Cyberint

Initial Access Brokers Report

August 2024

Table of Contents

Executive Summary

Initial Access Brokers (IABs) are threat actors who infiltrate networks, systems, or organizations and sell this unauthorized access to other malicious actors. Instead of executing the entire cyberattack, IABs focus on the initial breach and monetize it by selling access to compromised systems. They assist ransomware operations, particularly RaaS schemes, by streamlining attacks and reducing workload at the start.

The report, based on data from Cyberint's research team over the past year and a half on leading dark web forums, highlights that the US was the prime target of IABs in 2023, with over 48% of attacks targeting the country. In 2024, France and Brazil have been increasingly targeted. IABs target various industries, with the business services sector being the most frequently targeted, similar to ransomware trends. The retail industry has remained consistently in the top 3 in 2023 and 2024, but the manufacturing industry has been increasingly targeted in 2024, creeping up from just 14% of attacks in 2023 to 23% in 2024.

In 2024, large-scale organizations were the most targeted due to their high revenue potential. Threat actors increasingly targeted organizations with over $1 billion in revenue, making up 27% of all initial access listings for sale. This increased the average revenue of IAB attacks to $1,961,335,406.50, representing a 1000% increase.

There are three primary types of IABs driving most ransomware attacks today. In 2023, those offering servers compromised through exposed Remote Desktop Protocol (RDP) were the most common (>60%). However, in 2024, VPN access surged, challenging RDP access for the top spot (45% VPN vs. 41% RDP).

Most IAB posts fall within a price range of $500 to $2,000 for corporate access, though high-value listings occasionally appear, exceeding $10,000.
Protecting against IABs requires a multi-layered security approach, implementing both technical and organizational measures to minimize vulnerabilities.

Most Targeted Countries by IABs in 2024

USA	France	Brazil
42%	**19%**	**9%**

Most Targeted Industry by IABs in 2024

Business Services
36%

1,000%
Increase in Average Revenue of IAB Attacks

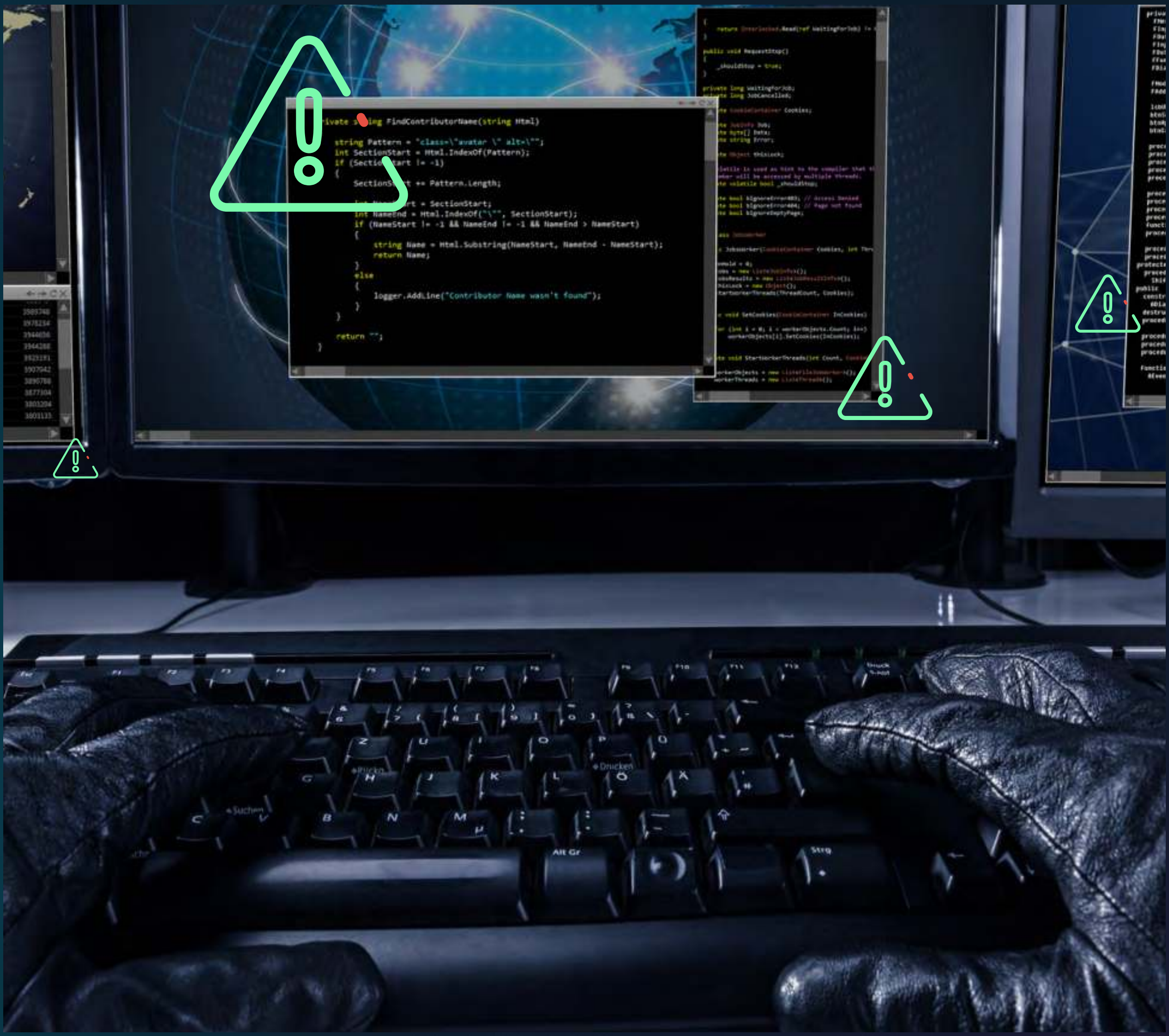
Introduction

Ransomware attacks, data breaches, leaks, espionage, and other significant cybersecurity incidents often originate from access purchased on dark web forums and marketplaces.

How do cybercriminals acquire this access? They buy it from Initial Access Brokers (IABs).

IABs are cybercriminals or groups that specialize in infiltrating networks, systems, or organizations and then selling this access to other malicious actors. Instead of carrying out the entire cyberattack themselves, IABs focus on the initial breach, which they monetize by then selling access to the compromised systems.

This report highlights data analyzed by Cyberint's research team over the past year and a half, gathered from prominent underground forums and marketplaces on the dark web. The data encompasses all the information we extracted from a single listing, allowing us to delve into details such as targeted countries, industries, average prices, organizational revenue, security products in use, number of hosts, and more.



```
rivate s  ing FindContributorName(string Html)

    string Pattern = "class=\"avatar \" alt=\"";
    int SectionStart = Html.IndexOf(Pattern);
    if (Sectio  tart != -1)
    {
        SectionS   t += Pattern.Length;

                 rt = SectionStart;
        int NameEnd = Html.IndexOf("\"", SectionStart);
        if (NameStart != -1 && NameEnd != -1 && NameEnd > NameStart)
        {
            string Name = Html.Substring(NameStart, NameEnd - NameStart);
            return Name;
        }
        else
        {
            logger.AddLine("Contributor Name wasn't found");
        }
    }

    return "";
}
```

What is an IAB?

An Initial Access Broker (IAB) is a threat actor specializing in infiltrating computer systems and networks, then selling unauthorized access to other malicious actors. IABs are skilled at identifying and exploiting security vulnerabilities, providing services to ransomware groups and other threat actors. IABs perpetuate malicious activities and enable entry into compromised systems by acting as intermediaries.

IABs are skilled at exploiting common hacking techniques to gain unauthorized access to networks, leveraging social engineering attacks, brute force attacks, and other attack vectors. The asking price for IAB services depends on factors such as the size and type of the target and the type of access offered.

By selling access instead of carrying out attacks themselves, IABs mitigate the risks associated with executing a ransomware attack, focusing instead on breaching networks and capitalizing on their expertise.

IABs primarily operate on dark web forums and underground markets and can function as individual actors or as part of larger organizations like Ransomware-as-a-Service (RaaS) gangs. Their clientele consists of groups with malicious intent who leverage the purchased access to launch ransomware attacks, execute data breaches, and engage in other malicious activities—typically for financial gain.

Dangers of IABs

In general, IABs help ransomware operations, particularly RaaS schemes, to streamline their attacks and reduce their workload at the beginning of an attack. IABs take on the difficult work of finding targets and gaining access. In doing so, they enable ransomware groups to attack at scale because they're not wasting time trying to secure a foothold in target networks. They can immediately procure that access via an IAB and get to work encrypting the victim's data.

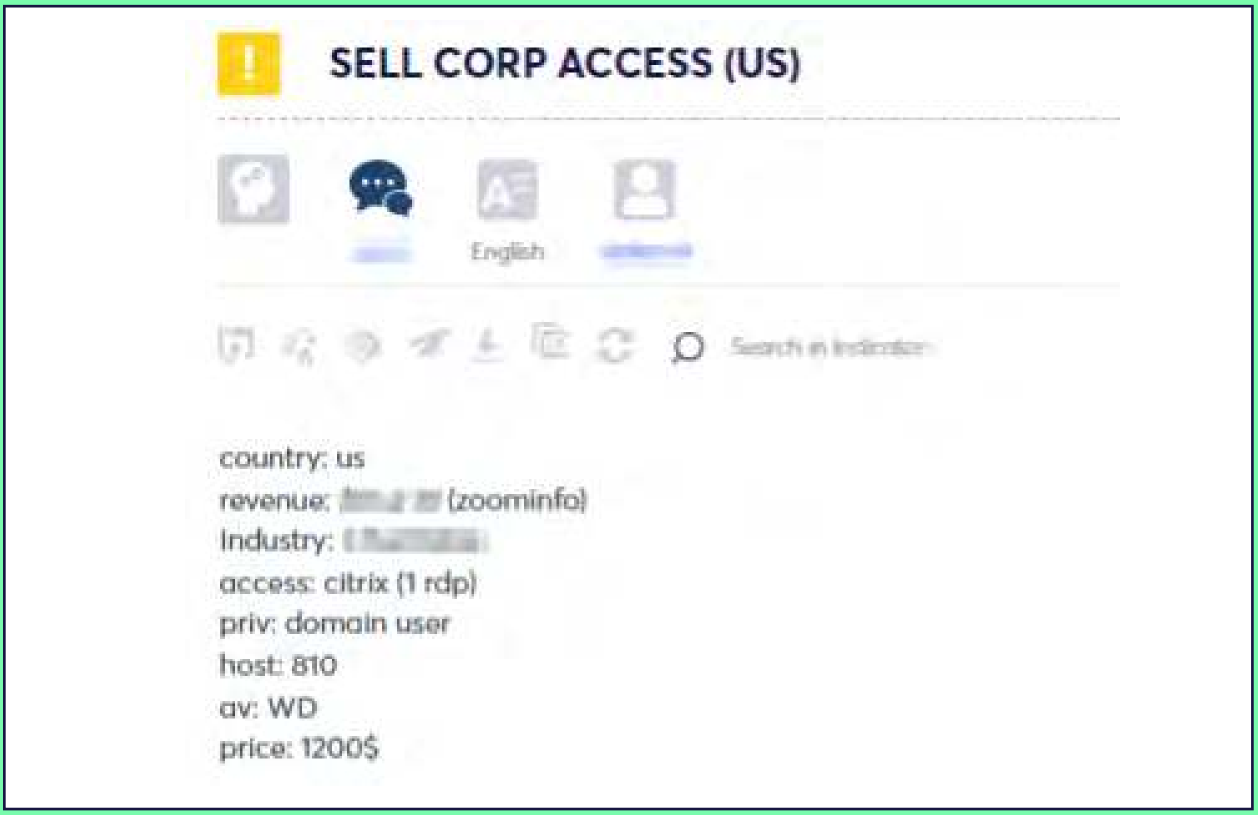
With certain RaaS groups, the benefit of working with IABs goes a step further. Evidence suggests that some IABs work directly for ransomware groups or affiliates of RaaS groups. This significantly speeds up a ransomware attack, as affiliates can leverage procured access and almost immediately conduct their attack rather than wasting time gaining access. The IAB passes access to the affiliate, who then launches the attack, infects the victim's network, and in turn passes things off to other parts of the operation to cash out.

Such direct collaboration doesn't just benefit RaaS groups. It also helps IABs. As discussed by Ransomware.org, IABs who work for RaaS groups don't need to advertise their services publicly on underground forums. They already have steady work, so there's no need to market themselves for more. This comes with the added bonus of reduced public visibility, which provides cover when law enforcement shuts down a marketplace and goes after its members.

Dive-in

Initial Access Brokers (IABs) serve as intermediaries in ransomware attacks and data breaches, becoming increasingly vital with the rise of Ransomware-as-a-Service (RaaS). Their services are in high demand, as seen in the growing number of dark web listings over recent years. These brokers typically advertise access to compromised organizations with vague details, attracting ransomware operators, state-sponsored actors, and hacktivists looking for potential targets. Listings on cybercriminal forums generally follow certain conventions: vendors avoid directly naming the targeted organizations to keep victims unaware of their compromise before the access is sold. Instead, they provide a vague description, often mentioning the victim's location, industry, revenue, and the type and privilege level of access being sold, along with technical details like the number of employees, hosts, antivirus used, and accessible data. Some IABs sell access individually, while others offer it in bundles. Highly trusted IABs may not advertise specific access at all, relying on pinned posts to indicate they sell initial access, requiring interested buyers to contact them privately for more information. On many Russian forums, vendors often use criminal slang and other writing conventions to further obscure details from outsiders.

Let's look at the example below (figure 1), where a familiar seller from a known underground Russian hacking forum is offering access to an American corporation for sale.
The access is by RDP session, using the Citrix platform to connect. Moreover, we can see the revenue and industry (which are obfuscated due to security reasons), the privilege (domain user), and the number of hosts, which is an indication of the number of employees, machines and users on the active directory. The price for that access stands at $1200.



country: us
revenue: [redacted] (zoominfo)
Industry: [redacted]
access: citrix (1 rdp)
priv: domain user
host: 810
av: WD
price: 1200$

Figure 1: United States corporation offered for sale on the underground

Countries

Initial access brokers, much like other cybercriminals such as ransomware gangs, carefully select their targets. They focus on the most competitive markets where they have the greatest chances of gaining access and selling it at the highest price while maximizing its attractiveness. And yes, you guessed it—the United States of America is their prime target.

The U.S. is the most targeted country in almost any cyber security matter. As we can see from the graph below, during 2023 the U.S. remained the number one targeted country by initial access brokers

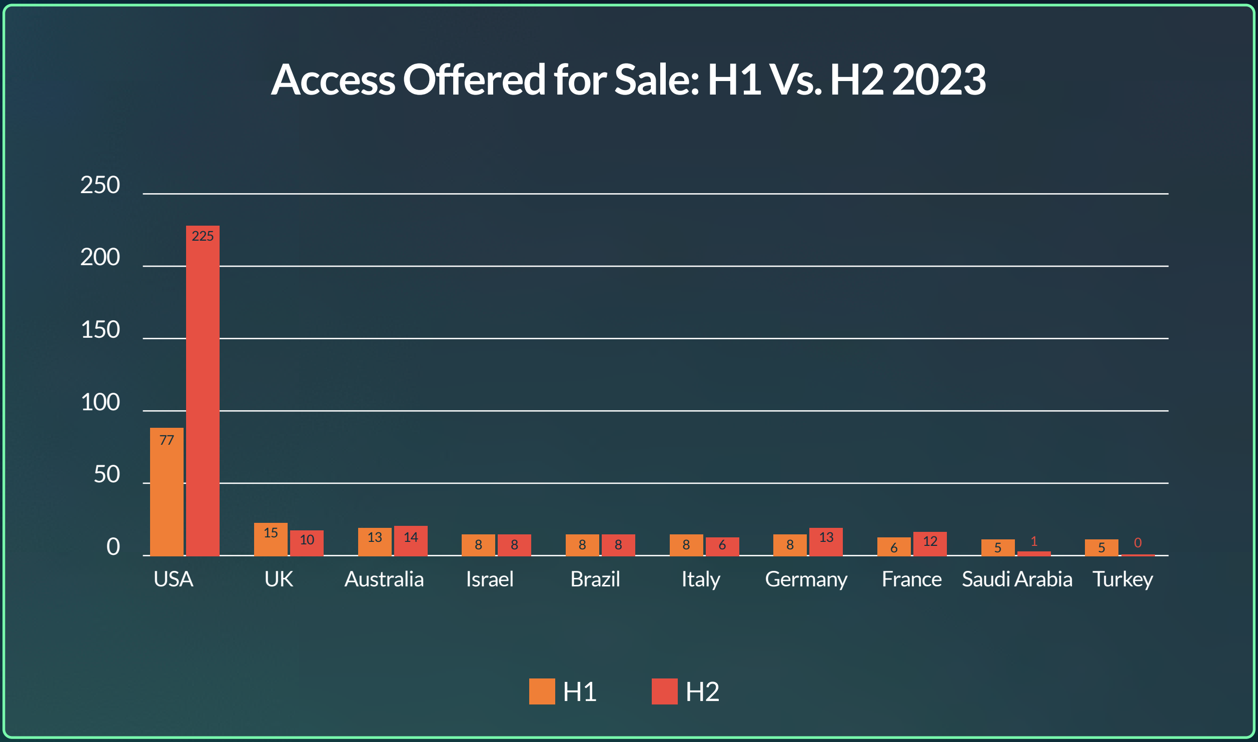


Figure 2: Access offered for sale in 2023, comparison between H1 and H2

Organizations in the U.S. are most targeted in cybersecurity attacks, and as we can see most threatened by IABs as well for several reasons:

Economic and Technological Power:

The U.S. is home to many of the world's largest and most influential corporations, financial institutions, and technology companies. These entities hold vast amounts of sensitive data, intellectual property, and financial assets, making them lucrative targets for cybercriminals.

Valuable Data:

U.S. companies and government agencies store significant amounts of personal data, intellectual property, and classified information. Theft or manipulation of this data can be extremely valuable for cybercriminals, foreign governments, or hacktivists.

High-Value Targets:

The presence of many high-value targets in both the public and private sectors, including government agencies, multinational corporations, and financial institutions, makes the U.S. a prime target for cyber-attacks.

As observed, the trend of targeting U.S. organizations more than any other country in the world continues in the first half of 2024 (see figure 3). Notably, France has moved into the top 10, securing the second spot with 50 unique initial access listings available for sale targeting organizations based there.

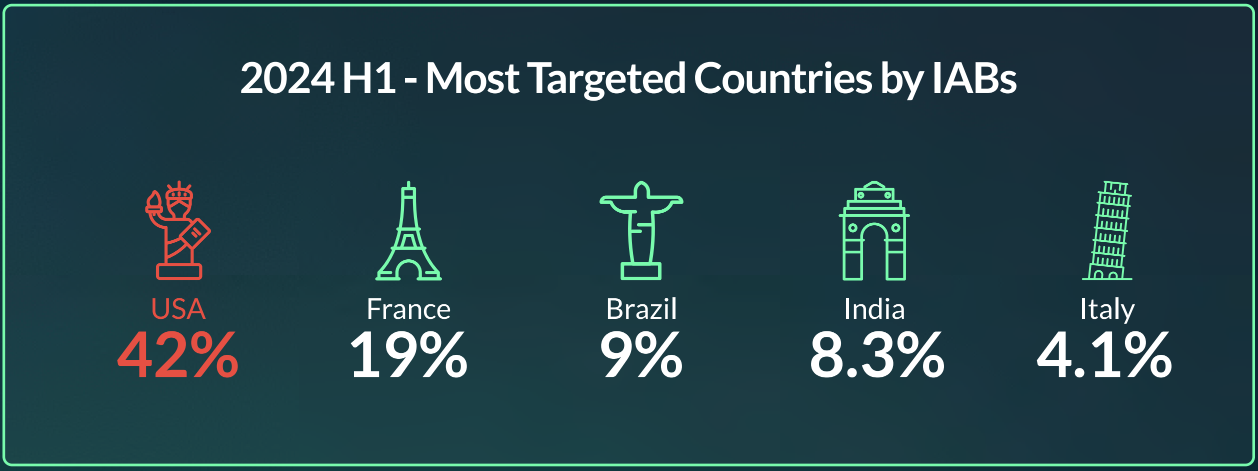


Figure 3: Most targeted Countries by IABs in the first half of 2024

Targeted Industry

The industry of an organization in an initial access listing for sale can provide several important insights:

Potential Value of Access:

Different industries have varying levels of data sensitivity, financial resources, and operational impact. For example, access to organizations in industries such as finance, healthcare, or critical infrastructure that hold sensitive data is critical to daily operations, which makes it more valuable and a prime target for further exploitation or ransomware attacks.

Revenue and Financial Resources:

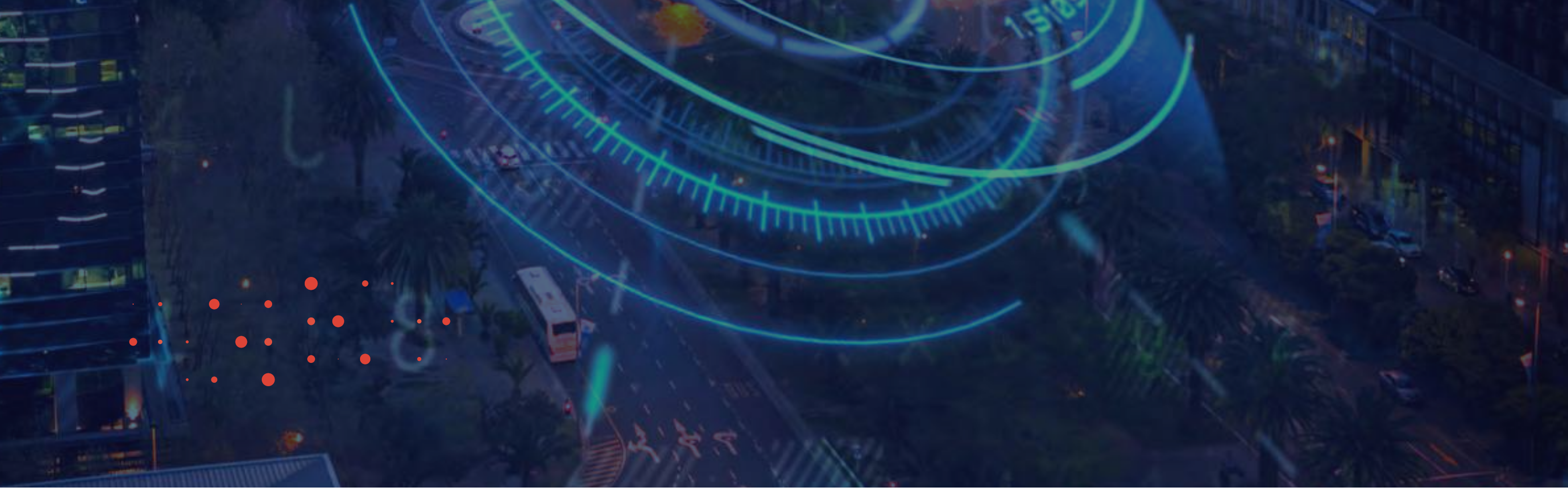
The industry often correlates with the organization's revenue and financial resources. Higher-revenue industries such as technology, oil and gas, or pharmaceuticals might be more willing to pay a higher ransom to regain control, making access more valuable.

Supply Chain Implications:

Access to an organization in a critical industry could have ripple effects across its supply chain. For example, targeting a company in the manufacturing sector could disrupt production lines and affect multiple businesses downstream.

Likelihood of Detection and Response:

Some industries, particularly those in highly regulated environments such as finance or defense, may have more robust cybersecurity measures in place. This could affect the ease with which the access can be used without detection and the potential for a swift response.



IABs target various industries, with the business services sector being the most frequently targeted, similar to trends observed in the ransomware landscape. However, it's important to recognize that the numbers may not fully capture the situation, as some listings lack information about the industry, which could potentially alter the statistics. That said, more than 75% of the listings do include the sector name, providing a solid foundation for these statistics.

Top 5 Targeted Industries by IABs in 2023

Business Service	Finance	Retail	Technology	Manufacturing
29%	21%	19%	17%	14%

Figure 4: Top five industries by Initial access brokers in 2023

In 2024, the business services sector continues to lead as the most targeted industry, while the financial sector has seen a significant drop, decreasing by 50% compared to the average number of listings in each half of 2023. Additionally, the education sector has become a more frequent target this year, rising to the fifth spot on the list.

Top 5 Targeted Industries by IABs in 2024

Business Service	Manufacturing	Retail	Technology	Education
36%	23%	18%	14%	9%

Figure 5: Top five industries by Initial access brokers in 2024

Revenue

Revenue is likely the key field for buyers to look at before buying access from the sellers. Revenue provides an indication of the size of the company. Higher revenue often suggests that the company has a significant market presence, a large customer base, or a broad product or service offering. Moreover, revenue reflects the demand for the company's products or services.

As a result, the largest organizations became more sought-after targets for access brokers, largely because of the increased income from the higher price they will demand. Not surprisingly, we see this trend of targeting large scale organizations took place in 2024, with an **average revenue of $1,961,335,406.50, which indicates an approximately 1000% increase**

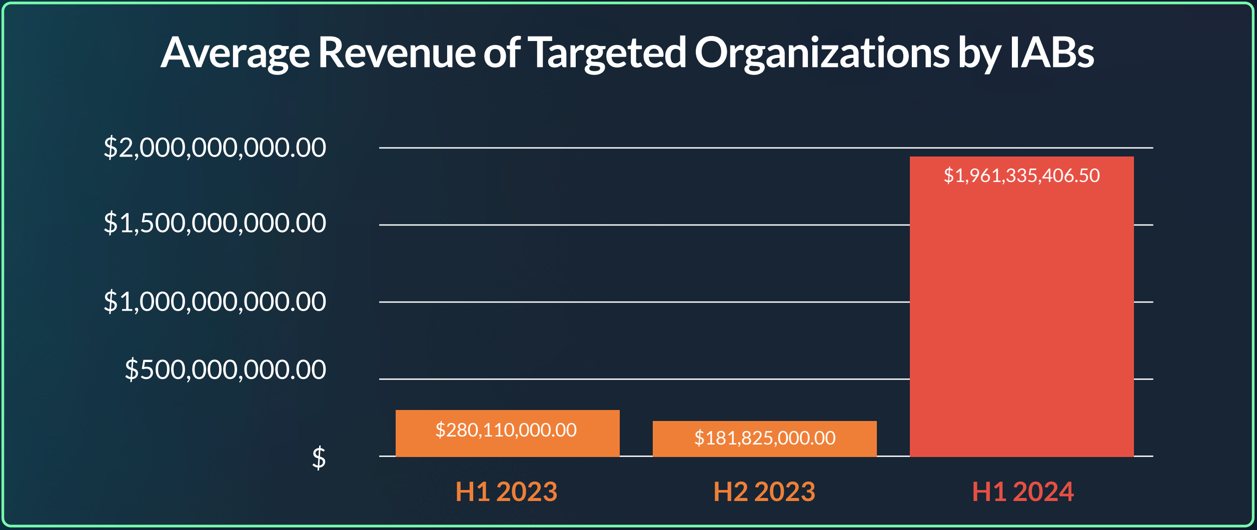


Figure 6: Average Revenue of Targeted Organizations by IABs

Usually, threat actors take the revenue data from known data sources providers, such as ZoomInfo. From the data we collected in 2023, we noticed that there are 4 major groups we can divide the targeted organizations' revenue into, as seen in the graph below.

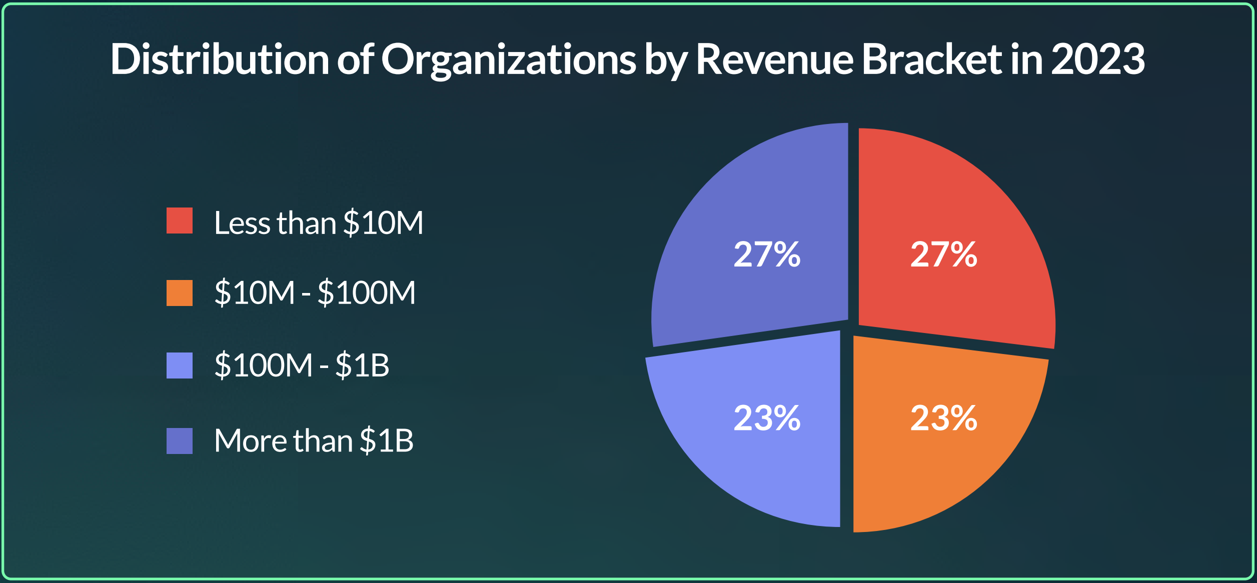


Figure 7: Distribution of Organizations by revenue bracket in 2023

However, the second quarter of 2024 shows a different distribution compared to 2023 and the first quarter of 2024. Threat actors are increasingly targeting organizations in the highest revenue bracket, with over $1 billion in revenue, making up 33% of all initial access listings for sale.

Additionally, the average revenue and distribution of organizations by revenue bracket over the past year and a half indicates that threat actors are focusing more on larger organizations. They are increasingly targeting the higher end of each revenue group, particularly in 2024, as they aim to carry out operations on a larger scale.

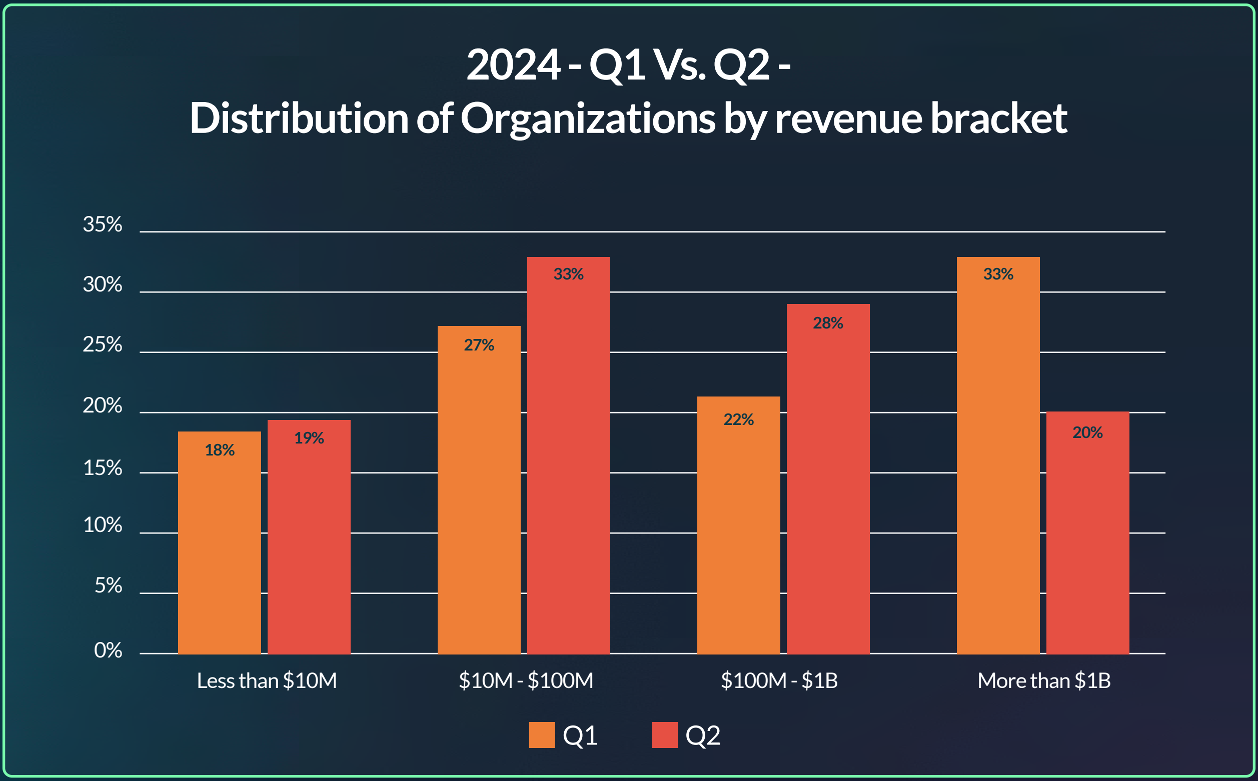


Figure 8: Distribution of Organizations by revenue bracket in both quarters of 2024

Access Type

IABs offer various types of access and privileges to compromised systems and networks. These access types and privileges can vary widely in terms of what they enable a buyer to do within a target organization.

There are three primary types of initial access brokers driving most ransomware attacks today: those selling access to systems compromised with backdoors or malware, those offering servers compromised through exposed Remote Desktop Protocol (RDP), and those dealing in compromised network devices. Brokers selling backdoored systems offer access to computers infected with malware, often within corporate networks, which are then sold to other cybercriminals, including ransomware groups. Brokers targeting RDP systems sell access to corporate servers compromised through brute-force attacks on unprotected systems with weak credentials. Finally, brokers exploit known vulnerabilities in network devices such as VPN servers and firewalls to gain control of internal networks, selling this access to threat actors on the dark web.

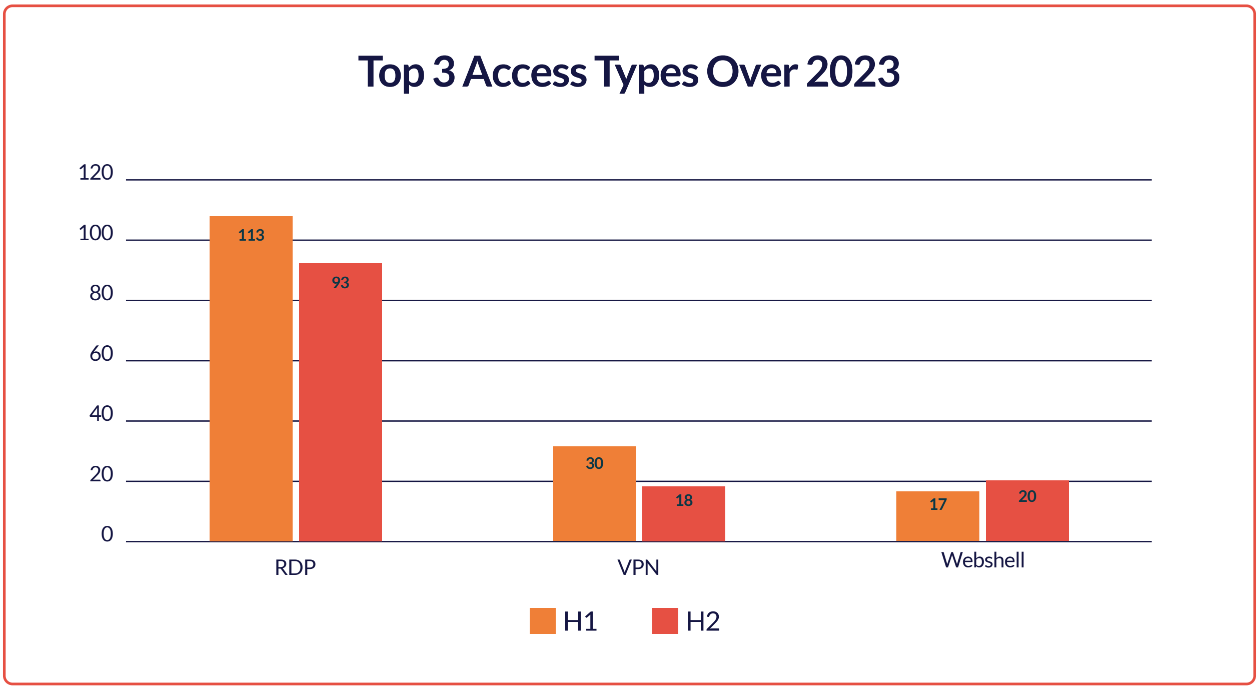


Figure 9: Top 3 Access Types over 2023

As shown in figure 9, **RDP access** was by far the most frequently offered type for sale. This suggests that RDP-related products and activities were particularly vulnerable to attacks by threat actors, who frequently employed techniques to steal credentials.

However, as we've observed various shifts in 2024 concerning IAB targets, VPN access has surged by hundreds of percentage points compared to 2023, challenging RDP access for the top spot (figure 10).

Top 3 Access Types in Initial Access Listings for Sale in H1 2024

VPN	RDP	Shell/Webshell
144	**133**	**20**

Figure 10: Top 3 Access types in Initial access Listings for Sale in 2024 H1

Generally, these are the most common types of access types:

- **Remote Desktop Protocol (RDP) Access:** This type of access allows the attacker to remotely control a compromised computer or server as if they were physically present at the machine.

- **VPN Access:** VPN access enables the attacker to connect to the organization's network through a virtual private network, mimicking legitimate remote access

- **Email Access:** Access to email accounts, often through compromised credentials, allows attackers to read, send, and manipulate emails.

- **Database Access:** This involves direct access to the organization's databases, typically through stolen credentials or exploiting vulnerabilities.

- **Web Shell Access:** A web shell is a script that allows remote administration of a web server. It provides an interface to execute commands on the server.

- **Shell/Command-Line Access:** This provides the attacker with a command-line interface to the compromised system, allowing them to execute commands directly.

- **File Share Access:** Access to shared drives and file servers within an organization, often through compromised credentials or lateral movement.

Privilege

User Authentication is a big deal in any organization. In most outfits, this is done through Windows. They deal with their users by making use of an Active Directory Server. In IAB sales we often see 3 types of privileges:

Domain Admin

A Domain Administrator is basically a user authorized to make changes to global policies that impact all the computers and users connected to that Active Directory organization. They have permission to go anywhere and do anything, with the limitation that they must remain within that specific outfit.

Local Admin

A Local Admin has permission to do anything but is restricted to one machine

Domain User

A Domain User Account refers to an account created on a Domain Controller (DC) in an Active Directory (AD) domain, which allows users to access various domain resources such as servers, file shares, printers, websites, and AD settings. These accounts are stored in the AD database and are replicated to all DCs in the domain, making them the preferred method for providing access to a Windows network. However, their level of rights in the domain could be any level granted to them.

As you might expect, the higher the privilege level, the more valuable the access becomes, which in turn drives up its price. **According to our data, the average price for "Domain Admin" privilege is 85% higher than the average price.**

According to figure 12, Domain Admin and Local Admin were the most common privilege types offered for sale as part of the initial access information provided. In general, they share almost 80% of all privilege types we collected in H1 2023.

However, the second half of 2023 was a bit different. Here we saw an increase in domain user privilege type, which made the distribution between these 3 privilege types more equal.

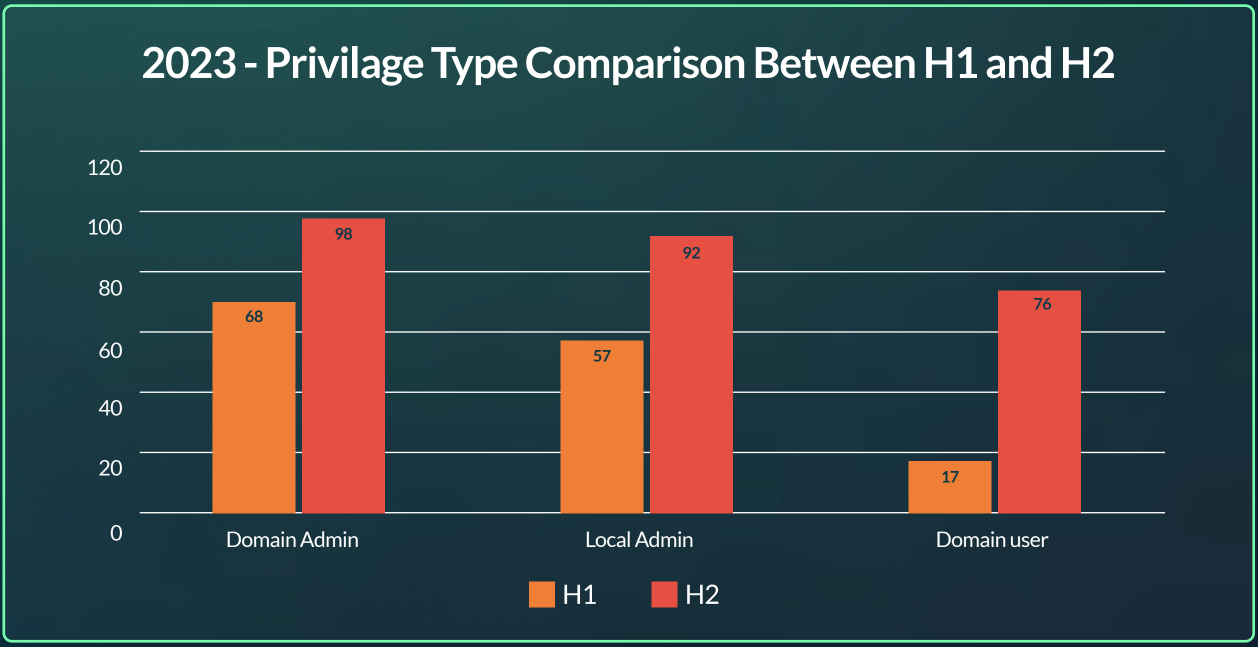


Figure 12: Top 3 Privilege types in Initial Access Listings for Sale in 2024 H1

In 2024 things have remained in order, as we can see in the graph below, the "Domain user" privilege type is the most common with 107 instances. The distribution remains as follows in 2024.

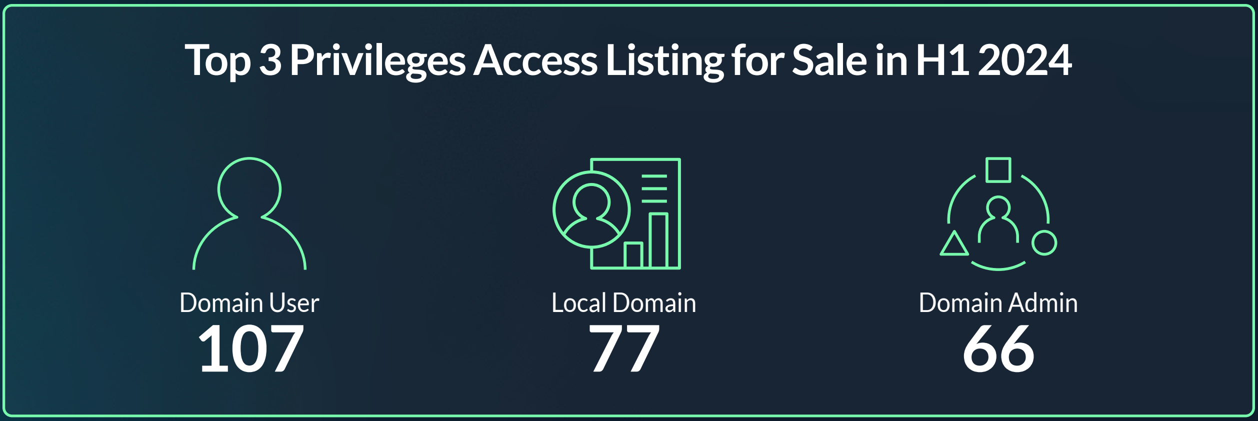


Figure 13: Top 3 Privilege types in Initial Access Listings for Sale in 2024 H1

Generally, we observed different privilege types offered as part of the access sale but in very small numbers compared to the other three mentioned, such as:

- **Enterprise Admin:** A highly privileged account in a Windows domain, capable of managing all aspects of the Active Directory Forest.
- **Server Operator:** Typically, could log onto servers, backup and restore files, and perform other server management tasks, but without full administrative rights.
- **Network Administrator:** Responsible for managing and maintaining network infrastructure, with access to network devices like routers, switches, and firewalls.
- **Database Administrator (DBA):** Manages and maintains databases, with access to all data in the database systems and control over database configurations.
- **Guest User:** Very limited privileges, typically used for temporary access or minimal access to a system.

Access Prices

The majority of IAB posts fell within a relatively narrow price range, typically between $500 and $2,000 for corporate access. However, on occasion, a particularly high value listing appears, offering access to a uniquely valuable environment, which can drive prices into the tens of thousands of dollars, with some listings exceeding $10,000.

In 2023, the average price for a listing was $3,066, while the median price was $1,500. Despite these figures, it's important to note that 65% of listings in 2023 were priced under $2,000, and 77% were under $3,000. The higher average price is skewed by these high value listings, where prices can be significantly higher, sometimes hundreds of percent above the average.

2023 IABs Average Listing Price

Less than $1,000	$1,000 - $2,000	$2,000 - $3,000	$3,000 and Above
31%	34%	14%	21%

Figure 14: Initial access brokers average price listings in 2023

In 2024, threat actors have shifted their focus to targeting higher-revenue organizations, yet they have reduced the prices relative to the access value of these organizations. **The average price has dropped significantly to $1,295, which is an approximately 60% decrease.**

As illustrated in the chart below, the vast majority of listings are now priced under $1,000, a notable change from what we observed in 2023. The proportion of high value accesses has also decreased, now accounting for only 9% of all listings available for sale.

It's important to highlight that there are hundreds of listings at these lower average prices, which can still cause significant damage and provide threat actors with substantial financial gain, even more so than the more expensive listings.

2024 IABs Average Listing Price

Less than $1,000	$1,000 - $2,000	$2,000 - $3,000	$3,000 and Above
62%	24%	6%	9%

Figure 15: Initial access brokers average price listings in H1 2024

Security Products

Most listings for sale pertain to personal machines of users, could allow an attacker to control various systems and private databases depending on the access type and privileges. However, purchasing initial access does not guarantee that the attacker will avoid detection or capture during their activities.

This is why the brokers sometimes add another information field to the listing called “AV”, which is a short cut for “Anti-Virus”. Not all the listings contain this information, whereas almost 40% don’t provide this information. Still, we extracted enough information from thousands of listings to create a picture of the leading security products that were installed on the compromised machines.

The graph below shows that over 60% of the machines are only equipped with Windows Defender, highlighting a significant security gap within the organization. This suggests a lack of additional protective software, which could leave these systems more vulnerable to attacks.

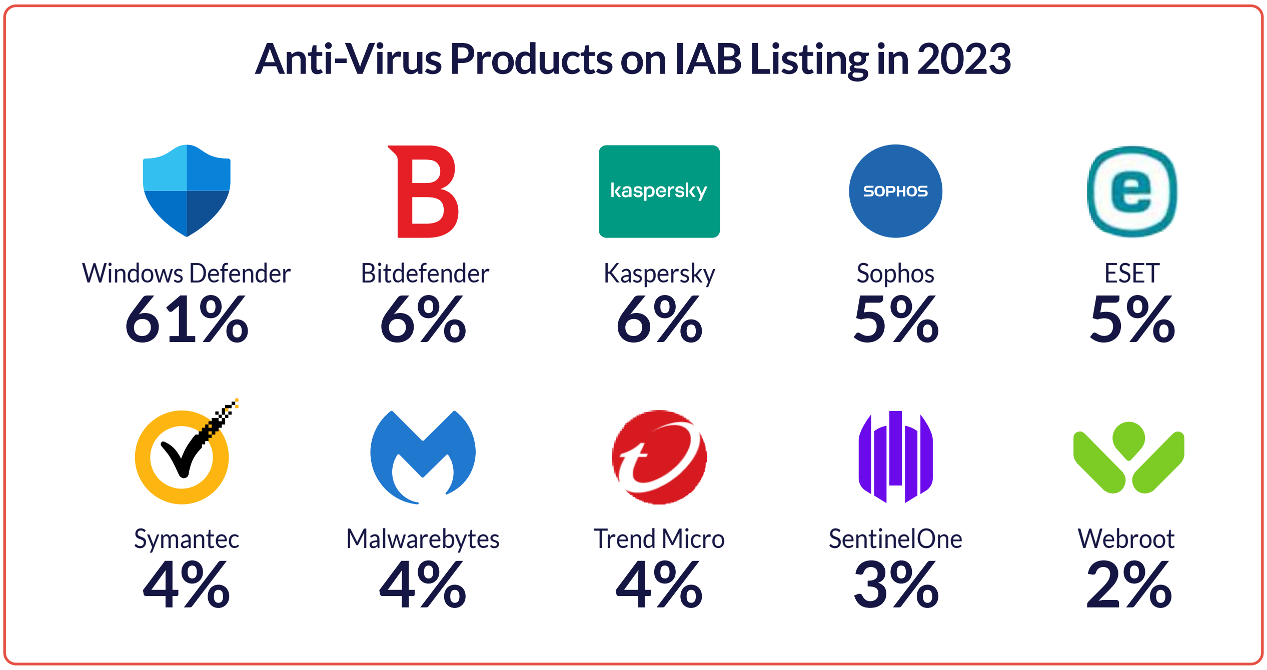


Figure 16: Security product on compromised machines on IABs listings 2023

In 2024, the trend continues with initial access brokers predominantly offering machines for sale that only have the default Windows Defender as their security product.

It's worth noting that there might be additional security measures on the compromised accounts that the broker either couldn't detect or overlooked.

The presence or type of security product on a compromised account doesn't necessarily reflect the value of the access or the organization itself. There are listings with only Windows Defender that are priced higher than accounts protected by three security products.

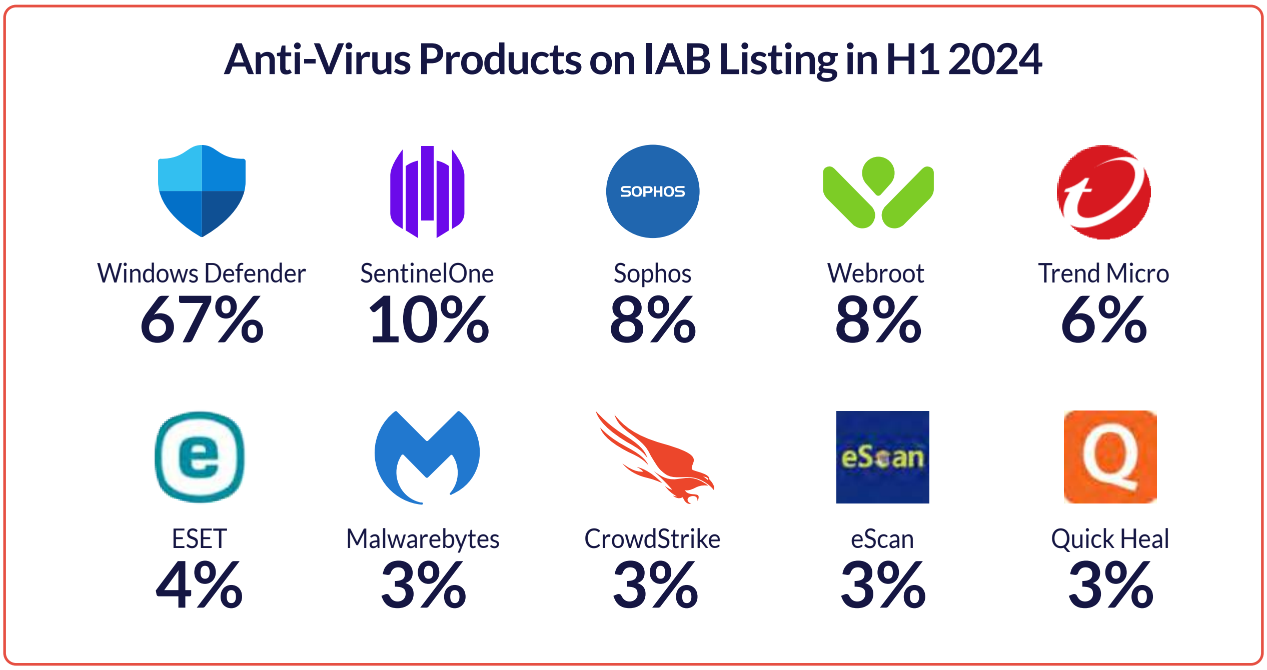


Figure 17: Security product on compromised machines on IABs listings 2024

Conclusions

IABs are a critical part of the broader cybercrime ecosystem. They provide the necessary foothold for more destructive activities like ransomware attacks, data breaches, and espionage, effectively lowering the barrier to entry for less technically skilled cybercriminals who can purchase ready-made access rather than gaining it themselves.

Protecting yourself and your organization from IABs requires a multi-layered approach to security. Since IABs specialize in gaining unauthorized access to networks and systems, it's crucial to implement both technical and organizational measures to minimize vulnerabilities.

Recommendations

Implement Strong Authentication Measures

- **Use Multi-Factor Authentication (MFA):** MFA adds an extra layer of security by requiring users to provide two or more verification factors to gain access to a resource such as an application or online account.

- **Enforce Strong Password Policies:** Require strong, unique passwords that are regularly updated. Encourage the use of password managers to help users manage complex passwords.

Patch and Update Regularly

- **Keep Software Up to Date:** Regularly update operating systems, applications, and software to patch vulnerabilities that could be exploited by attackers.

- **Patch Management:** Implement an effective patch management process to ensure that security patches are applied as soon as they are released.

Limit Privilege Access

- **Principle of Least Privilege (PoLP):** Restrict access rights for users to the bare minimum permissions they need to perform their work.

- **Regular Audits:** Regularly review user accounts and permissions to ensure that they are appropriate and up to date.

Secure Remote Access

- **Restrict RDP Access:** Disable Remote Desktop Protocol (RDP) if it's not needed. If necessary, ensure it is secured behind a VPN or other secure method of access.

- **Monitor Remote Connections:** Keep track of remote access attempts and consider using tools that alert you to unusual or unauthorized access attempts.

Monitor Deep & Dark Web Activity

- **Threat Intelligence:** Use threat intelligence services to monitor dark web forums and marketplaces where IABs may sell access to compromised networks. Early detection can help you take preventive actions.

- **Implement Network Security Measures:**
  - **Firewall and Intrusion Detection Systems (IDS/IPS):** Deploy and properly configure firewalls and intrusion detection/prevention systems to monitor and block unauthorized access.

  - **Network Segmentation:** Segment your network to limit the spread of attacks if a system is compromised.

Regular Security Training and Awareness

- **Educate Employees:** Conduct regular security training to help employees recognize phishing attacks and other social engineering tactics.

- **Simulated Phishing Campaigns:** Run simulated phishing campaigns to test and reinforce employee awareness and response to phishing attempts.

By implementing these measures, you can reduce the risk of becoming a target for IABs and enhance the overall security posture of your organization.

Contact Us

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

ISRAEL

Tel: +972 3-7286-777
17 Ha-Mefalsim St 4951447 Petah Tikva

UNITED KINGDOM

Tel: +44-203-514-1515
3rd Floor, Great Titchfield House
14-18 Great Titchfield Street,
London, W1W 8BD

USA – TX

Tel: +1-646-568-7813
7250 Dallas Pkwy STE 400
Plano, TX 75024-4931

SINGAPORE

Tel: +65-3163-5760
135 Cecil St. #10-01 MYP PLAZA 069536

USA - MA

Tel: +1-646-568-7813
22 Boston Wharf Road Boston, MA 02210

JAPAN

Tel: +81-3-3242-5601
27F, Tokyo Sankei Building, 1-7-2 Otemachi,
Chiyoda-ku, Tokyo 100-0004

ABOUT CYBERINT

Cyberint, the Impactful Intelligence company, reduces risk by helping organizations detect and mitigate external cyber threats before they have an adverse impact. The Cyberint Argos platform's patented technology provides superior visibility through continuous discovery of the evolving attack surface, combined with the automated collection and analysis of vast quantities of intelligence from across the open, deep and dark web. A team of global military-grade cybersecurity experts work alongside customers to rapidly detect, investigate, and disrupt relevant threats – before they have the chance to develop into major incidents. Global customers, including Fortune 500 leaders across all major market verticals, rely on Cyberint to protect themselves from an array of external risks, including vulnerabilities, misconfigurations, phishing, impersonation attacks, malware infections, exposed credentials, data leaks, fraud, and 3rd party risks.

For more information visit: https://Cyberint.com.