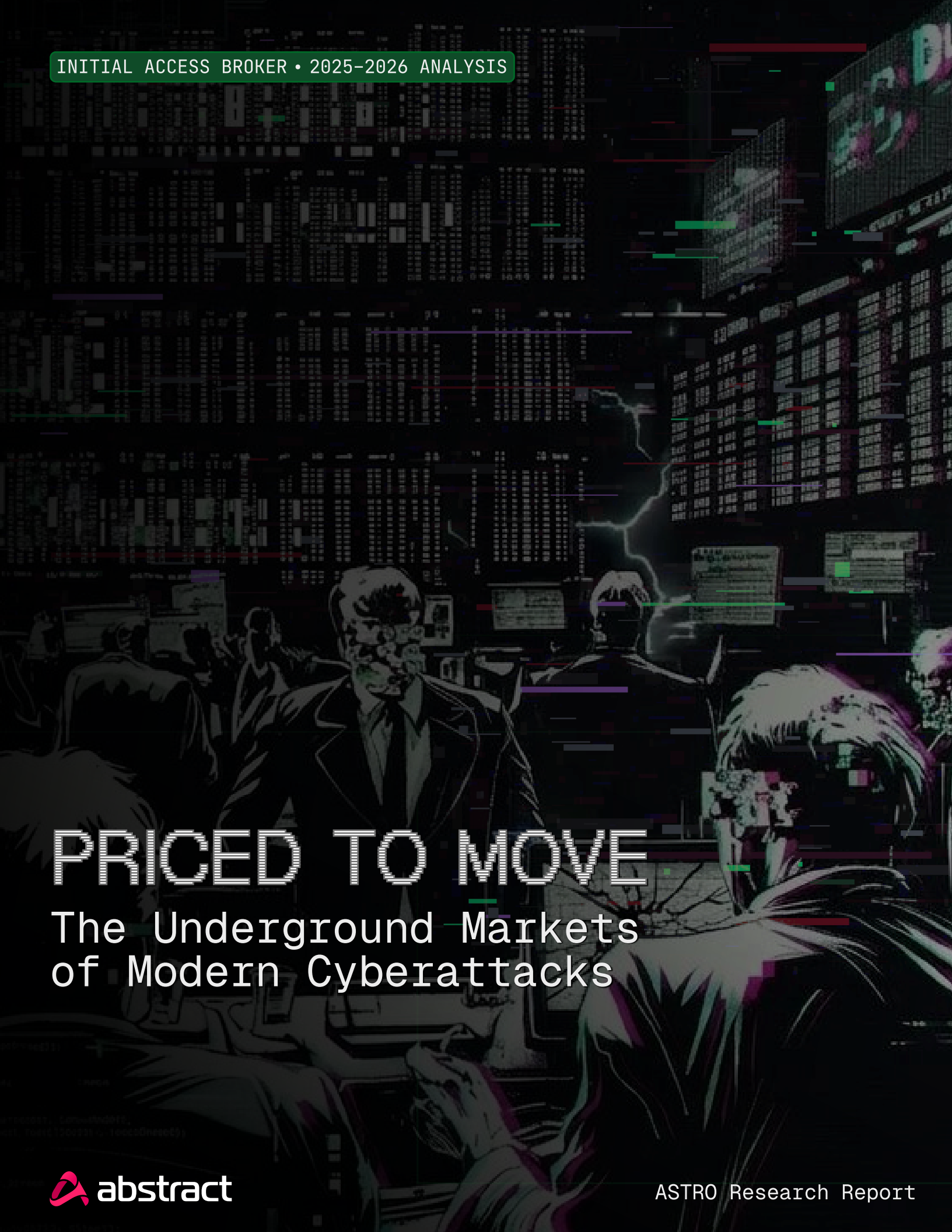

INITIAL ACCESS BROKER • 2025–2026 ANALYSIS
PRICED TO MOVE
The Underground Markets of Modern Cyberattacks
abstract
ASTRO Research Report

## Executive Summary

Intrusion is now industrialized. A mature market of Initial Access Brokers (IABs) now supplies pre-compromised footholds into enterprise networks, allowing ransomware and extortion groups to skip reconnaissance and move directly to monetization. By specializing in the initial access phase and selling unauthorized access to compromised networks, IABs have lowered the barriers to entry for sophisticated cyberattacks, making them faster, more scalable, and alarmingly efficient.

Modern intrusions increasingly rely on compromised credentials rather than exploit chains. Valid accounts — particularly those without multi-factor authentication — have become the dominant entry vector. At the same time, the rapid expansion of SaaS platforms alongside legacy VPN and on-premise infrastructure has created a dispersed identity surface that is difficult to inventory comprehensively and even harder to monitor in real time.

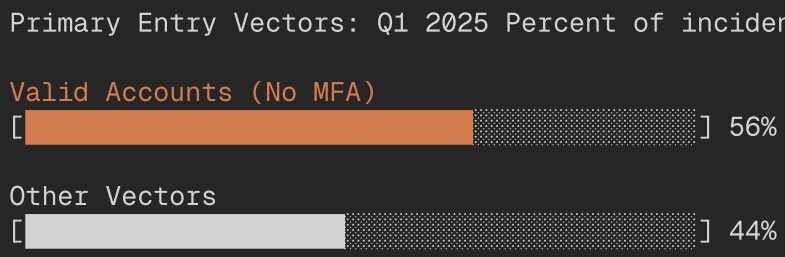
IABs operate within this fragmentation. By harvesting, validating, and reselling authenticated access across hybrid environments, they convert configuration gaps and visibility blind spots into tradable entry points.

Analysis of 2025 data reveals that the ransomware threat has intensified dramatically, with attack volumes surging 47% compared to the prior year while average costs to acquire network access have plummeted to unprecedented lows. [1,8,10]

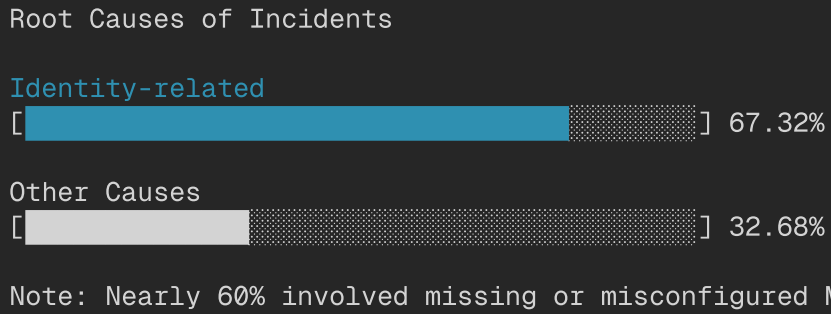
This research reflects ongoing monitoring conducted by the Abstract Security Threat Research Organization (ASTRO), including longitudinal tracking of active IAB operators and correlation of credential abuse and CVE exploitation patterns.

# Key Findings

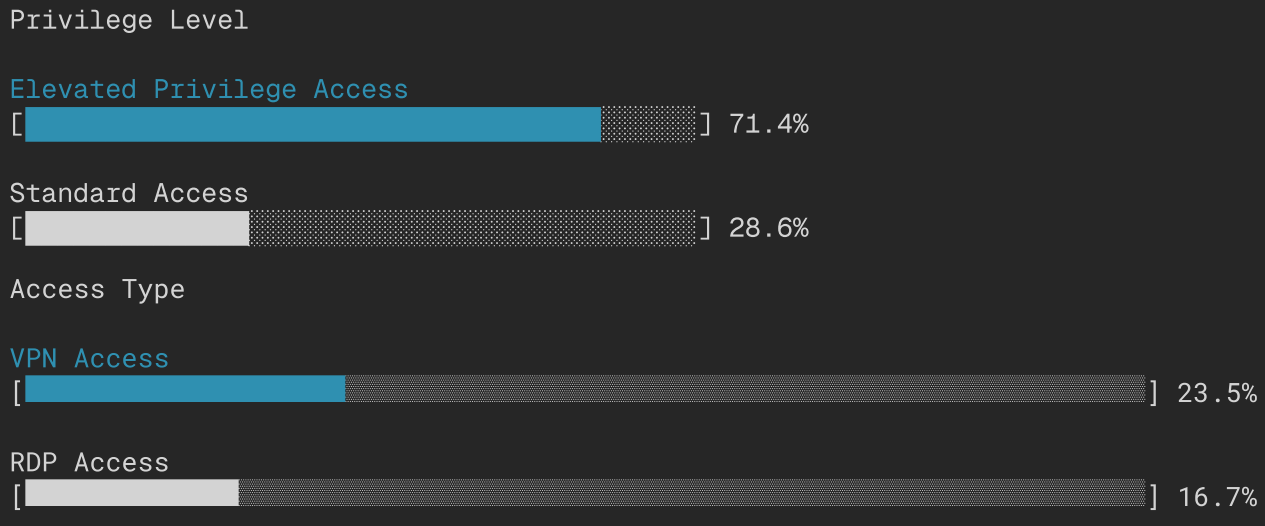
**Credential abuse has displaced vulnerability exploitation as the primary entry vector.** 56% of Q1 2025 incidents involved valid accounts without multi-factor authentication.




Sophos's 2026 Active Adversary Report corroborates this shift: 67.32% of all root causes in 2025 were identity-related, with MFA absent or misconfigured in nearly 60% of incidents.[33]

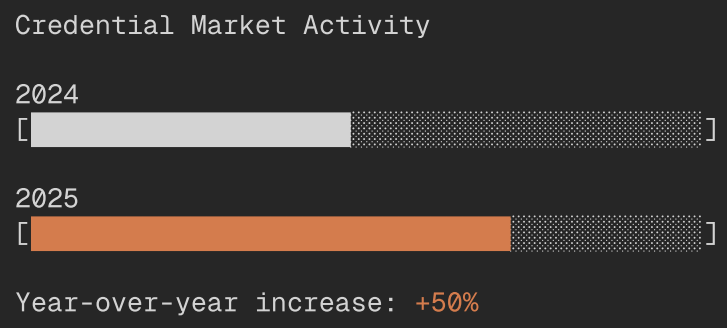



CrowdStrike's 2025 Global Threat Report recorded a 50% year-over-year surge in access broker advertisements selling stolen credentials. [34]

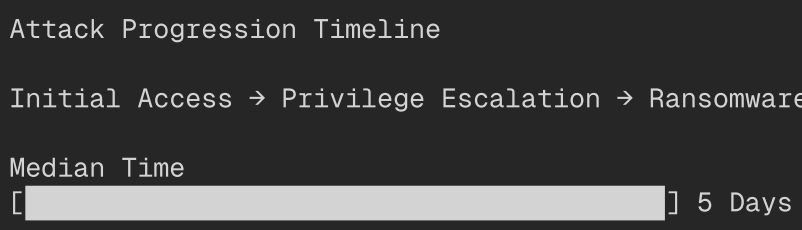


# Key Findings

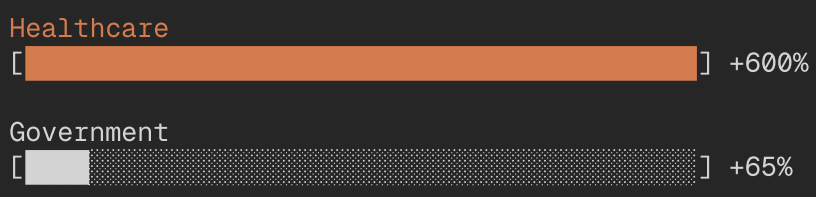
IAB offerings have matured: 71.4% of listings now include elevated privileges such as domain admin credentials or multiple entry points. VPN access emerged as the most common offering (23.5%), surpassing RDP (16.7%).




Execution speed is accelerating. Median dwell time from initial access to ransomware deployment compressed to just 5 days. [4,17]




Healthcare experienced a 600% increase in IAB-targeted attacks. Government saw a 65% year-over-year rise. Education recorded the highest overall attack volume of any sector. [6]

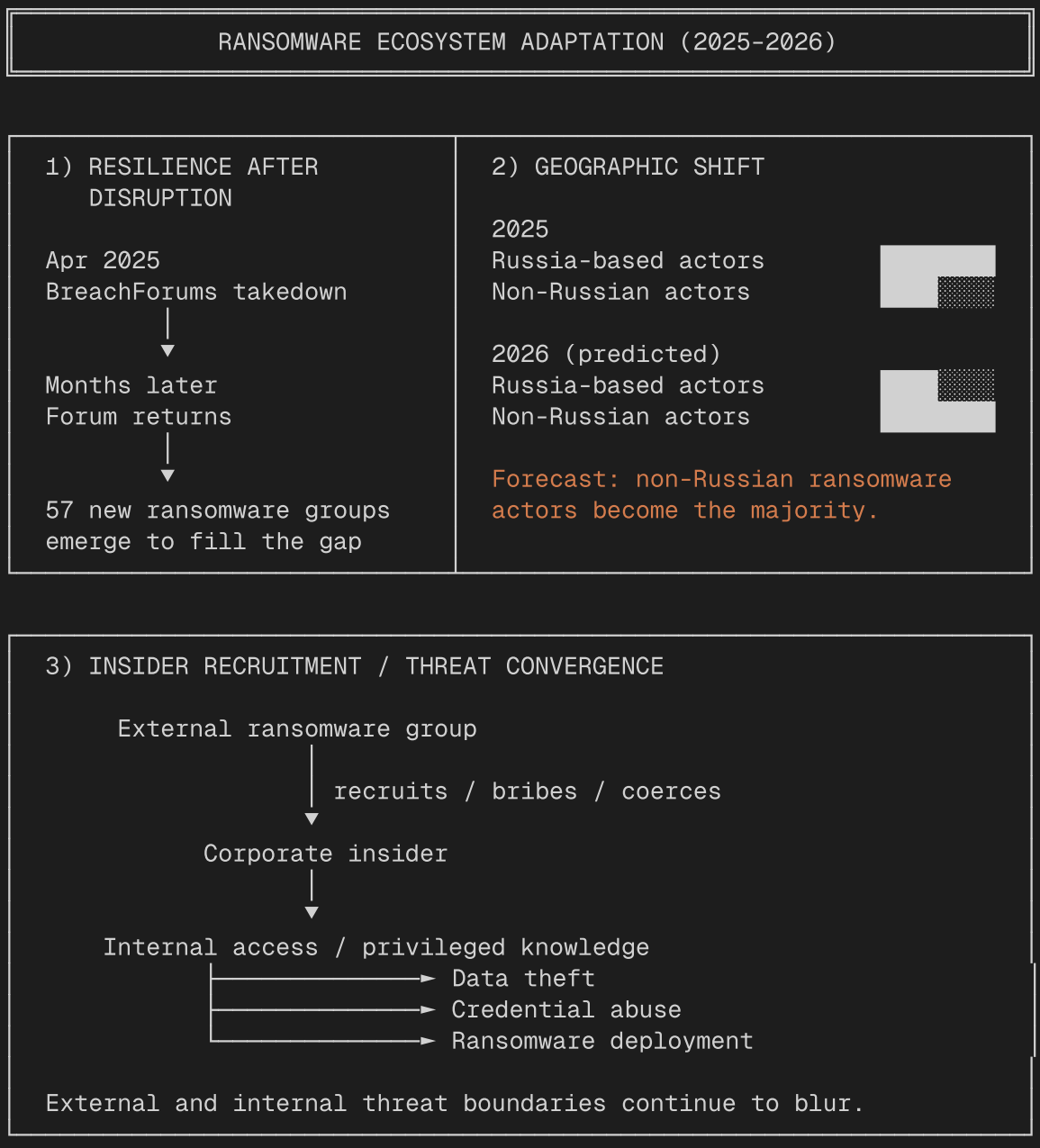


# Critical Threats for 2026

The ecosystem demonstrated remarkable resilience despite law enforcement successes: BreachForums returned months after its April 2025 takedown[31], and 57 new ransomware groups emerged to fill gaps left by disrupted operations.[8]

Intelligence assessments predict 2026 will mark the first year that non-Russian ransomware actors will outnumber those within Russia.[1,9]

An alarming trend of ransomware groups recruiting corporate insiders further blurs the line between external and internal threats.[13]



## Primary Recommendations

**Immediate (0–30 days):**
- Enforce universal MFA, prioritizing all remote access pathways including VPN and RDP.

**Near-Term (90–180 days):**
- Shift to identity-centric controls. Implement Zero Trust principles and deploy behavioral analytics capable of detecting anomalous use of valid accounts.

**Long-Term Resilience:**
- Assume intrusion is inevitable. Invest in immutable backups, enforce network segmentation, formalize insider risk monitoring, and actively participate in sector ISACs.

## Scope and Methodology

This paper synthesizes findings from Rapid7's 2025 Access Brokers Report [2], Recorded Future's ransomware tracking [1], Check Point's 2026 Cyber Security Report [9], Cyble's ransomware group analysis [8], and incident response data from Arctic Wolf, Sophos, and other leading vendors.[4,17]

Complementing the landscape analysis, this paper incorporates original threat research conducted by ASTRO, based on 12 months of continuous monitoring of a specific volume-based IAB operator (Section 6). This ground-level data — including credential analysis across 30,000+ compromised devices and temporal correlation between CVE proof-of-concept releases and exploitation surges — provides empirical validation of the trends and defensive recommendations described throughout.

# The Broker: Three Weeks of Silence!

[Staff] Sherlog Holmes

Researcher

ASTRO

Posts: 5
Threads: 1
Reputation: 88

On an otherwise unremarkable day, an attacker known as ToyMaker — tracked by researchers as GoldMelody and UNC961 — exploited known vulnerabilities in an internet-facing server belonging to a critical infrastructure enterprise. The intrusion itself was methodical. ToyMaker deployed a custom backdoor called LAGTOY, a reverse shell implant that persisted as a Windows service named "WmiPrvSV" and communicated with a hardcoded command-and-control server over TCP port 443 — a port that blends seamlessly with normal HTTPS traffic.

Within the first week, ToyMaker enumerated users, created a rogue administrator account named "support," extracted credentials using Magnet RAM Capture, and exfiltrated the memory dump via PuTTY's SCP utility. Then — nothing. For approximately three weeks, the network sat untouched.

ToyMaker made no attempt to steal data. They did not pivot to high-value systems. They did not deploy ransomware. The sole objective was to package what they had found and sell it.

After the three-week gap, the Cactus ransomware group entered the network using the credentials ToyMaker had harvested. Cactus deployed its own entirely independent tooling — PowerShell remoting scripts for enumeration, 7-Zip for compression, curl for exfiltration — before detonating ransomware across the environment. The entire chain, from ToyMaker's initial exploitation to Cactus's deployment, spanned roughly five weeks. [36]

The three-week silence was not inactivity. It was a transaction.


*Figure 1: cAcTuS.readme.txt*

## 1.1 GoldMelody/UNC961: Technical Deep-Dive

Active from October 2024 through March 2025, GoldMelody represents the upper tier of IAB sophistication. The group deployed in-memory IIS modules and exploited leaked ASP.NET machine keys to maintain stealthy persistence — techniques suggesting possible state-affiliated connections. [12]

| Phase | Activity |
|---|---|
| Day 0 - Initial Access | Exploit leaked ASP.NET machine keys to achieve view state deserialization on IIS servers. Upload initial web shell disguised as legitimate ASP.NET handler. |
| Day 1-3 - Persistence | Deploy custom in-memory IIS modules written in C++. Modules loaded directly into w3wp.exe, leaving minimal disk artifacts. Establish staging directory. |
| Week 1-2 - Recon | AD enumeration using native Windows commands. Network mapping, security product identification, backup system location. Credential harvesting from LSASS. |
| Week 2-4 - Escalation | Deploy custom C# binary "updf" (disguised as PDF utility) for local privilege escalation. Achieve SYSTEM-level access. Escalate to domain admin. |
| Week 4+ - Validation | Document network architecture, critical systems, and security controls. Compile intelligence package for sale via private channels or direct to RaaS operators. |

### Technical Details

The group exploited leaked ASP.NET machine keys hardcoded in web.config files, enabling arbitrary code execution on IIS servers. Custom C++ IIS modules were loaded directly into w3wp.exe memory, providing backdoor access and credential harvesting without writing malicious files to disk — evading signature-based detection. A binary named "updf" masqueraded as a PDF utility but performed Windows privilege escalation. The group made extensive use of living-off-the-land techniques: net.exe, nltest.exe, whoami.exe, PowerShell AD cmdlets. A consistent staging directory at C:\Windows\Temp\111t was used across multiple intrusions.

### Indicators of Compromise

- File System: C:\Windows\Temp\111t (staging directory); updf.exe (privilege escalation, C#); ASP.NET handlers with legitimate names (ErrorHandler.ashx, LoggingModule.ashx)
- Process: w3wp.exe loading unexpected modules without corresponding DLL files; unusual child processes (cmd.exe, powershell.exe, net.exe) from IIS worker
- Network: Outbound connections from w3wp.exe (C2); web server accessing domain controllers and backup systems
- Behavioral: Reconnaissance commands (net user /domain, nltest /dclist, whoami /all); LSASS memory access; data staging to Temp directories

## Disruption Opportunities

The three-week gap between initial compromise and ransomware deployment represents a detection window that most organizations struggle with. During that window, ToyMaker's activity generated multiple observable signals: a new local administrator account created outside of change management, memory dumping tools executing on production servers, SCP-based data exfiltration from unexpected processes, and a Windows service installed with a name mimicking a legitimate WMI component. Any one of these indicators, if detected and investigated, would have broken the attack chain before Cactus ever gained entry. [36]

## Lessons Learned

- Unprotected configuration secrets and machine keys in web.config files enable deserialization attacks.
- IIS web server processes spawning shells are high-confidence indicators. Monitor aggressively.
- Memory analysis is required for in-memory modules that evade disk-based detection.
- Network segmentation is essential: web servers should not directly access domain controllers or backup systems.

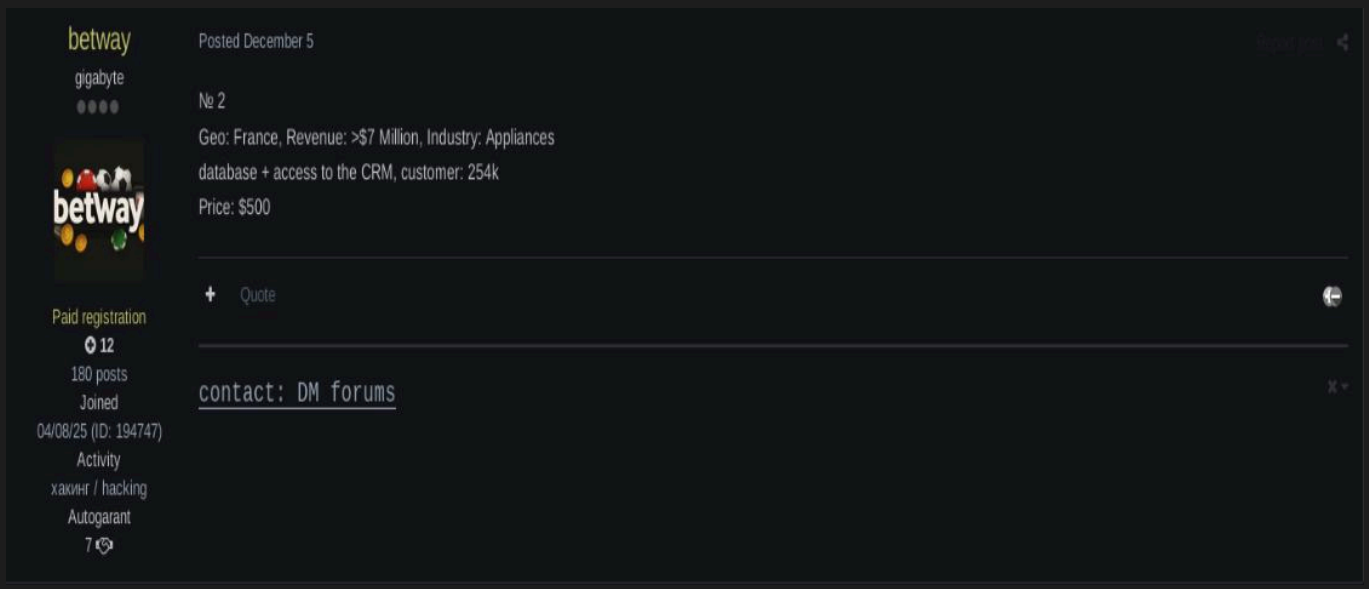



*Figure 2: IAB listing on exploit[.]in forum showing target attributes, access type, and pricing.*

# What just happened: The IAB Model

[Staff] Sherlog Holmes

Researcher

ASTRO

Posts: 5
Threads: 1
Reputation: 88

ToyMaker did not behave like a traditional hacker. They breached a network, packaged what they found, and sold it. That transaction is the defining feature of Initial Access Brokers.

## 2.1 The Evolution of Cybercrime Specialization

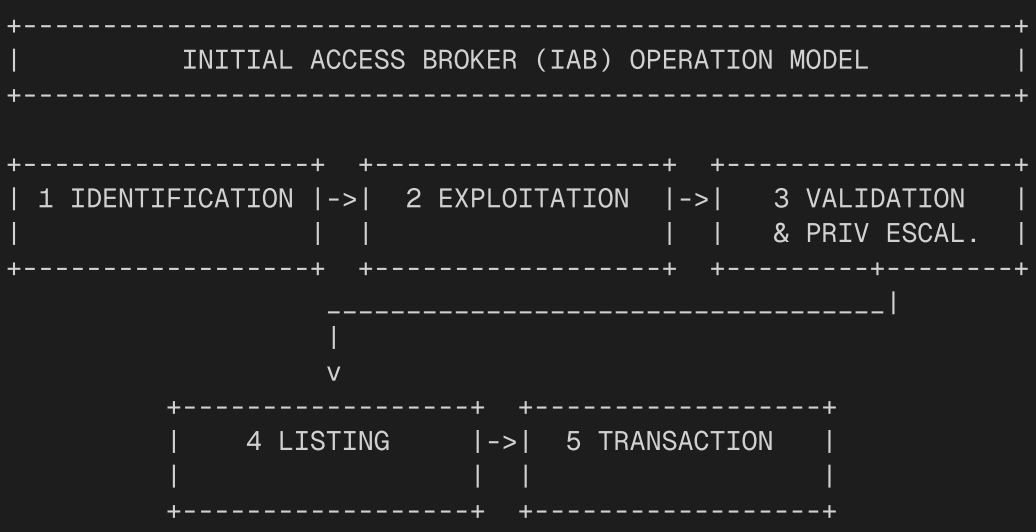
Over the past decade, cybercrime has reorganized into a segmented economy. Distinct actors now specialize in narrow functions across the intrusion lifecycle and sell those capabilities to one another.

Malware developers maintain and lease payloads through Ransomware-as-a-Service (RaaS) platforms. Bulletproof hosting providers sell infrastructure designed to withstand takedown attempts. Exploit developers monetize newly discovered vulnerabilities. Negotiators manage ransom payments. Access sellers source and resell footholds into corporate networks.

Each role focuses on a specific operational task, increasing efficiency through repetition and scale. Capabilities that once required a single actor to possess reconnaissance skill, exploit development expertise, lateral movement tradecraft, and monetization channels are now distributed across participants who optimize for one layer of the workflow.

## 2.2 What Are Initial Access Brokers?

Initial Access Brokers (IABs) are specialized cybercriminals who concentrate on a singular objective: gaining unauthorized entry into computer systems and corporate networks, then selling that access to other malicious actors. Unlike traditional hackers who exploit access for direct gain, IABs treat network intrusion as a product, and they breach, package, and sell access as a commodity on underground marketplaces.



## What just happened: The IAB Model

The IAB business model operates through five distinct phases [18]:

1. **Identification**
   Using automated scanning tools like Shodan, Censys, or custom scripts, IABs identify organizations with vulnerable external-facing assets. In 2025, the focus shifted dramatically toward VPN services (23.5% of listings), domain user accounts (19.9%), and RDP services (16.7%). These three vectors account for almost 60% of all IAB offerings. [2,11]

2. **Exploitation:**
   IABs leverage multiple attack vectors to establish initial footholds. Credential-based attacks have overtaken vulnerability exploitation as the dominant method: 23% of attacks used compromised credentials, 18% involved phishing, and 32% exploited vulnerabilities. Notably, 56% of all Q1 2025 incident response cases involved valid accounts without MFA. [2,4]

3. **Validation and Privilege Escalation:**
   Validation and Privilege Escalation: Rather than immediately selling basic access, modern IABs explore compromised networks to maximize value. Rapid7's analysis found that 71.4% of IAB listings now include elevated privileges, domain admin credentials, multiple entry points, or privileged user accounts. [2,11]

4. **Listing:**
   Access is advertised on dark web forums — primarily Exploit, XSS, and BreachForums. Listings describe the target industry, geographic location, approximate revenue, type of access, privilege level, and security posture.

5. **Transaction:**
   Buyers — typically ransomware affiliates, data extortion groups, or nation-state actors — purchase access through escrow services. 39% of listings fall between $500–$1,000, with an average sale price of $2,700. [14,16]

### 2.3 Why IABs Matter Now: The 2025 Inflection Point?

Three converging factors define why IABs demand immediate attention. First, ransomware attack volumes surged to 7,200 publicly reported incidents in 2025, a 47% increase, even as median ransom demands dropped to $217,000.[3,10,16] IABs enable this volume strategy: with access available for under $1,000, operators can target dozens of victims simultaneously.

Second, IABs have democratized sophisticated cyberattacks by eliminating the skill barrier. Bundled access packages with domain admin credentials let unsophisticated actors launch attacks that previously required advanced capabilities.

Third, the IAB marketplace has increasingly attracted nation-state actors, with groups like GoldMelody/UNC961 demonstrating dual financial and state-affiliated motivations, blurring the line between cybercrime and espionage.[12]

# The Marketplace

[Staff] Anna Lies

Researcher

ASTRO

Posts: 5
Threads: 1
Reputation: 88

The IAB marketplace operates as a sophisticated underground economy with transparent pricing, quality guarantees, and standardized service levels.

## 3.1 Market Size and Underground Marketplaces

The IAB market reached a minimum valuation of $6.3 million in 2024 based on publicly advertised prices across major forums. [15] The total revenue of organizations listed for sale exceeded $3 trillion. Growth has been explosive: IAB listings increased 147% from 2022 to 2023 [14], ransomware attacks grew 47% from 2024 to 2025 [1,8], 57 new ransomware groups emerged in 2025 [8], and access-for-sale listings in the top 10 targeted countries grew 90%. [15]

IABs primarily operate through four major dark web forums:

| Forum | Characteristics |
|---|---|
| Exploit | Russian-language forum with strict vetting; established reputation system; focuses on high-value targets |
| XSS | Primarily Russian language; longstanding marketplace with escrow services; diverse offerings |
| BreachForums | English-language; most accessible to Western actors; disrupted April 2025, returned July 2025 |
| Ramp | Multilingual platform; growing presence; focuses on volume sales with lower barriers to entry |

Forums implement escrow services (5–10% fee), reputation systems with verified seller badges, proof-of-access requirements, and replacement guarantees (24–72 hours) to professionalize transactions and reduce buyer friction. [14,15]

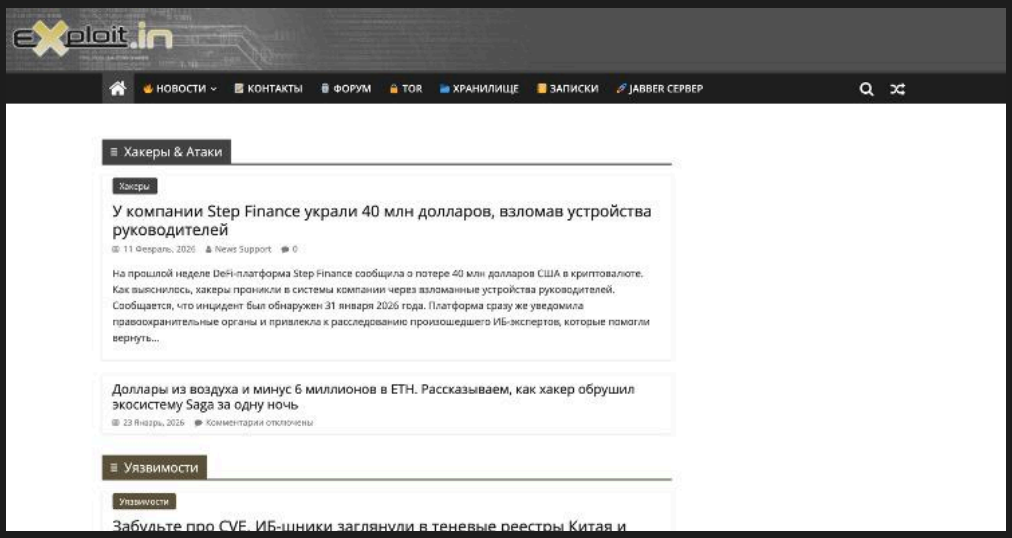



*Figure 3: The Exploit[.]IN dark web forum, one of the primary IAB marketplaces.*

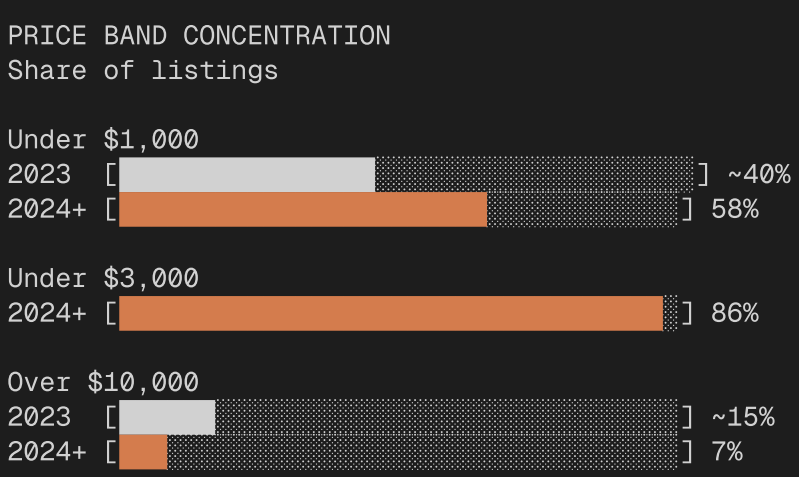
# The Marketplace

## 3.2 Pricing Dynamics

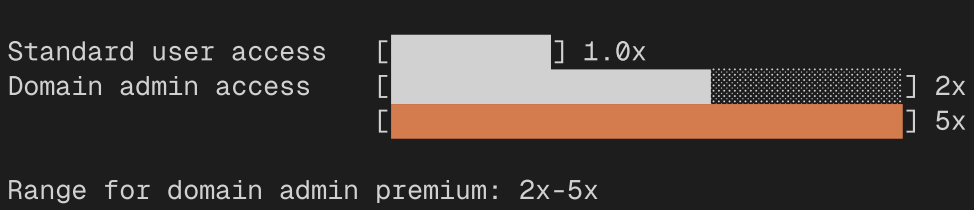
The 2025 IAB market demonstrates clear pricing stratification with a dramatic shift toward affordability:

| Price Range | % of Listings | Typical Access |
|---|---|---|
| $500–$1,000 | 39% | VPN/domain user, SMB targets |
| $1,000–$3,000 | 47% | Mid-market, some privileges |
| $3,000–$10,000 | 7% | Domain admin, enterprise targets |
| >$10,000 | 7% | Multiple vectors, Fortune 500 |

Average sale price: $2,700. The defining trend of 2024–2025 is the shift toward volume: 58% of listings fell under $1,000 (up from ~40% in 2023), and 86% under $3,000. High-value listings (>$10,000) declined from ~15% to 7%. [14]




Key pricing factors include organization revenue, access type (domain admin credentials command 2–5x premiums over standard user access), industry sector, security posture (absence of MFA and presence of only Windows Defender increase value), and geography (US targets represent 31–48% of listings and command 20–30% premiums).[2,15]



# The Marketplace

## 3.3 The IAB-Ransomware Connection

IABs and ransomware operations have evolved from transactional relationships into integrated partnerships. Many IABs maintain standing relationships with specific RaaS operations, receiving flat rates or revenue-sharing arrangements (typically 10–20% of ransom) rather than per-access fees.

This symbiosis drives attack acceleration: median dwell time from initial access to ransomware deployment dropped to just 5 days in Q4 2024, down from 9–11 days earlier in the year. [4,17] Some attacks achieved deployment in under 24 hours. [1]

The economics are compelling: with access priced at $500–$1,000, ransomware operators can launch simultaneous campaigns across dozens of targets. When 71.4% of purchases include elevated privileges, operators can begin lateral movement immediately without spending time on privilege escalation. [2]

## 3.4 Geographic Targeting

| Country | % of Listings | Trend | Key Sectors |
|---|---|---|---|
| $500–$1,000 | 39% | Stable | Healthcare, Tech, Finance |
| $1,000–$3,000 | 47% | ↑ Rising | Energy, Manufacturing |
| $3,000–$10,000 | 7% | ↑ Rising | Financial Services, Retail |
| >$10,000 | 7% | +90% growth | Concentrated targeting |

*Table 3.4: Geographic Distribution of IAB Listings, 2025 [2, 14, 15]*

## 3.5 Industry Sectors

| Sector | Share | Change vs 2023 | Key Sectors |
|---|---|---|---|
| Healthcare | ~18% | ↑ 600% IAB attacks | Healthcare, Tech, Finance |
| Manufacturing | ~15% | ↑ Into top 3 | Energy, Manufacturing |
| Business Services | 13% | ↓ Down from 29% | Financial Services, Retail |
| Retail | ~12% | Stable | Concentrated targeting |
| Government | ~10% | ↑ +65% YoY | Sensitive citizen data, geopolitical value |
| Education | ~9% | ↑ Highest volume | Weak security, research data, student PII |
| Financial Services | ~8% | 65% impacted | Direct financial access, regulatory pressure |

*Table 3.5: Industry Sector Targeting by IABs, 2025 [2, 6, 14, 15, 27, 29]*

# The Marketplace

## 3.6 Organization Size

| Revenue Range | 2024 Share | 2023 Share | Rationale |
|---|---|---|---|
| $5M–$50M | 60.5% | 53% | Weaker security, less backup sophistication |
| $50M–$100M | 15% | 12% | Balance of value vs. defenses |
| $100M–$1B | 12% | 16% | Stronger security teams |
| $1B+ | 12.5% | 19% | Mature SOCs, IR capabilities |

The shift toward mid-market ($5M–$50M) organizations reflects the volume strategy: these organizations typically lack dedicated security teams, operate with constrained IT budgets, often use only Windows Defender, and represent the "Goldilocks zone", valuable enough to pay moderate ransoms but not so large they can rebuild from backups. [14,15]

# Meet the Brokers: A Field Guide

[Staff] Sherlog Holmes

Researcher

ASTRO

Posts: 5
Threads: 1
Reputation: 88

The IAB landscape includes operators ranging from opportunistic credential sellers to sophisticated actors with potential nation-state connections. Understanding the tiers helps defenders prioritize and helps analysts attribute activity correctly. You already know Tier 1, that was ToyMaker.

## 4.1 Operational Tiers

Tier 1 (Elite):

Operators like GoldMelody/ToyMaker develop custom tooling, target high-value organizations, and maintain extended access before sale. Minimal public forum presence; direct RaaS relationships. Pricing $5K–$50K+. Weeks to months of dwell time. Comprehensive intelligence packages.

Tier 2 (Professional):

Actors like SGL and IntelBroker balance sophistication with volume. Established forum reputations, consistent quality. Pricing $1K–$10K. Days to weeks of dwell time.

Tier 3 (Opportunistic):

Operators like Br0k3r rely on automated scanning and purchased info-stealer logs. High volume, rapid turnover, minimal post-compromise activity. Pricing $200–$2K. Hours to days from compromise to listing.

## 4.2 Notable IAB Operators

| Operator | Tier | Specialization | Forums | Notable Pattern |
|---|---|---|---|---|
| GoldMelody / ToyMaker | 1 | Custom malware, IIS exploitation | Private | Advanced capability, long dwell, direct RaaS sales |
| IntelBroker (Kai West) | 2 | Enterprise targets, cloud misconfig, APIs | BreachForums | Fortune 500 focus; arrested Feb 2025 in France |
| SGL | 2 | VPN access, domain admin escalation | XSS, Exploit | High volume, budget pricing, established RaaS relationships |
| miyako | 2 | Asia-Pacific targets, credential stuffing | BF, XSS | Geographic specialization, multi-language |
| Br0k3r | 2 | RDP brute force, bulk sales | Exploit, Ramp | Automated scanning, low-cost ($200–$1K) |
| ASTRO-Tracked Operator | 3 | VPN appliances (Cisco, PAN, Fortinet) | Unknown | Industrial-scale credential spraying; 30,000+ devices on single credential pair |

# How They Get In

[Staff] Sherlog Holmes

Researcher

ASTRO

Posts: 5
Threads: 1
Reputation: 88

IAB operations follow predictable patterns driven by economic efficiency and technical feasibility. Understanding these TTPs enables defenders to identify and disrupt IAB activity before access reaches ransomware operators.

## 5.1 Initial Access Methods

| Sector | % of IAB Sales | % of Attacks | Key Characteristics |
|---|---|---|---|
| VPN Access | 23.5% | 23% (credentials) | Stealth, valid credentials, bypasses perimeter |
| Domain User Accounts | 19.9% | 56% (valid, no MFA) | Credential stuffing, phishing, password spraying |
| RDP Services | 16.7% | 32% (vuln exploit) | Exposed to internet, weak passwords |
| Phishing/Social Eng. | ~15% | 18% (up from 11%) | QR phishing, AI deepfakes rising |
| Domain Admin | 5.5% | — | Premium pricing, immediate lateral movement |

*IAB Sales figures from [2,14,15]; Attack percentages from [33,34,35]; Trend characteristics from [1,9]*

### VPN Compromise: The Rising Threat

VPN access surged to become the most common IAB offering (23.5% in 2025, more than doubled from 2023). [2,11] VPN access typically comes with working credentials and no MFA, allowing attackers to blend with legitimate traffic.

Multiple high-profile VPN platforms experienced critical vulnerabilities in 2024–2025, including Fortinet FortiOS (CVE-2024-21762, CVE-2024-55591), Ivanti products (CVE-2024-21887, CVE-2026-1281), and SonicWall SSL VPN.

IABs also increasingly purchase stolen VPN credentials from info-stealer operators rather than exploiting technical vulnerabilities. [4,32]

## How They Get In

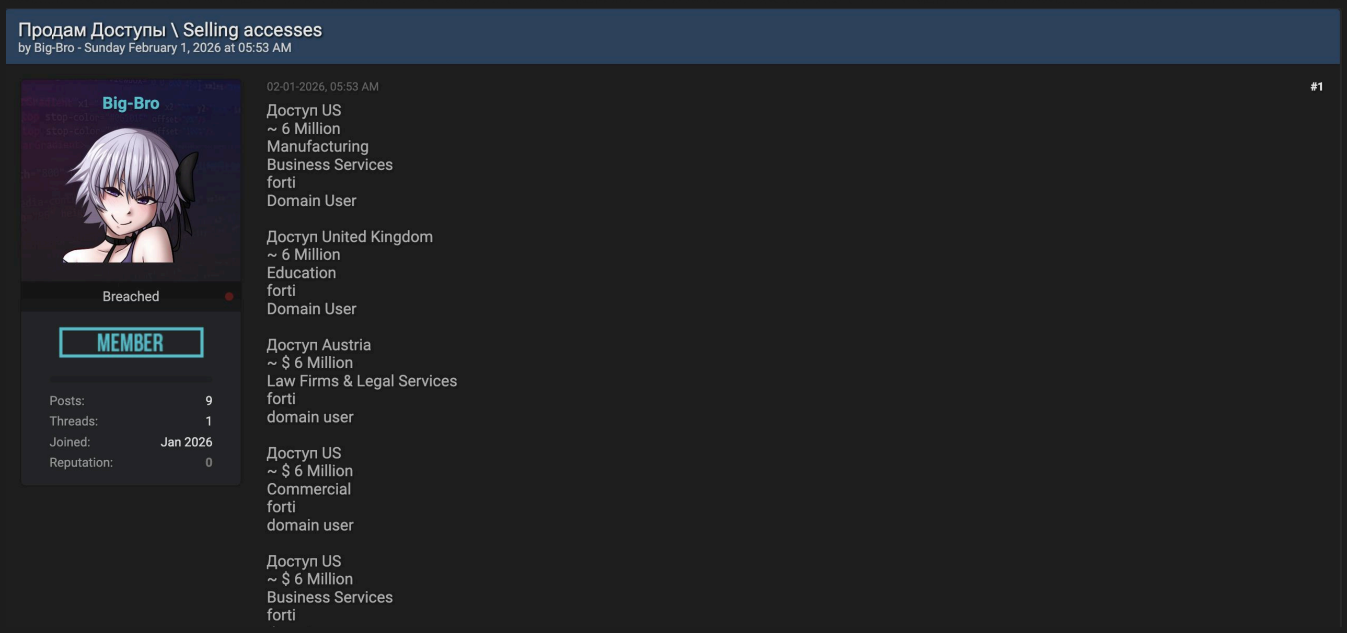



*Figure 4: IAB on breachforums[.]as selling multiple network accesses across different countries and industries.*

### The Credential Abuse Shift

The most significant tactical evolution in 2025 is the shift from vulnerability exploitation to credential-based access. At 56% of Q1 2025 incidents, valid accounts without MFA represent the single most common initial access vector. [2,4] This shift lowers technical barriers, evades detection (valid credentials bypass signature-based detection and EDR), and reflects the growing info-stealer ecosystem where malware operations like Raccoon Stealer, RedLine, Lumma, and Vidar feed credentials to IABs who in turn supply ransomware operators. [1]

## 5.2 Common Vulnerabilities Exploited

While credential abuse dominates, vulnerability exploitation remains significant at 32% of attacks. Original tracking data from ASTRO (Section 6) demonstrates a direct temporal correlation between PoC release dates and exploitation surges by opportunistic IABs.

| CVE | Product | Specialization |
|---|---|---|
| CVE-2024-55591 | Fortinet FortiOS | Websocket race condition, RCE as super_admin. Widespread Q1 2025 exploitation. IABs created admin accounts, ~1 month dwell time. [1, 34, 35] |
| CVE-2024-21762 | FortiOS SSL VPN | Out-of-bounds write, arbitrary code execution. Volt Typhoon deployed custom malware. [34, 35] |
| CVE-2024-57727 | SimpleHelp RMM | Password hash leak + RCE chain. Used to deploy INC Ransomware via PowerShell. [1, 34, 35] |
| CVE-2024-1708/1709 | ScreenConnect | Path traversal + auth bypass. Exploited by Play and Black Basta ransomware groups.[33, 34, 35] |
| CVE-2026-1281 | Ivanti EPMM | Zero-day RCE. Actively exploited Jan 2026, added to CISA KEV. [30, 32] |
| ASP.NET Machine Keys | IIS Servers | Leaked machine keys enable view state deserialization. GoldMelody deployed in-memory IIS modules. [12] |

*Table 5.2: Common Vulnerabilities Exploited in IAB-Enabled Attacks, 2024–2026 [1, 12, 30, 32, 33, 34, 35]*

# Twelve Months Inside One Operation

[Staff] Sherlog Holmes

Researcher

ASTRO

Posts: 5
Threads: 1
Reputation: 88

The preceding sections draw from published threat intelligence. This section presents original research conducted by ASTRO, based on 12 months of continuous monitoring of a specific IAB operator — a ground-level view of how a Tier 3 (opportunistic) broker operates at industrial scale. This operator was tracked from November 2024 through February 2026.

## 6.1 Operator Profile

This IAB specializes in compromised VPN appliances across three vendors: Cisco ASA, Palo Alto GlobalProtect, and Fortinet FortiGate. Their primary method is automating credential spraying against internet-facing VPN management interfaces using default or near-default credentials. The operator is purely opportunistic — no filtering of industry, revenue, or geography. The victim pool ranges from 15-host small businesses to networks with thousands of endpoints belonging to major enterprise subsidiaries.

Every listing from this operator follows a standardized template: VPN credentials with external IP and port, internal network range, domain controller IP, and host count. No security product inventory, no backup system mapping, no lateral movement scripts. Compare this to GoldMelody (Section 1), who spends weeks on reconnaissance and provides comprehensive intelligence packages. This operator's recon takes minutes and fits an index card — but the volume is what makes it dangerous. Pricing follows Tier 3 norms: $200–$2,000 per listing depending on host count and perceived organization size.

## 6.2 Credential Analysis

Analysis of the credential pairs used across the full tracking period reveals the scale of the configuration hygiene failure enabling this operator. The most common combination, user:user, was found on nearly 30,000 unique devices. Other high-frequency pairs include test:password (25,000+), user:12345678 (18,000+), and SSLVPN1:SSL@user#2025 (18,000+).

Several patterns emerge. First, vendor-specific defaults are well represented: cisco:password appears in the top 10, and the SSLVPN1 credential is specific to Fortinet SSL VPN test accounts, suggesting appliances deployed with factory settings and never hardened. Second, the long tail of credentials includes what appear to be real personal names, suggesting legitimate user accounts with weak passwords, indicating organizations where password policies are absent or unenforced. Third, the credential user@sslvpn:s3@!89fg%$&ssjd appears superficially complex but was found on over 5,000 devices, suggesting it may be a widely shared deployment template credential that administrators assumed was unique.

# Twelve Months Inside One Operation

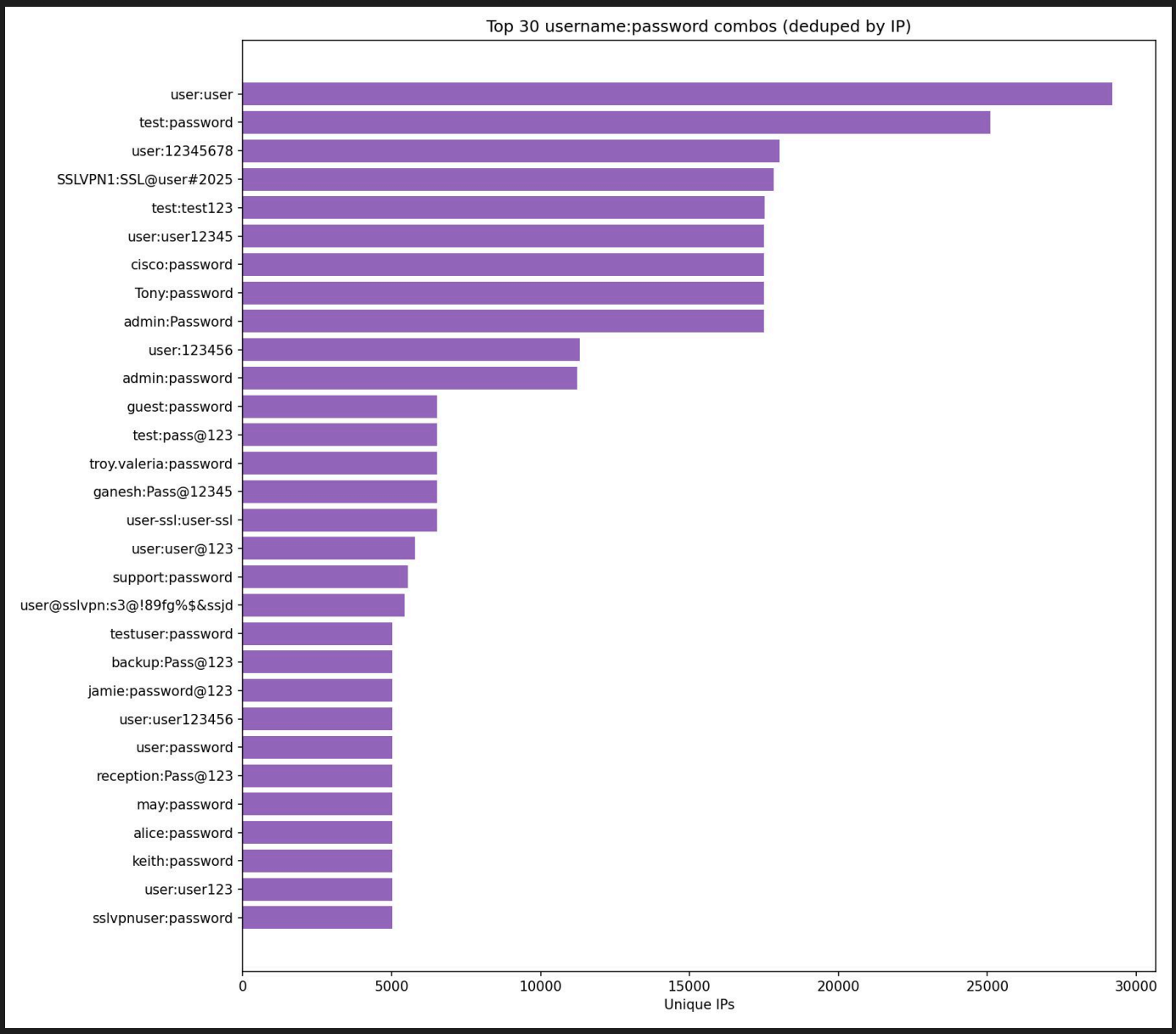



*Figure 5: Top 30 username:password combinations observed from tracked IAB operator, deduplicated by unique IP. Default and trivial credentials dominate, with user:user found on nearly 30,000 devices.*

# Twelve Months Inside One Operation

## 6.3 CVE Exploitation Correlation

While credential spraying forms this actor's baseline activity, the tracking data reveals a clear pattern of rapid pivoting to newly disclosed vulnerabilities.

In October 2024, Cisco disclosed a batch of critical ASA vulnerabilities. Six to eight weeks later (the typical patch reverse-engineering time) the Cisco line spiked to approximately 17,700 unique compromised IPs in December 2024. The most dramatic correlation appears with CVE-2025-32756, a Fortinet stack-based buffer overflow (CVSS 9.8) with proof-of-concept code released in late May 2025. Within six weeks, the Fortinet compromise count surged from approximately 400 to over 20,000 unique IPs, peaking at 23,000+ in September–October 2025 before dropping sharply in November, likely reflecting mass patching finally outpacing exploitation.

This demonstrates how an operator with scanning infrastructure already in place can weaponize a new CVE across the entire internet-facing attack surface within weeks, if not days.

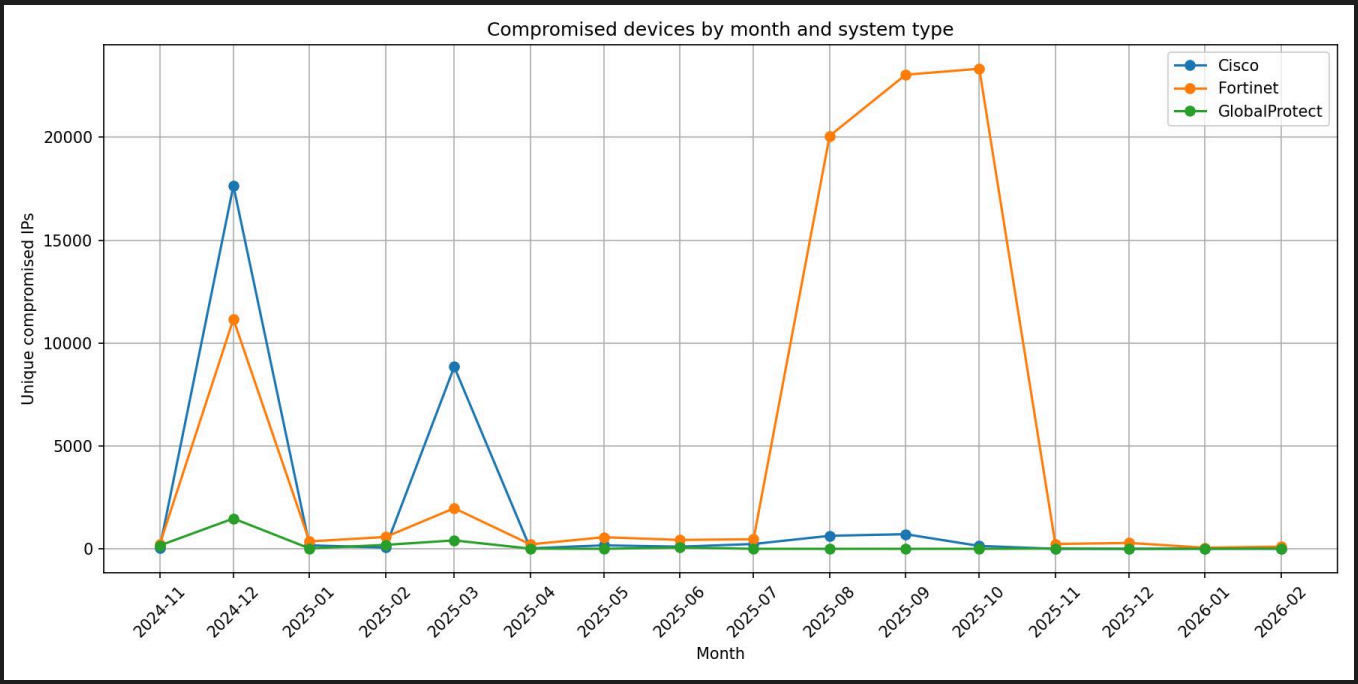



*Figure 6: Compromised devices by month and vendor, with CVE PoC release dates overlaid. The Cisco October 2024 batch correlates with the December 2024 spike; CVE-2025-32756 correlates with the July–October 2025 Fortinet surge.*

# Twelve Months Inside One Operation

## 6.4 Key Findings

- Every compromise observed resulted from one or more basic control failures: default credentials on production VPN appliances, absent MFA, flat network segmentation, and delayed patching.
- Multi-vendor targeting (Cisco, GlobalProtect, and Fortinet simultaneously) means no single vendor advisory protects an organization. Defense requires configuration hygiene across the entire VPN estate.
- The December 2024 baseline across all three vendors represents persistent credential-spraying activity; the CVE-driven spikes sit atop this baseline, demonstrating the operator's ability to rapidly integrate new exploit capabilities into existing infrastructure.
- The standardized listing format creates a detection opportunity: dark web monitoring that surfaces a listing matching an organization's VPN deployment constitutes actionable intelligence with a narrow response window before a ransomware affiliate acts on the purchased access.

# The Pipeline in Action

[Staff] Sherlog Holmes

Researcher

ASTRO

Posts: 5
Threads: 1
Reputation: 88

Note: This composite case study is constructed from multiple documented incidents and publicly reported data to illustrate a typical IAB-to-ransomware pipeline. Individual details are drawn from real-world events; the specific organization and financial figures are representative. A US healthcare organization with $45M in annual revenue. 450 workstations, 75 servers. Windows Defender only. Backups accessible from the production network. No MFA on VPN.

On July 15, an employee clicked a malicious ad, downloaded trojanized software containing RedLine Stealer, and their VPN credentials were harvested from the browser. An IAB validated the access over the following week, mapping the network, noting the security posture.
On July 26, a listing appeared on XSS forum: "US Healthcare | $45M revenue | VPN + Domain User | Defender only | Backups accessible | $2,500."

The access sold for $2,200 the next day.

| Date | Event |
|---|---|
| July 15 | IAB compromises VPN credentials via RedLine Stealer info-stealer malware. No MFA. |
| July 18–25 | IAB validates access, performs reconnaissance. 450 workstations, 75 servers mapped. Backups accessible from production networks. |
| July 26 | Access listed on XSS forum: "US Healthcare \| $45M revenue \| VPN + Domain User \| Defender only \| Backups accessible \| $2,500." |
| July 27 | Ransomware affiliate purchases for $2,200 via Monero. Escrow holds funds until access is verified. |
| July 29–Aug 3 | Operator escalates privileges via Kerberoasting, achieves domain admin. Ransomware payload staged across network. |
| August 4, 2:00 AM | Ransomware deployed. Backups encrypted first, then DCs, file servers, and 412 workstations. $850K demanded. |
| August 12 | Ransom negotiated to $450,000 and paid. Decryption keys provided; 21-day restoration begins. |

# The Pipeline in Action

## 7.1 Financial Impact

| Cost Category | Amount | Notes |
|---|---|---|
| Ransom Payment | $450,000 | Negotiated down from $850K demand |
| Incident Response & Forensics | $180,000 | External IR firm, forensic analysis |
| System Restoration | $320,000 | 21 days to full operations, new hardware |
| Revenue Loss (21 days) | $2,600,000 | Deferred procedures, patient diversion |
| Legal & Regulatory | $125,000 | Deferred procedures, patient diversion |
| Security Improvements | $275,000 | MFA, EDR, network segmentation |
| TOTAL DIRECT COSTS | $3,950,000 | 8.8% of annual revenue. The $2,200 IAB price = 0.056% of total costs (1,795x ROI for attacker). |

*Table 7.1: Composite financial impact based on industry benchmarks [4, 17, 25, 26, 30]*

# When the Broker Gets Caught

[Staff] Dr. Detector

Researcher

ASTRO

Posts: 5
Threads: 1
Reputation: 88

The June 2025 unsealing of charges against IntelBroker (Kai Logan West) demonstrates how operational security failures enable law enforcement attribution despite sophisticated anonymization practices. This case provides the most detailed public account of successful IAB identification to date. [20]

## 8.1 Background

Kai Logan West, a 25-year-old British national, operated as IntelBroker from approximately December 2022 through February 2025. During that period, he offered stolen data for sale at least 41 times and distributed it freely or for forum credits approximately 117 more times across BreachForums, causing over $25 million in documented damages to more than 40 victim organizations worldwide. [20] His targets included Cisco, AMD, Zscaler, Hewlett-Packard Enterprise, Europol, and DC Health Link. [22,23] From August 2024 through January 2025, West served as the owner of BreachForums itself. [24]

In an ironic detail revealed during the investigation, West had previously worked as a trainee at the UK's National Crime Agency, the very agency that cooperates with the FBI on cybercrime investigations. [23]

## 8.2 The Investigative Breakthrough

IntelBroker typically insisted on payment in Monero, a privacy-focused cryptocurrency resistant to blockchain analysis. The investigation's critical break came in January 2023 when an undercover law enforcement officer, posing as a buyer, successfully convinced IntelBroker to accept Bitcoin instead of Monero for a controlled purchase of stolen data. The Bitcoin address IntelBroker provided enabled a chain of attribution that unraveled his entire identity. [21]

Using Chainalysis Reactor, investigators traced cryptocurrency flows from IntelBroker's Bitcoin address to an account on the Ramp cryptocurrency exchange. Ramp's KYC records revealed the account was registered to "Kai Logan West," verified with a UK driver's license, the first concrete connection between the IntelBroker persona and a real-world identity. [20,21]

Additional corroboration: the same IP addresses were used for both West's personal activities and IntelBroker's forum operations. [22] West viewed YouTube videos covering his own breaches from his personal IP, then the IntelBroker account posted those same videos on BreachForums. [23]

# When the Broker Gets Caught

## 8.3 Arrest and Charges

French authorities arrested West at his residence in France in February 2025. The US Attorney for the Southern District of New York unsealed a four-count indictment on June 25, 2025, charging West with conspiracy to commit computer intrusions, conspiracy to commit wire fraud, unauthorized access to protected computers, and wire fraud. Each wire fraud count carries a maximum sentence of 20 years. West remains in French custody pending US extradition proceedings. [20]


*Figure 7: FBI seizure banner displayed on BreachForums following law enforcement action.*

## 8.4 Key Lessons

- A single cryptocurrency transaction was sufficient to unravel years of operational security.
- High-profile actors attract disproportionate investigative resources.
- Individual arrests have limited lasting impact on market activity; the infrastructure and buyer demand survive individual takedowns. IntelBroker's arrest created measurable but temporary disruption: forum activity decreased for 2–3 weeks then normalized.

# Detection and Defense

[Staff] Sherlog Holmes

Researcher

ASTRO

Posts: 5
Threads: 1
Reputation: 88

Given that 44% of incident response cases now involve IAB-provided access and the median time from initial access to ransomware deployment is just 5 days, organizations must implement both preventive measures and detective capabilities that exploit the critical window before access is sold or used. [2,4,17]

## 9.1 Preventive Controls

| Control | Priority | Threat Mitigated | Implementation |
|---|---|---|---|
| Universal MFA | CRITICAL | 56% of incidents: valid accounts without MFA | All users, all systems. Phishing-resistant preferred (FIDO2, hardware tokens). No exception. |
| VPN/RDP Hardening | CRITICAL | 40% of IAB sales (23.5% VPN + 16.7% RDP) | No internet-facing RDP. VPN with conditional access, geofencing, and device compliance. |
| Aggressive Patching | HIGH | 32% of attacks exploit vulnerabilities | 24–72 hour window for critical CVEs. Virtual patching for urgent cases. |
| Commercial EDR | HIGH | IABs note "Defender only" as weakness | Deploy within 60–90 days. Prioritize critical servers. |
| Network Segmentation | HIGH | Limits lateral movement after compromise | Air-gap backups immediately. Full segmentation 6–12 months. |
| Privileged Access Mgmt | MEDIUM | 71.4% of sales include elevated privileges | Just-in-time access, credential vaulting, session recording. |

*Table 9.1: Preventive Controls mapped to IAB threat data [1, 2, 14, 15, 33, 34, 35]*

# Detection and Defense

## 9.2 Detective Controls

The 5-day median dwell time creates a critical detection window:

- Behavioral Analytics (UBA/UEBA): Detect IAB activity that appears legitimate but deviates from normal pattern such as users accessing unfamiliar systems, logins from unusual locations, reconnaissance commands (net group, nltest), LSASS memory access, activity during unusual hours.
- Network Monitoring: Focus on east-west traffic (IAB lateral movement occurs internally). Alert on segmentation violations: production servers contacting backup networks, web servers accessing domain controllers.
- Threat Intelligence: Integrate IOC feeds into SIEM/EDR. Build TTP-based detection rules for documented IAB patterns (GoldMelody's staging directory, common reconnaissance commands). Monitor reporting on specific IAB operators targeting your sector.
- Dark Web Monitoring: Commercial services monitor IAB marketplaces for mentions matching your organization's characteristics. Early warnings can enable response within the 5-day window.

## 9.3 Response Capabilities

Rapid response during the 5-day window can prevent catastrophic outcomes. Organizations need:

- IAB-specific playbooks with pre-authorized disruptive actions (credential reset, account disablement, network isolation)
- Established incident response retainer relationships
- Comprehensive logging (Windows Security Events, PowerShell logging, 90+ day retention)
- Regular tabletop exercises simulating IAB scenarios including VPN compromise detection, reconnaissance alerts, and dark web listing notifications

## 9.4 CIS Critical Security Controls Alignment

| CIS Control | Description | IAB Defense Relevance |
|---|---|---|
| 5 | Account Management | Directly counters credential abuse (56% of incidents). MFA, privileged account management. |
| 6 | Access Control | Least privilege limits value of initial access. 71.4% of sales include elevated privileges. |
| 7 | Vulnerability Management | 32% of attacks exploit vulnerabilities. Aggressive patching prevents mass exploitation. |
| 8 | Audit Log Management | Critical for detecting reconnaissance during the 5-day dwell time window. |
| 10 | Malware Defenses | EDR deployment is critical. IABs note "Defender only" as a weakness. |
| 12 | Network Infrastructure | Segmentation limits lateral movement. VPN/RDP hardening prevents 40% of initial access. |
| 17 | Incident Response | Rapid response in 5-day window. IAB-specific playbooks and exercises. |

*Table 9.4: CIS Critical Security Controls alignment with IAB threat data [28]; threat statistics from [2, 14, 15, 33, 34, 35]*

# Impact and Trends

[Staff] Anna Lies

Researcher

ASTRO

Posts: 5
Threads: 1
Reputation: 88

## 10.1 Quantified Impact

| Metric | 2025 Data | Context |
|---|---|---|
| IR Cases with IAB Connection | 44% | Nearly half of ransomware incidents trace to IAB access |
| Total Ransomware Attacks | 7,200 | +47% from 4,900 in 2024 |
| Avg Weekly Attack Volume | 1,968 | +18% YoY, +70% from 2023 |
| Median Dwell Time | 5 days | Down from 9–11 days in 2023 |
| New Ransomware Groups | 57% | Plus 27 extortion-only groups, 350+ strains |
| Average Ransom Demand | $5.2M | +41% from 2024 |
| Organizations Paying Ransom | 56% | Majority pay despite guidance against it |

*Table 10.1: Quantified Impact of IAB-Enabled Ransomware, 2025 [1, 8, 19]*

## 10.2 Estimated Financial Losses

| Loss Category | 2025 Estimate | Source |
|---|---|---|
| Global Ransomware Damage Costs | $57 billion | Cybersecurity Ventures, April 2025. Projected to reach $265B by 2031. |
| IAB Market Value (Direct Sales) | $6.3 million | CYJAX. Minimum estimate, public listings only. |
| Avg Cost per Ransomware Incident | $4.91 million | Sophos; IBM ($5.08M global avg). |
| Avg US Healthcare Breach Cost | $10.22M/incident | IBM Cost of a Data Breach Report 2025. |
| Healthcare Downtime Cost | $1.9M per day | Comparitech (per-incident avg); $21.9B cumulative over 6 years. |
| ROI Multiplier (IAB → Damage) | ~2,200x | Derived: $2K avg access → $4.9M avg incident cost. |

*Table 10.2: Estimated Financial Losses from IAB-Enabled Ransomware, 2025 [5, 14, 17, 25, 26]*

## Impact and Trends

### 10.3 Emerging Threats

Several trends will shape IAB operations through 2026:

- AI and machine learning are being adopted for automated target selection, credential validation at scale, and personalized phishing. [9,13]
- IABs increasingly recognize supply chain value by compromising managed service providers and SaaS platforms to enable "one-to-many" access sales. Cloud infrastructure targeting (misconfigured S3 buckets, exposed Kubernetes APIs, identity federation abuse) continues to expand. [1]
- The line between financially motivated IAB activity and nation-state operations continues to blur. Intelligence assessments predict 2026 will see the first year where non-Russian ransomware actors outnumber Russian ones, reflecting geographic diversification. [1]
- Some state actors appear to use IAB channels for both monetization and intelligence collection, with IAB access to critical infrastructure creating strategic vulnerabilities beyond economic harm. [2,13]

# Law Enforcement and Policy

[Staff] Dr. Detector

Researcher

ASTRO

Posts: 5
Threads: 1
Reputation: 88

## 11.1 Recent Disruptions

BreachForums Timeline:

| Date | Event |
|---|---|
| March 2023 | FBI seizes BreachForums, arrests administrator Pompompurin (Conor Fitzpatrick). |
| April 2023 | New administrator relaunches under different domains. Operations resume within weeks. |
| April 2025 | Second FBI takedown. Servers seized, complete message history and user database obtained. |
| June 2025 | French authorities arrest five administrators including IntelBroker (Kai West) and ShinyHunters members. |
| July 2025 | BreachForums returns under new administration and new infrastructure. |
| October 2025 | Breach forums was again seized on October 10th 2025, BreachForums returns again under new infrastructure. |

These actions demonstrate improving law enforcement capabilities, particularly in cryptocurrency tracing and international coordination. However, ecosystem resilience limits lasting impact: BreachForums returned after each takedown, IAB activity normalized within weeks of high-profile arrests, and the decentralized nature of the market means other operators quickly fill vacuums. [20,22,31]

## 11.2 Policy Recommendations

| # | Recommendation | Expected Impact |
|---|---|---|
| 1 | Mandate MFA for critical infrastructure | Directly addresses 56% of incidents. Highest ROI defensive measure. Enforce through sector regulators (HHS, FERC, banking). |
| 2 | Expand CISA AIS to private sector | Real-time bidirectional threat intelligence enables proactive defense across sectors. |
| 3 | Mandatory IAB incident reporting (72 hrs) | Early warning enables victim notification before ransomware deployment (5-day window). |
| 4 | Strengthen cryptocurrency KYC enforcement | Reduces IAB monetization capability, improves attribution through financial trails. |
| 5 | Increase J-CAT funding and participation | Operational coordination is faster than formal diplomatic channels. Critical for time-sensitive operations. |

*Table 11.2: Policy Recommendations, 2025 [30]*

# Law Enforcement and Policy

[Staff] Sherlog Holmes

Researcher

ASTRO

Posts: 5
Threads: 1
Reputation: 88

## 12.1 The IAB Threat in Context

Initial Access Brokers have evolved from niche service providers into a key foundational piece of infrastructure for the ransomware economy. The core metrics are clear: 44% of incident response cases involve IAB-provided access [2], a $6.3 million direct market enables $57 billion in downstream damage [5,14], and a median 5-day window from compromise to ransomware deployment [4,17] defines a threat that is both economically rational for attackers and operationally devastating for victims.

Three characteristics make this threat persistent. First, professionalized bundled offerings mean ransomware operators receive attack blueprints rather than raw access. Second, the ecosystem demonstrates structural resilience from marketplace takedowns as individual arrests create only temporary disruption. Third, the shift to credential-based access renders perimeter-focused security insufficient against adversaries who authenticate as legitimate users.

The cold open of this paper, ToyMaker's three weeks of silence, is not an anomaly. It is the model. The three-week gap was a detection window that went unused. The signals were there. Organizations that build detection capabilities around the IAB operational pattern give themselves multiple opportunities to break the chain before ransomware ever becomes relevant.

## 12.2 Five Critical Actions

| # | Action | Threat Addressed | Timeline |
|---|---|---|---|
| 1 | Universal MFA | 56% of incidents exploited valid accounts without MFA | Immediate: deploy within 30 days |
| 2 | VPN/RDP Hardening | 40% of IAB sales (23.5% VPN + 16.7% RDP) | Immediate: remove internet-facing RDP, conditional access on VPN |
| 3 | 72-Hour Patching | 32% of attacks exploit vulnerabilities | Short-term: establish 24–72 hour patch window for critical CVEs |
| 4 | Commercial EDR | IABs note "Defender only" as weakness | Short-term: deploy within 60–90 days, prioritize critical servers |
| 5 | Network Segmentation | Limits lateral movement after compromise | Medium-term: air-gap backups immediately, full segmentation 6–12 months |

*Table 12.2: Five Critical Actions; threat statistics from [2, 14, 15, 33, 34, 35]*

## Law Enforcement and Policy

### 12.3 Call to Action

For Organizations: The attack vectors are well understood, and defenses are mature, but the gap is implementation. Every day without universal MFA leaves the dominant attack vector unaddressed. Frame IAB defense in terms of financial materiality: prevention costs a fraction of the average $4.9 million incident.

For Industry: Active participation in sector ISACs, contribution of IOCs, and consumption of shared intelligence should be standard practice. Support legislation requiring mandatory IAB incident reporting within 72 hours and MFA mandates in critical infrastructure sectors.

For Policymakers: Mandate phishing-resistant MFA for critical infrastructure, expand CISA's Automated Indicator Sharing program, establish legal safe harbor for good-faith breach information sharing, and strengthen cryptocurrency exchange KYC requirements.

Initial Access Brokers represent the fulcrum point in modern cyber threats, the critical juncture where defensive efforts yield maximum value. The analysis is clear, the defenses are proven, and the cost of delay far exceeds the cost of action.

## References

*[1] Recorded Future, Insikt Group, New Ransomware Tactics to Watch Out For in 2026, 2026.*
*[2] C. Hegde et al., 2025 Access Brokers Report, Rapid7 Labs, Aug. 12, 2025.*
*[3] J. Leyden, "Cybercriminals Exploit Low-Cost Initial Access Broker Market," Infosecurity Magazine, Oct. 16, 2025.*
*[4] Cyber Risk Leaders, "Rapid7 Q1 2025 Incident Response Findings," Jun. 9, 2025; Sophos, State of Ransomware 2025.*
*[5] S. Morgan, Global Ransomware Damage Costs Predicted to Exceed $275 Billion by 2031, Cybersecurity Ventures, Apr. 2025.*
*[6] Check Point Research, Initial Access Brokers Involved in More Attacks, Including on Critical Infrastructure, Dec. 8, 2025.*
*[7] VikingCloud, 46 Ransomware Statistics and Trends Report 2026.*
*[8] Cyble Research and Intelligence Labs, 10 New Ransomware Groups of 2025 & Threat Trends for 2026, Jan. 1, 2026.*
*[9] Check Point Research, Cyber Security Trends for 2026, Check Point Software Technologies, 2026.*
*[10] See [1]. Recorded Future, Insikt Group, New Ransomware Tactics to Watch Out For in 2026, Recorded Future Blog, 2026.*
*[11] — Globe Newswire, "Rapid7 Access Brokers Report: New Research Reveals Depth of Compromise," Aug. 12, 2025.*
*[12] Palo Alto Networks Unit 42, GoldMelody's Hidden Chords: Initial Access Broker In-Memory IIS Modules Revealed, Jul. 8, 2025.*
*[13] D. Lohrmann, "The Top 26 Security Predictions for 2026 (Part 2)," GovTech, Dec. 28, 2025.*
*[14] CYJAX, Initial Access Broker Market 2024 In Review, Feb. 6, 2025.*
*[15] Cyberint (Check Point), Initial Access Brokers Report 2025, Apr. 2025.*
*[16] R. Lakshmanan, "Initial Access Brokers Shift Tactics, Selling More for Less," The Hacker News, Apr. 11, 2025.*
*[17] Sophos, State of Ransomware 2025.*
*[18] LoginSoft, Initial Access Brokers: The Hidden Architects of Modern Cyberattacks, LoginSoft Blog, Jun. 9, 2025.*
*[19] DeepStrike, Ransomware Attack Statistics 2025, DeepStrike Threat Intelligence, 2025.*
*[20] U.S. Department of Justice, SDNY, Serial Hacker 'IntelBroker' Charged For Causing $25 Million In Damages, Jun. 25, 2025.*
*[21] Chainalysis, The IntelBroker Takedown: Following the Bitcoin Trail, Jul. 22, 2025.*
*[22] E. Kovacs, "British Man Suspected of Being the Hacker IntelBroker Arrested, Charged," SecurityWeek, Jun. 26, 2025.*
*[23] Picus Security, IntelBroker Unmasked — The Story of Hacker Kai Logan West, Jan. 20, 2026.*
*[24] Cato Networks, Threat Actor Profile: IntelBroker, Jul. 16, 2025.*
*[25] IBM Security, Cost of a Data Breach Report 2025.*
*[26] Comparitech / Healthcare IT News, Ransomware Downtime Costs U.S. Healthcare Organizations $1.9M Daily, 2025.*
*[27] Trellix, Advanced Research Center, 2025 Healthcare Cybersecurity Threat Intelligence Report.*
*[28] Center for Internet Security, CIS Critical Security Controls v8, 2021 (updated 2024).*
*[29] Europol, Internet Organised Crime Threat Assessment (IOCTA) 2024–2025, 2025.*
*[30] Cybersecurity and Infrastructure Security Agency, Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), CISA, 2022.*
*[31] Federal Bureau of Investigation, BreachForums Seized, Mar. 2023 and Apr. 2025.*
*[32] Barefoot Cyber, Cybersecurity Weekly Update: 26 January–2 February 2026.*
*[33] J. Shier, H. Wood, and A. Gunn, "Nowhere, Man: The 2026 Active Adversary Report," Sophos, 2026.*
*[34] CrowdStrike, "2025 Global Threat Report," February 2025.*
*[35] Mandiant/Google Cloud, "M-Trends 2025: Data, Insights, and Recommendations From the Frontlines," April 2025.*
*[36] J. Chen et al., "Introducing ToyMaker, an Initial Access Broker Working in Cahoots with Double Extortion Gangs," Cisco Talos Intelligence, April 23, 2025.*

# About Abstract

[Staff] Abby Stract


Researcher

ASTRO

Posts: 5
Threads: 1
Reputation: 88

Abstract modernizes security operations through a composable SIEM platform that is modular by design, AI by default. Where traditional SIEMs force organizations into monolithic architectures and runaway log costs, Abstract decouples ingestion from analytics, embeds threat intelligence inline, and gives detection engineering teams the control and coverage they actually need. Organizations adopt what they need—data pipelines, streaming detections, or the full platform—and scale at their own pace.

ASTRO, the Abstract Security Threat Research Organization, is Abstract's dedicated threat research function. ASTRO publishes original research across the threat landscape from threat actor campaign tracking and CVE analysis to emerging attack techniques in cloud and hybrid environments. Recent work includes research into North Korea's Contagious Interview campaign targeting developers through IDE infection chains, critical vulnerability analysis of Cisco Secure Firewall Management Center, and lateral movement techniques abusing managed identities in cloud infrastructure.

ASTRO also powers Abstract's proprietary threat intelligence feed, with active tracking of over 60 C2 frameworks and botnets including the IAB infrastructure documented in this report.

See more ASTRO research at abstract.security