CYJAX

Digital Intelligence
Securing the Future

Initial Access Broker market summary - Q3 2024

01

Introduction

Initial access brokers (IABs)[1] form a key part of the cybercriminal ecosystem. Active on cybercriminal forums, they facilitate access for ransomware groups, data leakers, and advanced persistent threat groups (APTs) into corporate networks. They are highly specialised, professional, and operate in an established, lucrative market often characterised by rigid rules and conventions. Every ransomware attack or data breach begins with initial access, following the reconnaissance phase of an attack. For a fee, IABs facilitate the entry of other bad actors into organisations' networks.

After conducting an analysis of the IAB ecosystem in both Q1 [2] and Q2 [3], 2024, CYJAX has continued to monitor IAB listings on these forums. With the data collected from both Q1 and Q2, it is possible to compare changes in the ecosystem and examine changes and trends in the market. This whitepaper reports the statistics and trends observed in initial access listings on the most prominent Russian- and English-language cybercriminal forums in Q3 2024.

02

Key Takeaways

- The top 10 most targeted countries in Q3 were **United States of America** (31% of all listings), **Brazil** (5.6%), **India** (4.9%), **Canada** (3.7%), **Italy** (3.0%), **Germany** (2.8%), **United Kingdom** (2.8%), **Australia** (2.5%), **Thailand** (2.1%), and **Türkiye** (2.1%). Türkiye was not recorded in the top 10 targeted countries in previous quarters in 2024, highlighting developments in the market and changes in geographical targeting.
- **Taiwan** saw a 270% increase in listings from Q2 to Q3. A significant portion of the listings in Q3 were for organisations related to industrial machinery, electronics, manufacturing, computer equipment, and peripherals. Taiwan saw a significant increase in semiconductor and advanced silicon production to meet growing demands from the global surge in artificial intelligence (AI), potentially increasing the value of Taiwan-based accesses for IABs.
- The top 10 targeted sectors in Q3 were **professional services** (12.9% of all listings), **manufacturing** (8.1%), **construction** (7.9%), **IT** (6.3%), **education** (6.0%), **retail** (4.4%), **financial** (4.4%), **government** (3.2%), **telecommunications** (2.8%), and **real estate** (2.3%). In comparison to country targeting, IABs remain largely sector-agnostic, except for commonly targeted sectors with potential value to ransomware groups such as professional services, manufacturing, and construction.
- The top 10 most commonly targeted access types in Q3 were **VPN** (31.9% of all listings), **RDP** (23.1%), **RDWeb** (8.8%), **Citrix** (6.5%), **VNC** (2.1%), **Webshell** (1.9%), **SSH** (1.9%), **Forti** (1.9%), **C2** (1.4%), and **Admin Panel** (0.9%). RDP, VPN, and RDWeb being the top three most targeted remains consistent from the previous quarters. This may indicate the comparative ease of compromise through brute forcing and vulnerability exploitation rather than other access types, in addition to their widespread enterprise use.
- The top 10 antivirus solutions active in listings in the quarter were **Windows Defender** (10.2% of all listings), **Sentinel** (3.5%), **CrowdStrike** (2.5%), **Trend Micro** (2.5%), **Webroot** (1.9%), **Sophos** (1.9%), **Kaspersky** (1.6%), **BitDefender** (1.4%), **Eset** (1.4%), and **Symantec** (0.7%). While likely due to selection bias, many listings with noted antivirus solutions are for Windows Defender. This potentially indicates the large ratio of compromised Windows-based infrastructure compared to other operating systems.
- Access listings with Russia-based Kaspersky antivirus stated as active in the network increased by 121.5% from Q2 to Q3 2024, for which there may be several explanations. This includes the release of the RegreSSHion vulnerability and the US' decision to ban Kaspersky in Q3. However, It is likely that this is due to the decrease in listings for the quarter, creating a larger market share for the antivirus.

The top 10 targeted sectors in Q3 were professional services (12.9% of all listings), manufacturing (8.1%), construction (7.9%), IT (6.3%), education (6.0%), retail (4.4%), financial (4.4%), government (3.2%), telecommunications (2.8%), and real estate (2.3%).

- The top 10 most prolific IABs in Q3 2024 were **SGL** (12.3% of all listings), **Кот Ученый** (5.1%), **DNI** (4.2%), **RelativelyCrazy** (3.9%), **budda12** (3.5%), **Panchitos** (2.5%), **BarmoleyAibolitov** (2.3%), **internetBandit** (2.1%), **sudo** (2.1%), and **darksoul** (2.1%). SGL has remained in the top two most prolific IABs across the past three quarters, with only 8.55% of brokers active in Q1 remaining active in Q3.

03

Overall statistics

Total listings

Compared to Q2 2024, there were **27.4% less listings** on the monitored cybercriminal forums. Several changes in this quarter may have caused this. For example, forum administrators and moderators took a more active role in moderating the IAB market, including by closing the listings of brokers that do not have a deposit on the forum. Having a deposit on the forum portrays higher credibility and dedication to operating a market on the forum, by way of proving monetary investment as motivation before making a profit. This allows administrators to prevent scamming, a common occurrence on cybercriminal forums. This increases the reputation and reliability of the forum and prospective sellers.

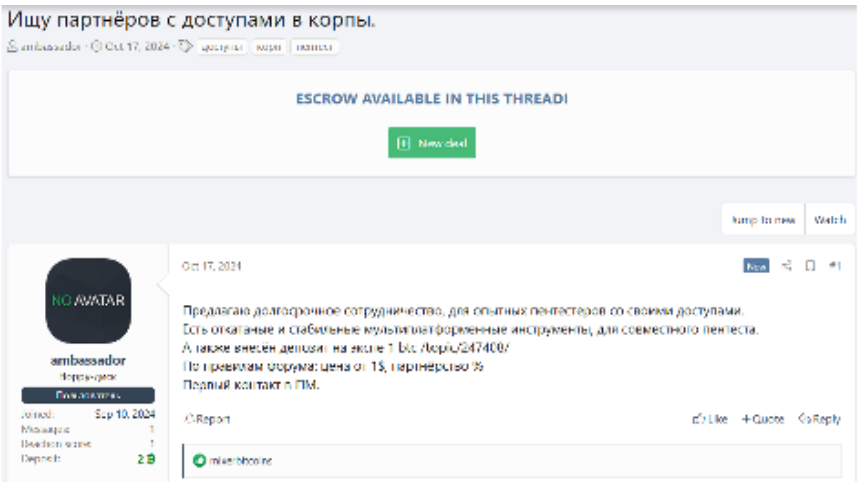

Figure 1: XSS user with a total forum deposit of BTC 3 ($162,500) across XSS and Exploit seeks to purchase initial access to corporate networks.

Average price

The **average listed price of IAB listings in Q3 was $6,115**, a 111.6% increase from the previous quarter. This may be due to supply and demand, as with less listings the price may raise accordingly.

The average listed price of IAB listings in Q3 was $6,115, a 111.6% increase from the previous quarter. This may be due to supply and demand, as with less listings the price may raise accordingly.

Figure 2: Graph showing average price ($) of IAB listings in Q1 to Q3.

Average revenue

The **average listed revenue of a company was $1.929 billion**, a 223.1% increase from the previous quarter. With less listings in the quarter, it is possible that IABs chose to target higher revenue organisations to demand increased prices and gain larger profits. Additionally, established IABs may have developed their capabilities to target companies with stronger defences, which often correspond to higher revenues. As indicated in CYJAX's Q2 report [3], as average victim revenue increases, so does listing price, albeit non-linearly, and with exceptions.

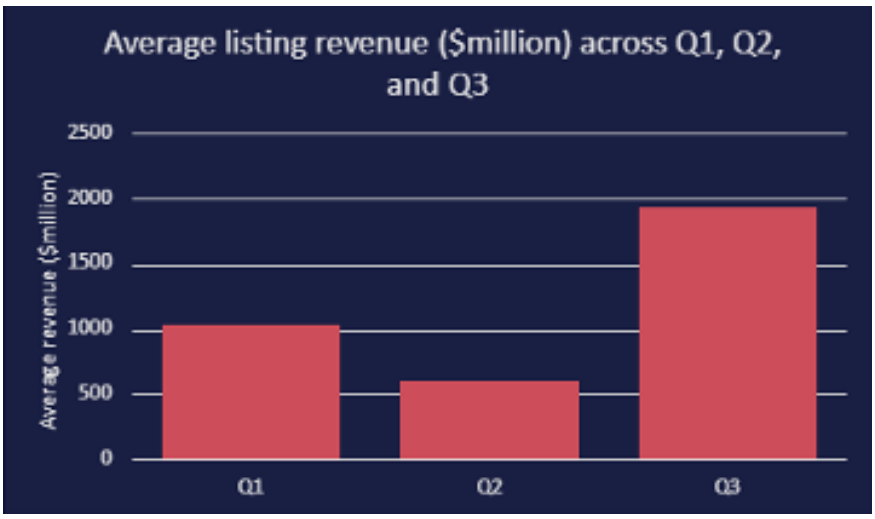

Figure 3: Graph showing average revenue (in $ millions) for IAB listings in Q1, Q2, and Q3.

The highest priced access listing during the quarter was advertised by Exploit user "Unsync" at $1,000,000. On 6 July 2024, Unsync initiated an English-language thread titled "Selling Access - [India Oil, Gas and Energy]" in the Auctions section of the prominent Russian-language cybercriminal forum Exploit. In their initial post in the thread, Unsync advertised "SOCKS" access with domain administrator privileges to an unnamed India-based infrastructure organisation with a revenue of $50 billion.

They also stated that there were over 10,000 hosts active on the network. Unsync priced their offering at $1,000,000. As of late October 2024, there have been no responses to the thread from other users, and no indication of sale.

SOCKS is a protocol which facilitates client-server communication through a proxy server and can be viewed as a unique form of VPN access. It is likely that by stating "SOCKS" as the access type, the broker is inferring credential access to an active SOCKS proxy service.

Figure 4: Exploit IAB post by Unsync advertising access to an India-based infrastructure organisation.

The largest listed revenue for a company was $130 billion. On 31 July 2024, user "zjdue123" initiated an English-language thread titled "130B A CIS country" in the Accesses section of the prominent Russian-language cybercriminal forum XSS. In their initial post in the thread, zjdue123 advertised Intranet access with no recorded privileges to an unnamed organisation with a revenue of $130.0 billion located in the Commonwealth of Independant States (CIS). User zjdue123 did not list to which sector the organisation pertained and priced their offering at $100,000.

The user has since been permanently banned by the forum for "work on Russia", potentially indicating that the listing was for a Russia-based organisation. On Russian-language cybercriminal forums such as XSS and Exploit, there are strict rules against targeting CIS countries and especially Russia. Work carried out against the CIS leads to permanent bans if a user is found to be attacking these countries, even if this occurred inadvertently.

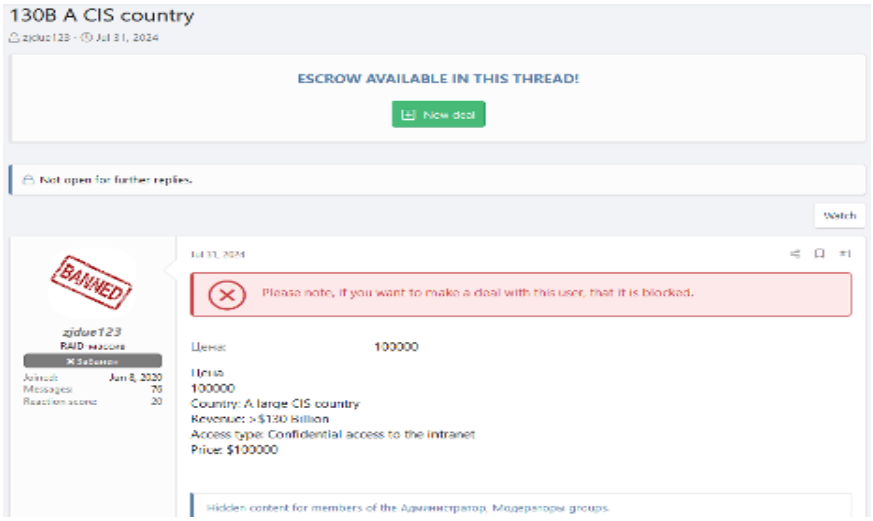

Figure 5: XSS post advertising access to a CIS country organisation

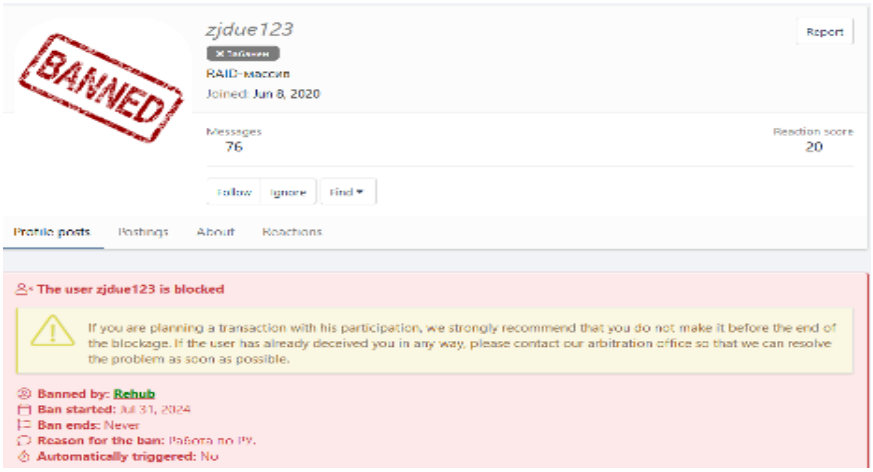

Figure 6: zjdue123's profile on XSS, portraying their permanent ban for "work on Russia".

Two things can be inferred from this account ban. Firstly, a user with a relatively high reaction score of 20 and post count of 76 was banned immediately following their advertisement of a CIS country access listing. This demonstrates the strict adherence to forum rules which are enforced by moderators. Secondly, it is abnormal that a user which has been active for over four years, that is highly likely aware of the forum rules, would knowingly advertise an access that goes against said rules. It is possible that the account was sold by the original operator to another user. Users are known to sell access and ownership of forum accounts to others to provide them with a more aged account, a higher reputation, or for other monetary gain. For example, the below post portrays a user on BreachForums selling a two-month-old XSS account with no posts for $100.

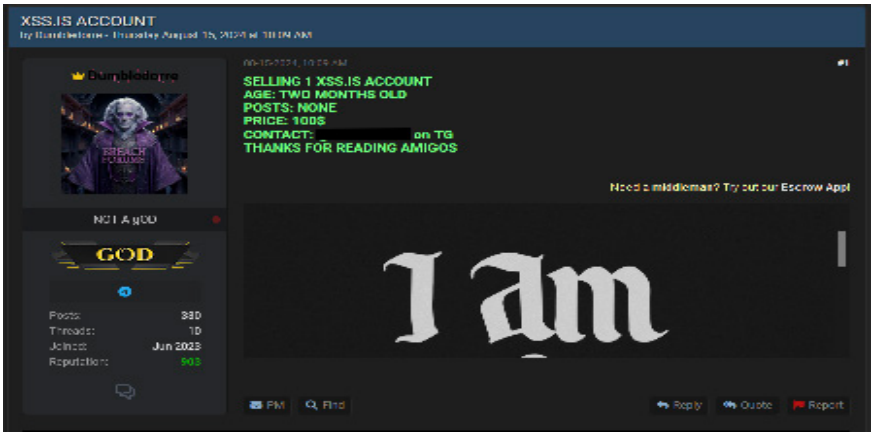

Figure 7: BreachForums user advertising XSS account for sale

Country stats

Figure 8. shows that the top 10 most targeted countries in Q3 were the **United States** (31% of all listings), **Brazil** (5.6%), **India** (4.9%), **Canada** (3.7%), **Italy** (3.0%), **Germany** (2.8%), **United Kingdom** (2.8%), **Australia** (2.5%), **Thailand** (2.1%), and **Türkiye** (2.1%).

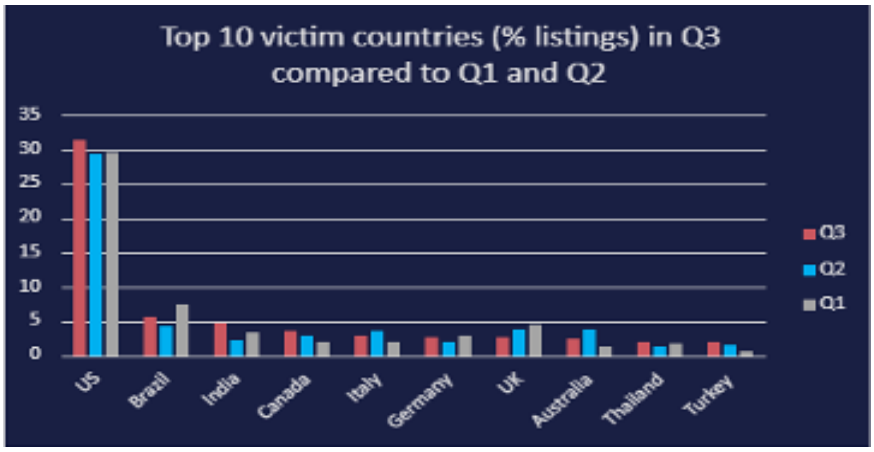

Figure 8: Graph showing top 10 targeted countries by market share in Q1 to Q3 2024

The **United States** has remained the most targeted country throughout the three analysed quarters, portraying consistent popularity in both supply and demand of IAB listings in the country. This appears to solidify the general anti-Western sentiment showed by Russian-language cybercriminal forums.

The United States has remained the most targeted country throughout the three analysed quarters, portraying consistent popularity in both supply and demand of IAB listings in the country.

04

Countries in the spotlight

Taiwan

Taiwan saw a 270% increase in listings from Q2 to Q3. A significant portion of the listings in Q3 were for organisations related to industrial machinery, electronics, manufacturing, computer equipment, and peripherals. Taiwan saw [4] a significant increase in semiconductor and advanced silicon production to meet growing demands from the global surge in artificial intelligence (AI). This surge likely increased the potential value of access to such organisations in the country, leading to the observed growth in Taiwan-based listings. Threat actors operating towards the interest of other countries in the South China Sea, such as China, would likely be interested in these accesses due to the general negative geopolitical sentiment between the countries. Similarly, threat actors would likely see high value in intellectual property (IP) regarding the manufacturing of semiconductors, creating a large demand for these organisations.

On 8 August 2024, user "PirateJack" initiated an English-language thread on XSS titled "Taiwan $20B Electronics Access (Need 2FA Bypass)". In their initial post on the thread, PirateJack advertised VPN access to an unnamed Taiwan-based electronics organisation with a revenue of $20 billion. PirateJack stated that "the access is valid, but has 2fa configured on the dana-na panel". This suggests that the broker gained credential access to the panel but was unable to bypass the 2FA mechanism on it. Alternatively, it could suggest that PirateJack did not value the time necessary to perform the bypass when the credentials could be sold.

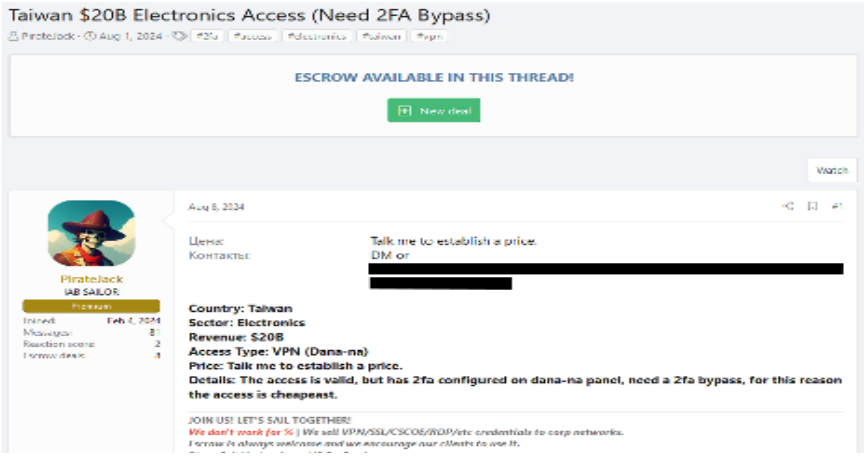

Figure 9: PirateJack XSS IAB listing for Taiwan-based organisation

> Threat actors operating towards the interest of other countries in the South China Sea, such as China, would likely be interested in these accesses due to the general negative geopolitical sentiment between the countries.

Türkiye

Access listings for organisations in Türkiye have increased over the past three quarters, growing from 0.5% of the market share in Q1 2024, to 1.5% in Q2, and 2.1% in Q3. Türkiye made the top 10 most targeted in Q3 2024, highlighting the growing interest in the country for IAB listings. As noted in the following section, the average listing price for Türkiye-based organisations when adjusted for an organisation's revenue was also in the top 10 in Q3 2024.

Third-party sources state that cybercrime both originating from and affecting Türkiye has been increasing, with cybercrime incidents [5] "on the rise in both volume and frequency". In September 2024 alone, there were [6] 28 ransomware listings for organisations in the country, with groups such as LockBit, RansomHub, DarkPower, Arcus, Medusa, HuntersInternational, Qilin, Red Ransomware, and ALPHV targeting Türkiye.

Figure 10 is an example of a Türkiye-based IAB listing. On 10 July 2024, user "raywood" initiated an English-language thread in the Accesses section of XSS titled "Selling access (webshell) TR Company". In their initial post in the thread, raywood advertised web shell access to an unnamed Türkiye-based manufacturing organisation with a revenue of $15 million. The broker stated that the access was to an Apache server, which also allegedly contained MariaDB and Kerberos.

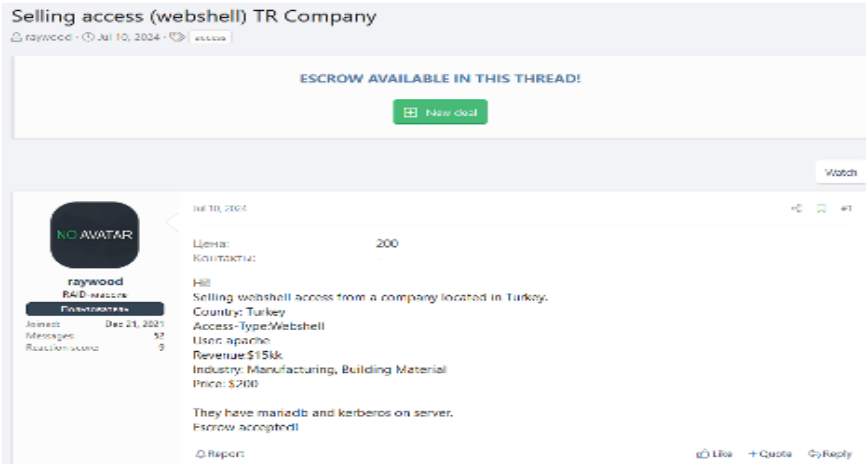

Figure 10: XSS post for unnamed Türkiye-based organisation

> Cybercrime both originating from and affecting Türkiye has been increasing, with cybercrime incidents [5] "on the rise in both volume and frequency".

Value when adjusted for listed revenue

The top 10 most valuable average listings by country when adjusted for revenue were **Portugal** ($74 per $million in revenue), **Switzerland** ($55 per $million), **Sweden** ($49.67 per $million), **Italy** ($32.39 per $million), **Canada** ($26.32 per $million), **Brazil** ($20.68 per $million), **Saudi Arabia** ($12.34 per $million), **Mexico** ($11.52 per $million), **Australia** ($11.35 per $million), and **Türkiye** ($9.90 per $million).

Figure 11: Graph showing the average IAB listing price by country when adjusted for the target organisation's revenue

Brazil, Italy, Canada, Australia, and Türkiye were in the top 10 targeted countries in Q3. This indicates that IABs list higher prices for larger revenue organisations in popular or valuable countries, a hypothesis mentioned in analysis of previous quarters. However, the remaining countries in the top 10 consisted of less than 2.1% market share each, possibly portraying that less targeted countries may be seen as rare or unique listings. This allows IABs to charge more for these accesses.

While its sample size of listings in Q3 was too small to discount anomalies, the average price for access to Israel-based organisations remained proportionally high compared to other countries at $51,750. This was similarly high in previous quarters and is likely due to the ongoing Israel-Palestine conflict affecting the value of accesses in the country. As of late October 2024, however, Israel-based access listings with prices between $50,000 and $150,000 have been deleted. As such, further analysis of these highly priced listings is impossible. However, Figure 12 shows example of another Israel-based IAB listing in Q3 2024.

On 6 August 2024, user "ZeroSevenGroup" initiated an English-language thread in the Sellers Place section of BreachForums titled "[SOLD] Israeli Financial Software & Technology Company". In their initial post on the thread, ZeroSevenGroup advertised "C2" access to an unnamed Israel-based "Financial Software & Technology" company. The broker priced the listing at $2,000, and the title indicates that the access was sold. CYJAX assesses that the victim organisation fitting the description provided by ZeroSevenGroup is Autosoft, a point of sale (PoS) company based in Israel.

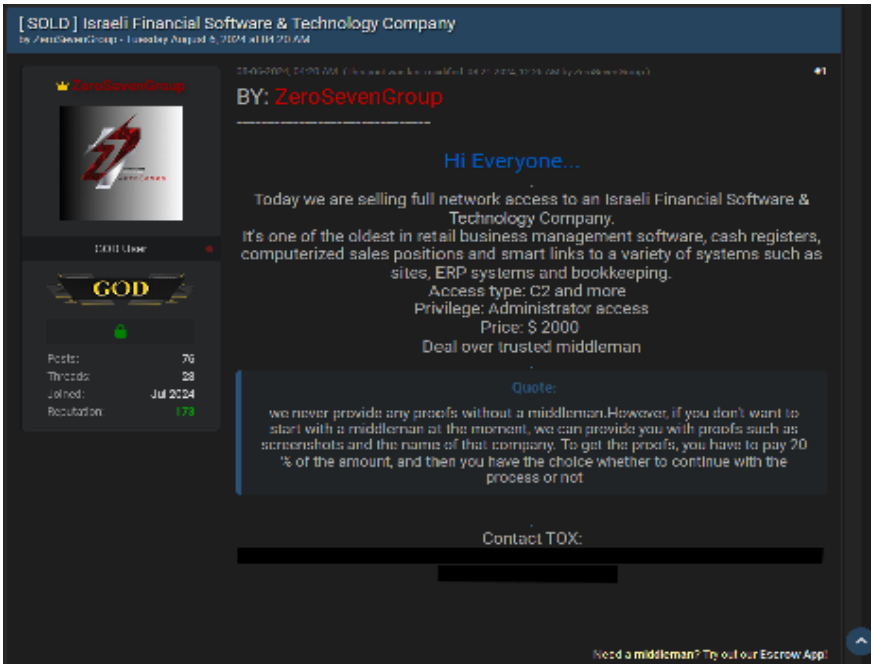

Figure 12: BreachForums IAB listing advertising access to an Israel-based IT company

Interestingly, a significant change in Q3 was an IAB listing for an organisation based in **Russia**. This is particularly relevant due to the often-strict moderation against listings in Commonwealth of Independant States (CIS) countries, especially Russia, on Russian-language cybercriminal forums. These rules also likely affect the number of such listings on other forums, as IABs using multiple forums to advertise accesses may desire to maintain their reputation across all forums. They often do this by adhering to common restrictions, such as that against targeting CIS countries, regardless of the rules on one particular forum.

On 4 September 2024, user "STARGROUP" initiated an English-language thread titled "RUSSIAN Petroleum Company VPN access" in the "Access Market" section of BreachForums. In their initial post in the thread, STARGROUP advertised VPN access to a Russia-based petroleum company with an unstated revenue. The broker provided a screenshot as proof of compromise, and stated that the access contained a database, panels, and "lots of confidential data".

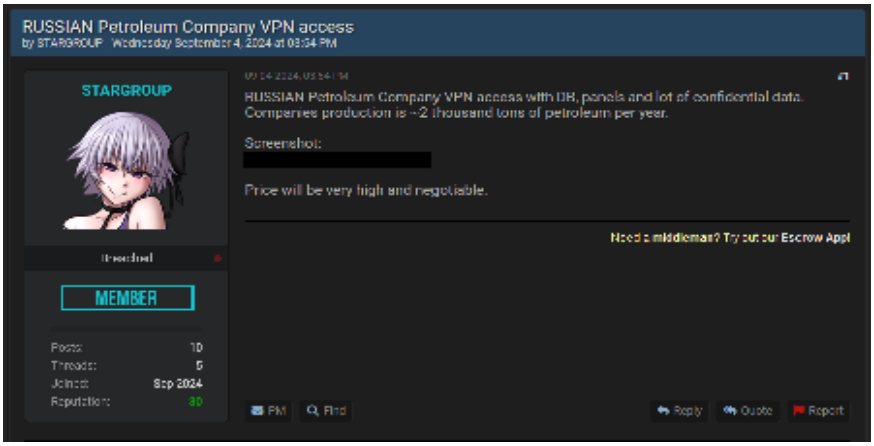

Figure 13: BreachForums IAB listing for Russia-based petroleum organisation.

05

Sector stats

The top 10 targeted sectors in Q3 were **professional services** (12.9% of all listings), **manufacturing** (8.1%), **construction** (7.9%), **IT** (6.3%), **education** (6.0%), **retail** (4.4%), **financial** (4.4%), **government** (3.2%), **telecommunications** (2.8%), and **real estate** (2.3%).

Targeting from Q1 to Q3 has seen consistency in its top 10 targeted sectors, with the **professional services, manufacturing, construction, IT, education, retail, and financial sectors** appearing in each quarter. **Professional services** has been the most targeted sector across each quarter.

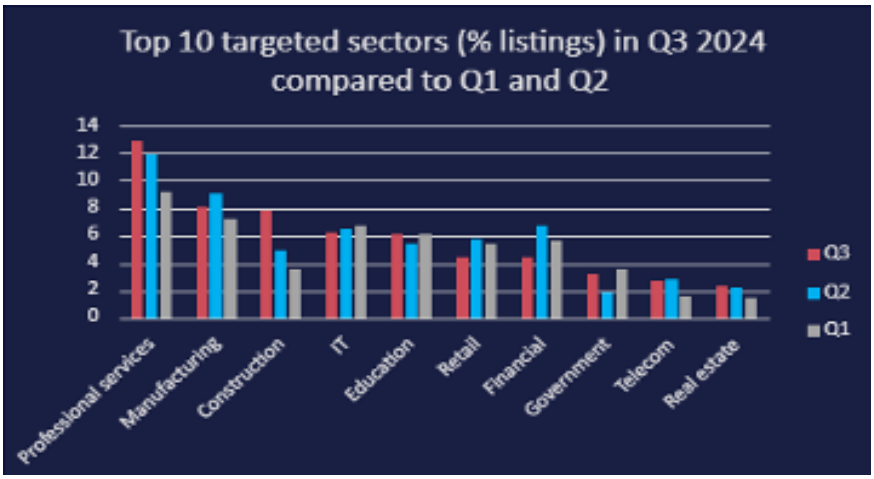

Figure 14: Graph showing top 10 targeted sectors in Q3 2024

Sectoral targeting appears to have remained relatively agnostic, with the top 10 most targeted changing significantly. However, **the professional services and construction sectors** have reached the top 10 targeted sectors in each quarter so far in 2024, indicating the value of them to prospective buyers. These organisations are particularly valuable to ransomware threat groups due to the potential supply-chain compromise from the likely many clients these organisations may have.

Education is an outlier in the top 10 targeted sectors. The sector is similar to healthcare in that there may be stigma attached to attacking education organisations, and it may be discouraged in forum sentiment. However, there is less stigma than healthcare, and education organisations often use unpatched or legacy systems so are often more likely to be vulnerable to attacks. Additionally, during term times, such organisations may not be able to afford downtime and are more motivated to pay ransoms. Education organisations are also motivated to prevent the potential exposure of student personal data from such attacks.

The professional services and construction sectors are particularly valuable to ransomware threat groups due to the potential supply-chain compromise.

On 30 August 2024, user and BreachForums administrator "IntelBroker" initiated a thread in the Access Market section of the forum titled "Global Leader in Education Services". In their initial post on the thread, IntelBroker advertised multiple access methods to an unnamed India-based education organisation with a revenue of $140 million. Access types included RDP, AWS S3, AWS SES, API, and Database, indicating that the broker had significant and potentially high-level access to the organisation.

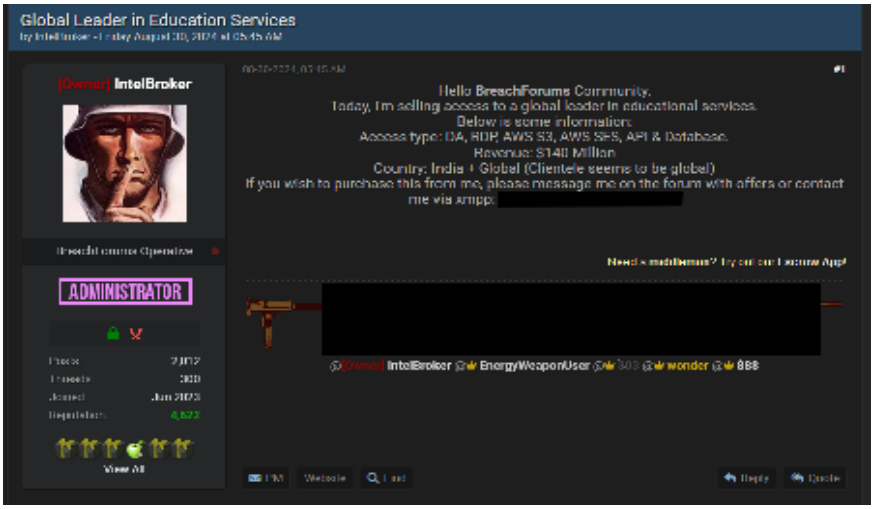

Figure 15: BreachForums post advertising access to an India-based education organisation

Value when adjusted for listed revenue

The top 10 most valuable sectors when adjusted for revenue were **financial** ($70.91 per $million in revenue), **hospitality** ($67.55 per $million), **retail** ($52.73 per $million), **construction** ($26.76 per $million), **manufacturing** ($17.17 per $million), **FMCG** ($15.39 per $million), **IT** ($13.00 per $million), **professional services** ($12.42 per $million), **automotive** ($12.16 per $million), and **government** ($9.17 per $million).

Figure 16: Graph showing IAB listing price when adjusted for revenue, comparing each sector

The **financial sector** is the most valuable sector per $million in revenue. This is likely due to the potential monetary gain through attacking the company, as well as valuable personal information which may be used in further malicious activity such as fraud and personal data sale. Financial organisations may be more likely to pay ransoms, as they contain significant sensitive and personal data on clients and are more highly regulated. Organisations may choose to prevent public disclosure of an attack by quietly paying ransoms, also avoiding large fines and potential legal action following customer data loss.

The sector is valuable for threat actors and contains many large-revenue organisations, allowing IABs to charge higher prices for initial access. The fact that these organisations often have large amounts of liquidity increases the risk of monetary theft. This is similar to large-scale cryptocurrency heists conducted by the North Korean state-sponsored advanced persistent threat (APT) group Lazarus, which has been responsible for the theft of billions of dollars.

On 6 September 2024, user "STARGROUP" initiated an English-language thread in the Access Market section of BreachForums titled "Taiwanese Bank access user in network ~17 Billion Revenue". In their initial post on the thread, STARGROUP advertised VPN access to an unnamed Taiwan-based bank headquarted in Taipei, with a revenue of approximately $17 billion. In a reply to the thread on 7 September 2024, the broker stated that the access had been sold.

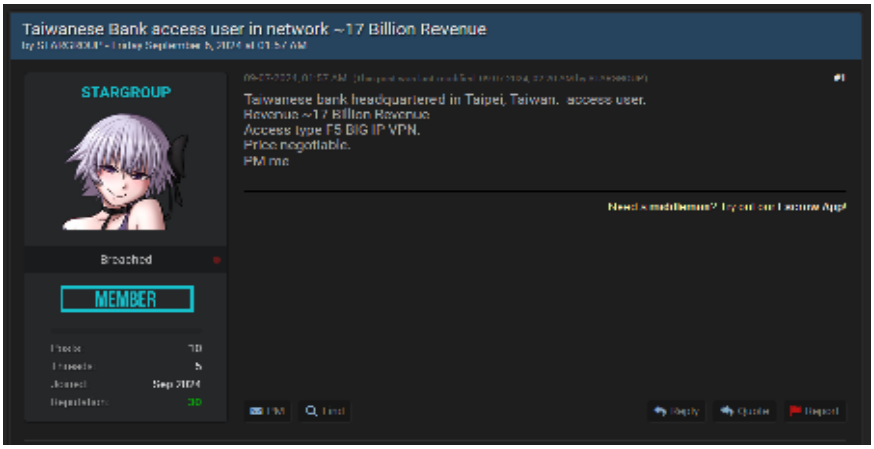

Figure 17: BreachForums IAB post advertising access to a Taiwan-based bank.

The financial sector is the most valuable sector due to the potential monetary gain as well as valuable personal information.

06

Access types

The top 10 most commonly targeted access types in Q3 were **VPN** (31.9% of all listings), **RDP** (23.1%), **RDWeb** (8.8%), **Citrix** (6.5%), **VNC** (2.1%), **Webshell** (1.9%), **SSH** (1.9%), **Forti** (1.9%), **C2** (1.4%), and **Admin Panel** (0.9%).

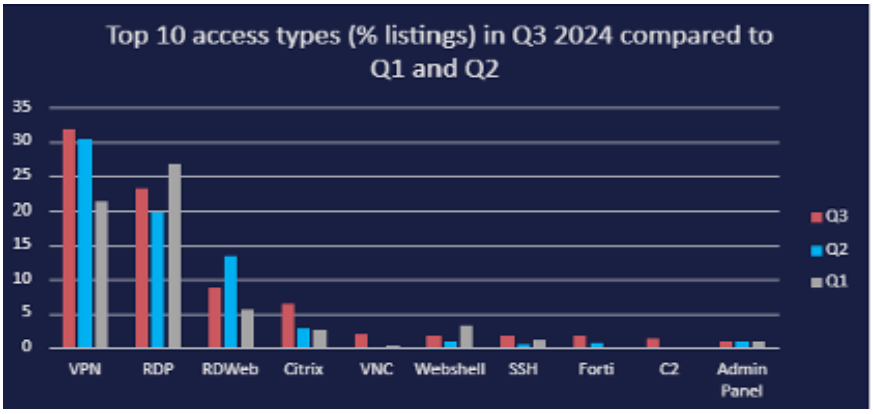

Figure 18: Graph showing top 10 targeted access types in Q3 2024 compared to Q1 and Q2.

As with the previous sectors in 2024, **RDP** and **VPN** remain the top two most targeted access types. This indicates a consistent use of TTPs such as brute force and vulnerability exploitation to gain initial access to organisations through these types.

Listings containing accesses gained through **SSH** increased by 270% from Q2 to Q3, the majority of which had local administrator privileges. Such accesses would provide an attacker with the ability to compromise an individual machine with administrator privileges. This would give the capability to manipulate and exfiltrate sensitive files stored on the machine.

A particularly relevant vulnerability which was released [7] in the quarter was a flaw in OpenSSH with the CVE identifier CVE-2024-6387, also referred to as "regreSSHion". The vulnerability, which was patched on 1 July 2024, makes use of a race condition within sshd to allow an attacker to execute arbitrary code with root privileges. Through this, an attacker could fully compromise a system to deliver further malware, create backdoors, and compromise its integrity. CYJAX has observed this vulnerability being actively discussed on forums, with at least three Proof-of-Concepts (PoC) shared across the dark web. This allows other threat actors to compromise potentially vulnerable Linux servers quickly and easily without the need to develop custom exploitation kits.

One such discussion thread on XSS was initiated by highly reputable user DreadPirateRoberts, on the same day Qualys released [8] their initial report regarding the vulnerability.

RDP and VPN remain the top two most targeted access types. This indicates a consistent use of TTPs such as brute force and vulnerability exploitation to gain initial access to organisations through these types.

Figure 19: Screenshot of XSS post discussing the RegreSSHion vulnerability

SSH access listings have been commonly listed in previous quarters. In the below example, On 23 April 2024 RAMP user "xss_0x2" advertised access to a Switzerland-based education organisation with a revenue of over $1 billion. The stated access type was "SSH Linux", indicating access to an SSH instance on a Linux-based environment.

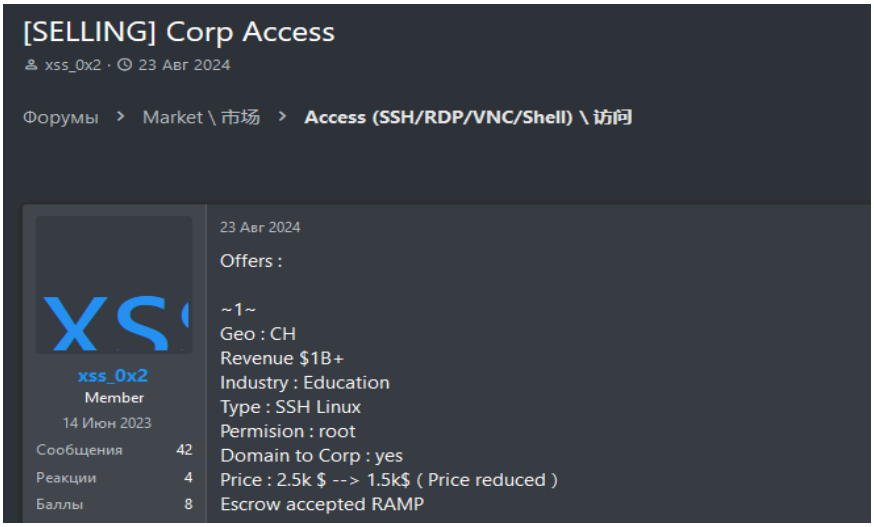

Figure 20: RAMP IAB listing advertising SHH access to a Switzerland-based education organisation.

Value when adjusted for listed revenue

The top nine most valuable access types when adjusted for revenue were **RDWeb** ($15.95 per $million in revenue), **Web shell** ($8.45 per $million), **Citrix** ($6.11 per $million), **SSH** ($4.05 per $million), **RDP** ($3.69 per $million), **VPN** ($2.07 per $million), **Forti** ($1.99 per $million), **VNC** ($1.48 per $million), and **C2** ($1.32 per $million).

RDWeb was particularly more valuable when compared to other access types. RDWeb is an implementation developed by Microsoft which allows access to remote desktop services over a web browser. RDWeb does not require the user to have an RDP client and operates by only connecting through a web browser, a flexibility that is taken advantage of by remote attackers.

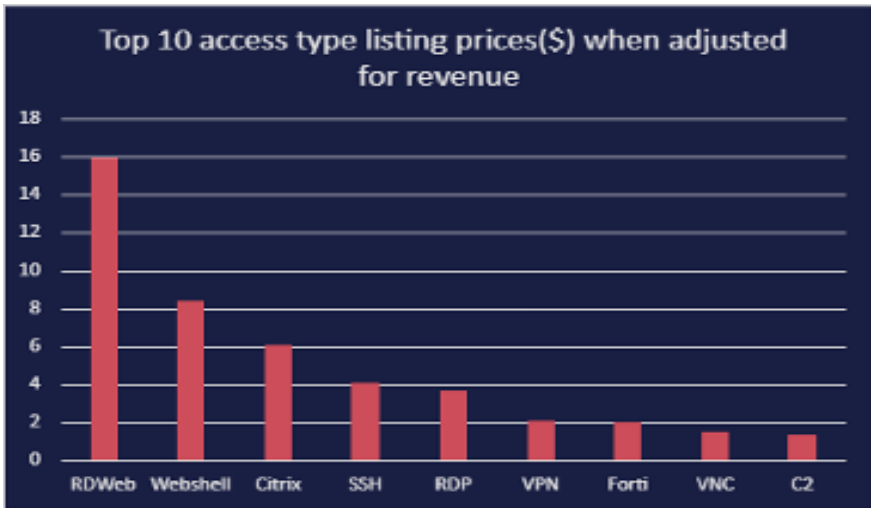

Figure 21: Graph showing price for various access types when adjusted for revenue.

07

Antivirus

The top 10 antivirus solutions active in listings in the quarter were **Windows Defender** (10.2% of all listings), **Sentinel** (3.5%), **CrowdStrike** (2.5%), **Trend Micro** (2.5%), **Webroot** (1.9%), **Sophos** (1.9%), **Kaspersky** (1.6%), **BitDefender** (1.4%), **Eset** (1.4%), and **Symantec** (0.7%).

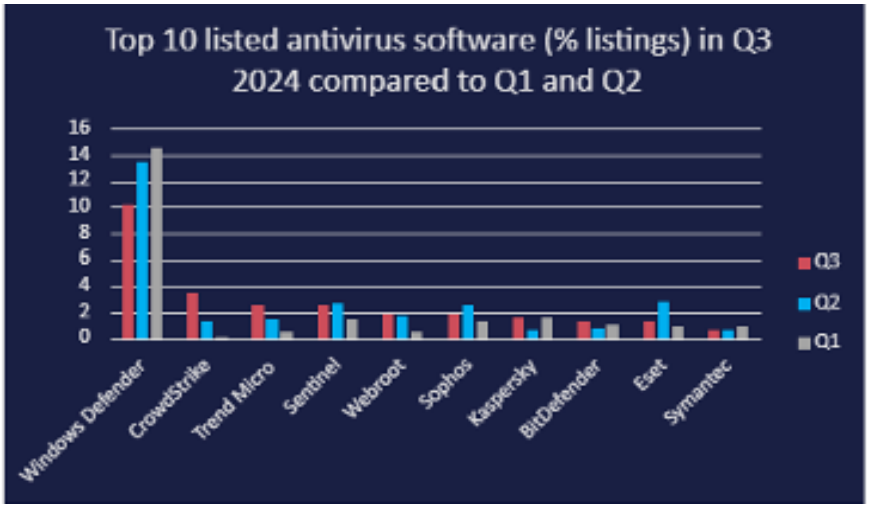

Figure 22: Graph showing the top 10 targeted antivirus solutions in Q3 2024 compared to Q1 and Q2

Windows Defender has remained the most popular and active antivirus solution on IAB listings.

Windows Defender has remained the most popular and active antivirus solution on IAB listings, highlighting the continued significant targeting of Windows-based devices. Only small percentages of access adverts list other antivirus software, and only 30.1% of listings in Q3 2024 contained antivirus information. It is possible that the ratios would change if all listings included antivirus details due to selection bias.

Kaspersky

Accesses with Kaspersky listed as the active antivirus software increased by 121.5% from Q2 to Q3 2024. In late June 2024, the US announced [9] that it would be banning the sale, resale, licensing, and updating of Kaspersky products starting from 29 September 2024, due to its ties with Russia reportedly posing a significant risk to the country's infrastructure and services. This announcement was synonymous to declaring a software to be at end of life (EoL), wherein the service would no longer be maintained after the designated date. It is realistically possible that this enticed threat actors to begin specifically targeting organisations with Kaspersky active for several reasons. For example, the antivirus was banned in the US in due to geopolitical motivations; meaning IABs with Russian ties may have intended to retaliate against this decision. However, none of the listings with Kaspersky active in Q3 were for US-based organisations.

The ban also essentially means that those in the US with the antivirus active will likely be unable to update to later versions and would, therefore, be vulnerable to flaws identified in that current version. The previously mentioned SSH vulnerability, regreSSHion, was included in a July security advisory [10] published by Kaspersky. This highlighted the versions of Kaspersky-owned software affected by the flaw. In particular, the vulnerability affects three solutions, namely Kaspersky Secure Mail Gateway, Kaspersky Anti Targeted Attack Platform, and Kaspersky Security for Virtualization Light Agent. This may have urged IABs to target vulnerable versions of the software. However, none of the related accesses were through SSH.

One possible explanation regarding both above hypotheses is that these phenomena may have enticed IABs to identify exposed organisations with active Kaspersky solutions, though the organisation's location may not be visible from initial reconnaissance. This is often conducted through active and passive scanning of exposed devices or shows that IABs took the opportunity to compromise such organisations once identified, regardless of exploitability or geographic location. Any accesses of interest to IABs are potential targets. Alternatively, it is realistically possible that the number of listings with Kaspersky as the listed antivirus solution may have simply taken more of the market share due to the reduced number of listings observed in Q3 2024.

08

Users

The top 10 most prolific IABs in Q3 2024 were **SGL** (12.3% of all listings), **Кот Ученый** (5.1%), **DNI** (4.2%), **RelativelyCrazy** (3.9%), **budda12** (3.5%), **Panchitos** (2.5%), **BarmoleyAibolitov** (2.3%), **internetBandit** (2.1%), **sudo** (2.1%), and **darksoul** (2.1%).

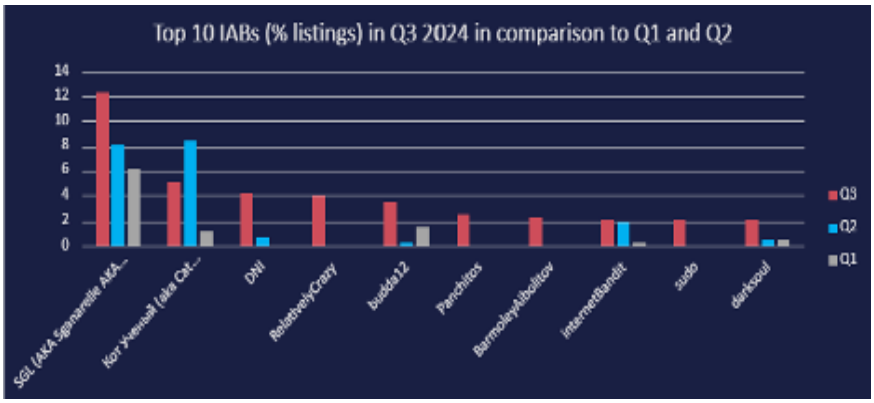

Figure 23: Graph showing top 10 most prolific IABs in Q3 2024.

SGL has remained in the top two as a prolific and established IAB. Interestingly, **SGL** is the only IAB that has remained in the top 10 in 2024, and no other IABs in the top 10 in Q1 are in the top 10 in Q3. Similarly, **SGL and Кот Ученый** are the only IABs in which appeared in the top 10 IABs in both Q2 and Q3.

Кот Ученый

Кот Ученый (Kot Uchenyy), also known as CatScientist, has steadily developed their activity from Q1. This user originally occupied 1.1% of listings in Q1, 8.1% in Q2, and 5% in Q3. The broker has continued posting all IAB listings in a single thread titled "I sell accesses" (translated from Russian), providing listing information such as revenue, country, access type, privilege level, sector, and price.

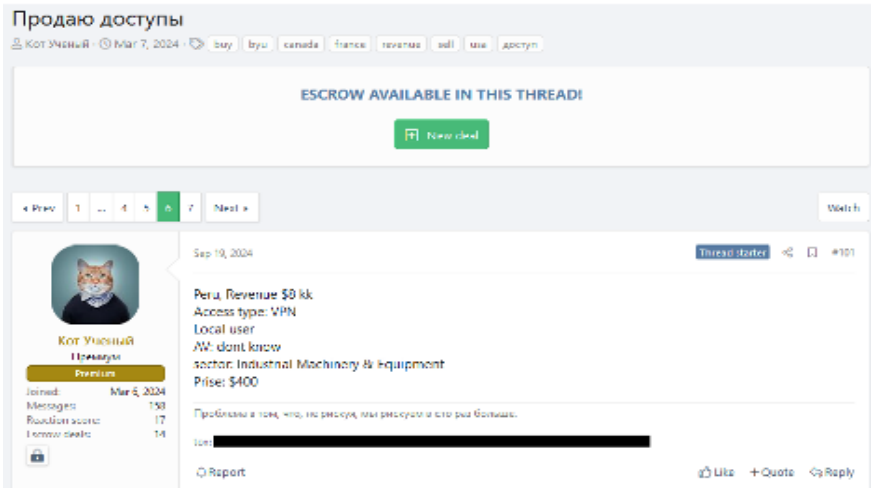

Figure 24: XSS listing by CatScientist in Q3 2024.

Further analysis of the IAB ecosystem will likely portray changes in this distribution, and these established brokers may stop posting. This could be due to them creating new accounts for operational security (OpSec) reasons. Additionally, the brokers may decide to retire from selling accesses once they have gained enough money. The IAB market has an extremely high turnover, with just 8.54% of IABs active in Q1 remaining active in Q3 2024. There is a common user retainment of 20-30% each quarter. This is likely due to the above reasons, as well as potential arbitration against these brokers.

The IAB market has an extremely high turnover, with just 8.54% of IABs active in Q1 remaining active in Q3 2024.

SGL

The most active IAB in Q3 2024 was SGL. Also known as Sganarelle, SGL is an English-speaking initial access broker (IAB) who likely began advertising initial access to corporate networks on 10 August 2023. This IAB has been active on prominent Russian-language cybercriminal forums Exploit and XSS since August 2019. SGL has primarily advertised RDP and VPN accesses with domain user privilege levels to organisations in the United States and Spain. However, information around sectors is unavailable as listings often do not contain those targeted. Whilst no concrete information regarding SGL's TTPs is available, they likely use phishing or brute forcing software to gain access and harvest credentials.

Figure 25: Screenshot of initial access listing made by SGL.

As an established IAB, SGL appears to sell only to other reputable users, and states that they will only send details to forum members with a deposit or a high reputation. This may suggest that more prolific brokers are more likely to only sell access listings to established and reputable buyers, such as ransomware groups or other known forum users.

More prolific brokers are more likely to only sell access listings to established and reputable buyers, such as ransomware groups or other known forum users.

09

Further observations

Non-standardised access descriptions

IABs are often ambiguous when describing access listings, likely to provide the minimal amount of information required to sell the access. This also means they can avoid divulging information which could lead to the identification of the victim organisation, exposing the access and preventing a successful sale and subsequent malicious activity.

There are three main ways that IABs describe accesses:

1. Accesses which occur through a technical medium or protocol, such as SSH, RDP, RDWeb, and VPN, for which access if often gained through brute force or vulnerability exploitation.
2. Access to an active instance or physical medium, such as a server, enterprise software including particular firewalls, panels, or an Active Directory (AD), for which the access method may vary. This could be facilitated through other means or protocols that remain unspecified.
3. Exceptions to the above types, where the access is more ambiguous. For example, the "Bot" access was defined in the IAB Q2 report [3], whilst other anomalous access types include "Insider", where the IAB may have contact with an employee of the organisation, or the ability to access an employee's credentials. Similarly, the "Payload" access type infers the ability to load a malware strain or other payload of the buyer's choice to the organisation, and the aforementioned "SOCKS" access type.

An example of a non-standard access type observed in Q3 2024 was "RCE", likely meaning that the broker exploited a remote code execution (RCE) vulnerability in the victim organisation. From here, the access could be sold to another threat actor to execute code for further malicious activity.

On 6 July 2024, user "Str0ng" initiated an English-language thread titled "initial access company peru 20kk" in the Accesses section of XSS. In their initial post on the thread, Str0ng advertised RCE access to an unnamed Peru-based company with a revenue of over $20 million. The broker stated that they attempted to upload a shell but were unsuccessful. However, command execution capabilities were available. Str0ng also shared alleged proof of compromise through apparent successful payload deployment on the victim's network. The broker also offered to work for percentage, wherein the broker receives a percentage of the profit derived from attacking the victim organisation, rather than a flat fee for the access.

IABs are often ambiguous when describing access listings. This also means they can avoid divulging information which could lead to the identification of the victim organisation.

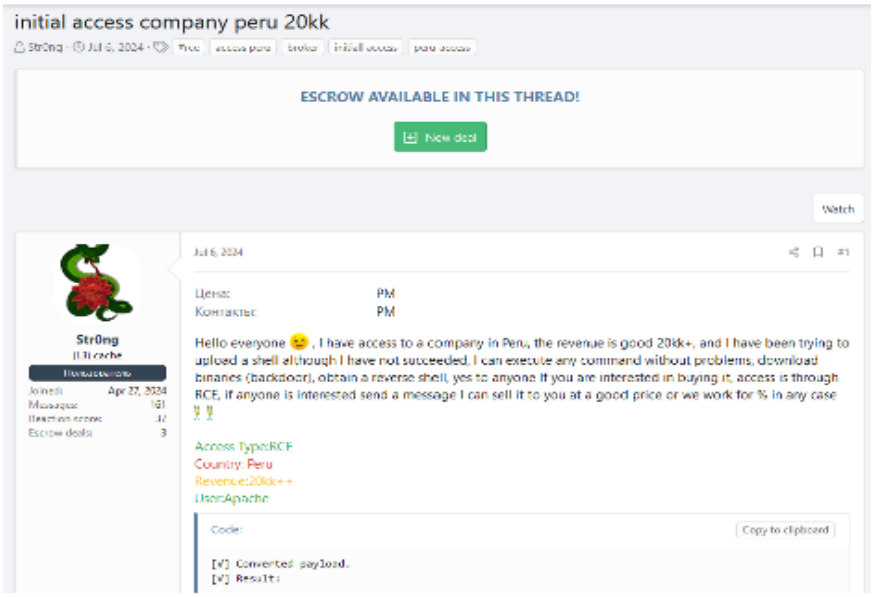

Figure 26: XSS IAB listing advertising "RCE" access to a Peru-based company

Attempts to standardise IAB listings

In July 2024, BreachForums was updated to split the "Sellers Place" into four separate markets, namely the Leaks, Leads, Exams, and Access markets. With this, the forum rules were updated to stipulate which information must be provided in any access listing. As in Figure 27, IAB listings should include the revenue and country of the victim organisation, as well as the access type being advertised.

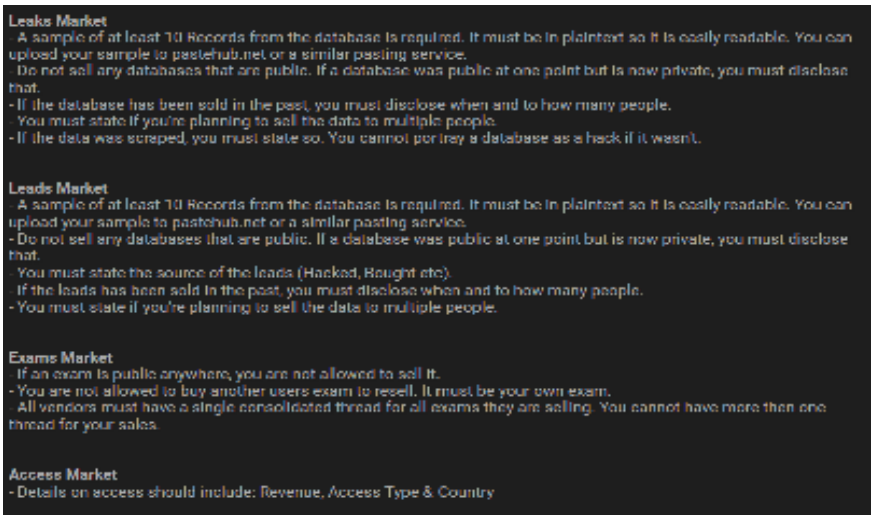

Figure 27: Screenshot of BreachForums rules regarding Sellers Place markets

Attempts to standardise IAB listings

In July 2024, BreachForums was updated to split the "Sellers Place" into four separate markets, namely the Leaks, Leads, Exams, and Access markets. With this, the forum rules were updated to stipulate which information must be provided in any access listing. As in Figure 27, IAB listings should include the revenue and country of the victim organisation, as well as the access type being advertised.

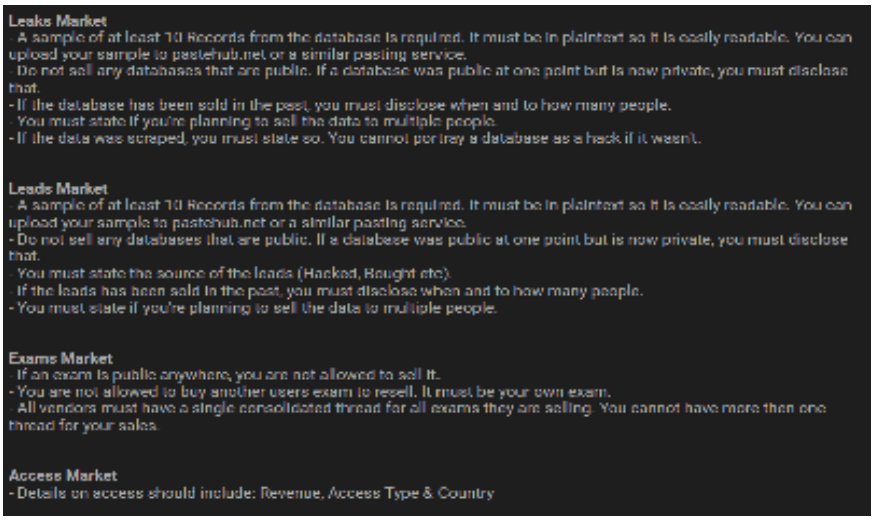

Figure 27: Screenshot of BreachForums rules regarding Sellers Place markets

Evidence of these rules being enforced can be seen in several BreachForums listings in Q3 2024. For example, previously analysed IAB listings shown in Figures 13 and 17 both included replies from IntelBroker. Here, the user asked the brokers to edit their thread and add relevant information to adhere to the rules. The example below refers to the listing for a Taiwan-based bank, indicating that the initial post in the thread was edited to include the approximate revenue of $17 billion.

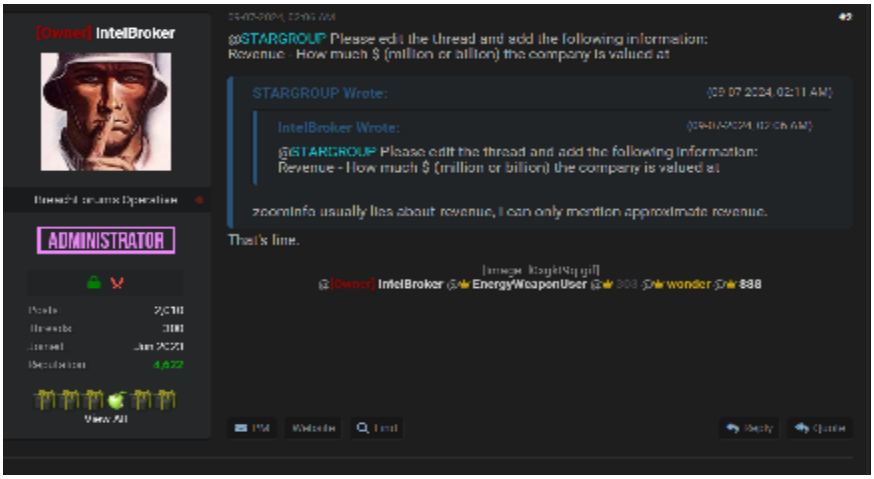

Figure 28: Screenshot of IntelBroker enforcing forum rules on IAB listing.

10

Concluding remarks

Throughout the first three quarters of 2024, the number of listings has continued to decrease whilst the average price of IAB listings increases. This has continued into Q3, though analysis of the entire year after Q4 2024 may solidify these trends. Brokers are emerging and disappearing with extremely high turnover, though there appear to be few constant brokers such as SGL and CatScientist. Western countries are still highly targeted, while sectoral targeting continues to appear opportunistic. VPN and RDP remain the most popular access types, though less commonly targeted types vary widely, as seen in previous quarters. Finally, both organisations with revenues of less than $5 million, as well as multi-billion-dollar companies, are still being advertised. This solidifies the assessment that any organisation of any size is at risk of compromise and may be abused for monetary gain in the IAB market. CYJAX will continue to track and analyse the IAB market into Q4 2024 and beyond.

Endnotes

1 https://www.CYJAX.com/resources/blog/initial-access-brokers-explained/
2 https://www.cyjax.com/initial-access-broker-market-summary/
3 https://www.CYJAX.com/resources/blog/initial-access-broker-market-q2-summary/
4 https://www.theregister.com/2024/10/22/taiwans_ai_chip_boom_sparks
5 https://www.darkreading.com/cyber-risk/mideast-turkey-cyber-threats-spike-defense-changes
6 https://www.ransomware.live/map/TR
7 https://www.qualys.com/2024/07/01/cve-2024-6387/regresshion.txt
8 https://blog.qualys.com/vulnerabilities-threat-research/2024/07/01/regresshion-remote-unauthenticated-code-execution-vulnerability-in-openssh-server
9 https://cybernews.com/news/kaspersky-ban-us/
10 https://support.kaspersky.com/vulnerability/list-of-advisories/12430#120724

About Cyjax

Cyjax was formed in 2012. Working closely with the financial sector, we developed technologies and methodologies to help stem the advance of digital threats impacting banks and consumers around the world. We quickly established ourselves as a leading provider of cyber threat intelligence capabilities across all industry verticals, a journey we continue today. Cyjax is built on its own growth and remains wholly owned by its founding members in the UK.

Cyjax Limited
The Old Chapel, Union Way
Witney
Oxon OX 6HD

info@cyjax.com
+44 (0)20 7096 0668
www.cyjax.com