2024-2025
INITIAL ACCESS REPORT

ThreatMon
Under Cyber Wings

What Are Initial Access Brokers (IABs)?

The term Initial Access Broker (IAB) refers to threat actors in the cyber threat landscape who gain unauthorized access to systems and then sell that access to third parties for profit. These actors typically compromise valid credentials or system access to corporate networks, Remote Desktop Protocol (RDP) connections, VPNs, cloud management panels, or email servers.IABs do not directly deploy ransomware or exfiltrate data themselves. Instead, they act as a key link in the cybercrime supply chain by marketing the access they acquire. The access they provide is often used by ransomware groups, Advanced Persistent Threats (APTs), or fraud-oriented actors for second-stage attacks. These attacks may include data exfiltration, ransomware deployment, financial fraud, or corporate espionage.

IAB operations are primarily conducted through dark web forums, Telegram channels, onion-based marketplaces, and closed groups. The pricing of access listings varies depending on the size of the target organization, its industry, infrastructure, and other metrics that influence the potential financial gain.In this context, to better understand the industrial scale of Initial Access Broker (IAB) operations and the commercial structures of threat actors, ThreatMon conducted a comprehensive Open-Source Intelligence (OSINT) investigation covering the period from early 2024 to mid-2025.

Based on data collected from various sources such as darknet forums, Telegram channels, and onion-based marketplaces, the research strikingly reveals the scale and level of organization behind unauthorized access sales. The findings demonstrate that threats have significantly expanded across a wide range of sectors—from government agencies to education, finance, e-commerce, and telecommunications.Since early 2024 through to mid-2025, ThreatMon has conducted a comprehensive open-source intelligence (OSINT) investigation into the underground trade of initial access to compromised digital systems. Drawing from a wide range of sources including darknet forums, Telegram channels, and onion-based marketplaces, our research reveals the alarming scale and industrialization of unauthorized access sales. The findings offer critical insights into the rapidly evolving threat landscape that now affects nearly every sector — from government administration and education to financial institutions, e-commerce, and telecommunications.

Our data indicates that the United States remains the most heavily targeted nation, accounting for over 55% of all recorded incidents in 2025, a significant increase from 2024 levels. Meanwhile, emerging economies such as India, Indonesia, and Vietnam continue to experience high levels of exploitation, largely due to weaker cybersecurity posture, legacy infrastructure, and unpatched public-facing services. Europe — particularly France and the UK — also experienced a notable increase in listings involving financial portals, education systems, and telecom firms.

From an industry standpoint, government institutions (23.96%) and e-commerce platforms (17.57%) were the most impacted, followed closely by financial services and educational institutions. The increasing convergence between targeted ransomware operations and initial access trading suggests that access brokers now function as upstream suppliers for broader cybercriminal supply chains. Unauthorized access sold in underground forums often serves as the entry point for subsequent attacks such as data exfiltration, ransomware deployment, or financial fraud.

This report aims to provide cyber defenders, policy-makers, security researchers, and digital business leaders with actionable intelligence on the current state of initial access markets. Through quantitative breakdowns, threat actor profiling, platform correlations, and regional incident mapping, we offer a holistic overview of the underground access trade economy and its growing threat to global digital stability.

Critical Statistics – Initial Access (2024–2025)

- Over 6,000 initial access listings were documented across dark web forums and Telegram channels during the analysis period.
- The United States was the most targeted country, accounting for 55–56% of incidents in both 2024 and 2025.
- A total of 156 countries were affected by unauthorized access sales, with India, Indonesia, France, and China following the U.S. in volume.
- Initial Access Brokers (IABs) demonstrated up to 92% success rates in obtaining admin-level access through CMS and RDWeb vulnerabilities.
- Government Administration (24%) and E-Commerce platforms (17.6%) were the most impacted sectors, followed by Financial Services and Education.
- The most active threat actors were *miyako*, *ProfessorKliq*, *diamond*, and *sentap*, dominating the underground access economy.
- Forums such as breachforums.st and exploit.in hosted over 70% of all known access listings, serving as the primary hubs for cybercriminal activity.
- Listings often included full server control: RDWeb, VPN, shell, CMS admin, cPanel, and even database access, with prices ranging from $2 to $500.
- May and June 2025 recorded the highest spike in initial access offers and breach claims, indicating intensified underground market activity.
- The majority of affected organizations came from sectors with poor patch management and minimal access control, enabling privilege escalation and resale.

Glossary of Technical Terms

Initial Access – The first unauthorized entry point into a network, system, or device, usually sold to third parties.

RDP (Remote Desktop Protocol) – A Microsoft protocol that allows users to connect to and control remote computers. Often abused in unauthorized access sales.

VPN (Virtual Private Network) – Encrypted tunnel between a user and a network. Frequently exploited to bypass internal firewalls.

Webshell – A malicious script uploaded to a compromised server that provides remote command-line access.

Admin Access – Privileged-level system or CMS access allowing full control over the platform, often sold on dark web.

CMS (Content Management System) – Software like WordPress or Magento used to manage web content; often exploited via outdated plugins.

Forum Marketplace – Online platform (often on dark web) where threat actors trade stolen data, access credentials, and exploits.

Threat Actor – An individual or group conducting cyberattacks, including hackers, brokers, ransomware groups.

Dark Web – Encrypted part of the internet, accessible via Tor, where illegal cyber activity frequently occurs.

RDWeb – A web-based gateway interface for Microsoft RDP sessions, increasingly targeted for initial access.

Shell Access – Terminal or command-line-level control of a server, typically achieved via webshell or SSH backdoor.

SSH (Secure Shell) – Encrypted protocol used to securely access servers; occasionally exploited when misconfigured.

Actor Alias – Pseudonym used by threat actors on forums (e.g., *miyako*, *ProfessorKliq*), often associated with specific TTPs.

Onion Service – Websites hosted on the Tor network, typically with .onion domains, used for anonymized communications and trade.

Access Broker – A cybercriminal who specializes in gaining and reselling initial access to compromised systems.

Threat Landscape Overview

Between January 2024 and July 2025, the landscape of Initial Access Brokerage (IAB) has undergone a significant transformation, evolving from sporadic access sales into a deeply structured and demand-driven underground economy. Leveraging detailed telemetry from breach forums, deepweb marketplaces, and Telegram groups, our analysis underscores how threat actors have institutionalized the trade of unauthorized access, offering entry points into high-value digital infrastructures across 156 countries. These access points range from VPN and RDWeb credentials to full administrative rights on government, financial, and IT systems, with a growing emphasis on bundled privileges such as control over firewalls, email servers, and domain panels.

Threat actors such as **ProfessorKliq**, **diamond**, and various aliases of **miyako** dominate the scene, not only by the volume of listings but also by the strategic sectors they target — including **government administration**, **e-commerce**, **education**, and **network services**. In 2025 alone, over 56% of all identified access breaches were traced back to U.S.-based systems, while Southeast Asian and European entities saw a sharp rise in breaches, particularly in countries like **Indonesia**, **India**, **France**, and **China**. The methods of compromise have also diversified: alongside credential theft and misconfigured services, attackers increasingly leverage zero-day exploitation, social engineering, and remote access mismanagement to infiltrate networks.

What distinguishes today's IAB environment is the level of segmentation and specialization within the ecosystem. Access brokers operate more like wholesalers acquiring access through low-cost automation and malware campaigns, and reselling it to ransomware groups, data extortion crews, or cyber-mercenaries. Listings across platforms like **breachforums.st** and **exploit.in** are now accompanied by revenue estimates, organizational profiles, and even system topologies — evidence of a maturing marketplace where buyers seek precision, persistence, and profit. This commodification of access not only lowers the barrier for complex cyberattacks but also blurs the lines between financially motivated crime and state-level operations, posing a multidimensional threat to global cybersecurity resilience.

Attack Vector Dynamics in the Initial Access Market

The mechanisms through which initial access brokers penetrate and monetize enterprise systems have become more intricate and multi-layered between late 2024 and mid-2025. Rather than relying solely on brute-force or credential stuffing tactics, threat actors now exploit a blend of structural weaknesses, misconfigured services, and overlooked access points across digital infrastructures. Remote Desktop Protocol (RDP) and RDWeb services have emerged as key targets — frequently listed for sale with active domain user privileges. In numerous cases, brokers leverage exposed ports or weak authentication protocols to obtain these footholds, which are then resold on forums such as exploit.in or xss.is with precise operational details like system type, user level, and organizational revenue estimates.

Beyond remote desktop services, VPN credential abuse has sharply increased, especially in high-security sectors such as government, finance, and aerospace.
Our data reveals that threat actors like miyak000 and ProfessorKliq have routinely offered VPN access to sensitive entities, including defense contractors and government healthcare networks. In other listings, full control over backend infrastructures — including admin panels, firewall gateways, and email servers — is offered, indicating post-exploitation privilege escalation and lateral movement.
These high-privilege access points are typically obtained via social engineering, infostealer logs, or through piggybacking on legacy software modules within networks.

Critical vulnerabilities in exposed web assets also remain a prominent attack vector. Misconfigured SSH services, outdated CMS installations, and unpatched backend dashboards are commonly exploited to gain persistent access. In particular, Shell access sales — as observed on platforms like breachforums.st — indicate that attackers frequently install web shells or reverse proxies to maintain long-term control over compromised hosts. Once embedded, these footholds enable secondary exploitation: data harvesting, ransomware deployment, or credential pivoting into connected systems. The breadth of access observed across sectors — from educational portals in Taiwan to financial dashboards in France — demonstrates that initial access vectors are no longer limited to traditional endpoints, but now span the full attack surface of modern digital enterprises.

Statistical Breakdown and Operational Insights on Initial Access

Based on the aggregation of 2359 unique incidents logged between 2024 and mid-2025, our statistical analysis of the Initial Access Brokerage (IAB) ecosystem reveals an expansive and intensifying threat matrix.

The United States stands out as the most frequently targeted geography, with over 56% of all cases in 2025 involving U.S.-based institutions — a marked increase from 43% in 2024. Countries like India (18.15%), Indonesia (18.80%), and France (14.16%) also feature prominently, with localized breaches often involving financial portals, public education systems, and government platforms.

This geographic clustering indicates a deliberate actor focus on nations with either high-value data ecosystems or structural cybersecurity gaps.

At the sectoral level, the Government Administration (23.96%) and E-commerce & Online Stores (17.57%) industries bear the brunt of activity, though the Financial Services (14.44%) and Education (12.92%) verticals remain persistently targeted.

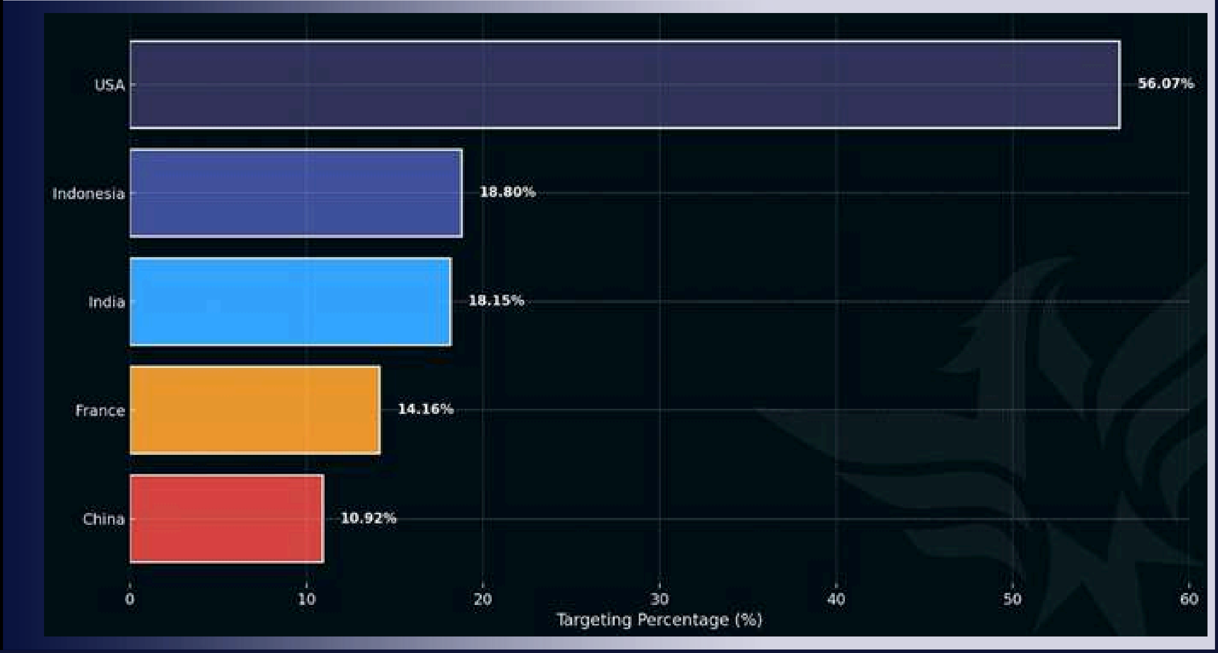
Listings often specify organizational attributes such as annual revenue, employee count, or infrastructure type, suggesting a maturity in adversary reconnaissance and operational intelligence gathering.

Forums like breachforums.st and exploit.in account for over 67% of total listings, reinforcing their status as primary hubs for access trade.

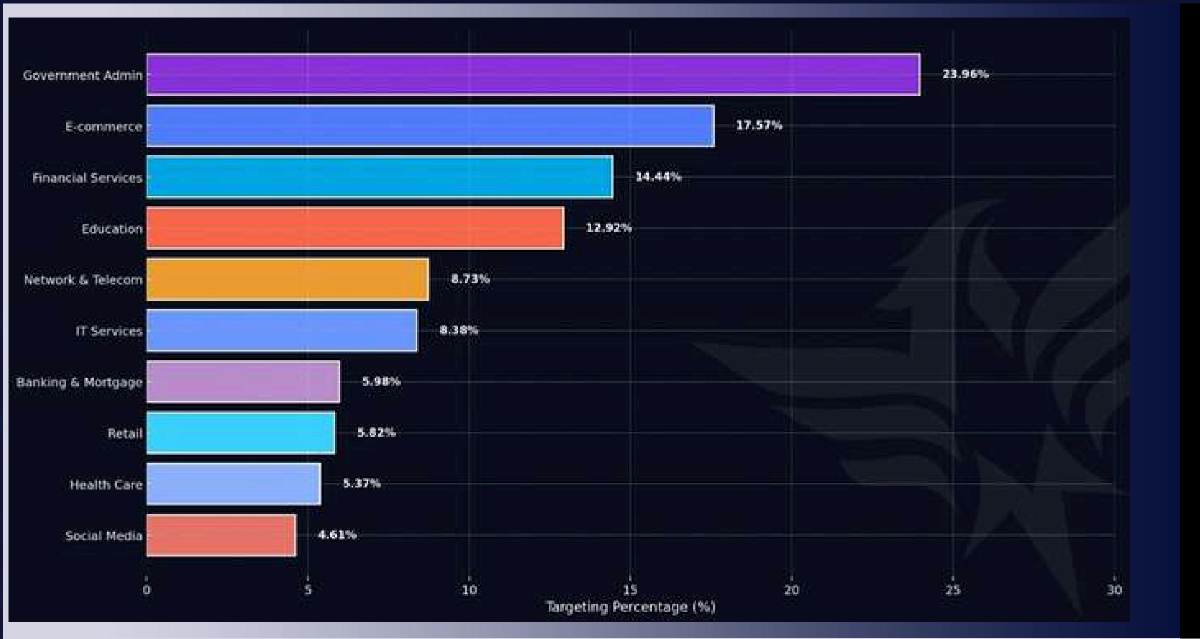
In these environments, actors such as ProfessorKliq, miyak0, and sentap are responsible for the majority of high-impact access sales — collectively involved in nearly 45% of observed incidents in 2025 alone.

Initial Access Landscape: 2025 Key Statistics

The 2025 Initial Access ecosystem reflects a sharp concentration of threat actor activity targeting key global regions and critical industries. The **United States** dominated as the primary target, involved in over **56%** of access listings, followed by **Indonesia (18.80%)**, **India (18.15%)**, and **France (14.16%)**.

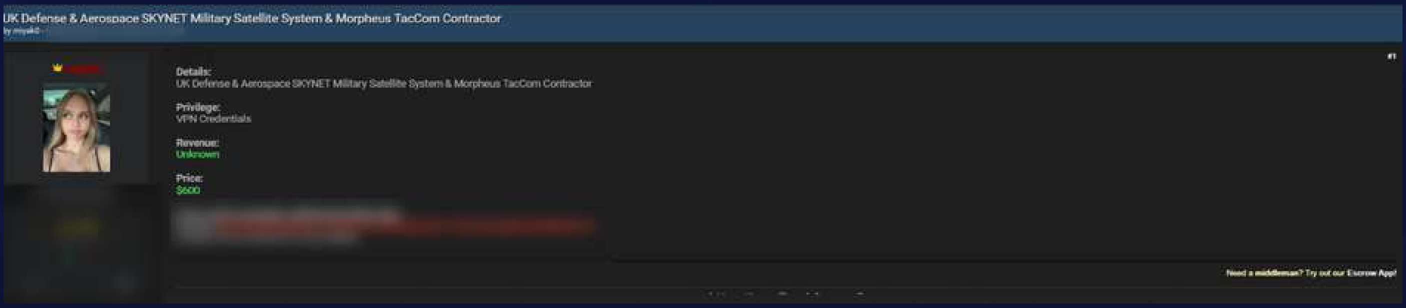


Sector-wise, Government Administration (23.96%) and E-commerce platforms (17.57%) were the most impacted, with substantial exposure also observed across Financial Services (14.44%) and Education (12.92%).



Breachforums.st: Total 192 Incıdent

- **Threat Actors:** miyak0 (53.2%)
- **Countries:** USA (15.11%), India (6.21%), Indonesia (6.15%).
- **Industries:** Government Administration (7.93%), Education (6.49%), Financial Services (4.64%).



UK Defense & Aerospace SKYNET Military Satellite System & Morpheus TacCom Contractor
by miyak0

#1

Details:
UK Defense & Aerospace SKYNET Military Satellite System & Morpheus TacCom Contractor

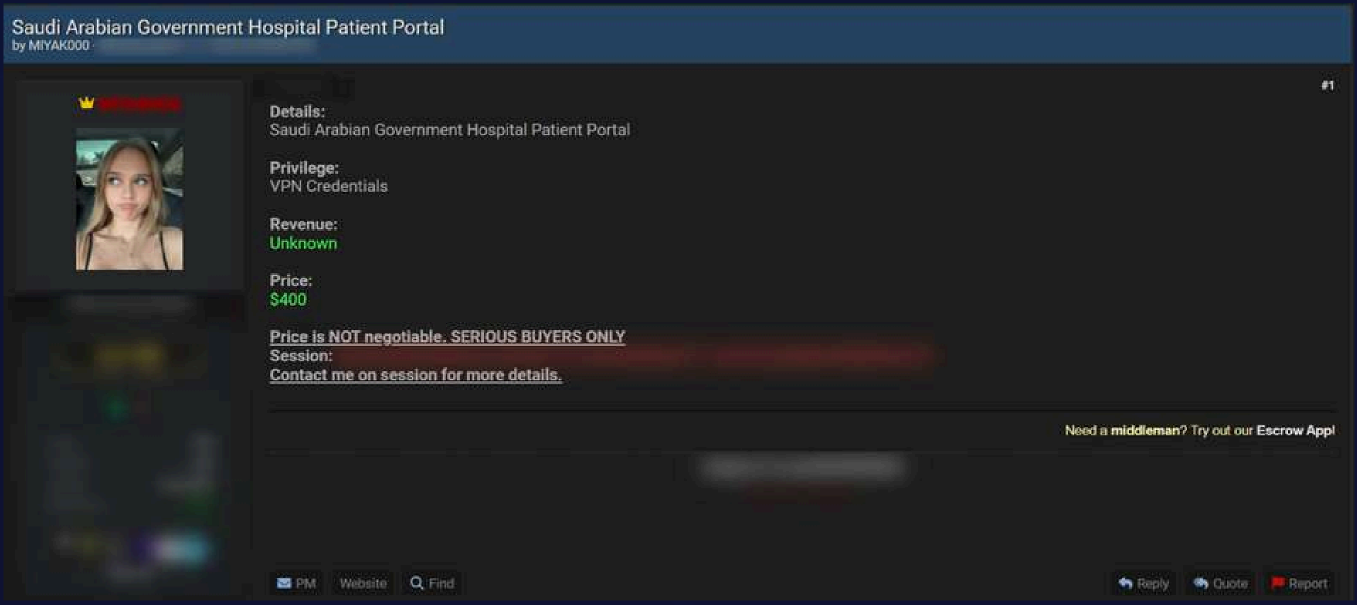
Privilege:
VPN Credentials

Revenue:
Unknown

Price:
$600

Need a middleman? Try out our Escrow App!

The threat actor claims to be selling VPN credentials for the UK Defense & Aerospace SKYNET Military Satellite System and Morpheus TacCom Contractor.



Saudi Arabian Government Hospital Patient Portal
by MIYAK000

#1

Details:
Saudi Arabian Government Hospital Patient Portal

Privilege:
VPN Credentials

Revenue:
Unknown

Price:
$400

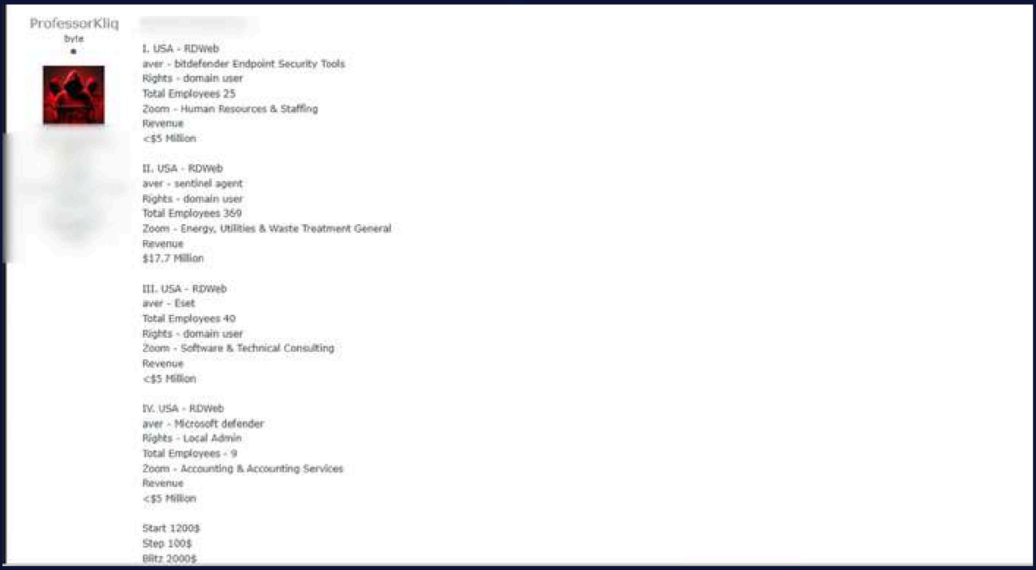
Price is NOT negotiable. SERIOUS BUYERS ONLY
Session:
Contact me on session for more details.

Need a middleman? Try out our Escrow App!

The threat actor claims to be selling access to a Saudi Arabian government hospital's patient portal through VPN credentials

Exploit.in: 174 Total Incident

- **Threat Actors:** ProfessorKliq (35.5%), Reve (26.02%), rassvettt (21.08%).
- **Countries:** USA (29.24%), UK (5.51%), Spain (4.23%).
- **Industries:** E-commerce & Online Stores (37.6%), Financial Services (21.2%), Retail Industry (14.2%).



ProfessorKliq
byte
●

[redacted]

I. USA - RDWeb
aver - bitdefender Endpoint Security Tools
Rights - domain user
Total Employees 25
Zoom - Human Resources & Staffing
Revenue
<$5 Million

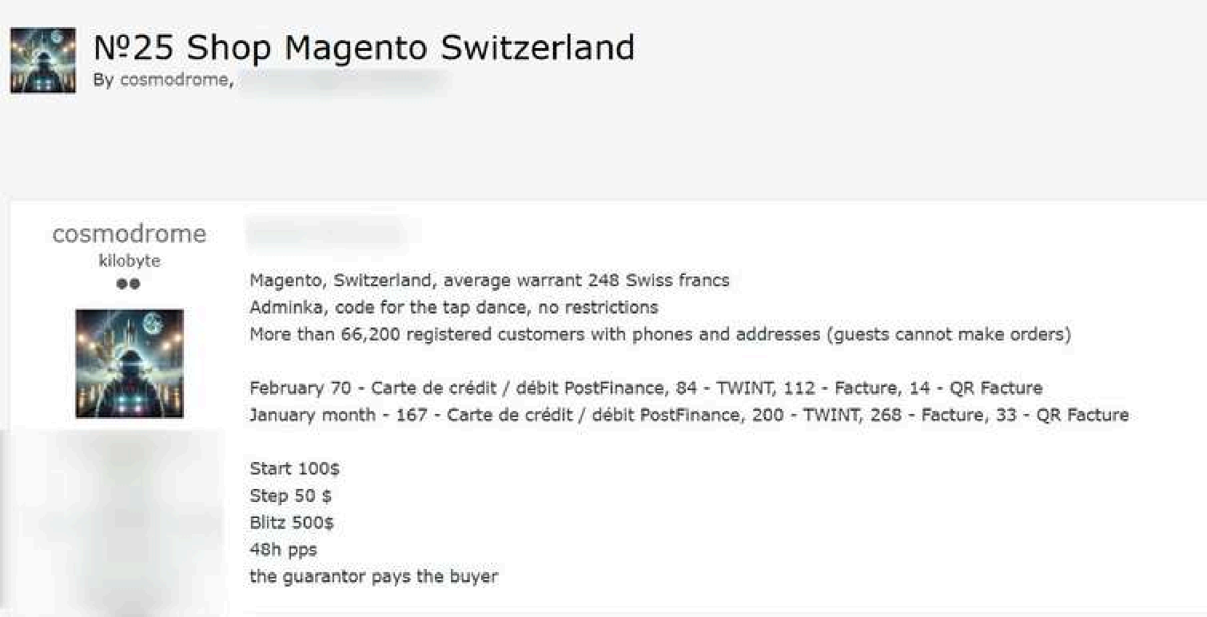
II. USA - RDWeb
aver - sentinel agent
Rights - domain user
Total Employees 369
Zoom - Energy, Utilities & Waste Treatment General
Revenue
$17.7 Million

III. USA - RDWeb
aver - Eset
Total Employees 40
Rights - domain user
Zoom - Software & Technical Consulting
Revenue
<$5 Million

IV. USA - RDWeb
aver - Microsoft defender
Rights - Local Admin
Total Employees - 9
Zoom - Accounting & Accounting Services
Revenue
<$5 Million

Start 1200$
Step 100$
Blitz 2000$

Threat actor claims to be selling unauthorized access to several companies in the USA.



№25 Shop Magento Switzerland
By cosmodrome, [redacted]

cosmodrome
kilobyte
●●

[redacted]

Magento, Switzerland, average warrant 248 Swiss francs
Adminka, code for the tap dance, no restrictions
More than 66,200 registered customers with phones and addresses (guests cannot make orders)

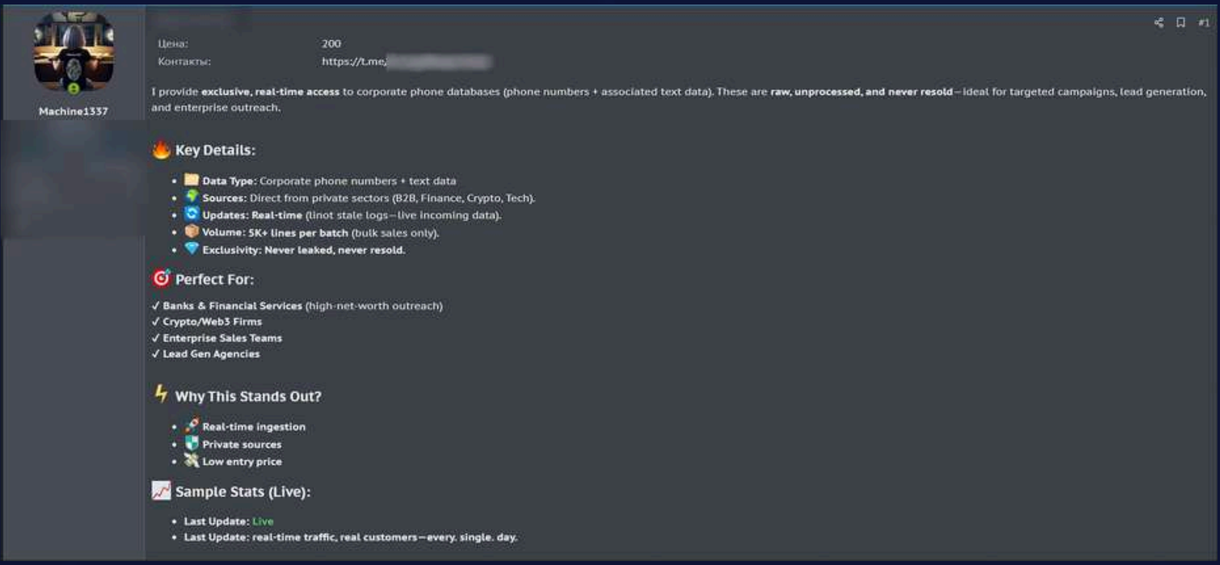
February 70 - Carte de crédit / débit PostFinance, 84 - TWINT, 112 - Facture, 14 - QR Facture
January month - 167 - Carte de crédit / débit PostFinance, 200 - TWINT, 268 - Facture, 33 - QR Facture

Start 100$
Step 50 $
Blitz 500$
48h pps
the guarantor pays the buyer

The threat actor claims to be selling access to Magento Switzerland, which includes more than 66,200 registered customers with phones and addresses.

Xss.is: Total 103 Incıdent

- **Threat Actors:** diamond (28.6%), Machine1337 (12.7%).
- **Countries:** USA (22.44%), Brazil (3.11%), UK (3.11%).
- **Industries:** Financial Services (23.5%), IT Services (12.9%), Government Administration (9.6%).



Machine1337

[redacted]

Цена: 200
Контакты: https://t.me/[redacted]

I provide **exclusive, real-time access** to corporate phone databases (phone numbers + associated text data). These are **raw, unprocessed, and never resold** – ideal for targeted campaigns, lead generation, and enterprise outreach.

🔥 **Key Details:**

- 📁 **Data Type:** Corporate phone numbers + text data
- 🌍 **Sources:** Direct from private sectors (B2B, Finance, Crypto, Tech).
- 🔄 **Updates: Real-time** (Ünot stale logs – live incoming data).
- 📦 **Volume: 5K+ lines per batch** (bulk sales only).
- 💎 **Exclusivity: Never leaked, never resold.**

🎯 **Perfect For:**

✓ **Banks & Financial Services** (high-net-worth outreach)
✓ **Crypto/Web3 Firms**
✓ **Enterprise Sales Teams**
✓ **Lead Gen Agencies**

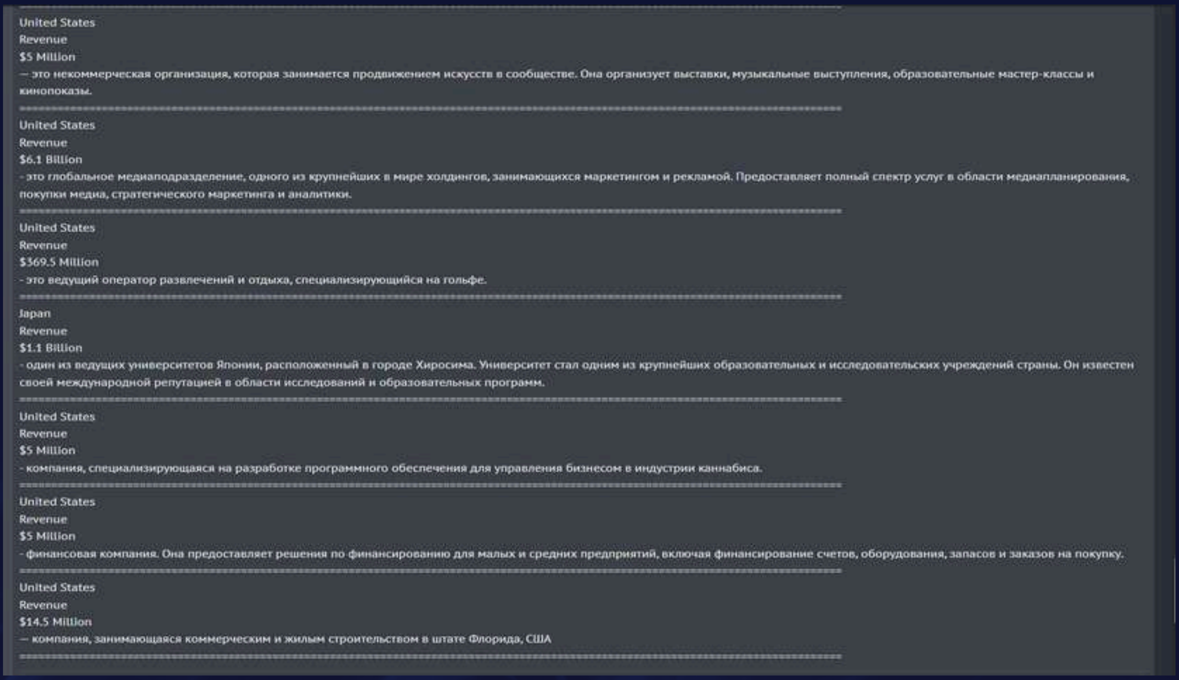
⚡ **Why This Stands Out?**

- 🚀 **Real-time ingestion**
- 🛡 **Private sources**
- 💸 **Low entry price**

📈 **Sample Stats (Live):**

- **Last Update:** Live
- **Last Update: real-time traffic, real customers—every. single. day.**

Machine1337 is offering exclusive, real-time access to raw corporate phone databases (including phone numbers and associated text messages) sourced directly from private sectors.



```
United States
Revenue
$5 Million
— это некоммерческая организация, которая занимается продвижением искусств в сообществе. Она организует выставки, музыкальные выступления, образовательные мастер-классы и кинопоказы.
==========================================================================================
United States
Revenue
$6.1 Billion
- это глобальное медиаподразделение, одного из крупнейших в мире холдингов, занимающихся маркетингом и рекламой. Предоставляет полный спектр услуг в области медиапланирования, покупки медиа, стратегического маркетинга и аналитики.
==========================================================================================
United States
Revenue
$369.5 Million
- это ведущий оператор развлечений и отдыха, специализирующийся на гольфе.
==========================================================================================
Japan
Revenue
$1.1 Billion
- один из ведущих университетов Японии, расположенный в городе Хиросима. Университет стал одним из крупнейших образовательных и исследовательских учреждений страны. Он известен своей международной репутацией в области исследований и образовательных программ.
==========================================================================================
United States
Revenue
$5 Million
- компания, специализирующаяся на разработке программного обеспечения для управления бизнесом в индустрии каннабиса.
==========================================================================================
United States
Revenue
$5 Million
- финансовая компания. Она предоставляет решения по финансированию для малых и средних предприятий, включая финансирование счетов, оборудования, запасов и заказов на покупку.
==========================================================================================
United States
Revenue
$14.5 Million
— компания, занимающаяся коммерческим и жилым строительством в штате Флорида, США
==========================================================================================
```

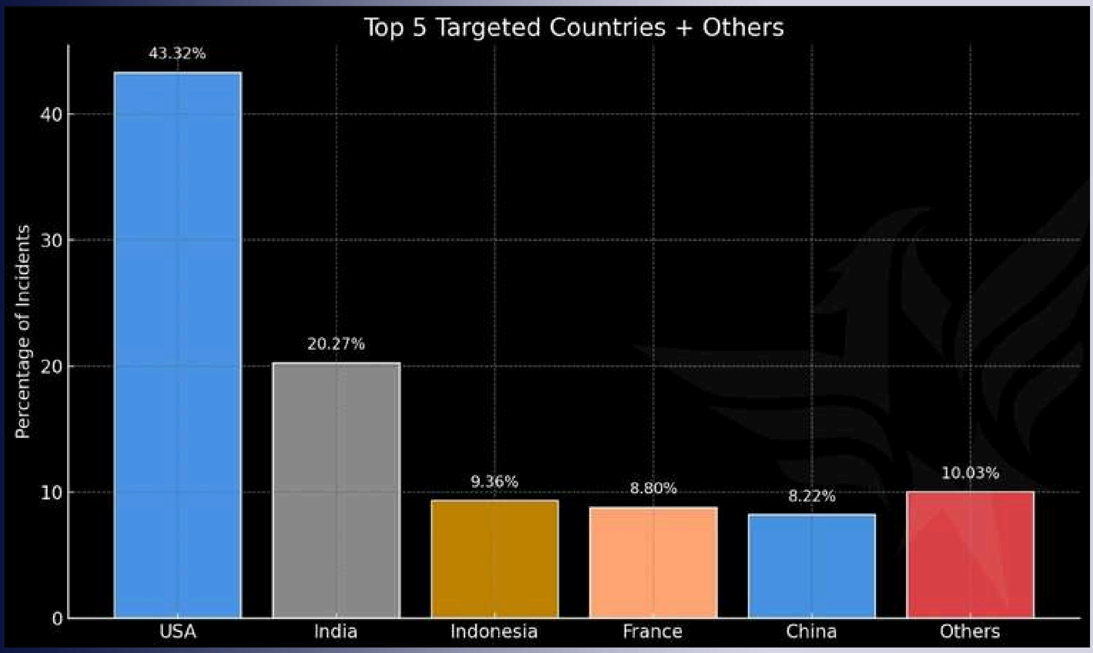
Threat actor "diamond" claims to be selling unauthorized accesses to several companies in Japan and United States

Actor Keyword Correlations:

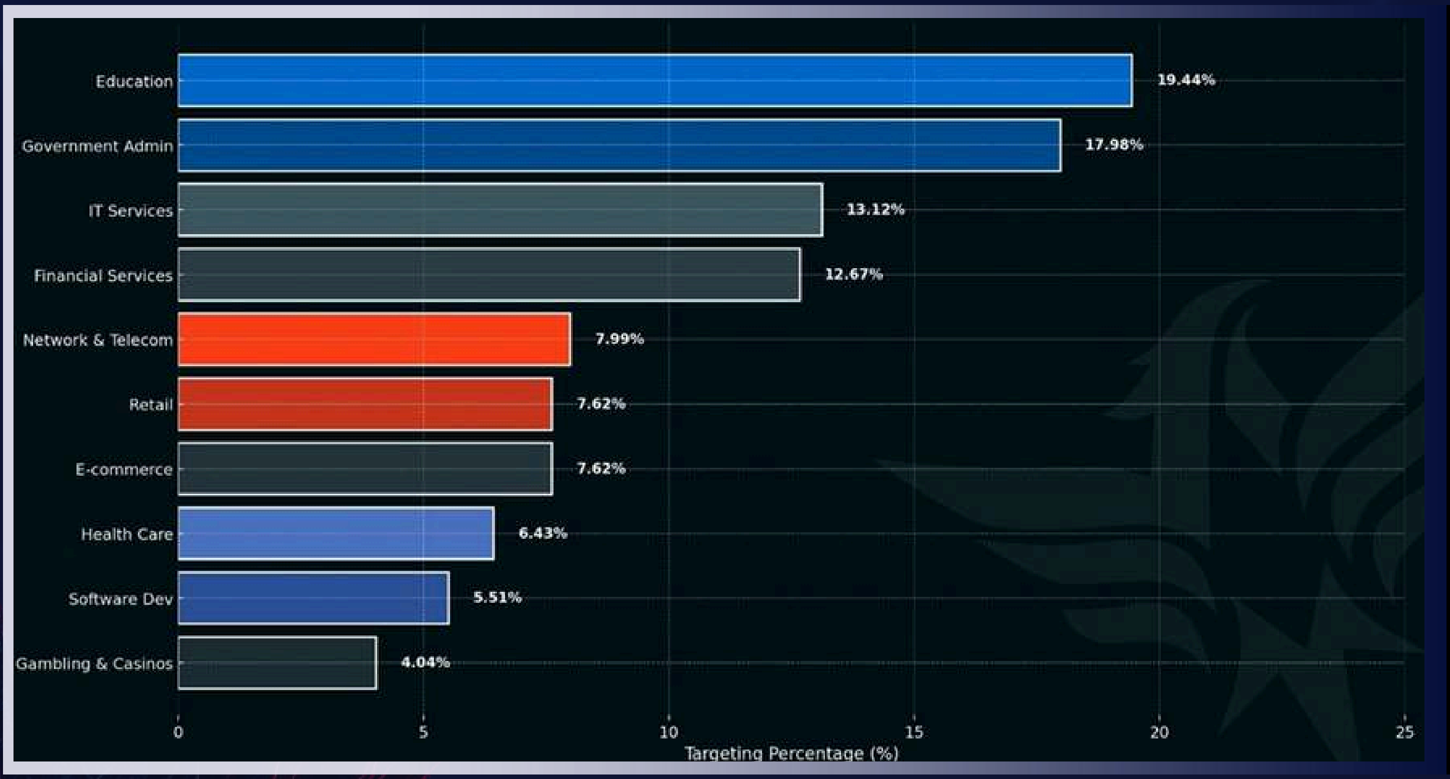
- **ProfessorKliq (219):** exploit.in (41.55%), RDWeb access (24.66%), selling unauthorized (18.26%).
- **diamond (192):** xss.is (33.33%), unauthorized access (33.33%), selling unauthorized (33.33%).
- **Reve (96):** exploit.in (35.42%), admin access (26.04%), selling unauthorized (16.67%).
- **cosmodrome (78):** exploit.in (37.18%), admin access (20.51%), selling unauthorized (17.95%).

Initial Access Landscape: 2024 Key Statistics

In 2024, threat actors continued to favor high-value geopolitical and economic targets, with the United States accounting for the largest share of initial access incidents at 43.32%.
Other heavily targeted nations included India (20.27%), Indonesia (9.36%), France (8.80%), and China (8.22%), highlighting a focus on both developed digital economies and regions with uneven cybersecurity enforcement.

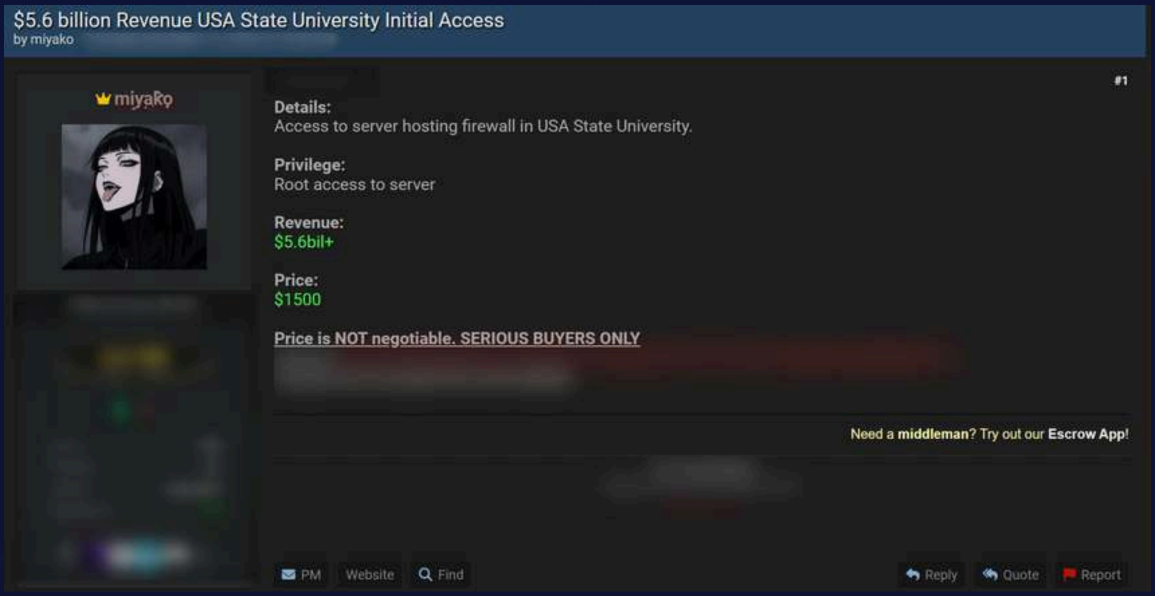


In 2024, threat actors continued to favor high-value geopolitical and economic targets, with the United States accounting for the largest share of initial access incidents at 43.32%. Other heavily targeted nations included India (20.27%), Indonesia (9.36%), France (8.80%), and China (8.22%), highlighting a focus on both developed digital economies and regions with uneven cybersecurity enforcement.



Breachforums.st: Total 223 Incıdent

- **Threat Actors:** miyako (46.7%) dominates.
- **Countries:** USA (18.28%), India (9.63%), Indonesia (5.08%).
- **Industries:** Education (32%), Government Administration (17.2%), IT Services (12.5%).



$5.6 billion Revenue USA State University Initial Access
by miyako

miyako

#1

Details:
Access to server hosting firewall in USA State University.

Privilege:
Root access to server

Revenue:
$5.6bil+

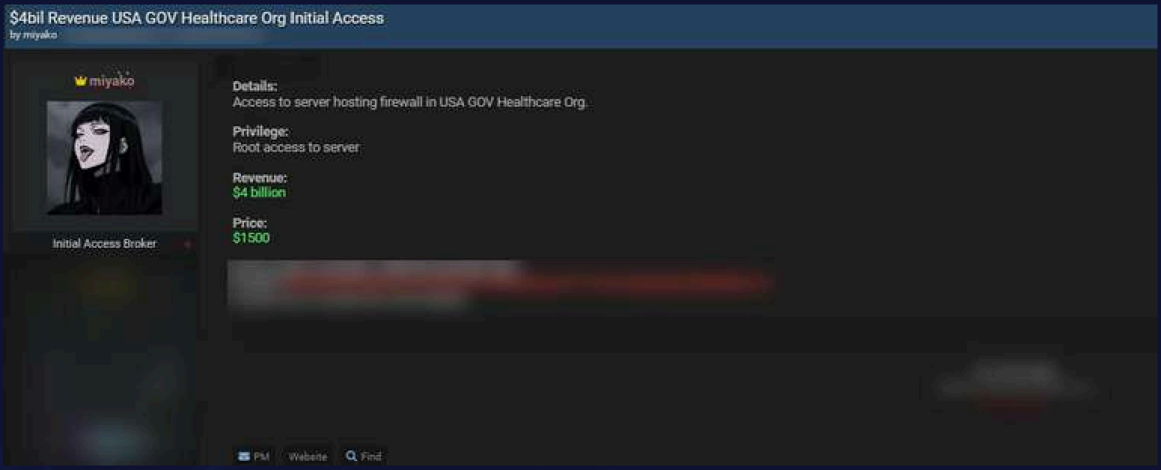
Price:
$1500

Price is NOT negotiable. SERIOUS BUYERS ONLY

[redacted]

Need a **middleman**? Try out our **Escrow App!**

Threat actor claims to be selling root access to the server's firewall of an unidentified State University in the USA.



$4bil Revenue USA GOV Healthcare Org Initial Access
by miyako

miyako

Initial Access Broker

Details:
Access to server hosting firewall in USA GOV Healthcare Org.

Privilege:
Root access to server

Revenue:
$4 billion

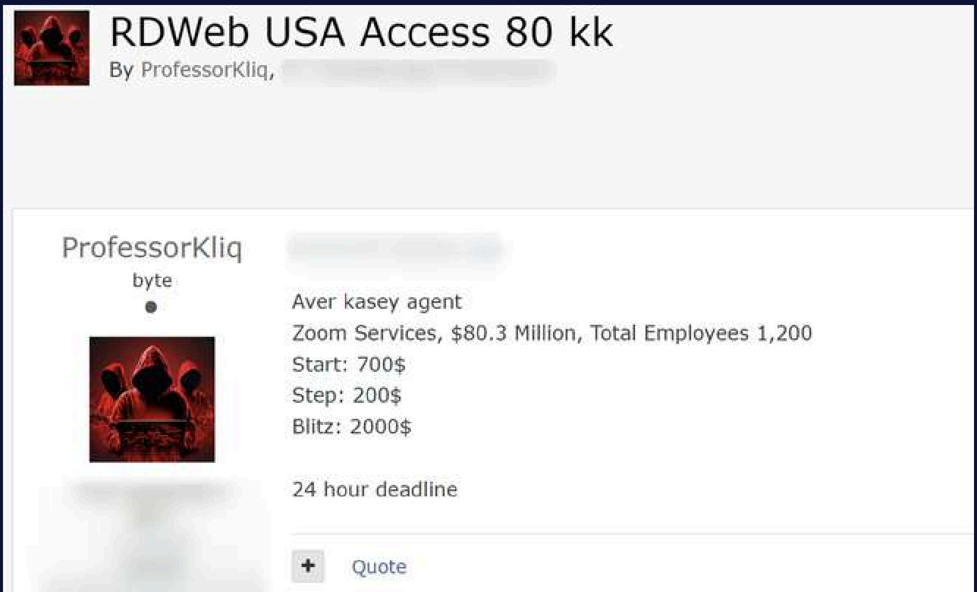
Price:
$1500

[redacted]

Threat actor claims to be selling root access to the firewall server of a government healthcare organization in the USA.

Exploit.in: Total 189 Incıdent

- **Threat Actors:** ProfessorKliq (37.54%), lordcms (19.23%), DNI (7.4%).
- **Countries:** USA (37.50%), UK (7.81%), Canada (6.77%).
- **Industries:** Financial Services (27.2%), Building and Construction (16.7%), Retail Industry (10.2%).



RDWeb USA Access 80 kk

By ProfessorKliq,

ProfessorKliq

byte

Aver kasey agent

Zoom Services, $80.3 Million, Total Employees 1,200

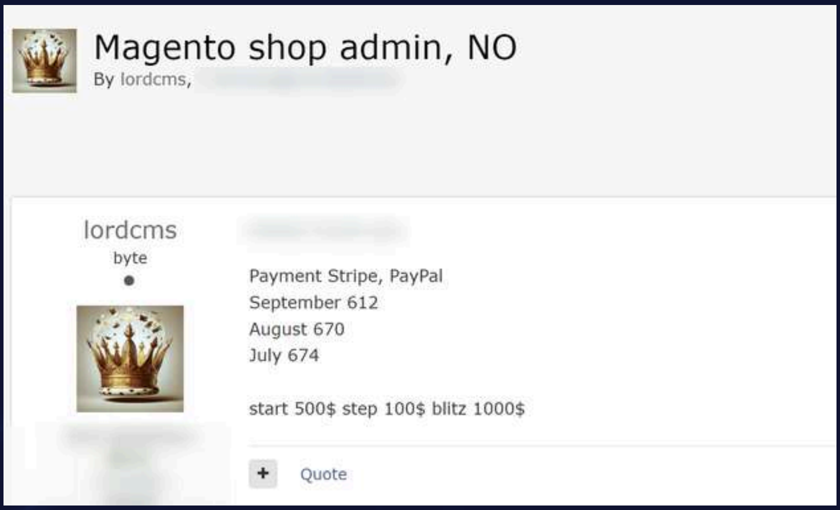
Start: 700$

Step: 200$

Blitz: 2000$

24 hour deadline

The threat actor claims to be selling RDWeb access of unidentified company in USA. The company has an annual turnover of 80.3 million.



Magento shop admin, NO

By lordcms,

lordcms

byte

Payment Stripe, PayPal

September 612

August 670

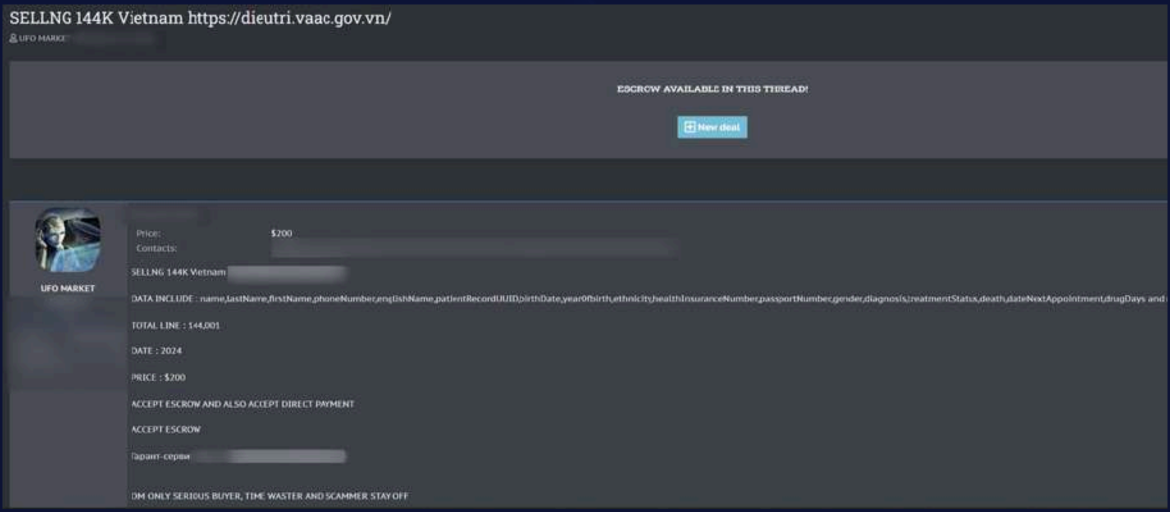
July 674

start 500$ step 100$ blitz 1000$

The threat actor offering to sell Magento admin access sale of an unidentified shop in Norway.

Xss.is: Total 192 Incıdent

- **Threat Actors:** UFO MARKET (32.1%), Mr Robot (17.4%).
- **Countries:** USA (30.30%), UK (8.48%), India (6.67%).
- **Industries:** Education (37.4%), Financial Services (21.2%), Hospital & Health Care (12.3%).



SELLNG 144K Vietnam https://dieutri.vaac.gov.vn/

UFO MARKE [redacted]

ESCROW AVAILABLE IN THIS THREAD!

⊞ New deal

UFO MARKET

Price: $200

Contacts: [redacted]

SELLNG 144K Vietnam [redacted]

DATA INCLUDE : name,lastName,firstName,phoneNumber,englishName,patientRecordUUID,birthDate,yearOfbirth,ethnicity,healthInsuranceNumber,passportNumber,gender,diagnosis,treatmentStatus,death,dateNextAppointment,drugDays and

TOTAL LINE : 144,001

DATE : 2024

PRICE : $200

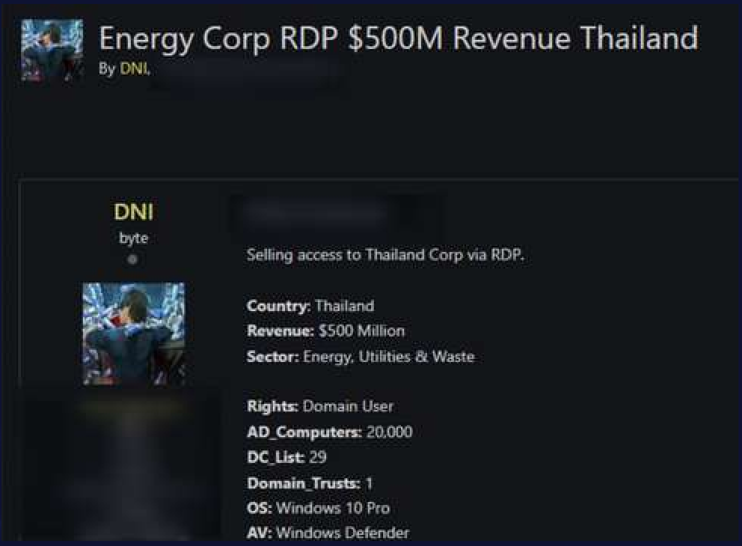
ACCEPT ESCROW AND ALSO ACCEPT DIRECT PAYMENT

ACCEPT ESCROW

Гарант-серви [redacted]

DM ONLY SERIOUS BUYER, TIME WASTER AND SCAMMER STAY OFF

The threat actor claims to be selling a database of the Department of HIV/AIDS Prevention and Control. The leaked data reportedly contains 1,44,001 rows, which includes Name, Phone Number, Patient Record ID, Date of Birth, Passport Number, etc.



Energy Corp RDP $500M Revenue Thailand

By DNI, [redacted]

DNI

byte

[redacted]

Selling access to Thailand Corp via RDP.

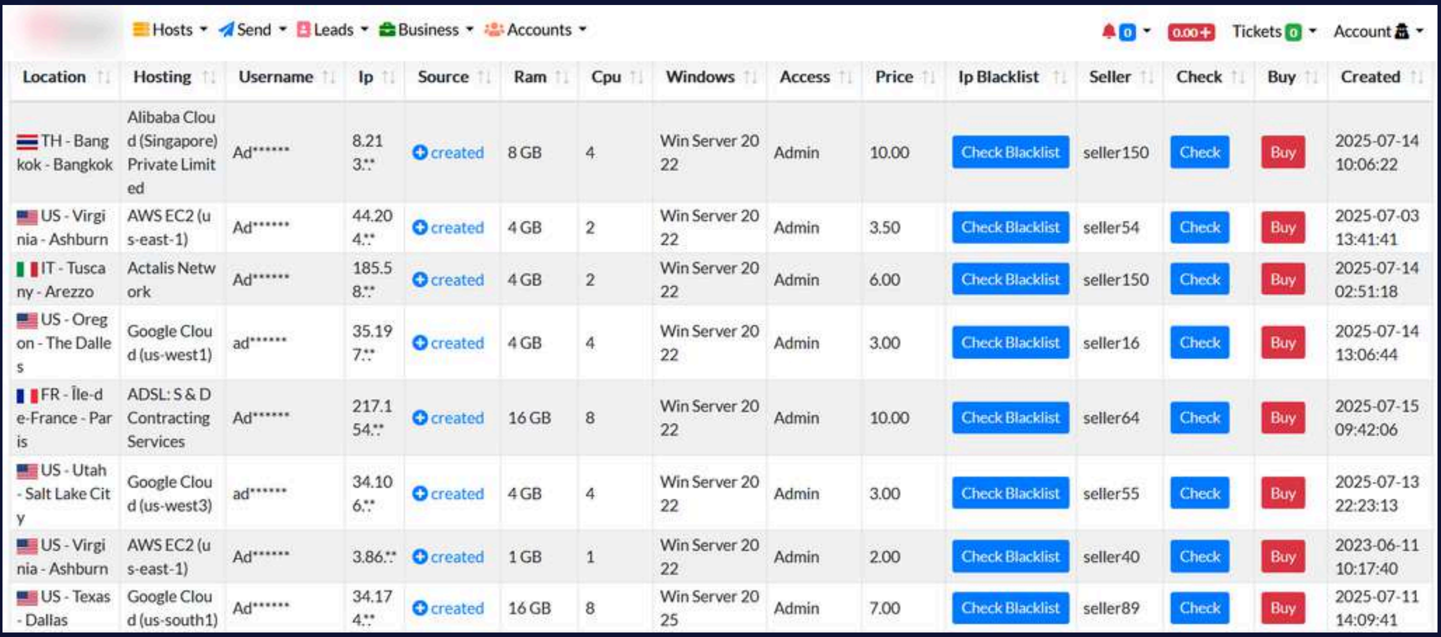
Country: Thailand
Revenue: $500 Million
Sector: Energy, Utilities & Waste

Rights: Domain User
AD_Computers: 20,000
DC_List: 29
Domain_Trusts: 1
OS: Windows 10 Pro
AV: Windows Defender

The threat actor claims to be selling unauthorized access through an RDP panel with domain user rights to an unidentified organization in Thailand. The company has an annual turnover of $500 million and operates in the Energy & Utilities industry.

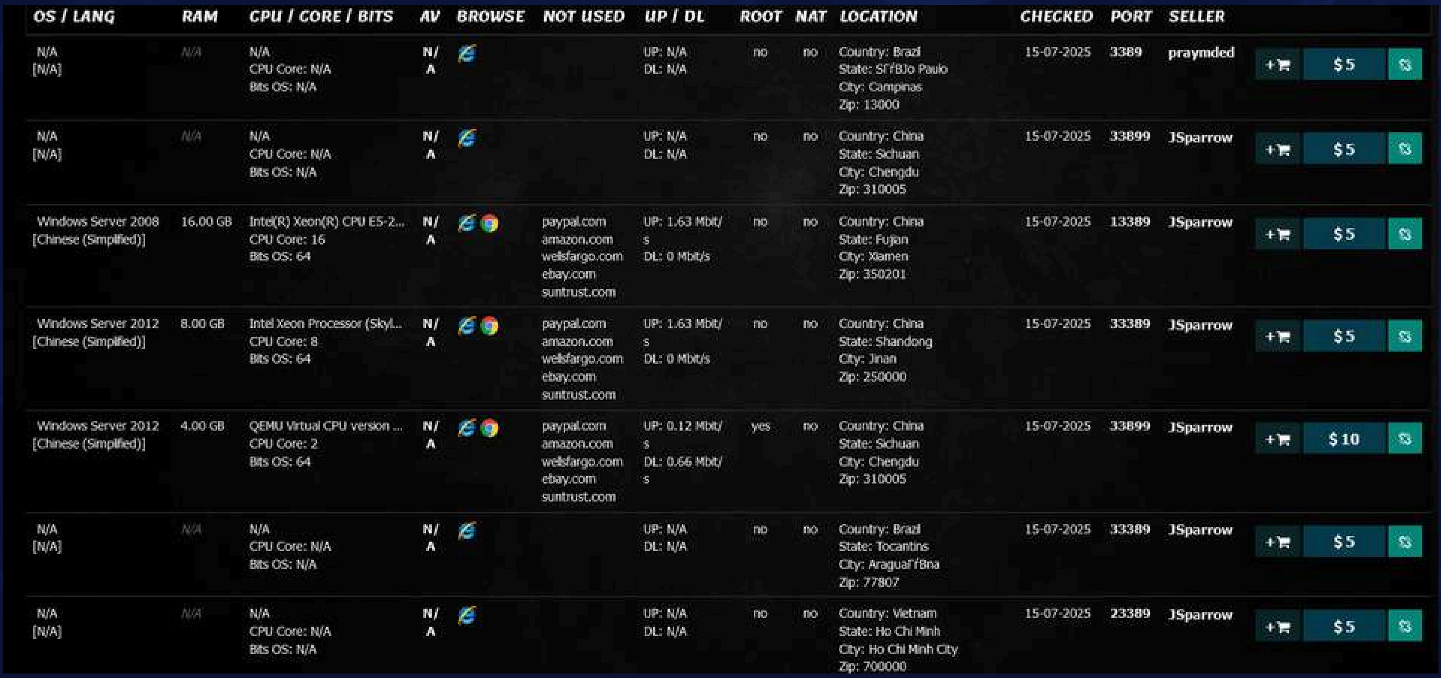
Role of Dark Markets in Initial Access Trade

Dark markets played a crucial role in sustaining the illicit economy of initial access sales throughout 2024 and 2025. Various .onion platforms such as xleet, darkode, and blackpass actively facilitated transactions involving thousands of compromised assets — including cPanel accounts, webmail access, shells, RDP credentials, and SSH connections. Listings often spanned a global range, with access offered to systems located in the USA, India, Israel, Romania, Thailand, and more, at prices ranging from as low as $2 to over $190 depending on access level and target profile. For instance, xleet alone advertised over 259,000 webmail logins and nearly 10,000 shell access points, underscoring the scale of commodified compromise.



Location	Hosting	Username	Ip	Source	Ram	Cpu	Windows	Access	Price	Ip Blacklist	Seller	Check	Buy	Created
TH - Bangkok - Bangkok	Alibaba Cloud (Singapore) Private Limited	Ad******	8.213.*.*	created	8 GB	4	Win Server 2022	Admin	10.00	Check Blacklist	seller150	Check	Buy	2025-07-14 10:06:22
US - Virginia - Ashburn	AWS EC2 (us-east-1)	Ad******	44.204.*.*	created	4 GB	2	Win Server 2022	Admin	3.50	Check Blacklist	seller54	Check	Buy	2025-07-03 13:41:41
IT - Tuscany - Arezzo	Actalis Network	Ad******	185.58.*.*	created	4 GB	2	Win Server 2022	Admin	6.00	Check Blacklist	seller150	Check	Buy	2025-07-14 02:51:18
US - Oregon - The Dalles	Google Cloud (us-west1)	ad******	35.197.*.*	created	4 GB	4	Win Server 2022	Admin	3.00	Check Blacklist	seller16	Check	Buy	2025-07-14 13:06:44
FR - Île-de-France - Paris	ADSL: S & D Contracting Services	Ad******	217.154.*.*	created	16 GB	8	Win Server 2022	Admin	10.00	Check Blacklist	seller64	Check	Buy	2025-07-15 09:42:06
US - Utah - Salt Lake City	Google Cloud (us-west3)	ad******	34.106.*.*	created	4 GB	4	Win Server 2022	Admin	3.00	Check Blacklist	seller55	Check	Buy	2025-07-13 22:23:13
US - Virginia - Ashburn	AWS EC2 (us-east-1)	Ad******	3.86.*.*	created	1 GB	1	Win Server 2022	Admin	2.00	Check Blacklist	seller40	Check	Buy	2023-06-11 10:17:40
US - Texas - Dallas	Google Cloud (us-south1)	Ad******	34.174.*.*	created	16 GB	8	Win Server 2025	Admin	7.00	Check Blacklist	seller89	Check	Buy	2025-07-11 14:09:41

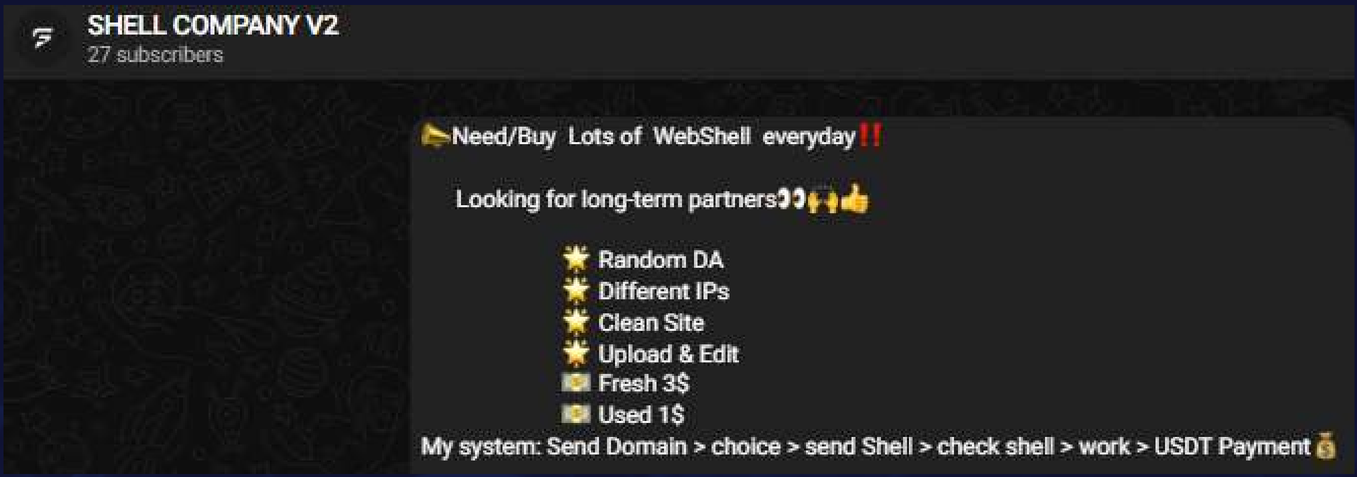
Sellers frequently bundled services, offering multi-layered access (e.g., cPanel + SMTP + webmail) and even control over boutique WordPress or Magento stores — many of which originated from Asian countries. Several markets, such as blackpass, included thousands of listings with an emphasis on Windows 10 systems, often localized with Chinese, English, or Spanish interfaces, revealing target demographics.
Overall, these underground platforms serve not just as distribution points, but as fully functional marketplaces where cybercriminals advertise, negotiate, and monetize persistent access at scale.



OS / LANG	RAM	CPU / CORE / BITS	AV	BROWSE	NOT USED	UP / DL	ROOT	NAT	LOCATION	CHECKED	PORT	SELLER	
N/A [N/A]	N/A	N/A CPU Core: N/A Bits OS: N/A	N/A			UP: N/A DL: N/A	no	no	Country: Brazil State: SГЈo Paulo City: Campinas Zip: 13000	15-07-2025	3389	praymded	+🛒 $5
N/A [N/A]	N/A	N/A CPU Core: N/A Bits OS: N/A	N/A			UP: N/A DL: N/A	no	no	Country: China State: Sichuan City: Chengdu Zip: 310005	15-07-2025	33899	JSparrow	+🛒 $5
Windows Server 2008 [Chinese (Simplified)]	16.00 GB	Intel(R) Xeon(R) CPU E5-2... CPU Core: 16 Bits OS: 64	N/A		paypal.com amazon.com wellsfargo.com ebay.com suntrust.com	UP: 1.63 Mbit/s DL: 0 Mbit/s	no	no	Country: China State: Fujian City: Xiamen Zip: 350201	15-07-2025	13389	JSparrow	+🛒 $5
Windows Server 2012 [Chinese (Simplified)]	8.00 GB	Intel Xeon Processor (Skyl... CPU Core: 8 Bits OS: 64	N/A		paypal.com amazon.com wellsfargo.com ebay.com suntrust.com	UP: 1.63 Mbit/s DL: 0 Mbit/s	no	no	Country: China State: Shandong City: Jinan Zip: 250000	15-07-2025	33389	JSparrow	+🛒 $5
Windows Server 2012 [Chinese (Simplified)]	4.00 GB	QEMU Virtual CPU version ... CPU Core: 2 Bits OS: 64	N/A		paypal.com amazon.com wellsfargo.com ebay.com suntrust.com	UP: 0.12 Mbit/s DL: 0.66 Mbit/s	yes	no	Country: China State: Sichuan City: Chengdu Zip: 310005	15-07-2025	33899	JSparrow	+🛒 $10
N/A [N/A]	N/A	N/A CPU Core: N/A Bits OS: N/A	N/A			UP: N/A DL: N/A	no	no	Country: Brazil State: Tocantins City: AraguaГna Zip: 77807	15-07-2025	33389	JSparrow	+🛒 $5
N/A [N/A]	N/A	N/A CPU Core: N/A Bits OS: N/A	N/A			UP: N/A DL: N/A	no	no	Country: Vietnam State: Ho Chi Minh City: Ho Chi Minh City Zip: 700000	15-07-2025	23389	JSparrow	+🛒 $5

Telegram’s Role in Initial Access Trade

Telegram has become a parallel channel for the advertisement and negotiation of initial access sales, complementing darknet marketplaces with its real-time, decentralized communication model. Our analysis identified multiple Telegram groups explicitly focused on **selling webshells**, **cPanel access**, **WordPress admin credentials**, and **mail server logins**, often labeled under names such as **"SHELL COMPANY V2"**, **"RANDOM ONLY"**, and **"MARKET WEBSHELL"**. A notable portion of these offerings originate from countries like **Thailand** and **India**, with a heavy focus on compromised boutique websites and exposed CMS environments. Sellers frequently operate anonymously, posting samples or access metadata (e.g., domain names, CMS type, location)



SHELL COMPANY V2
27 subscribers

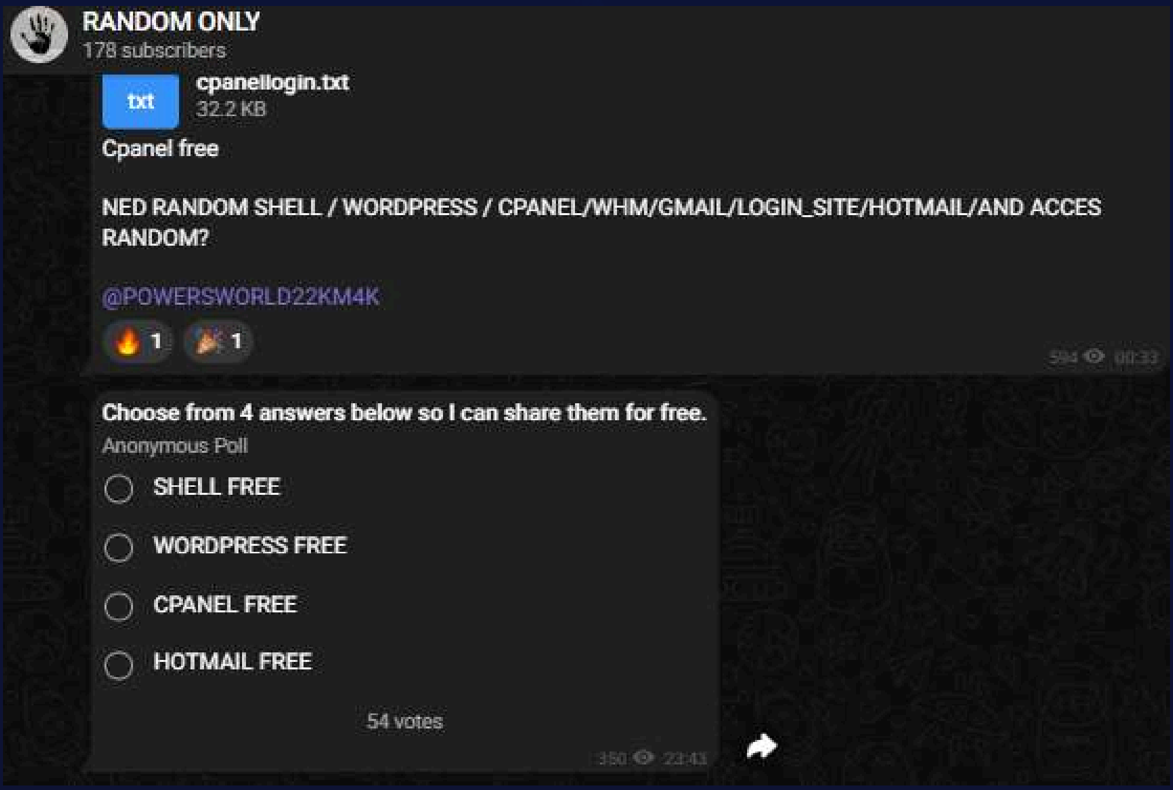
📢Need/Buy Lots of WebShell everyday‼️

Looking for long-term partners👀🙌👍

⭐ Random DA
⭐ Different IPs
⭐ Clean Site
⭐ Upload & Edit
💵 Fresh 3$
💵 Used 1$

My system: Send Domain > choice > send Shell > check shell > work > USDT Payment💰

The growing reliance on Telegram reflects a shift toward **informal and agile access distribution**, where listings are ephemeral but volume is high, and traceability is significantly reduced. Unlike structured dark markets, Telegram groups provide a dynamic ecosystem for access resale and actor coordination, especially for lower-tier access types like **WordPress shells** or shared **webmail panels**.



RANDOM ONLY
178 subscribers

txt cpanellogin.txt
32.2 KB

Cpanel free

NED RANDOM SHELL / WORDPRESS / CPANEL/WHM/GMAIL/LOGIN_SITE/HOTMAIL/AND ACCES RANDOM?

@POWERSWORLD22KM4K

🔥 1 🎉 1

594 👁 00:33

Choose from 4 answers below so I can share them for free.
Anonymous Poll

○ SHELL FREE

○ WORDPRESS FREE

○ CPANEL FREE

○ HOTMAIL FREE

54 votes

350 👁 23:43

Mitigation Strategies

As the Initial Access Brokerage (IAB) ecosystem continues to mature and expand, organizations must adopt a layered, proactive defense model to prevent unauthorized access. The following mitigation strategies are essential to disrupt access broker operations and reduce organizational exposure:

- **Credential Hygiene and MFA**: Enforce strong, unique passwords across all systems, and mandate multi-factor authentication (MFA) — particularly for remote access services like VPN, RDP, and administrative dashboards.

- **Attack Surface Management**: Regularly scan for exposed assets (e.g., open RDP ports, outdated CMS plugins) and decommission or secure unused services and interfaces.

- **Timely Patch Management**: Ensure operating systems, applications, and third-party plugins are updated consistently to prevent exploitation through known vulnerabilities.

- **Threat Intelligence Integration**: Monitor underground forums, Telegram channels, and breach platforms for mentions of your assets. Early identification of exposure enables faster response and containment.

- **Access Segmentation and Logging**: Limit user privileges, implement network segmentation, and monitor login attempts and access anomalies to detect lateral movement or unauthorized behavior.

- **Incident Response Readiness**: Establish clear response protocols for credential leaks, unauthorized access detections, and third-party vendor breaches.

By combining technical controls, continuous monitoring, and cross-departmental response planning, organizations can significantly reduce their appeal and exposure within the initial access economy.

Conclusion

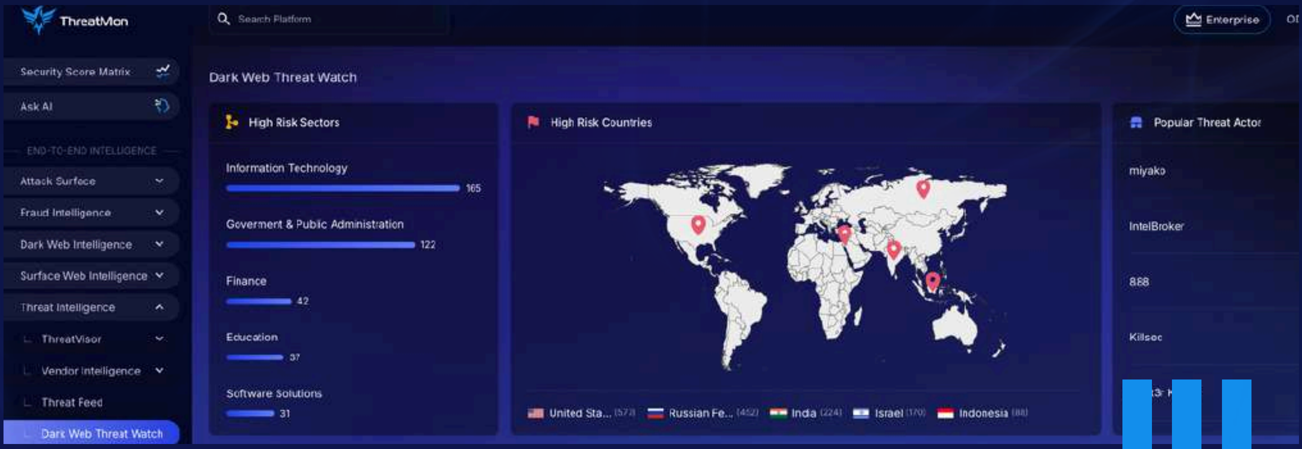
The findings from this research underscore the scale, sophistication, and global reach of Initial Access Brokerage as a central pillar of today's cybercrime economy. From darknet forums and Telegram groups to targeted attacks across 150+ countries, IAB activity in 2024–2025 has proven to be both pervasive and persistent.

The growing presence of professionalized threat actors — such as ProfessorKliq, miyak0, and diamond — combined with the targeting of critical sectors like government, education, and finance, demonstrates that initial access is no longer a niche commodity, but a core enabler of broader cybercriminal operations.

The industrialization of access trade through structured marketplaces, bundled offerings, and reputation-based actor ecosystems has further reduced the barriers to entry for malicious actors.

Ultimately, defending against initial access threats requires more than reactive security. It demands visibility, vigilance, and strategic investment in cybersecurity posture across all layers of digital infrastructure. As access continues to be weaponized, the stakes for proactive defense have never been higher.

More Information About ThreatMon



One Platform for all intelligence needs.

ThreatMon End-to-end intelligence is a cutting-edge, cloud-based SaaS platform that continuously monitors the dark and surface web, providing early warnings and actionable insights into emerging threats.

We are a SaaS platform designed to help businesses proactively detect and address threats before a cyber attack occurs. Unlike traditional cyber threat intelligence, we provide comprehensive and holistic cyber intelligence.

- *Attack Surface Intelligence*
- *Fraud Intelligence*
- *Dark and Surface Web Intelligence*
- *Threat Intelligence*
- *Security Score matrix*
- *ThreatMon AI Agent*

APPLY

FREE ACCESS

Contact Us :

Email Address
info@threatmonit.io

https://x.com/MonThreat

https://www.linkedin.com/company/threatmon