SOCRadar®
Your Eyes Beyond

WHITE PAPER · CYBER THREAT INTELLIGENCE

Stolen, Sold, Weaponized

How the infostealer economy turns one infected laptop into your breach, and the narrow window where defenders can still win.

Jeffrey Ten Eyck
Senior Product Advocate, SOCRadar

June 2026 · Version 1.0

Executive summary

This paper traces how the infostealer economy turns a single stolen credential into a full-blown breach, and shows how the SOCRadar and Cyware integration helps defenders detect and act on exposed credentials inside the narrow window before attackers can weaponize them.

Most intrusions today don't start with malware on your network. Attackers aren't breaking in. They're signing in, with credentials that already work.

Those credentials come from somewhere specific: the infostealer economy. Commodity malware infects a laptop, harvests every saved password, autofill entry, and live session cookie, and packages them into a log that gets sold. IBM's X-Force team recorded an 84% year-over-year increase in infostealers delivered through phishing in its 2025 index. The scale is industrial now.

Here's the part that should change how you think about it. This is a supply chain, and a supply chain is observable. Stolen credentials move from infostealer to malware-as-a-service panel to access broker to ransomware affiliate, and most of that movement happens in forums, automated shops, and Telegram channels that can be watched. Verizon's 2025 Data Breach Investigations Report found that 54% of ransomware victims had their domains appear in infostealer logs before the attack.

The credential that breaches you is probably already for sale. That sounds like bad news. It's actually an opportunity. There's a window between the moment a credential appears in a log and the moment an affiliate uses it, and Verizon's data shows ransomware activity spiking just one to two days after credentials surface. Days, sometimes hours. This paper is about that window: why it exists, why most programs can't act inside it, and what it takes to win the race. At the end I'll show one way SOCRadar and Cyware close it together.

The intrusion you won't see coming

Picture how this actually plays out. An employee, or more often a contractor, downloads what looks like a legitimate tool on a personal laptop. It carries an infostealer. In a few seconds the malware copies saved browser passwords, autofill data, and active session cookies, sends them to a panel, and goes quiet. The person never notices. There's no ransom note, no obvious infection, nothing to report.

Weeks or months later, someone logs into your VPN or your SaaS tenant with a valid corporate credential pulled from that log. No exploit. No malware on your network. No anomaly that signals attack. Your SIEM records a successful authentication, which is the most normal event there is.

The reason your stack misses it is that the theft never happened on your stack. It happened on a device you don't manage and can't see. Verizon's 2025 report found that 46% of systems with corporate credentials in infostealer logs were unmanaged or personal devices, outside any endpoint protection you deployed. The tooling worked fine. It just wasn't installed on the laptop that mattered.

And because no one is looking, it festers. IBM's 2024 Cost of a Data Breach report found that breaches involving stolen credentials took the longest of any type to identify and contain, an average of 292 days. So the uncomfortable reframe is this. The breach that's coming for you has, in a sense, already happened.

It happened on someone else's machine, and the only thing standing between that stolen credential and an intrusion is whether anyone uses it before you find it.

The supply chain behind the login

Stolen credentials don't travel in a straight line from victim to attacker. They move through a market with specialized roles, and understanding that market is what makes it defensible.

1 · Harvest	2 · Monetize	3 · Broker	4 · Weaponize
Infostealers copy saved passwords, autofill data, and live session cookies into a log.	Logs sell through malware-as-a-service panels, autoshops, and Telegram channels.	Access brokers validate, enrich, and bundle working access for resale.	A ransomware affiliate buys the access and logs in. No exploit required.

Figure 1. The credential supply chain. Every stage happens somewhere a digital risk platform can watch.

It runs in four stages. First, harvest. Commodity infostealers like Lumma, StealC, RedLine, and Vidar infect devices through phishing, malicious ads, poisoned search results for cracked software, and fake update prompts. SOCRadar analyzed more than 4.6 billion stealer log records tied to 809 million unique users, with Q3 2025 alone producing 1.19 billion records - the highest single quarter on record. Five families - LummaC2, RedLine, Raccoon, Vidar, and Stealc - drive most of that activity, and all of them run as malware-as-a-service. These tools are cheap. They sell on a subscription model that averaged around 200 dollars a month in 2024, which is what puts them in so many hands.

Second, monetization. Logs flow into malware-as-a-service panels and sell on forums, automated shops, and Telegram channels. Fresh logs are gated behind subscriptions. Stale ones are often free.

Third, brokerage. Access brokers buy logs, validate which credentials still work, enrich them with context, and bundle them into ready-to-use access. Analysis put the average price of broker-sold access at around 2,000 dollars, and organizations above a billion dollars in revenue made up 27% of listings. Access to a large enterprise costs about what a laptop does.

Fourth, weaponization. A ransomware affiliate buys the validated access and walks in. CrowdStrike reported that access broker advertisements rose 50% year-over-year to 4,486 in its 2025 report, a direct measure of how much this handoff has scaled. Every one of those stages happens somewhere a digital risk platform can watch. The data is a traded commodity, and commodities leave a trail.

The clock you're racing

There's a window between the moment your credential appears in a log and the moment someone uses it against you. Verizon's 2025 report put numbers on it: ransomware activity tied to leaked credentials tends to spike one to two days after those credentials surface in infostealer logs and marketplace posts. And once an attacker is inside with valid access, the clock speeds up. CrowdStrike measured an average breakout time, from initial access to lateral movement, of 48 minutes in its 2025 report, with the fastest case under a minute.

Credential stolen	Listed for sale	Bought and used	Inside and moving
T + 0 Harvested from a device you don't manage, often without the user ever knowing.	**Hours to days** The credential surfaces in stealer logs and marketplace posts.	**1 to 2 days** Ransomware activity tied to leaked credentials spikes here. (Verizon, 2025)	**48 minutes** Average breakout time once an attacker has valid access. (CrowdStrike, 2025)

Figure 2. The window. The defensible ground is the gap between exposure and weaponization, not the theft itself.

The defensible ground isn't preventing the theft. It happens on devices you don't control. The defensible ground is the window. If you can find the credential in the log and kill it before the buyer logs in, the supply chain breaks at the last mile, on your terms.

Two things make winning that window harder than it sounds. The first is reach. Because so much exposure originates on unmanaged and personal devices, you can't rely on catching the infection. You have to catch the credential after it's stolen and before it's used, which means watching the market, not just your endpoints.

The second is session cookies. Infostealers don't only take passwords. They take live session tokens, and a stolen token lets an attacker replay an authenticated session with no password and no MFA prompt. Microsoft's 2025 Digital Defense Report attributed 80% of MFA-bypass breaches to session-token theft. This matters for a practical reason most playbooks miss: a password reset does nothing to a stolen session that's already live. You have to invalidate the token too.

SOCRadar's Identity & Access Intelligence module recovers these live session cookies straight from stealer logs and scores them with entropy analysis through Cookie Insights, surfacing the exact tokens an attacker would replay.

> A password reset doesn't kill a live session. You have to invalidate the token, and you have to do it before the buyer logs in.

Why watching isn't the same as acting

Plenty of programs already monitor the dark web. The trouble is that monitoring produces a feed, and a feed isn't an action.

Here's the failure I see most often. A credential hit lands in a monitoring console. An analyst notices it, opens the identity provider in another tab to force a reset, files a ticket in a third system, and emails a forum or registrar to ask for the listing to come down. Each step is a manual handoff, and the window is closing the whole time. By the time the credential is actually dead and the listing is actually gone, the one-to-two-day clock may have already run out.

The gap isn't visibility into the supply chain. Most teams can see the exposure. The gap is the speed of turning a sighting into a killed credential, an invalidated session, and a removed listing. Generic monitoring tells you a credential leaked. It doesn't reset the account, it doesn't invalidate the session, and it doesn't take down the seller. Those are the things that break the chain, and they have to happen fast and together.

Closing the window

This is where the SOCRadar and Cyware integration earns its place, by turning a sighting into a coordinated response inside the window rather than after it.

SOCRadar's digital risk protection watches the supply chain directly. Across thousands of sources spanning the surface, deep, and dark web, it surfaces stealer logs, combolists, leaked credentials, exposed session cookies, and the forum and Telegram chatter where access is traded, scoped to your domains, your executives, and your third parties. Because it watches the market rather than your endpoints, it sees exposure that originated on devices you'll never manage. That's the sighting, early.

Cyware turns the alert into action. Inside the intelligence backbone, the finding is correlated, enriched, scored against your assets, and mapped to MITRE ATT&CK, where this chain lines up cleanly with Valid Accounts, Steal Web Session Cookie, and Credentials from Password Stores. Cyware Orchestrate then automates the response: trigger the password reset, invalidate the live session, and open the incident, with no analyst carrying the finding from tool to tool.

Exposure signal	Defensive action	ATT&CK technique
Leaked password in a stealer log	Force a credential reset	**T1078 Valid Accounts**
Stolen session cookie or token	Invalidate the live session	**T1539 Steal Web Session Cookie**
Saved credentials pulled from a browser	Rotate, then enforce phishing-resistant MFA	**T1555 Credentials from Password Stores**
Seller listing and infrastructure	Managed takedown of post and infrastructure	**T1589 Gather Victim Identity Information**

Figure 3. Matching the response to the exposure. Each signal has a specific action, fired from one workflow.

And SOCRadar Managed Takedown removes the seller's listing and the malicious infrastructure behind it, launched from the same workflow. The result is one operational loop where an exposed credential becomes a dead credential and a removed listing in the time it used to take just to open the second console. The integration is available as an add-on module within the Cyware Intelligence Suite.

Where to start

You don't need the full picture to make progress this quarter. Here's a sequence that front-loads the highest-impact moves.

Now, the first 30 days. Stand up continuous credential and stealer-log monitoring scoped to your domains, your executives, and your contractor and third-party identities, and treat a domain hit as an incident trigger rather than a line in a report. At the same time, add session-token invalidation to your standard remediation, right next to the password reset. That one change closes the gap that lets a stolen cookie outlive the reset.

Next, 30 to 90 days. Move to phishing-resistant, device-bound authentication like passkeys on internet-facing and SaaS access, because that's what actually defeats session theft and replay. Close the unmanaged-device gap with device-trust checks before SaaS and single sign-on, so a credential stolen off a personal laptop can't quietly walk back in. Add network allow-listing to your highest-value data stores. The 2024 Snowflake intrusions, which have been traced to infostealer-harvested credentials against accounts without MFA, are the case study for why these three controls matter.

Ongoing, past 90 days. Assume the access exists and build to detect its use. Instrument identity analytics for impossible travel, anomalous session reuse, and abuse of connected OAuth apps, the same identity-centered tradecraft that groups like Scattered Spider and ShinyHunters used in their 2025 campaigns. And track one number as your north star: the time between a credential appearing in a log and your team killing it. Measured against the one-to-two-day clock the data describes, that window tells you whether you're winning.

Where this is going

The trend lines all point the same way. Infostealer volumes keep climbing. macOS stealers are rising fast, which matters because Macs cluster among developers, engineers, and executives, the high-privilege accounts. Adversary-in-the-middle kits have made MFA bypass through session theft routine rather than exotic. And takedowns, while worth doing, buy time rather than victory: when a Microsoft-led operation disrupted the Lumma Stealer infrastructure in May 2025 after linking it to nearly 400,000 infections, the operation resurfaced within weeks and competitors absorbed the demand.

There's a second signal worth watching. The Salesforce-related extortion campaigns of 2025, run by the crews tracked as ShinyHunters and Scattered Spider, showed the same identity-abuse playbook working with no commodity malware at all, just social engineering and OAuth abuse. The common thread across all of it is the credential, and the identity behind it. The malware is interchangeable.

Which is the real shift. The perimeter is an identity perimeter now, and the credential that breaches it is, more often than not, already for sale by the time you'd think to look. The programs that hold up are the ones that treat the credential supply chain as a surface they watch and act on continuously, not a thing they read about in the post-mortem.

About the author and the approach

Jeffrey Ten Eyck is Senior Product Advocate at SOCRadar, with around fourteen years in cyber threat intelligence across roles at Accenture, Cyware, TruSTAR, and IBM. He works with CISOs, security executives, MSSPs, and global systems integrators on turning external intelligence into operational outcomes.

The capability this paper describes is a category, and there's more than one way to assemble it. The way SOCRadar and Cyware do it together is one. SOCRadar provides the external visibility into the credential supply chain: digital risk protection across thousands of sources spanning the surface, deep, and dark web, covering credential, session, brand, and executive exposure, with analyst-led managed takedowns. Cyware provides the intelligence backbone and the orchestration that correlates, scores, and automates the response. Together they compress the distance between an exposed credential and a dead one, inside the window that decides whether exposure becomes a breach. The integration is available as an add-on module within the Cyware Intelligence Suite.

If your team can already see credentials leaking but still can't kill them fast enough to matter, that's the gap worth closing first.

References

1. CrowdStrike, 2025 Global Threat Report. Malware-free detections, average breakout time, and access broker advertisement growth.
2. Verizon, 2025 Data Breach Investigations Report. Stolen credentials as an initial access vector, ransomware, and infostealer-log correlation, unmanaged-device exposure.
3. IBM X-Force Threat Intelligence Index 2025. Year-over-year growth in infostealers delivered via phishing.
4. IBM, Cost of a Data Breach Report 2024. Cost and containment time for credential-based breaches.
5. Microsoft Digital Defense Report 2025. Session-token theft as the primary MFA-bypass technique.
6. SOCRadar, Identity Threat Landscape Report 2026. Stealer log record and unique-user volumes, leading infostealer families, and malware-as-a-service pricing.
7. Cyberint, a Check Point company, Initial Access Brokers Report 2025. Access pricing and enterprise targeting.
8. Mandiant, reporting on the 2024 Snowflake customer intrusions (UNC5537).