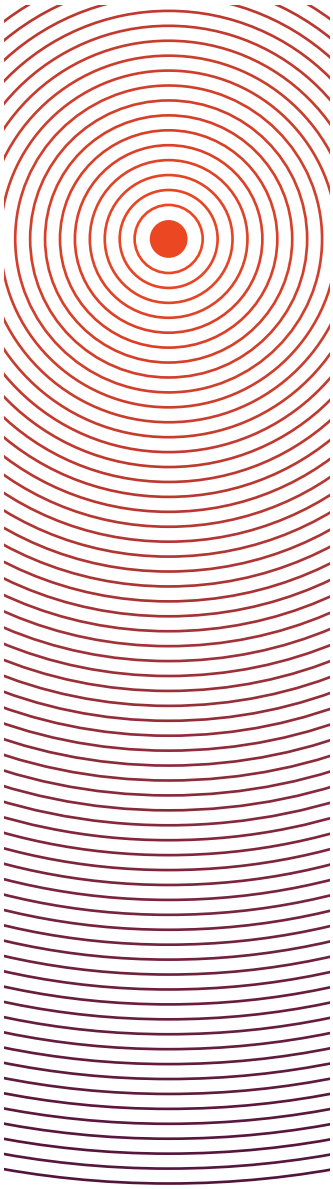
SEARCHLIGHT. CYBER

COMBATING INITIAL ACCESS BROKERS WITH DARK WEB INTELLIGENCE

THE CHALLENGE



Initial Access Brokers are one of the most common threats to organizations that we observe on the dark web. They are cybercriminals that specialize in breaking into networks and establishing a foothold. They then sell this foothold, or "access", onto other cybercriminals to exploit.

This makes them a critical part of the cybercriminal ecosystem. Cybercriminal gangs, in particular ransomware operators, routinely use Initial Access Brokers so they don't have to go through the effort of breaking into the network themselves. In return, Initial Access Brokers can generate consistent returns while taking on a relatively low-risk portion of the attack.

In order for this ecosystem to function there has to be a point of exchange - and that takes place on dark web forums such as Exploit, XSS, and BreachForums. Here, Initial Access Brokers sell or auction their exploits to the cybercriminal community. The example overleaf is a real Initial Access Broker post from the Exploit forum and is broadly typical in the details it contains.

While it is alarming to see organizations targeted so explicitly on the dark web, Initial Access Broker posts actually provide a huge opportunity for security teams to spot an early warning sign of attack and take mitigative action.

It is a point when the cybercriminals are exposed - forced to give away key information about their targets, their tactics, and even their identities. In this report we outline the steps organizations can take to mitigate cyberattacks based on the intelligence held within Initial Access Broker posts.

THE ANATOMY OF AN INITIAL ACCESS BROKER POST

2 days ago, 07:12:00am
- Posted by **xxxxxxxxxx**

BANK ACCESS

Revenue: $3-10 Billion (For secirity reasons, I won't tell exact company information)
Access type: RDP
Access level: Domain admin

Extra info :)

Many hosts in the network
Esxi + Vshpere + Veeem
Can manage all AVs
+ Garant
+ New users with no reputation, I ignore

Start: 15 BTC
Step: 1 BTC
Blitz: 20 BTC

End of auction: 72h
Geo: Not CIS country, not USA

A typical Initial Access Broker Post on the dark web hacking forum, Exploit

VICTIM INFORMATION

The Initial Access Broker says they are not naming the company for "security reasons" but does provide details on the industry, revenue, and location of the victim.

INFORMATION ON ACCESS

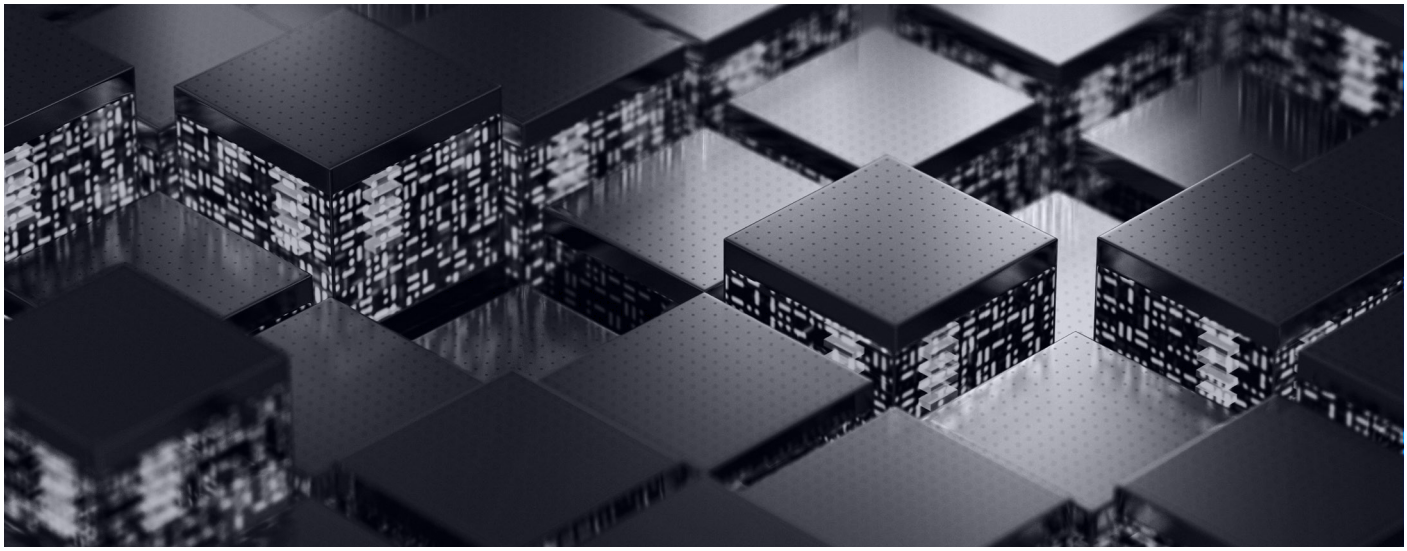
The Initial Access Broker provides technical detail on what they are selling, such as the system "RDP" (Remote Desktop Protocol) and the access level "Domain admin".

NETWORK INFORMATION

The post also provides information on technologies on the network "Esxi + Vshphere + Veeam" and promises to "manage all AVs" (anti-viruses).

THE AUCTION PROCESS

The Initial Access Broker provides three prices labeled "Start", "Step", and "Blitz". This is a common dark web lexicon for auctions. In this case, it indicates that bidding starts at 15 Bitcoin and bids will be placed at increments of 1 Bitcoin. However, if an individual wanted to purchase the access outright they could do so at the "Blitz" price of 20 Bitcoin. The Broker also indicates that he is not interested in buyers with "no reputation".



INITIAL ACCESS BROKERS IN NUMBERS

100% INCREASE IN THE NUMBER OF **CORPORATE ACCESS LISTINGS** ON THE DARK WEB FROM 2021-2022.[1]

#1 THREAT TO THE BANKING SECTOR SEEN ON THE DARK WEB IS FROM **INITIAL ACCESS BROKER POSTS.**[2]

89% OF BREACHES INVOLVE THE USE OF **STOLEN CREDENTIALS** TO ESTABLISH INITIAL ACCESS.[3]

$4,699.31 IS THE AVERAGE PRICE TO **PURCHASE ACCESS** TO A CORPORATE IT ENVIRONMENT.[4]

GET STARTED RIGHT AWAY WITH OUR NO-INSTALL PLATFORM

- DEFEND AGAINST IAB AND DARK WEB THREATS
- SEARCH LIVE AND HISTORIC DARK WEB DATA
- UNCOVER THREAT ACTOR ALIASES AND PATTERNS

[1] https://www.infosecurity-magazine.com/news/initial-access-broker-activity/
[2] https://www.slcyber.io/whitepapers-reports/dark-web-threats-against-the-banking-sector/
[3] https://www.verizon.com/business/en-gb/resources/reports/dbir/
[4] https://www.bleepingcomputer.com/news/security/the-initial-access-broker-economy-a-deep-dive-into-dark-web-hacking-forums/

FIVE WAYS YOU CAN COMBAT INITIAL ACCESS BROKERS TARGETING YOUR ORGANIZATION

1

IDENTIFY THE TARGET

Security teams should be monitoring the dark web for Initial Access Broker posts that might pertain to their business.

It sounds unbelievable, but some cybercriminals name the organization they are selling access to - presumably with the belief that security teams are not monitoring the dark web or, even if they are, that they are sufficiently anonymous that they don't have to worry about repercussions. In these cases, security teams have a clear indication that they are a potential victim and can start to investigate the possible paths of attack.

However, in most cases, Initial Access Brokers don't make it quite that easy and security teams have to do some work to identify whether they are the potential victim of the attack. While many Initial Access Broker posts won't have the victim's actual name - because the cybercriminal doesn't want to tip the organization off before the access is sold - the advertisement does need to have some information about the victim, otherwise potential buyers won't be able to identify what they are purchasing.

22 Dec 2022, 03:04:00pm
- Posted by **xxxxxxxxxx**

Geo: USA
Rev: 12 billion (zoominfo)
Industry: Manufacturing
Level: Domain user

Many many users and computers.

Start: $4,000
Step: $1,000
Blitz: $10,000

An Initial Access Broker provides details on a victim organization taken from ZoomInfo to help attract buyers.

Often this information is pulled by the Broker from public sources such as the sales intelligence software, Zoominfo, and they sometimes even provide the source. This means security teams can cross reference the information to determine the exact organization being targeted. Security teams can use these details to determine whether their organization (or perhaps one of their suppliers) fits the profile of the advertisement, which would then warrant further investigation.

This information typically includes:

- **Industry** - the sector of the victim is almost always included.
- **Company description** - sometimes additional information on the company is provided.
- **Geography** - which is important to threat actors who want to determine the region they are attacking.
- **Revenue** - either as a range or with a set figure to give buyers an indication of the potential "yield".
- **Technology stack** - Initial Access Brokers will often give an indication of the victim's infrastructure and sometimes the security tooling they have in place. Once again, this can help organizations determine if they match the profile of the victim.

HOW TO COMBAT INITIAL ACCESS BROKERS

Cybercriminals can buy access into an organization's network for as little as $10 on the dark web. This access can be used to install malware, exfiltrate data, and launch ransomware attacks against your organization. That's why it's vital security teams have a strategy in place to identify these threats before they become attacks. Searchlight Cyber gives security professionals instant access to the data and tools they need to identify the first sign that their organization's access is being listed for sale on the dark web.

MONITOR FOR INITIAL ACCESS BROKER POSTS AND STOLEN CREDS

Our platform monitors the dark web and sends alerts to SOC teams, prioritizing leaked company credentials or any mention of the organization which could be sold or exploited. Threat hunters can also quickly set up alerts to track specific keywords, such as "Access + webshell + your industry", known threat actors, and groups of interest - helping you spot threats earlier.

2

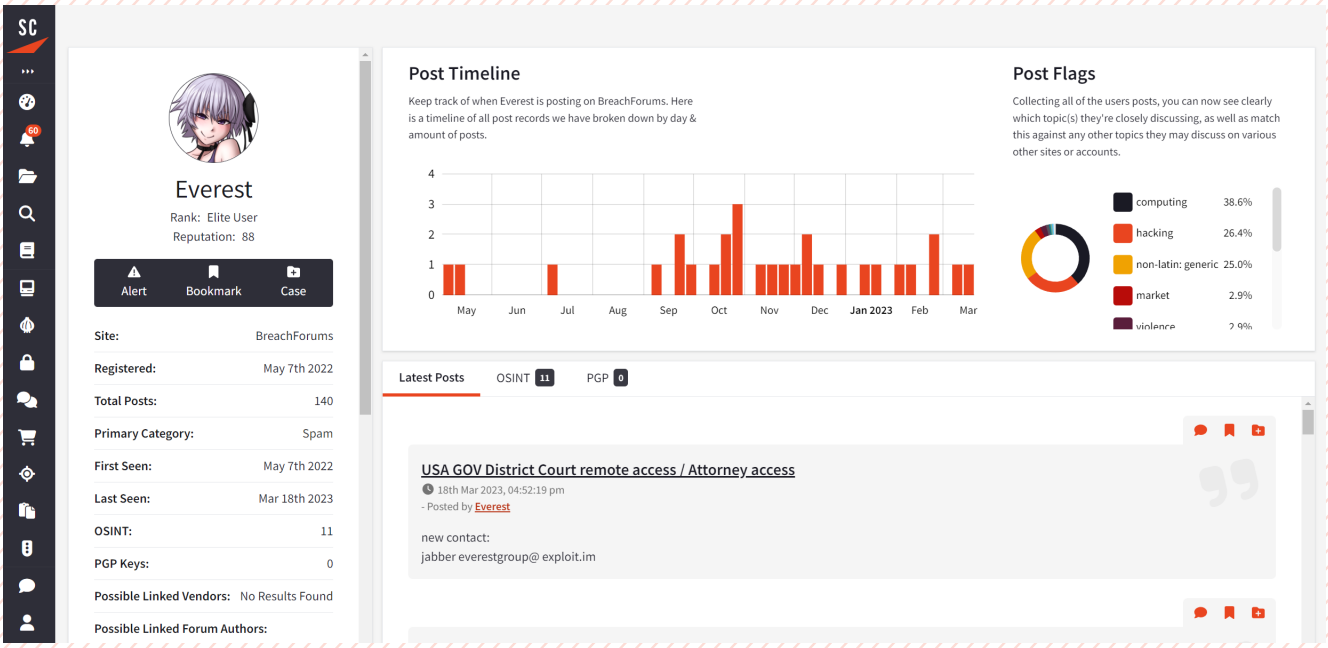
PIVOT ON THE BROKER

If an organization determines that they fit the profile of the victim the next step is to verify the credibility of the post.

Modern day defenders are overwhelmed with alerts, data, and threats - they can't chase every single lead they have. Pivoting on the profile of the Initial Access Broker can help them determine the likelihood of whether the threat is genuine and potentially gather more intelligence on the nature of the threat, based on the Initial Access Broker's past activity.

This activity can help triage out any threat actors that are not assessed as credible threats. For example, a threat actor who has previously posted on the dark web asking what a webshell is might not be considered worthy of investigation, even if they make big claims about the access they have.

It can also help security professionals prioritize the investigation if the Initial Access Broker is assessed to have high-caliber capabilities. For example, a threat actor such as Everest - who has been observed increasingly selling initial access - would be considered high-risk based on their previous activity as a ransomware operator.



The Cerberus profile of the threat actor Everest, who operates as both an Initial Access Broker and ransomware operator.

In their assessment of Initial Access Brokers, security teams should analyze:

- **Previous posts from the Broker** - to determine whether they have a track record of selling initial access.
- **Associated profiles on other dark web forums** - as many Initial Access Brokers conduct activity across multiple forums using various accounts.
- **Linked accounts** - which can be determined by looking for shared details including email addresses, crypto-wallets, Telegram / TOX / Jabber accounts.
- **The Broker's reputation scores on dark web forums** - which can be a good indicator of whether other cybercriminals view the Initial Access Broker as legitimate.
- **The Broker's association or affiliation with other cybercriminals or threat groups** - which can help establish whether they are acting as part of a wider operation.
- **The tactics and technologies the Broker has used in the past** - which may be vital to pinpointing where the vulnerability may be. For example, if the threat actor has posted frequently about hacking a particular Wordpress extension, or abusing a CVE in software running on a web server.

HOW TO COMBAT INITIAL ACCESS BROKERS

INVESTIGATE ACTORS AND IDENTIFY CREDIBLE THREATS

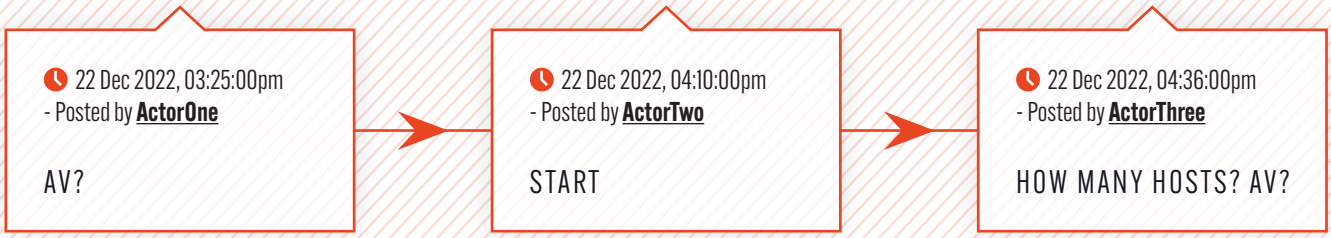
Searchlight makes it easy for threat intelligence teams to search and pivot on dark web actors, helping them assess the credibility of the threats based on their historic activity and correlate this data with other malicious activity, including dark web traffic to your organization's infrastructure. This enables you to recognize and act on the pre-attack warning signs and stop breaches in their tracks. That's the power of pre-attack intelligence from the deep and dark web.

3

PIVOT ON THE BUYER

If the security team has assessed that the Initial Access Broker post is of high credibility it then becomes imperative to monitor for cybercriminals interacting with the post to determine whether the access has been sold, to who, and the capabilities of the buyer.

The actual bidding process sometimes takes place in private messages but you will often observe threat actors enquiring about the access or interacting with the post.



Minutes after the Initial Access Broker post shown on page 4 was published, cybercriminals began commenting on the post. Two of the actors enquired for more information about the anti-virus (AV) technology of the victim organization. One actor responded with "start", which is a bid at the starting price indicated in the Initial Access Broker's post as $4,000.

This can be invaluable information that could allow a security team to harden their internal defenses and monitoring, even if the initial attack vector cannot be remediated. For example, we have observed threat actors that are known to be associated with ransomware groups interacting with Initial Access Broker posts, which has allowed the organizations to prepare for that specific threat.

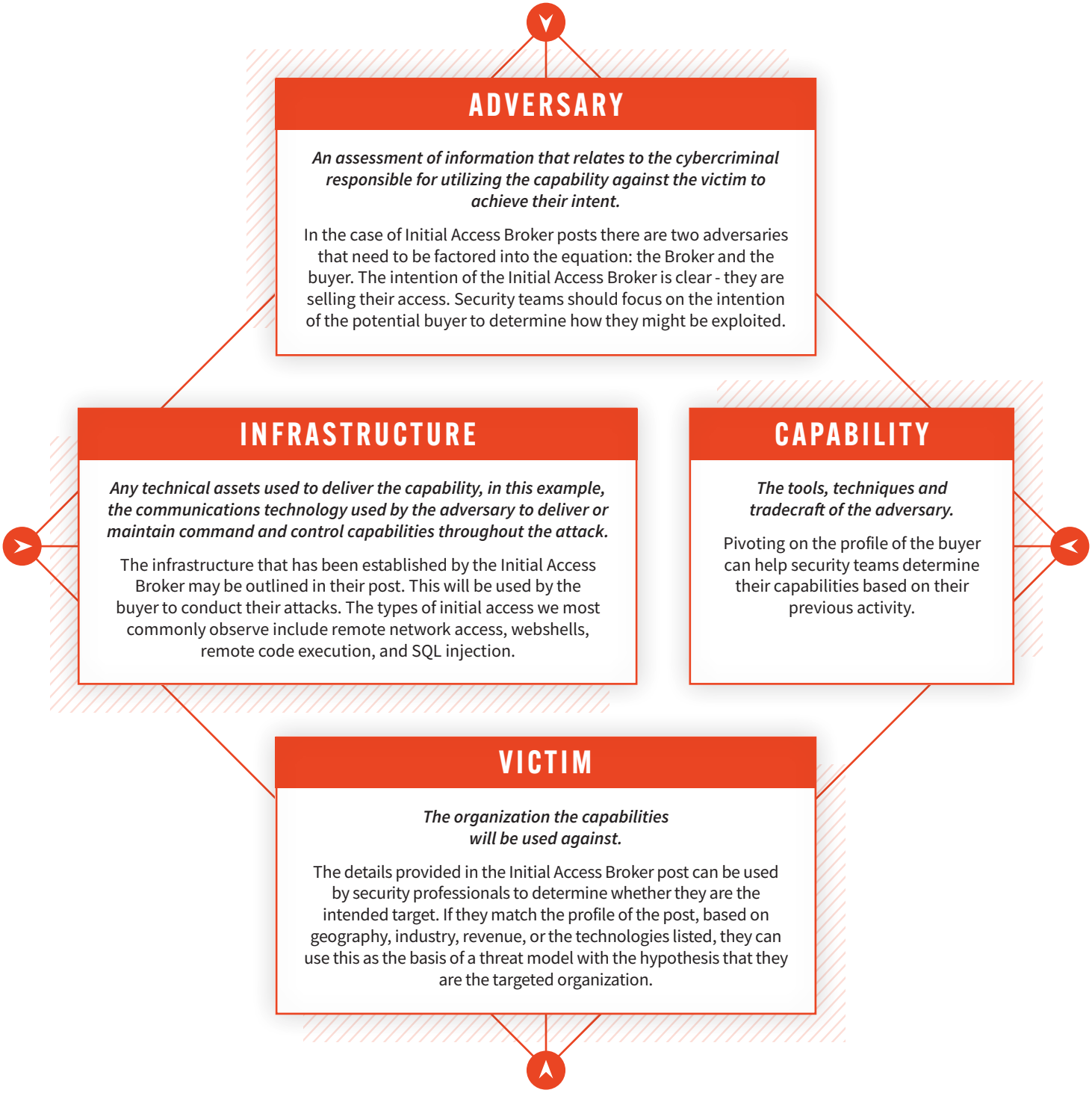
Security teams investigating potential buyers should be assessing details such as:

- **The reputation of the buyer** - which is an indicator of the level of threat they pose.
- **The buyer's association with larger criminal enterprises** - such as ransomware gangs.
- **The tools used by the buyer** - based on information they have previously posted on dark web forums.

4 ASSESSING THE THREAT

The next step involves accumulating all of the data that has been gathered and continuously analyzing it holistically against activity groups. The Diamond Model is an established approach security professionals can use to analyze information and produce intelligence based on four basic elements: adversary, capability, infrastructure, and victim.

Security professionals can input the information they have gathered from the dark web into this model to identify gaps - both in terms of collection breadth (do you have access to enough data sources) and depth (how far back in time do those data sources go etc). Based off the assessments made using the diamond model, security teams can then determine mitigating actions that can be taken.

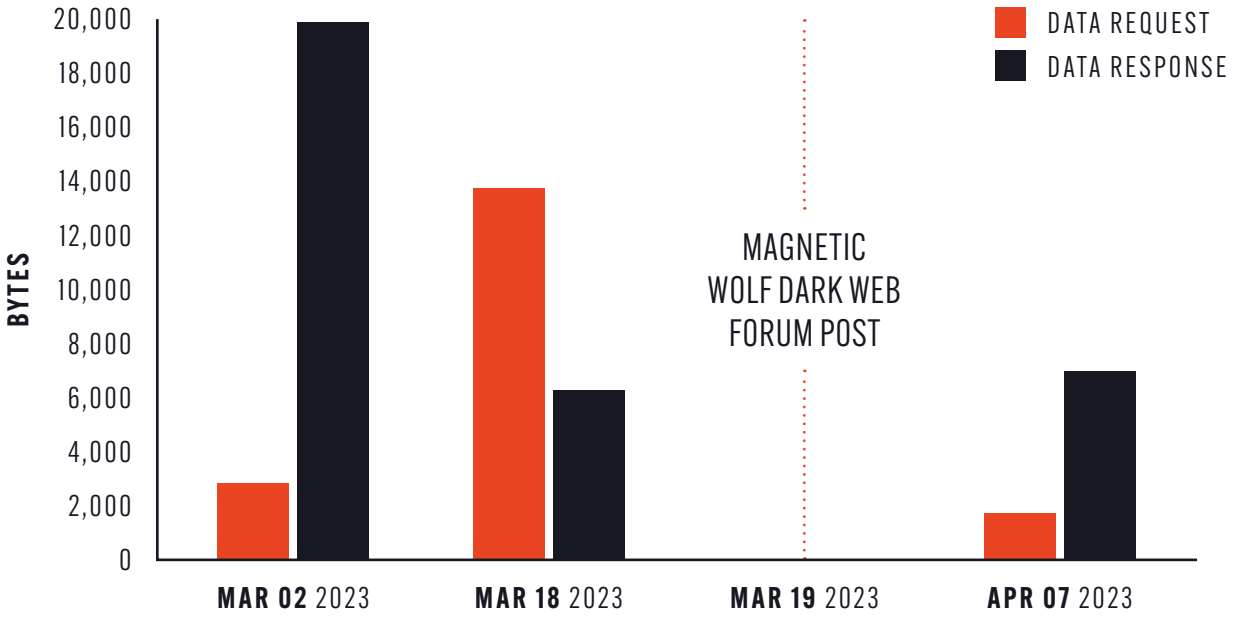


5

PIVOT TO INTERNAL SECURITY

If security teams are continuously monitoring for Initial Access Brokers posts as part of their intelligence requirements, this gives them a good chance of identifying the fact they are the victim before the access is exploited by the buyer. Effectively, they are catching the buyer right at the beginning of their "kill chain", when they are purchasing the access they need to execute their attack. This provides security professionals with invaluable time to identify the access that has been sold and mitigate it before it can be exploited - effectively stopping the attack in its tracks.

Of course, those mitigative steps will vary based on the type of access that is being sold. Deactivating an installed webshell is very different to identifying a compromised VPN. However, in all cases the process will involve triaging the intelligence that has been gathered from the dark web to internal security teams to investigate and take the correct actions. Depending on the size of the organization, the sophistication of its security operation, and the nature of the threat, this could involve the Security Operations Center (SOC), Incident Response teams, Vulnerability Management, or Cybersecurity, Governance and Risk Management.

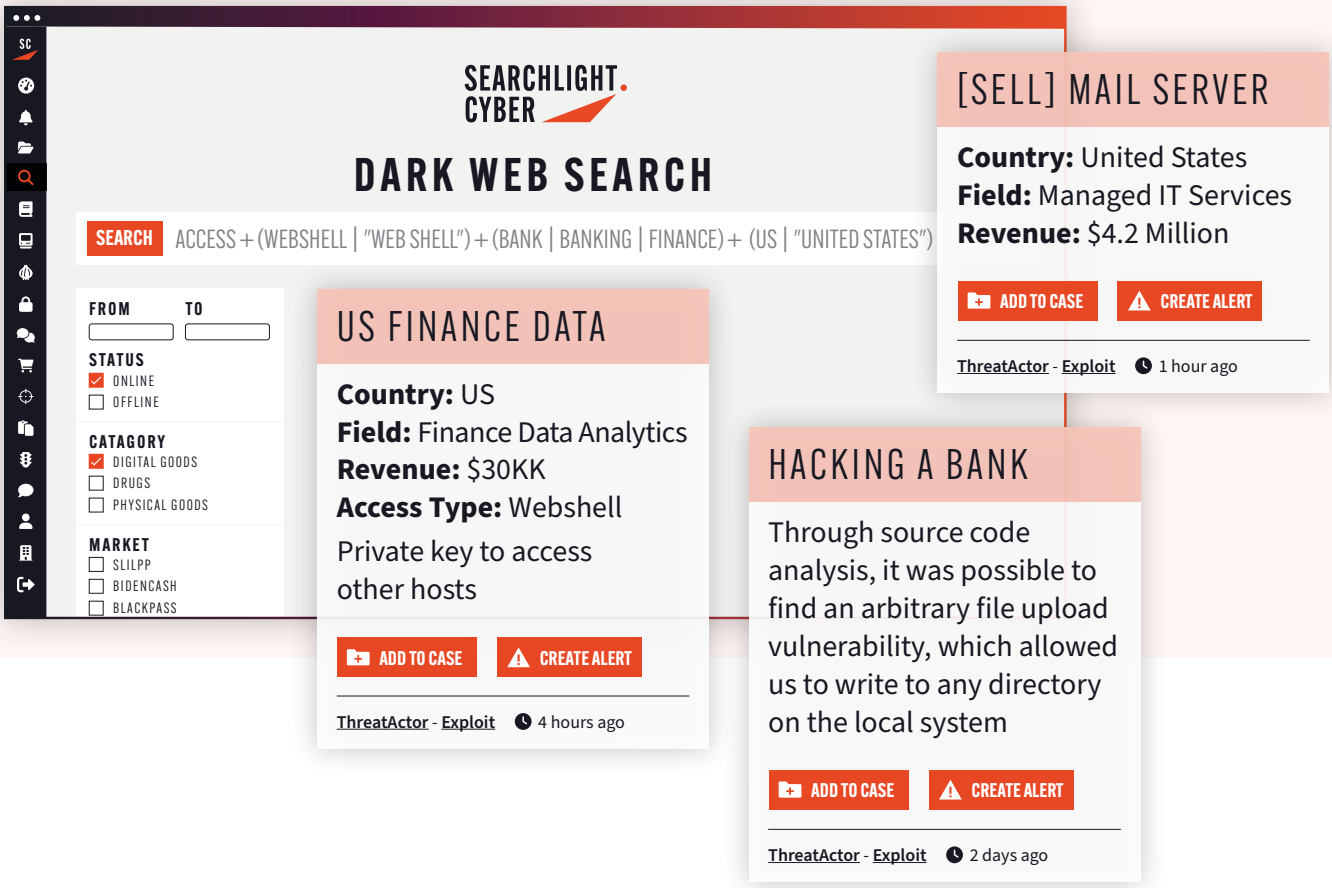


In 2023 we observed an Initial Access Broker we track as "Magnetic Wolf" advertising access to a government agency. We alerted the agency, who were able to mitigate the webshell Magnetic Wolf had installed before it was exploited. On investigation, the installation of the malware could be seen in an influx of data from the dark web to the government agency's network just hours before the actor posted about the access.

HOW TO COMBAT INITIAL ACCESS BROKERS

TIMELY AND ACTIONABLE THREAT INTELLIGENCE

Searchlight Cyber uses a combination of manual and cutting-edge automated data collection methods to give your organization up-to-the-minute dark web data. By not solely relying on analysts to gather intelligence, our methods enable us to deliver timely and context-rich data from deep and dark web sources, including underground forums, marketplaces, and encrypted chats. Even if the post is deleted, the data is stored in Searchlight forever – allowing analysts to easily query, retrieve, and make accurate decisions based on more than 15 years of live and archived dark web data.



BENEFITS: TIMELY AND ACTIONABLE DARK WEB INTELLIGENCE

- AGENTLESS DEPLOYMENT WITH OUR OUTSIDE-IN APPROACH TO DATA COLLECTION
- GET ALERTED WHEN YOUR ORGANIZATION OR PEOPLE ARE MENTIONED
- SEARCH LIVE AND HISTORIC DATA, INCLUDING POSTS THAT HAVE BEEN DELETED
- DEFEND YOUR ORGANIZATION FROM IAB AND DARK WEB THREATS

SEARCHLIGHT CYBER

SEARCHLIGHT CYBER HELPS ORGANIZATIONS SAVE TIME AND MONEY BY SPOTTING THE FIRST WARNING SIGNS OF AN ATTACK.

★★★★★

"Good Product For Hunting PII Data On The Dark Web. The information they have provided about corporate data on the dark web has been invaluable."

INDUSTRY: BANKING (SOURCE: GARTNER PEER INSIGHTS)

SCAN THE QR CODE TO BOOK YOUR FREE DEMO TODAY OR VISIT **WWW.SLCYBER.IO** TO FIND OUT MORE.

UK HEADQUARTERS
Suite 63, Pure Offices,
1 Port Way, Port Solent,
Portsmouth PO6 4TY
United Kingdom

US HEADQUARTERS
900 16th Street NW,
Suite 450, Washington,
DC 20006
United States