Rise of Initial Access Brokers:

Threat actors who facilitate cyber-attacks, APT groups, and ransomware campaigns

Author: Anandeshwar Unnikrishnan, Cyber Threat Analyst, CloudSEK

CloudSEK

Cybersecurity during a Pandemic

Starting in early 2020, the COVID 19 pandemic has forced businesses across the globe to go online. From remote working and online shopping to digital transactions and virtual socialization, there has been a paradigm shift in how we work, communicate, and collaborate. This has further stressed the already delicate cybersecurity apparatus of governments, enterprises, small businesses, and individuals.

These changes have led to a multifold increase in the usage of Virtual Private Network (VPN), Remote Desktop Protocol (RDP) and other endpoints that are used to remotely connect to the internal networks of organizations. While this has ensured that businesses can continue to operate without significant productivity or financial loss, it has exposed companies' internal infrastructure to hackers and threat actors.

In the first quarter of 2021, CloudSEK has identified about 400 posts, which is 20% of the total threats identified, across dark web and underground forums, advertising accesses such as VPN, RDP etc. to various organizations across the world. This warrants a closer look at how and why accesses are sold and their impacts on organizations and individuals.

Initial Access Brokers and Access Markets

Initial Access Brokers (IABs) are threat actors whose primary objective is to gather and sell accesses to various organizations. They specialize in "breach and infiltrate" to collate initial accesses that are then sold to the highest bidder.

The question that often comes up is: why stop at gaining access? There are several reasons for this. One, it takes concerted effort and resources to carry out a full-fledged cyber attack once they have access to an organization's internal networks. While organized black-hat groups have the manpower, money, and infrastructure capabilities to escalate their privileges, to achieve lateral movement across the network, and to identify and exfiltrate data, individual actors lack the resources to manage the volume and complexity of these activities. Secondly, given that most enterprises have a mature cybersecurity program, it would be difficult for an inexperienced actor to compromise an organization and get away without leaving breadcrumbs that can be

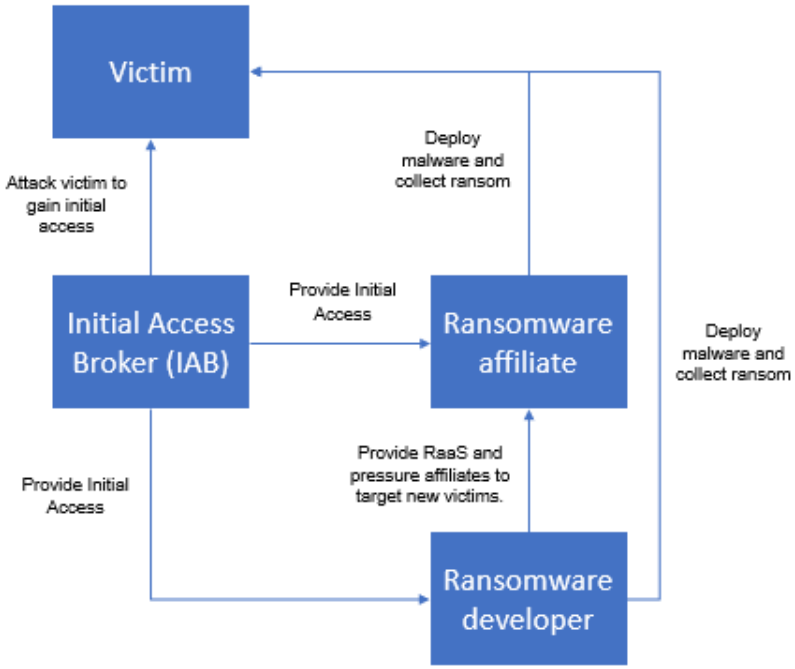
traced back to them. Hence, there is a new breed of actors, in the form of IABs, who are happy to make a quick buck with minimal risk involved.

The Nexus Between IABs and Other Threat Actors

IABs cater to a variety of threat actors and often serve as a starting point for attacks. Understanding how they facilitate other threat actors illustrates their motivations and modus operandi.

IABs usually cater to:

- Ransomware developers
- Ransomware affiliates
- APT groups
- Other blackhat groups



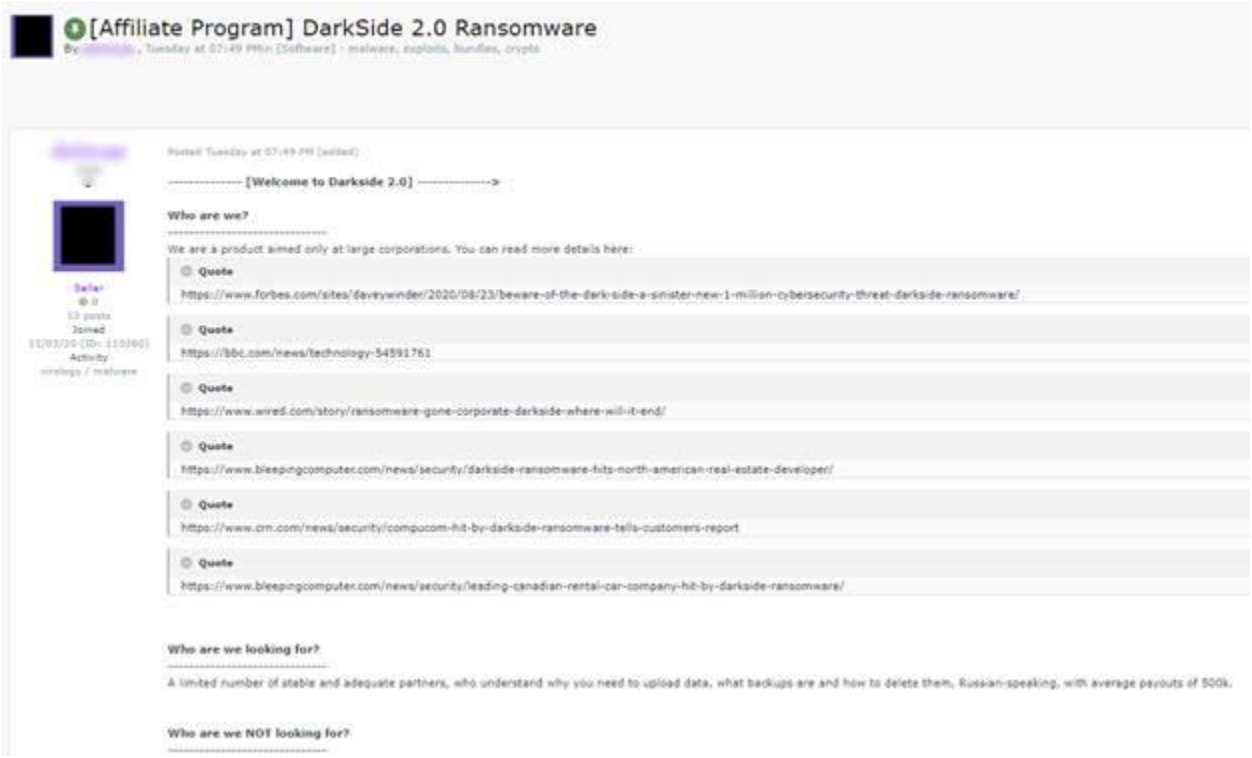
Akin to any business, IABs obey the laws of supply and demand. So, the companies they target largely depend on the demand from their core customer base, which is primarily ransomware developers and affiliates. Given that IABs carry out enumeration of the target environment and even privilege escalation in some cases, it offsets the amount of ground work that ransomware gangs need to do. They can instead focus on their core objectives of deploying payload, carrying out lateral movement, cryptolocking, and exfiltration.

Ransomware Affiliate Programs

Apart from the rise in remote working, the other reason for the proliferation of IABs is the spike in ransomware affiliates. Ransomware developers are recruiting affiliates to deploy their malware payload that will lock victims' files. Making it a Ransomware as a Service (RaaS) and allowing more threat actors to spread malware without having to develop it from scratch. To

recruit affiliates, the developers post advertisements calling for interested parties, across underground forums.

To be a ransomware affiliate a threat actor has to infect new victims continuously. Ransomware operators mount pressure on the affiliates to target new victims or risk being expelled from the program. To fulfill these targets ransomware affiliates turn to IABs on underground forums.


[Affiliate Program] DarkSide 2.0 Ransomware

[redacted], Tuesday at 07:49 PM in [Software] - malware, exploits, bundles, crypto

[redacted]

Seller

0

13 posts

Joined

11/03/20 (ID: 110360)

Activity

virology / malware

Posted Tuesday at 07:49 PM (edited)

---------- [Welcome to Darkside 2.0] ---------->

Who are we?

We are a product aimed only at large corporations. You can read more details here:

Quote

https://www.forbes.com/sites/daveywinder/2020/08/23/beware-of-the-darkside-a-sinister-new-1-million-cybersecurity-threat-darkside-ransomware/

Quote

https://bbc.com/news/technology-54591761

Quote

https://www.wired.com/story/ransomware-gone-corporate-darkside-where-will-it-end/

Quote

https://www.bleepingcomputer.com/news/security/darkside-ransomware-hits-north-american-real-estate-developer/

Quote

https://www.cm.com/news/security/compucom-hit-by-darkside-ransomware-tells-customers-report

Quote

https://www.bleepingcomputer.com/news/security/leading-canadian-rental-car-company-hit-by-darkside-ransomware/

Who are we looking for?

A limited number of stable and adequate partners, who understand why you need to upload data, what backups are and how to delete them, Russian-speaking, with average payouts of 500k.

Who are we NOT looking for?

Post advertising ransomware affiliate program

IABs' Modus Operandi

IABs usually stick to the following steps when it comes to gaining access:

- Target Selection
- Attack
- Internal Reconnaissance
- Finding a Buyer

Target Selection

Since ransomware developers and affiliates target high net-worth victims, so do IABs. Access brokers usually scout for businesses that would be attractive to ransomware gangs.

Attack

Once a target has been zeroed on, the attack vector depends on the security maturity of the target.

To gather the initial access vectors, IABs use a variety of attack vectors such as:

- Social Engineering
- Exploiting endpoint vulnerabilities

Social Engineering

Social engineering attacks such as phishing and spear phishing campaigns are used to steal user credentials that can serve as an initial foothold to an organization's internal network. Social engineering ruses include fake domains and email attachments that mislead unsuspecting users into sharing their credentials.

Exploiting endpoint vulnerabilities

- RDP brute force attacks/ Misconfigured RDPs: RDP endpoints can be brute forced to compromise user accounts
- VPN vulnerabilities: VPN gateway vulnerabilities can be exploited to:
    - ❖ Steal user credentials
    - ❖ Perform Remote code execution (RCE) on target gateway servers

Once a VPN endpoint is compromised it can be leveraged to gain RDP access because corporate networks often provide RDP access without authentication, if a user is authenticated via VPN. As a result, CloudSEK researchers have observed a rise in threat actors selling exploits for vulnerabilities in major VPN vendors, soon after the vulnerabilities have been disclosed.

The most common vulnerabilities of 2020 for which exploits were being widely circulated are:

Vulnerability	Description
CVE-2019-11510	Pulse Secure Pulse Connect Secure, unauthenticated arbitrary file reading vulnerability
CVE-2019-11539	Pulse Secure Pulse Connect Secure RCE
CVE-2018-13379	Fortinet FortiOS Path Traversal vulnerability
CVE-2018-13382	Fortinet FortiOS unauthenticated password change on SSL VPN web portal.
CVE-2018-13383	Fortinet FortiOS Heap buffer overflow
CVE-2019-1579	Palo Alto PanOS RCE GlobalProtect Portal or GlobalProtect Gateway Interface enabled
CVE-2019-19781	Citrix Application Delivery Controller, Citrix Gateway, and Citrix SD-WAN WANOP RCE
CVE-2019-0604	Microsoft SharePoint RCE
CVE-2020-0688	Microsoft Exchange Validation Key RCE
CVE-2020-10189	Zoho ManageEngine Desktop Central RCE

Internal Reconnaissance

Once an IAB gets initial access they log into the network to perform primary recon and basic enumeration of the environment. Since most large internal networks are managed by directory services such as Microsoft Active Directory, the IAB's recon involves using PowerShell tools such as PowerView to retrieve the following information:

- Domain Users
- Domain Computers

- Domain Controller (Including IP address)
- Trust policies
- Access Control Lists (ACLs)

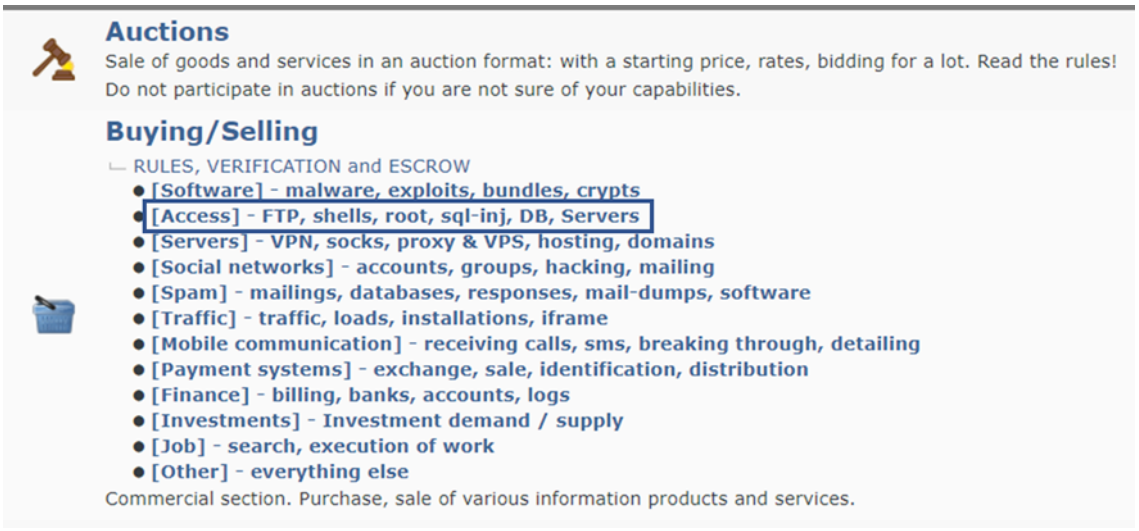
Finding a Buyer

Once the IAB has gathered all the relevant information, they need to find a reliable buyer. For this they turn to underground forums and access markets across the dark web and surface web.

Access Markets

Most popular threat actor forums have a dedicated section to buy and sell accesses, in addition to other sections for data leaks, exploits etc. However, there are also exclusive access markets that deal only with accesses. These markets have further sub-sections for RDP accesses, hacked servers, etc.

Dedicated access markets



Sub-section on popular forum for buying and selling accesses

IAB Posts on Access Markets

IABs usually sell access in the form of:

- Credentials that provide access to a specific system
- A webshell/ malicious script hosted on a web server that gives access to the host operating system via a specific URL

IAB posts advertising accesses

IABs are cautious about sharing too much information about the compromised target. Since this could tip off the affected company to take necessary action to secure the compromised endpoints. However, they still need to share relevant information to attract potential buyers. To strike a balance between revealing too much, versus revealing too little, IABs use B2B data aggregating platforms such as Zoominfo to gather indicative but non-conclusive information about the impacted company.

This includes details such as:

- Industry/Sector
- Net Worth in dollars
- No. of employees/Computers

In some cases the details of the company remain cryptic, and instead the IAB shares information about the targeted endpoint or server.

This includes details such as:

- ID/User/Machine Name [OS dependant]
- IP Address
- Geo Location
- Online Status
- Upload/Download Rate
- Uptime
- Logs
- Price

Cost of Access

The cost of access typically depends on the networth of the compromised victim. Our research and monitoring has identified that the price for VPN and RDP accesses range from $10 - $50 USD for local or standalone businesses to thousands of dollars for multinational companies and highly valued businesses. The buyer is usually shortlisted based on public auctioning in the comments of the post or after private discussions with the seller.

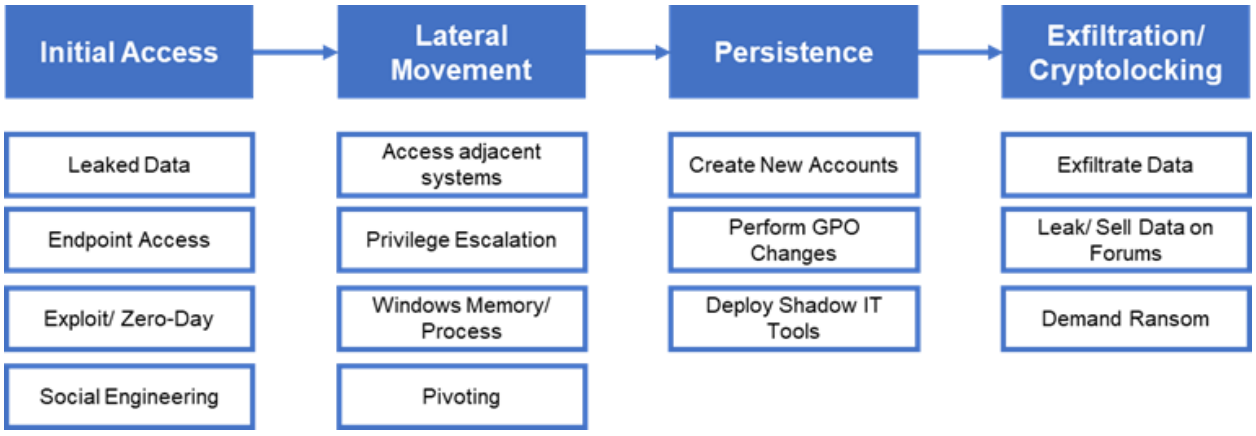
IABs use middlemen or forum administrators to carry out the transactions securely. These middlemen validate the access being sold and verify the credibility of the buyer. This gives both

buyers and sellers a security net and reduces the instances of fraud. Once the deal has been struck the exchange of money is done using bitcoin or other cryptocurrency.

How does Initial Access Impel a Cyber Attack

Most cyber attacks originate and culminate on the internet. Depending on the threat actor's objectives, a cyber attack is carried out in the following phases:

- Initial Access
- Lateral Movement
- Persistence
- Data Exfiltration/ Cryptolocking



Initial Access

A threat actor looking to launch a full-fledged attack begins by scouring dark web and underground forums for vectors that will give them initial foothold to the internal network of the company they want to compromise. The most common initial access vectors include:

- Leaked data from previous breaches
- VPN and RDP accesses sold by IABs
- Exploits or zero-days that target flaws in the victim's internet facing assets, endpoints, and networks
- Social engineering tactics

Lateral Movement

Once the attacker gains control of one asset within the victim's network, they try to:

- Target other adjacent assets in the network
- Use privilege escalation techniques to become the highest privilege user in the network
- Compromise password hashes stored in the Windows memory/process and use them to log onto other assets within the subnet
- Carry out pivoting, which involves crossing subnet boundaries to access assets on another subnet in the victim's network

Persistence

The phase involves activities that allow the attacker to remain the network unidentified and without raising red flags. To ensure this, the actor will:

- Create new accounts that allow them to log into assets without alerting the network administrators
- Perform Group Policy Changes that gives them extended access
- Deploy shadow IT tools and resources

Data Exfiltration/ Cryptolocking

Threat actors may exfiltrate confidential documents, user information, credentials, and other sensitive records. They then sell this on underground forums to the highest bidder or use it to carry out other attacks. If the attacker is a ransomware affiliate or developer they lock the victim's documents and systems and blackmail the victim to pay a ransom, failing which they shame the victim and release their data.

Convenience Versus Security

While VPNs and RDPs are allowing businesses to function despite the restrictions of a pandemic and social distancing, they are making them more vulnerable to cyber attacks. Endpoint access, leaked credentials, and software bugs can be used in tandem to carry out a full-fledged cyber attack that could damage a company's revenue and reputation.

This threat is further exacerbated by the growing number of Initial Access Brokers who are making it easy to initiate attacks. With the ubiquitous availability of initial access, ransomware affiliates, APT groups, and other threat actors can focus on further perpetrating and exploiting the victim's network.

Hence it is incumbent on organizations to have:

- Strong security policies that mandate complex passwords and cybersecurity hygiene
- Processes that enable periodic updates and cybersecurity audits
- Cybersecurity tools and platforms that allow real-time continuous monitoring of the surface web and dark web for the presence of data leaks, accesses, etc.

About CloudSEK

CloudSEK is an AI-driven Digital Risk Management Enterprise. CloudSEK's XVigil platform helps clients assess their security posture in real-time from the perspective of an attacker. XVigil scours thousands of sources (across the surface, deep and dark web), to detect cyber threats, data leaks, brand threats, identity thefts, etc. To learn more about how the CloudSEK XVigil platform can strengthen your external security posture and deliver value from Day 1, visit https://cloudsek.com/ or drop a note to sales@cloudsek.com.