CR X

IABs
Cultural Report

JUNE 2024

XG3 UNIT

xMDR
powered by Cipher

Introduction

Initial Access Brokers (IABs) are a fundamental component in the world of cybercrime. These specialists facilitate entry for ransomware groups, hacktivists, and advanced persistent threat (APT) groups into corporate networks. They operate in a well-established and lucrative market, with clear rules and conventions that maintain order among them.

Essentially, IABs function like open back doors, allowing other cybercriminals to access organizational networks. Each ransomware attack or data breach generally begins with this initial access.

What is an Initial Access Broker?

In short, an IABs acts as an intermediary to access corporate networks of companies. They specialize in obtaining and selling unauthorized access to computer systems, websites, servers, and other key components that companies use.

Threat actors need to access a network to deploy malware, steal, or encrypt sensitive information. Instead of investing their time and resources in infiltrating, they now have the option to purchase these accesses through IABs.

How do they get unauthorised access?

They might purchase compromised credentials on cybercriminal forums or use credential stealers to collect them. Often, they scan the internet for exposed ports that are protected by weak or default passwords and exploit vulnerabilities in systems that haven't been updated.

Also use social engineering tactics like phishing to trick people into giving them access and they perform brute-force attacks to guess passwords. In addition, they can buy low-level access from other IAB and then increase their access privileges to sell more valuable access.

How do IABs usually operate?

IABs sometimes sell access individually or in bundles, and additionally trusted intermediaries often use fixed postings indicating that they are selling access and asking buyers to contact them privately for more details.
When posting their offers on cybercriminal forums they use certain "rules" to prevent victims from realising that they have been compromised before access is sold, such as:

- Avoid naming target organisations directly.
- Only indicate the victim's geography, industry sector or income.
- Specify the type of access and level of privileges, type and amount of data accessed.
- Detail the number of employees, technical details such as the number of hosts or the type of anti-virus software.

Where do IABs usually operate?

Some threat groups have insiders who gain initial access to corporate networks, while others use the open market, in particular cybercriminal forums hosted primarily on Tor. Prominent forums such as Exploit and XSS, which have been active since 2005 and 2013 respectively, are known for their longevity, strict rules and competent administration. English-language forums, such a BreachForum, are less stable and are often targeted by law enforcement.

By 2024, the IAB market has consolidated around a few mainly Russian-language forums, many of which require a fee or a cybercrime knowledge test to join. Access lists are also occasionally available on Telegram channels of individual actors, but are generally less reliable.

Cybercriminal forums offer IABs encrypted messaging, escrow services and reputation systems to trade anonymously and securely. These platforms solve trading problems and allow IABs to operate without creating their own markets and the work involved.

What IABs sell?

They have significant control over network access and can set their own prices and terms. The cost of their services varies based on the type of organization they target, with factors such as industry, size, number of employees, and annual revenue influencing the price. Additional factors include the vulnerability of the company and the type of access being sold.

Types of access

- **Remote Desktop Protocol (RDP):** Allows remote control of a computer via a network connection. IABs sell compromised systems with RDP access enabled, enabling buyers to exploit these systems remotely.
- **Active Directory (AD):** A directory service that manages information about network resources. IABs infiltrate AD to sell access to private networks.
- **VPN:** Used for secure internet connections. Misconfigured VPN servers can be accessed by IABs, who then sell the compromised credentials.
- **Server Root Credentials:** Provides full control over a server, allowing extensive exploitation.
- **Web Shell Access:** Involves implanting malicious files on web servers, establishing backdoor access.
- **Control Panels:** Access to administrative control panels for managing network resources.

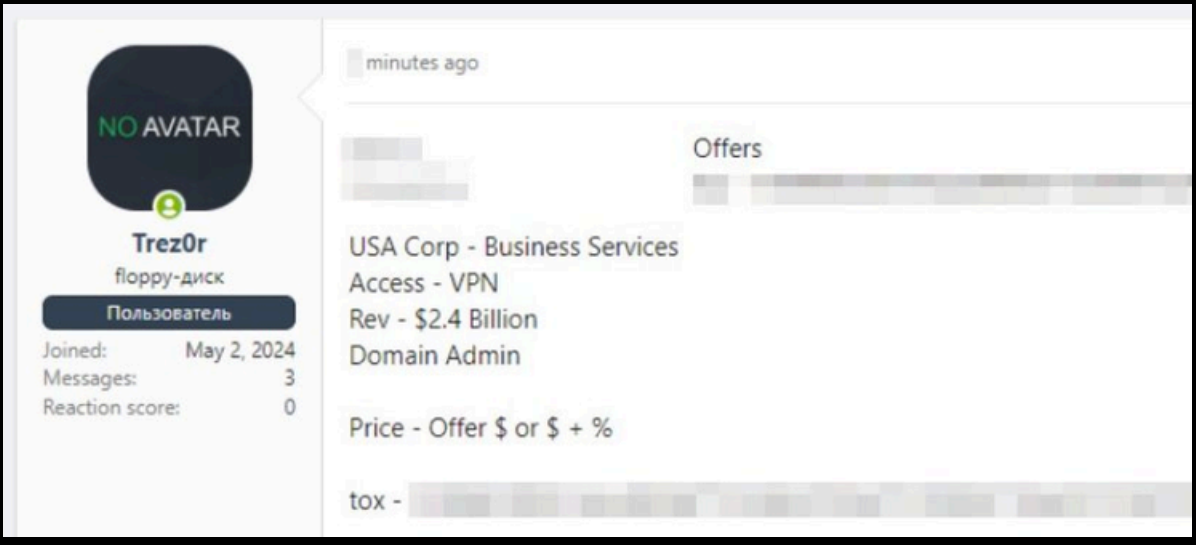

Image. Example of sell in XSS.in

Why do IABs exist and are they effective?

Initial Access Brokers play a crucial role in cybercriminal ecosystems. While technically proficient ransomware operators can likely gain network access themselves, IABs offer specialization. This allows other threat actors to focus on their expertise, like lateral movement or encryption, without the hassle of gaining access. Cybercrime, like any business, has specialists. IABs excel at network infiltration, streamlining the process for other groups.

For IABs, specialization also means avoiding the complexities and risks of ransomware attacks or data theft. They can monetize access without engaging in such activities. By selling access, IABs keep their activities discreet and profitable, while avoiding the legal risks associated with ransomware attacks.

In essence, they act as middlemen, facilitating access to valuable networks for other threat groups and moving on to the next opportunity.

Threat actor available in xMDR Platform

Cornflowerblue Cosmos Taurus sells unauthorised access to a Brazilian currency exchange.

Blueviolet Cosmos Taurus sells RDWeb access with domain user & admin rights to a German company.

Sunflower Yellow Cosmos Taurus sells VPN access to an Ecuadorian corporation.

Lion Cosmos Taurus sells RDP access to an software development Argentinean company.

Fuchsia Cosmos Taurus sells RDP access to a Spanish company

ResolutionBlue Cosmos Taurus sells webshell access to the Generalitat Valenciana's subdomain

Conclusion

- **Evolution of cybercrime models:** IABs represent an evolution in cybercrime, enabling faster and more efficient attacks by selling pre-compromised access to corporate networks.
- **Key facilitators in cybercrime:** IABs are crucial in cybercrime, providing initial access that facilitates complex and damaging attacks.
- **Impact on organizations:** The access sold by IABs can cause financial losses, reputational damage, and exposure of sensitive data.
- **Increased risk of coordinated attacks:** The specialization of IABs can lead to an increase in the coordination and sophistication of attacks, with multiple actors collaborating to maximize impact.
- **Future projection of cybercrime:** It is likely that the business model of IABs will expand, with more malicious actors resorting to buying initial access instead of attempting to compromise networks themselves.

Recomendations

- **Implement Multi-Factor Authentication (MFA):** Utilize MFA for all critical accounts to reduce the risk of unauthorized access through compromised credentials, making it harder for IABs to sell access.
- **Network Segmentation:** Divide the network into smaller, secure segments to contain potential breaches and limit lateral movement by attackers, making it harder for IABs to gain broad access.
- **Security Audits and Reviews:** Conduct regular security audits and system configuration reviews to identify and correct vulnerabilities, making it more difficult for IABs to find and exploit weak points.
- **Incident Response Policy Implementation:** Develop and maintain updated incident response policies and procedures to quickly act in the event of an attack, minimizing the impact of access sold by IABs.
- **Intrusion Detection and Prevention Systems (IDS/IPS):** Implement IDS/IPS to identify and block malicious activities in real-time, making it harder for IABs to maintain and sell compromised access.

xMDR

IABs

Cultural Report

JUNE 2024

xMDR
powered by Cipher