Brief

The Role of Initial Access Brokers in Ransomware Operations

B-2026-05-26a

Classification: TLP:CLEAR

Criticality: Low

Intelligence Requirements: Initial Access Brokers, Ransomware, Artificial Intelligence

May 26, 2026

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 12:00 PM (EDT) on May 20, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Brief | The Role of Initial Access Brokers in Ransomware Operations

| Executive Summary

Initial Access Brokers (IABs) have become a key part of the ransomware ecosystem by obtaining and selling unauthorized network access to threat actors. Several ransomware affiliates, such as Akira, BlackBasta, and Conti, have been known to purchase access directly rather than conducting the initial intrusion themselves, accelerating attack timelines and reducing operational effort.[1][2]

The decline in publicly visible IAB listings between Q1 2025 and Q1 2026 likely reflects market maturation rather than reduced activity. High-value access is very likely being increasingly sold through private channels, while some ransomware groups appear to be internalizing access operations. Credential theft, infostealer malware, and exploitation of internet-facing infrastructure remain common access vectors, making early detection and monitoring increasingly critical.

[1] hXXps://www.cisa[.]gov/news-events/cybersecurity-advisories/aa24-109a
[2] hXXps://www.cisecurity[.]org/insights/blog/initial-access-brokers-how-theyre-changing-cybercrime

Details

IABs are cybercriminals that specialize in acquiring unauthorized access to computer systems, networks, and databases and selling that access to other cyber threat actors (particularly ransomware operators).[3] IABs are intermediaries whose actions—including compromise and intrusion of networks—shape the initial phases of a ransomware attack; their involvement is typically separate from the later downstream exploitation, which is usually primarily headed by the ransomware actors. This compartmentalization of malicious actions enables ransomware affiliates to accelerate intrusion timelines and make their operations scalable, while the IABs mitigate direct risks associated with ransomware operations (such as detection).

The Role of IABs in Ransomware Operation

The framework of today's typical ransomware attacks includes a highly structured and layered operational model. The initial stages are usually primarily dedicated to IAB activity, but IABs are not directly involved in the main ransomware acts (i.e., encryption and ransoming). The division of responsibilities enables more efficient scaling of operations, as it frees up resources that can be leveraged in other stages of the attack.[4] In this model, IABs are responsible for the earliest stages of the compromise, wherein they gain access to the target systems, maintain persistence, and prepare the access for sale to ransomware affiliates.

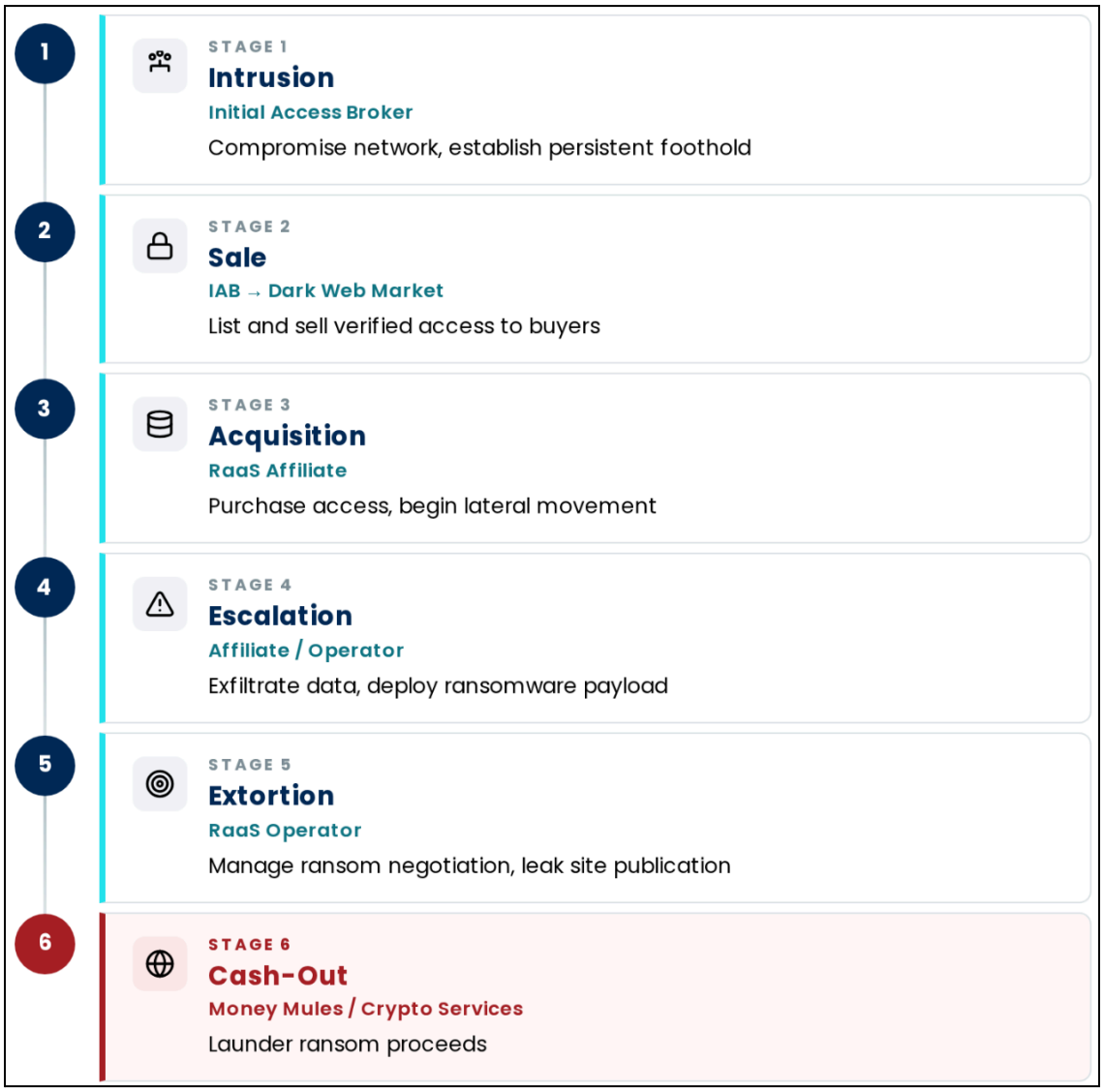
- IABs commonly compromise networks through stolen credentials, phishing campaigns, exposed remote desktop protocol (RDP) services, or vulnerable edge infrastructure.
- Verified access is often sold through dark web forums, encrypted channels, or private broker networks.[5]

[3] hXXps://thehackernews[.]com/2025/04/initial-access-brokers-shift-tactics.html
[4] hXXps://www.cyberdaily[.]au/security/12494-special-report-what-makes-initial-access-brokers-tick
[5] hXXps://www.securityweek[.]com/inside-the-dark-webs-access-economy-how-hackers-sell-the-keys-to-enterprise-networks/

- Access listings may include admin privilege-level, geographic location, revenue estimates, and details regarding endpoint protection or security tooling present within the environment.

Once access is purchased, ransomware affiliates can rapidly move into later stages of the intrusion lifecycle, including lateral movement, privilege escalation, data exfiltration, and ransomware deployment. This operational separation significantly reduces the time required for affiliates to initiate attacks.

- IABs absorb much of the reconnaissance and initial intrusion effort that usually requires weeks of work.
- Ransomware-as-a-service (RaaS) affiliates can transition from credential acquisition to ransomware deployment within hours.
- RaaS operators often focus primarily on payload deployment, negotiation infrastructure, and extortion management rather than initial compromise activity.



The stages of a typical ransomware attack

Source: ZeroFox Intelligence

Why IABs Often Go Unnoticed

IAB activity very likely often remains undetected because it occurs at the earliest stage of intrusion, where activity is limited, intent is unclear, and monitoring is usually focused on post-compromise indicators. Credential harvesting, reconnaissance, persistence, and other such actions likely enable IABs to bypass generic detection measures and are frequently treated as routine anomalies, rather than immediate threats to the targeted systems.

- Early-stage activity often blends with routine network behavior and low-level anomalies, reducing the likelihood of detection during initial compromise.
- The distinction between the process of gaining the access and its exploitation limits visibility across the intrusion lifecycle, making attribution and correlation more difficult.
- The use of common intrusion techniques such as phishing and credential-based access makes this activity more difficult to detect without deeper analysis.

Access Types, Buying and Selling Process, and Price Ranges

IABs typically focus on a small set of high-demand access types obtained through repeatable intrusion methods and sold at relatively low price points compared to downstream ransomware impact, enabling scalable and low-risk monetization.

Types of Access Sold

IABs primarily trade in three categories of access: RDP, virtual private network (VPN) or corporate credentials, and web shell or administrative panel access. These access types offer varying levels of control ranging from basic entry points to near-complete network visibility, depending on privilege level and system exposure.

- RDP access provides direct remote entry into systems—often with user-level privileges, which can sometimes be escalated.[6]
- VPN or corporate credentials enable access to internal enterprise networks, often bypassing perimeter defenses.
- Web shells or admin panels can be used to maintain access to servers and are often utilized as staging points for lateral movement.

Methodologies Used to Obtain Access

Access is typically obtained by combining credential theft, exploitation of exposed services, and malware deployment. These methods are low-cost and scalable and rely on common security gaps across organizations.

---

6 hXXps://www.bleepingcomputer[.]com/news/security/the-initial-access-broker-economy-a-deep-dive-into-dark-web-hacking-forums/

- Phishing and credential harvesting remain widely used for initial compromise.
- Exploitation of unpatched vulnerabilities in internet-facing systems enables direct access.
- Infostealer malware and credential-stuffing using leaked databases support large-scale access collection.

Average Price Points Across Markets

The pricing varies based on access capabilities, sector, and geographic location but remains relatively low compared to the value extracted in later stages of intrusion, such as in ransomware attacks. The primary pricing determinants are:

- **Victim annual revenue**: This is the primary deciding factor to determine the ransom potential.
- **Country of incorporation**: Target organizations based out of Western Europe, North America, and Australia are usually listed as premium victims.
- **Sector**: Access to entities in the government, healthcare, finance, and critical infrastructure sectors attract higher bids.
- **Access type and privilege level**: Domain admin access enables multiple standard user accesses and hence is priced higher.
- **Persistence**: The likelihood of the access being discovered factors into pricing; the less likely it is, the higher the price.

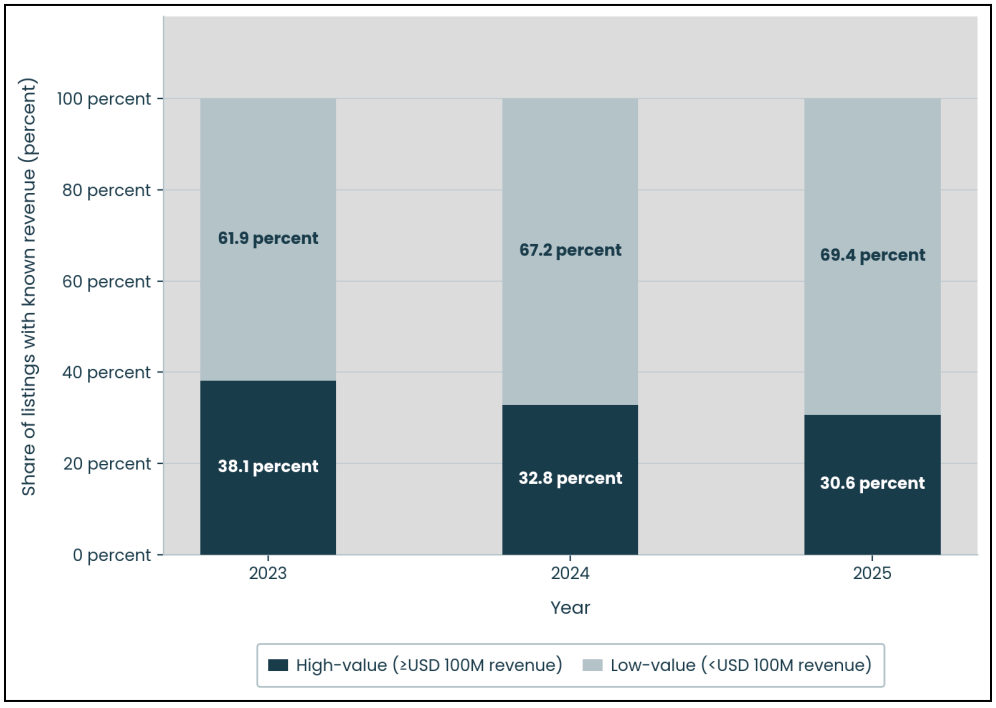
Access Type	Typical Price Range	Notes
Corporate VPN / Citrix (low privilege)	USD 100–2,000	Commodity tier; high volume
Corporate VPN (verified, avg.)	~USD 2,871	Per cybersecurity researchers
Domain user credentials	USD 500–5,000	Most common listing type

Access Type	Typical Price Range	Notes
Local admin access	USD 1,000–10,000	Elevated; limited lateral constraints
Domain admin credentials (avg.)	~USD 8,167	High tier; enables rapid ransomware deployment
Large enterprise / critical sector	USD 50,000– 100,000+	Premium; often publicly auctioned or negotiated privately

Average price ranges for various types of accesses

Source: ZeroFox Intelligence

Between 2023 and 2025, ZeroFox has observed a gradual shift of targets from higher-value organizations to lower-value ones. High-value targets (with greater than or equal to USD 100M in annual revenue) declined from 38.1 percent of listings in 2023 to 30.6 percent in 2025.



High- vs. low-value targeting from 2023–2025

Source: ZeroFox Intelligence

Why Defenders Miss Early Signals

IABs heavily depend on specialized techniques to persist in networks, systems, and devices that shroud their digital footprint and suppress signals defenders require to detect such activity.

Use of Valid Credentials

IABs often use valid credentials collected from either previous breaches or legit data aggregators to access corporate systems—in which case the initial event fails to generate any malicious intrusion attempt alert, a malware signature, or even a behavioral anomaly beyond an authenticated login. It also fails to trigger standard SIEM rules tuned to flag anomalous activity frequently, which ultimately fail to distinguish between an employee logging in from a new location and an attacker using that employee's credentials. This method also enables IABs to maintain stealth and long-term persistence, which they use to conduct extensive reconnaissance before listing the access for sale. Persistence time also factors into the price at which the access is listed for sale.

Living Off the Land Techniques

Exploitation of unpatched vulnerabilities—especially in internet-facing devices that do not run endpoint detection and response tools—often leaves very little evidence on affected systems. Threat actors frequently use malware that runs only in memory along with legitimate remote access software, enabling malicious activity to blend with normal administrative operations in environments without strong monitoring controls.

Gaps in Prioritization and Alert Fatigue

Even when monitoring systems detect suspicious activity, large alert volumes and understaffed security operations center (SOC) teams often result in prioritization gaps. Unusual authentication activity from residential proxy internet protocol addresses, infrequent failed login attempts spread across several hours, and after-hours access from unfamiliar devices are often overlooked or deprioritized in favor of more obvious malicious activity.

Absence of Public Traces Before Actual Impact

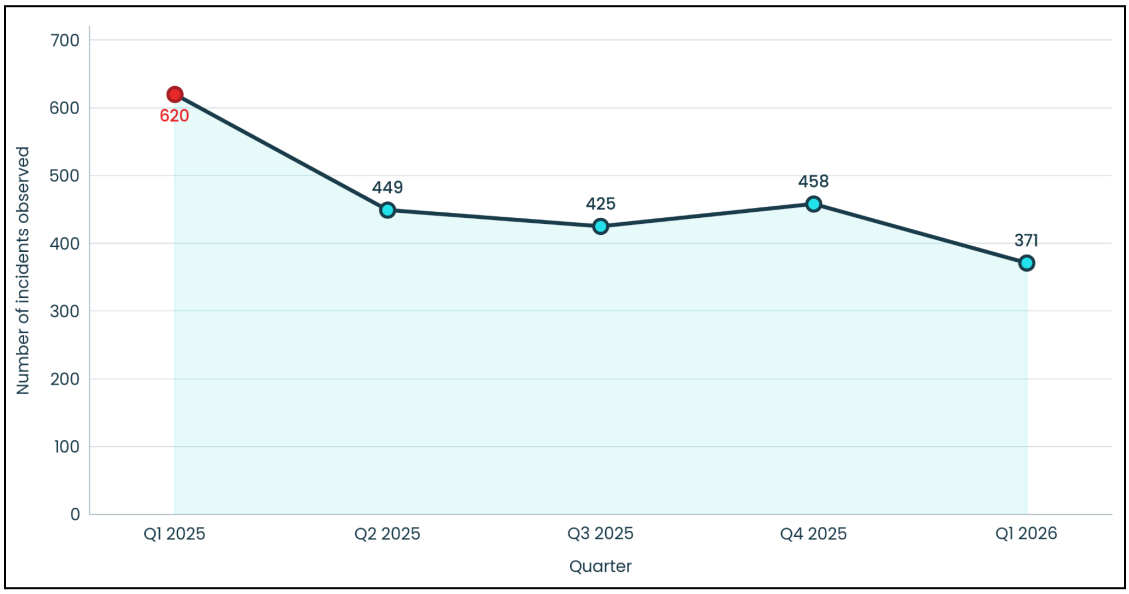
IAB listings often appear on closed dark web forums days or weeks before another threat actor purchases them. Organizations without active dark web monitoring usually remain unaware that access to their networks is being sold. By the time incident response

begins, the IAB is typically gone, and the ransomware operator has already established persistent access within the environment.

IAB Sales: Market Economics

Declining Sales in 2026

In the first quarter of 2026, ZeroFox saw about 370 instances of network access listed for sale on the deep and dark web (DDW), which is a sharp decline from the 620 instances it observed in the first quarter of 2025. Activity decreased through Q2 2025 (449 incidents) and Q3 2025 (425 incidents), briefly increasing slightly (458 incidents) in Q4 2025 before resuming its downward trend. Q1 2026 listings dropped even further.



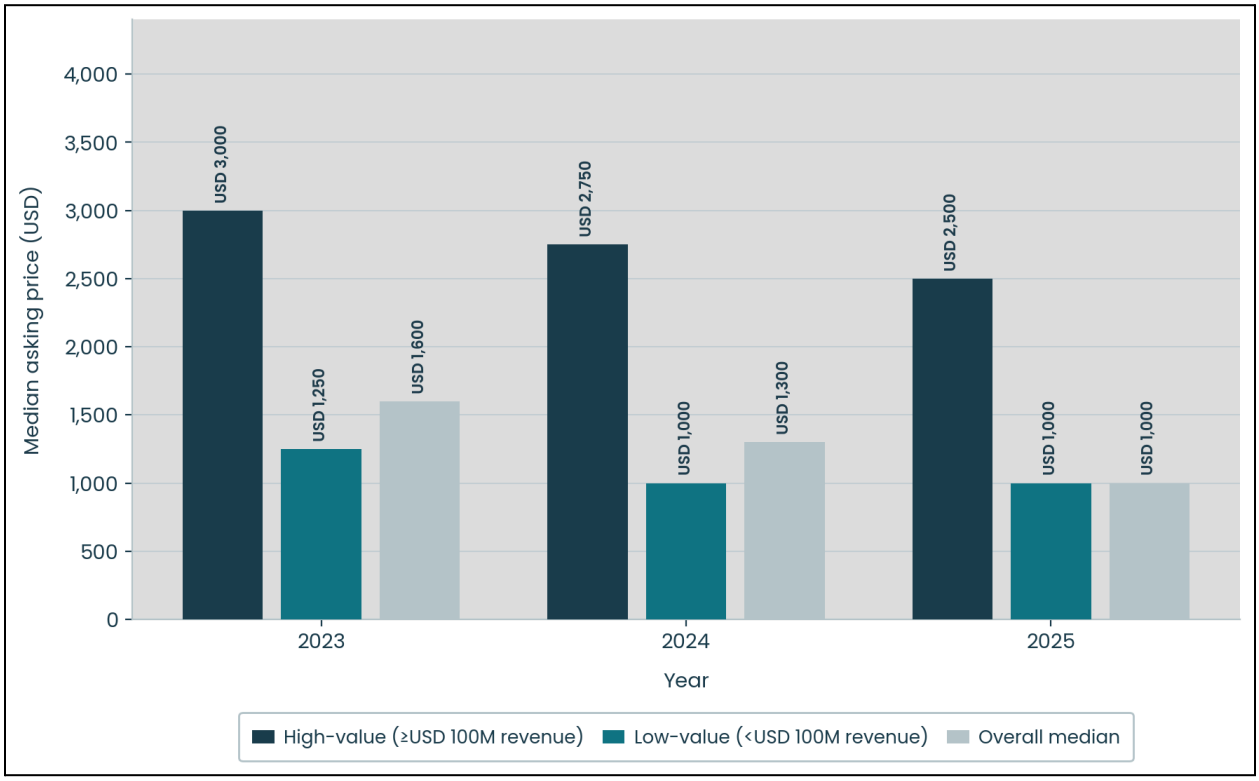
Number of network access sale posts observed (Q1 2025—Q1 2026)

Source: ZeroFox Intelligence

However, the decline in network access sale is very likely not reflective of reduced ransomware activity. Rather, the declining network access sales likely suggests structural changes within the IAB ecosystems, fueled by factors such as seizure of major forums by law enforcement (LE). Increased LE scrutiny has also likely compelled IABs to shift transactions farther away from public forums and toward private channels. In 2025 alone, law enforcement operations have resulted in the closure of major dark web

forums that used to be breeding grounds for IAB activities, including Russian-language dark web forums XSS and RAMP and English-language dark web forum BreachForums.

Over the past three years, ZeroFox has also observed a decline in median sale prices across all access types. Although high-value access continues to sell at roughly 2.5 times the price of lower-tier access, overall prices across the ecosystem are steadily decreasing.



Median listing price by value tier

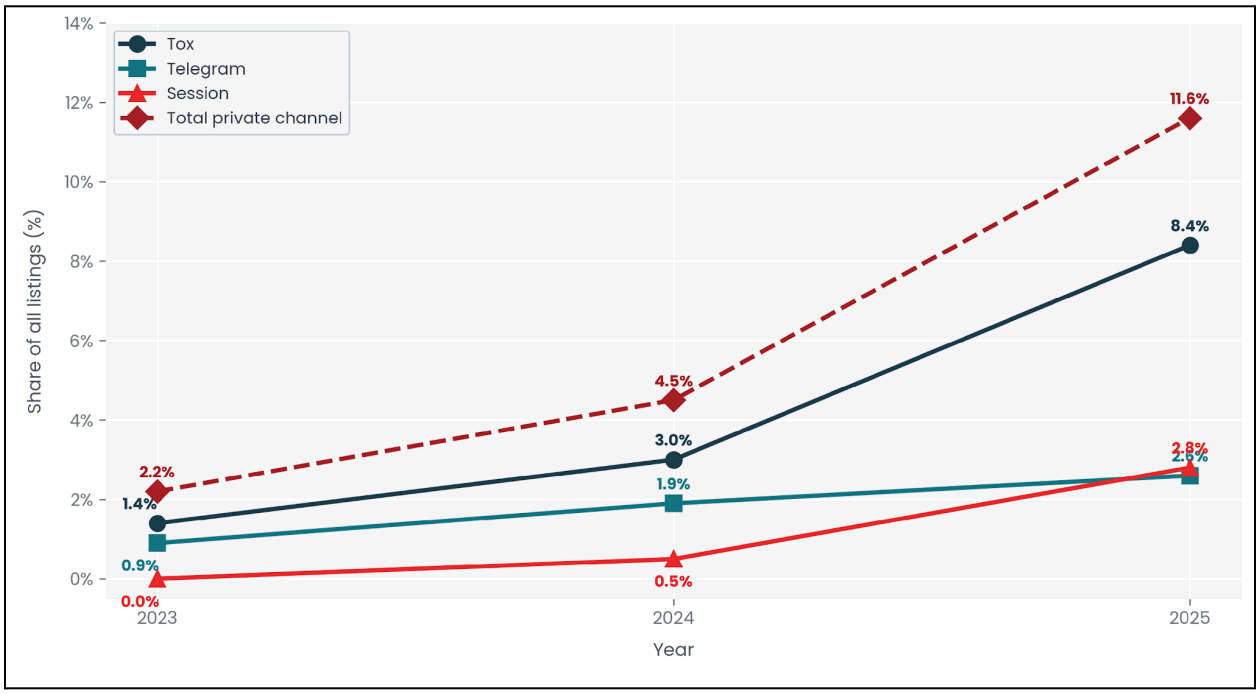
Source: ZeroFox Intelligence

The decline can likely be further attributed to a few structural dynamics that are actively contributing to a more stable and standardized market with an established customer base: migration to private channels and prioritization of quality over volume.

Privatization of Communication

Listings referencing encrypted or private messaging tools increased almost fivefold in two years, from 2.2 percent of all network access listings in 2023 to 11.6 percent by 2025.

ZeroFox has observed that communication via Tox is the dominant choice among IABs, with data showing that threat actors have increasingly been shifting to Tox transactions in 2025. This shift to private channels is very likely a result of attempts to evade conventional monitoring procedures.



Trends in IABs using private messaging platforms

Source: ZeroFox Intelligence

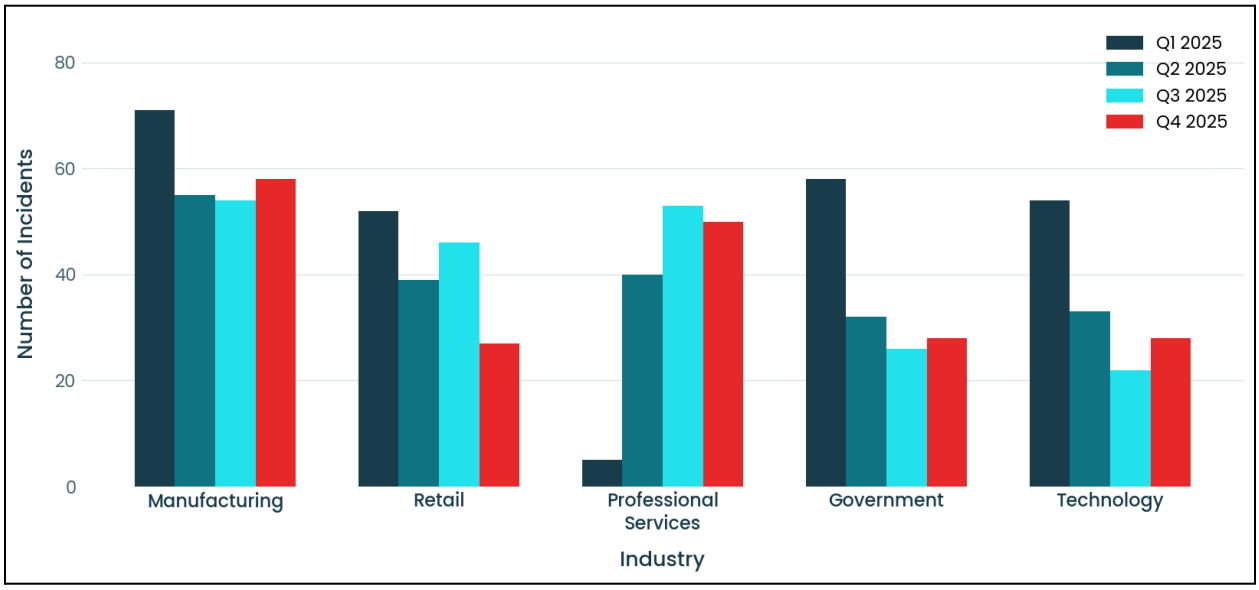
Prioritization of Quality over Volume

ZeroFox has observed that average prices for lower-tier access declined from approximately USD 1,427 in early 2023 to below USD 500 by Q1 2026, reducing profitability for common, lower-value network access sales. This is likely a reflection of IABs dedicating more time and resources to develop high-value access via escalated privileges in higher-target environments. The increase observed in Q4 2025 likely reflected the sale of accumulated high-value access from the slower Q3 period rather than a broader increase in activity.

Industrial and Regional Trends Across 2025

The manufacturing and the retail industries recorded consistently high numbers of network access sales across 2025—very likely due to a higher concentration of more

lucrative targets in both of those sectors. Other industries that were frequent targets in network access sales were professional services, technology, and government.



Top five industries mentioned in network access sale posts in 2025

Source: ZeroFox Intelligence

Detection and Disruption Opportunities

The timeframe for an IAB operation, which is typically limited to between the initial compromise and the eventual sale of the access to a different threat actor, can last several days or even weeks and is one of the most critical opportunities for detection and disruption. There is a roughly even chance that identifying unauthorized access during this stage will prevent a ransomware intrusion before the ransomware operator establishes persistence or deploys payloads within the environment.

Continuous monitoring of dark web forums and underground marketplaces where compromised access is advertised is one of the most effective methods of detection. IAB listings are very likely to include operational details—including the targeted entity's location and annual revenue and the type of access and its capabilities—by design to lure interested buyers.

- Threat actors often include company names, email domains, IP ranges, or remote access technologies directly within listings.

- These types of access advertisements are very likely to appear days or weeks before a ransomware deployment occurs.
- Organizations without active dark web monitoring are likely to remain unaware that access to their environments is being sold publicly or privately.

Credential leak monitoring also remains an important early-warning mechanism. Infostealer malware markets continuously publish compromised credentials harvested from infected systems, including corporate logins later used by IABs. Compromised VPN credentials and corporate email accounts frequently appear in stealer logs before intrusion activity escalates. In many cases, credential exposure precedes observable IAB activity by several days or weeks. Monitoring credential leaks can provide organizations with time to rotate credentials before access is weaponized.

Future Trends in IAB Operations

The IAB ecosystem is likely to continue evolving throughout 2026 as ransomware groups, brokers, and other cybercriminal actors adapt to increasing law enforcement pressure and changing market conditions. Current activity suggests that the market is becoming more selective and operationally mature rather than growing in size. Targeting of entities that already maintain access to multiple customer environments, such as third-party vendors or other upstream suppliers, is likely to increase in 2026. One successful intrusion into such an entity can provide access to dozens or even hundreds of downstream networks in the supply chain, significantly increasing the operational value of a single compromise.

The market itself is likely splitting into two separate segments: lower-tier access involving cheap, large-scale credential sales and a higher-value tier that increasingly involves administrator-level or enterprise-wide access sold privately through trusted relationships rather than within public forums.

- Commodity access is often linked to opportunistic targeting and large-scale campaigns.
- Premium access typically reflects deliberate targeting of high-value organizations.

- Private sales are becoming more common for enterprise-level access with elevated privileges.

Operational technology and critical infrastructure continue to be primary targets in IAB and ransomware operations, with several operational technology environments still relying on older systems with limited visibility. Meanwhile, industrial networks, manufacturing environments, logistics systems, and energy infrastructure remain lucrative because disruption in these sectors can create immediate operational and financial pressure.

Internet-facing infrastructure remains another major attack surface for IABs. Threat actors frequently exploit known vulnerabilities affecting VPN appliances, remote access gateways, and externally exposed collaboration platforms because these systems often sit outside traditional endpoint monitoring coverage. ZeroFox has observed IABs disproportionately targeting perimeter devices with publicly available common vulnerabilities and exposures (CVE) exploits. Such exploitation can likely be avoided by maintaining a log of discovered vulnerabilities, releasing quick patches, and implementing them promptly.

AI-powered tools are increasingly gaining traction among IABs and ransomware groups, who are actively experimenting with automation to identify targets, generate social engineering lures, discover vulnerabilities, develop malware, and organize stolen access. AI and deepfakes have not only made phishing lures difficult to detect but also easier to obtain. Meanwhile, AI-powered automation is likely to reduce the time required to identify and validate access. Faster operational cycles will likely shorten the time period between compromise and ransomware deployment.

Conclusion

IABs are no longer peripheral actors within the ransomware ecosystem. They now operate as a critical enabler, connecting credential theft, network intrusion, and ransomware deployment. While publicly visible IAB activity appears to be declining, the market itself is almost certainly becoming more private, targeted, and difficult to monitor. Organizations that fail to detect broker activity early may only become aware of

the intrusion once ransomware operators have already established persistence within their environments.

Recommendations

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are patched with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud servers at least once per year—and ideally more frequently.
- Implement secure password policies, phishing-resistant multi-factor authentication (MFA), and unique credentials.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Proactively monitor for compromised accounts and credentials being brokered in DDW forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated tactics, techniques, and procedures (TTPs).

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:RED** when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** **TLP:AMBER** when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	**Recipients may NOT share** **TLP:RED** with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	**Recipients may ONLY share** **TLP:AMBER** information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. **Note that** **TLP:AMBER+STRICT** restricts sharing to the organization only.

	Green	Clear
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:GREEN** when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	**Sources may use** **TLP:CLEAR** when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	**Recipients may share** **TLP:GREEN** information with peers and partner organizations within their sector or community but not via publicly accessible channels.	**Recipients may share** **TLP:CLEAR** information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%