shows the total volume of password-containing records detected on the dark web per quarter, split between credential dumps and infostealer logs. From 2020 through early 2023, credential dumps comprised the bulk of password leaks. However, beginning in late 2023, infostealer-derived credentials began to overtake dumps in volume – culminating in a dramatic spike in 2024 and 2025. In Q1 2025 alone, over 6 billion password records were identified, with infostealers accounting for the clear majority. This highlights how infostealers are not only more prevalent but also more efficient at harvesting credentials at scale.



(Figure 2: Quarterly total dark web password records, by source — HackNotice Threat Monitoring Data, 2020–2025.)



Exploitation in Action: Real-World Examples

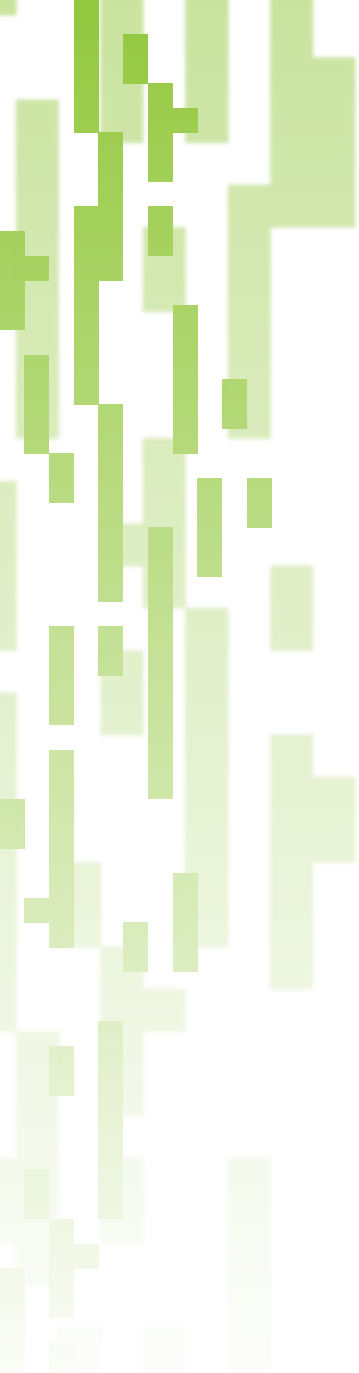
The following examples illustrate how threat actors are actively exploiting infostealer-sourced data to compromise organizations:

Cloud Accounts Breached via Stolen Logs (2024):

In April 2024, a criminal group leveraged credentials obtained from infostealer logs to breach as many as **165 customer accounts** of a major cloud data platform (Snowflake). Mandiant investigators revealed that hundreds of valid usernames and passwords – stolen by common malware strains like RedLine, Raccoon, Vidar, and others – were used to access numerous companies' Snowflake cloud environments. Some of the stolen credentials had been pilfered from victims' machines **years earlier** (in one case as far back as 2020) yet were never reset, allowing the attackers to reuse them for illicit access.⁵ This incident exposed hundreds of millions of customer records and demonstrates how infostealer data, even aged data, can enable broad and stealthy account takeovers across multiple organizations.

Business Email Compromise Enabled by Infostealers:

Infostealer logs often contain not only personal web accounts but also **corporate email credentials** – which are a gateway to BEC scams. In a recent analysis, nearly 40% of infostealer-infected machines had credentials for corporate systems like company email or remote access portals.³ Armed with an employee's email login (and possibly session cookies), an attacker can directly access the email account and impersonate that user. For example, an infostealer that steals a Microsoft 365 session token from an employee's browser would let an intruder access Outlook email and



Teams chats as that employee, without ever needing to phish for a password or MFA code. There have been numerous cases of threat actors using stolen corporate logins from malware to initiate BEC fraud. In one FBI case, criminals obtained a finance officer's email account credentials (likely from a malware infection) and then used that access to send falsified invoices to customers, attempting to divert payments to accounts under the attackers' control. BEC schemes like this collectively cost businesses billions each year.¹ The ready availability of corporate logins on dark web markets means that an adversary can simply purchase an employee's email password (or authentication cookie) and immediately have the ability to send out convincing fraudulent emails as a trusted insider. Enterprises have reported incidents of fraudulent wire transfers, payroll diversions, and sensitive data leaks all stemming from such account compromises.

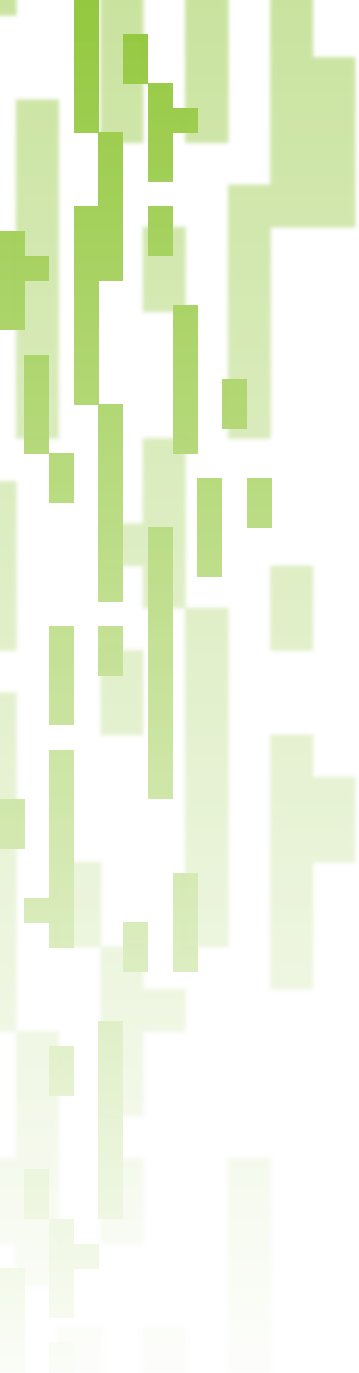
These examples underscore a troubling reality: **infostealer malware is feeding a broad spectrum of cybercrime**, from opportunistic fraud to large-scale breaches. Whether the end goal is to steal money via BEC or to infiltrate a network for ransomware, having valid user credentials or session tokens makes the attacker's job far easier. Criminals no longer always need to spear-phish a target or exploit a zero-day vulnerability – often they can simply log in with stolen credentials obtained on the underground market. In today's threat landscape, a single malware infection on an employee's home computer might ultimately lead to an enterprise data breach or a fraudulent transaction weeks or months later.



Infostealer Data: Bypassing MFA and Enabling Stealthy Intrusions

One of the most dangerous aspects of infostealer-derived data is how it lets attackers **bypass authentication barriers (like MFA)** and operate with stealth. Many organizations have invested in MFA to protect accounts, requiring users to enter a one-time code or push notification in addition to their password. However, if an attacker can capture a user's active session cookie or authentication token (which infostealer malware often does, depending on the strain), the attacker may not need the user's password or second factor at all. By importing a stolen session cookie into their own browser, a threat actor can **hijack the user's login session** and impersonate them on the target service – effectively **bypassing MFA entirely**. This “pass-the-cookie” technique has been observed in the wild, where attackers use infostealer-harvested browser cookies to gain access to cloud services, email accounts, VPNs, and other systems without ever triggering an MFA challenge.

In addition to cookies, infostealers may grab other artifacts like OAuth tokens, API keys, or backup codes if they are stored on the system, which can be used to circumvent login safeguards. With a valid session token in hand, the attacker essentially walks through the front door as an authenticated user. From the service's perspective, nothing is unusual – the session was already validated on that device. This makes detection much harder, as traditional security tools that look for failed logins or strange authentication events might see no red flags. Attackers will often take steps to maintain this façade: using the victim's IP address or a proxy in the same region (this information can also be commonly found on the dark web), emulating the victim's browser user-agent and operating system, and generally blending in with expected usage patterns. Advanced threat actors have even deployed custom



malicious browser extensions to continuously steal fresh cookies and keep their illicit access alive persistently.

The net result is **stealthy intrusions** that can go unnoticed for long periods. An attacker with stolen credentials doesn't need to "hack in" – they login in a legitimate manner. Many companies have learned the hard way that an absence of security alerts does not mean all logins are benign. For instance, in the Snowflake-related breaches mentioned earlier, some victim organizations were unaware that outsiders were accessing their data with valid (but stolen) credentials for an extended time. In several cases, the credentials had been stolen years prior, lying in wait on the dark web until an enterprising hacker used them. By bypassing MFA and avoiding noisy intrusion methods, attackers using infostealer-sourced data can operate as stealthy "insiders." They can quietly search emails for useful information, reset additional passwords, enroll new devices for MFA, or escalate privileges – all while appearing to be just another authenticated user. This compounds the damage potential of ATO and BEC incidents. Not only can the attacker gain access, but they may be able to maintain access and deepen it (for example, using an email account compromise to pivot into an organization's wider cloud environment or to trick other employees). It is a true assault on the principle of trust: the trust that a known username and session token belong to the legitimate user.



Recommendations for Detecting and Mitigating ATO/BEC Threats

Defending against infostealer-driven ATO and BEC attacks requires a multi-faceted approach. Enterprise security teams should consider the following measures to reduce risk:

Strengthen Endpoint Security:

Prevent infection at the source. Deploy advanced endpoint protection (EDR/antivirus) to detect and block infostealer malware before it can exfiltrate data. Ensure systems are kept patched, and remove local admin rights where possible, to hinder malware installation. Network controls like web filtering can also block known infostealer command-and-control URLs. By stopping infostealers on employee devices, you cut off the supply of stolen credentials at its root.

Monitor for Compromised Credentials:

Know if your accounts are exposed. Security teams should proactively monitor dark web forums, breach data caches, and infostealer log marketplaces for signs that corporate credentials or cookies have been leaked. If an employee's work email and password show up in a dump, treat it as an incident – initiate a forced password reset and further investigation. Consider subscribing to threat intelligence feeds or services that track stolen credentials (including infostealer logs) relevant to your organization. Early detection of exposed credentials can prevent an account takeover before an attacker uses it.



Enforce Strong Authentication (and Go Beyond MFA):

Make logins harder to abuse. Continue to enforce multi-factor authentication for all users, especially for email, VPN, and administrative access – MFA still thwarts many attacks. However, be aware of its limits and supplement it with additional context-based controls. Use device posture checks and conditional access policies (e.g. geolocation, IP reputation, impossible travel rules) to detect anomalies that might indicate a cookie hijacking or suspicious login, and require re-authentication in those cases. Where feasible, implement phishing-resistant MFA methods (such as FIDO2 security keys or device-bound passkeys) which are less susceptible to theft by malware. Reducing reliance on persistent browser cookies (by shortening session lifetimes or using conditional re-auth) can also limit the window for attackers to reuse stolen tokens.

Enhance Email Security and Verification:

Protect the target of BEC. Since BEC attacks often start with or involve email compromise, invest in robust email security gateways that can detect suspicious login patterns or configurations (e.g. alerts on forwarding rules added, or logins from new IPs on an email account). Enable domain protections like SPF, DKIM, and DMARC to make it harder for attackers to spoof your domain in emails. Train employees – especially those in finance and HR – to verify any request for funds or sensitive data that comes via email, even if it appears internal. An out-of-band verification (a phone call to the supposed sender, for instance) can catch a fraudulent request that originated from a compromised email account before money or data changes hands.



Implement Least Privilege and Segmentation:

Limit the blast radius. Not all accounts should have equal power. Use the principle of least privilege for user accounts to ensure that a single compromised login doesn't provide unlimited access. For high-risk roles (executives, IT admins, finance personnel), consider dedicated devices or strict network segmentation. That way, even if an infostealer compromises one user, the attacker's lateral movement and potential impact are constrained. Regularly audit privilege allocations and remove unnecessary access. Also, monitor for sudden privilege escalations or unusual resource access patterns, which could indicate an attacker using a stolen account to probe your environment.

User Education and Vigilance:

Reduce risky behaviors. Educate employees about infostealers and how these threats commonly spread – for example, through phishing attachments or illicit software downloads. Emphasize the dangers of downloading unknown programs or browser extensions, which might secretly be stealers. Encourage good password hygiene (unique passwords, use of password managers) so that even if one set of credentials is stolen, it doesn't unlock other accounts via reuse. Train staff to recognize BEC social engineering cues: urgent tone, requests to bypass normal procedures, etc. Cultivating a security-aware culture can prevent that initial foothold, whether it's avoiding a malware infection or questioning a suspicious email directive.

Incident Response for Account Compromises:

Be ready to react fast. Develop an incident response playbook specifically for account compromise scenarios. This should include steps for containment (disabling accounts or sessions), eradication (removing malware from an infected device, if present), recovery (forcing password changes, reviewing settings), and communication (notifying affected parties, such as customers, if their data or transactions might be impacted). Incorporate threat intelligence – for instance, if you learn of an infostealer dump containing your users’ credentials, treat it as a breach and respond accordingly. Having MFA logs and centralized authentication logs integrated with your Security Operations Center can help quickly identify which accounts may have been accessed illegitimately, so you can take action (like terminating sessions or invalidating tokens). Time is of the essence with ATO/BEC; the sooner you can identify and disrupt an ongoing compromise, the less damage will be done.

By taking these steps, organizations can mitigate the risks from the surge of infostealer-fueled attacks. In essence, security teams must **assume that some credentials are already compromised** and build layered defenses accordingly. This means not only preventing theft of data but also limiting the usefulness of stolen data (through strong authentication and vigilant monitoring) and preparing to rapidly detect and respond to misuse. ATO and BEC threats will likely continue to evolve as long as cybercriminals find success, but with a combination of smart technology, user awareness, and proactive intelligence, enterprises can significantly reduce their exposure. In today’s environment, guarding identities and sessions is as crucial as guarding the network perimeter – because the new “keys to the kingdom” are being traded in underground bazaars every day. Staying ahead of this trend is now a core part of the mission for enterprise security teams, as the line between an infostealer malware infection and a full-blown business compromise has never been thinner.



About HackNotice

HackNotice is the leader in dark web intelligence and breach monitoring, helping organizations around the world reduce risk from credential exposure, data leaks, and supply chain threats. Our platform continuously monitors the global dark web—including criminal forums, Telegram, marketplaces, and breach archives—for stolen credentials, infostealer logs, and leaked corporate data.

HackNotice provides real-time alerts for ransomware events, data breaches, and account exposures, empowering security teams to take immediate action. From individual employee protection to comprehensive vendor monitoring, we help enterprises detect and mitigate risk before it becomes a compromise.

Our services include:

Credential and Session Exposure Monitoring

Discover when your employees, customers, or systems appear in infostealer logs or breach dumps.

Third Party and Supply Chain Risk Intelligence

Track vendors and partners for breaches, ransomware attacks, or data leaks that may put your business at risk.

Ransomware & Data Breach Alerts

Get real-time, actionable notifications about new attacks across your ecosystem.

Dark Web Incident Analysis

Receive deep-dive investigations into specific dark web data incidents, including attribution, scope, and remediation guidance.

With HackNotice, your team gains early visibility into attacker data and behavior—enabling you to respond quickly, protect identities, and minimize business disruption. [Learn more at hacknotice.com](https://hacknotice.com) or [contact us](#) to schedule a tailored threat briefing.

References

- ¹ Expert Insights. BEC Attacks Among Most Costly Forms of Cybercrime.
<https://expertinsights.com/email-security/20-stats-and-trends-for-email-threats>
- ² Push Security. Infostealers Are the New Phishing.
<https://pushsecurity.com/blog/what-the-rise-of-infostealers-says-about-identity-attacks/>
- ³ KELA. Annual Infostealer Report 2024.
<https://info.ke-la.com/hubfs/Reports/KELA%20Report%20-%20The%20Infostealer%20Epidemic.pdf>
- ⁴ Trellix. Cookie Monster Operation and the Takedown of Genesis Market.
<https://www.trellix.com/blogs/research/genesis-market-no-longer-feeds-the-evil-cookie-monster/>
- ⁵ The Register. Snowflake Hackers Used Infostealer Malware Logs.
https://www.theregister.com/AMP/2025/04/23/stolen_credentials_mandiant/