SEARCHLIGHT.
CYBER

DARK WEB THREATS AGAINST THE BANKING SECTOR

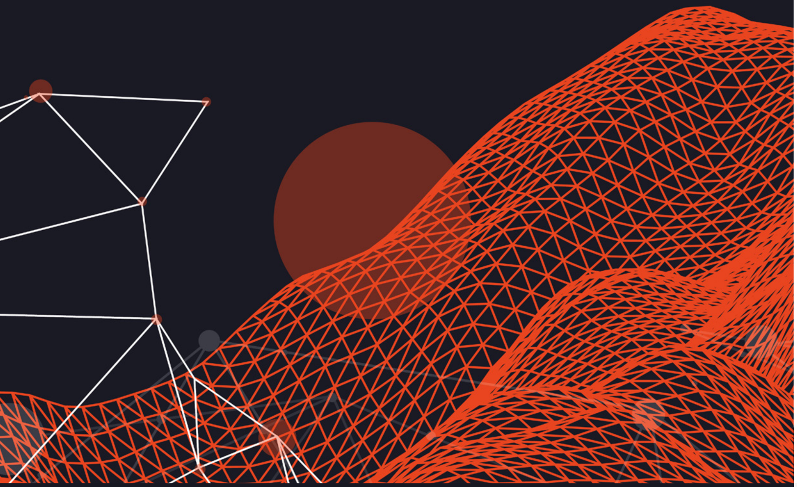
INITIAL ACCESS BROKERS, INSIDER THREATS, AND SUPPLY CHAIN ATTACKS

ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM

CYBER ESSENTIALS

AICPA SOC

Crown
Commercial
Service
Supplier



SEARCHLIGHT CYBER

Searchlight Cyber provides organizations with relevant and actionable dark web intelligence, to help them identify and prevent criminal activity. Founded in 2017 with a mission to stop criminals acting with impunity on the dark web, we have been involved in some of the world's largest dark web investigations and have the most comprehensive dataset based on proprietary techniques and ground-breaking academic research. Today we help government and law enforcement, enterprises, and managed security services providers around the world to illuminate deep and dark web threats and prevent attacks.

ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM

CYBER ESSENTIALS

AICPA SOC

Crown
Commercial
Service
Supplier

CONTENTS

INTRODUCTION

Security teams in the finance sector are some of the most conscious of risks emanating from the dark web. In our recent survey of CISOs, a commanding 99 percent of those at financial services companies said they were concerned about dark web threats against their organization.[1] Many of these businesses have also started gathering data from the dark web but our research showed that there are missed opportunities in how this data is being used. For example, of those who collect dark web data, only 24 percent are using it for threat hunting.

The purpose of this report is to further the understanding within the banking sector of exactly what kind of threats they face on the dark web, and provide guidance on how this dark web intelligence can be used by a defending team to protect their organization from cyberattacks.

One major finding of our investigation was that organizations in the banking sector are being targeted by Initial Access Brokers on the dark web - criminals who sell entry points into the network onto other threat actors to exploit. We found evidence of malicious insiders - i.e. employees - sharing information on their organization or being recruited by cybercriminals. We also observed threat actors undertaking infrastructure reconnaissance and targeting financial service supply chains.

While this activity - and the dark web in general - sounds scary, the point of this report is not to alarm. In fact, it's to demonstrate the opportunity the dark web provides to security teams to identify threats and stop follow-on actions using data collected from the dark web, before the criminals launch the subsequent attack on their network.

Banks are always going to be a target for threat actors. What can change is how banks meet this threat. With dark web intelligence that alerts them to potential malicious activity while criminals are still in the "pre-attack" stage of their operations, security teams can adjust and improve their defenses based on what might happen in the future - not just respond to things that have happened in the past.

For example, we have observed threat actors that are known to be associated with ransomware groups interacting with some of the examples used in the report. Knowledge is power, and identifying these threats before the ransomware operator is able to successfully connect into your organization is a huge win for a defender. We hope this report sheds light on how dark web intelligence can help you identify threats earlier, and prevent attacks.

JIM SIMPSON
Director of Threat Intelligence
Searchlight Cyber

[1] https://www.slcyber.io/whitepapers-reports/proactive-defence-how-enterprises-are-using-dark-web-threat-intelligence/

THE DARK WEB THREAT LANDSCAPE FOR THE BANKING SECTOR

METHODOLOGY

This research is based on an investigation by Searchlight Cyber analysts using dark web data gathered from 2020 to date. The examples used in this report are a small sample of the posts, which have been selected because they are indicative of the types of activity observed against organizations in the banking sector. The examples are displayed through Cerberus, our dark web investigation platform, which archives dark web text even when the post or the site has been deleted or taken down.

KEY FINDINGS

- Initial Access Brokerage - where threat actors sell system access on forums - makes up the vast majority of dark web activity we observe against the banking sector.
- The types of initial access commonly observed include remote network access, webshells, remote code execution, and SQL injection.
- As well as Initial Access Broker activity, we observed posts related to insider threat, infrastructure reconnaissance, and supply chain risk.
- We observed the most threats against banks in the United States, followed closely by European countries with the most common being the UK, France, and Spain. Victims were also listed across South America and Asia.
- Forums used by threat actors include XSS, Exploit, RaidForums, Dread, and Ramp.
- In a number of cases the target bank is named by threat actors, or a number of identifying details on the bank are given, which would allow security teams to identify and investigate a potential attack.

INITIAL ACCESS BROKERS

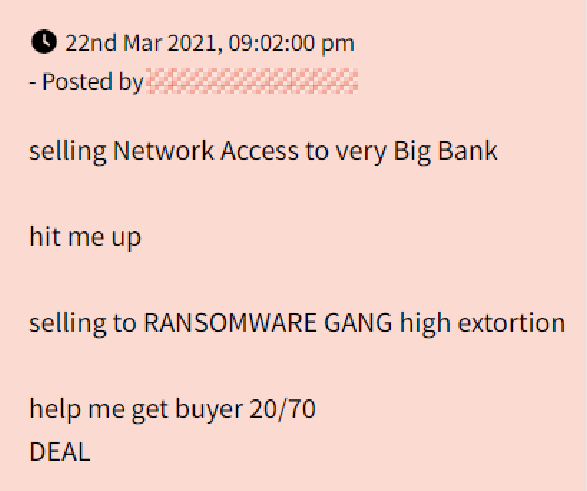
The vast majority of activity we observe against the banking sector on the dark web is Initial Access Broker posts. An Initial Access Broker is a type of cybercriminal who provides access for third party threat actors into an organization. They don't orchestrate attacks themselves but their specialization in gaining network access is relied on by other cybercriminals who either don't have the skills to gain access or prefer to focus their resources further down the attack chain, where profits are higher. In return, Initial Access Brokers can generate consistent returns while taking on a relatively low-risk portion of the attack.

It is unsurprising that this is the most common activity we observe because Initial Access Brokers have a clear incentive to post on the dark web: they need to sell their goods. They can gain access without posting on the dark web, and cybercriminals can use the access they have bought without shouting about it. However, there is a point in time when they need to communicate - and that is at the point of sale.

These communications provide cybersecurity professionals with a valuable opportunity to learn about their attackers and their techniques. As this section of the report will show, there is a variety of different types of access that are advertised on dark web hacking forums such as Exploit, XSS, and BreachForums.

For security teams, data on Initial Access Broker activity can be a valuable source of "pre-attack" intelligence. Knowledge of potential access being sold to their organization - or an organization that matches their profile - can alert security professionals to the need to take action before the access is exploited in a full blown cyberattack.

For example, we have observed threat actors that are known to be associated with ransomware groups interacting with some of the Initial Access Broker posts used as examples in this section. Knowledge is power, and identifying access being sold before the ransomware operator is able to successfully breach your organization is a huge win for defenders.



🕓 22nd Mar 2021, 09:02:00 pm
- Posted by [redacted]

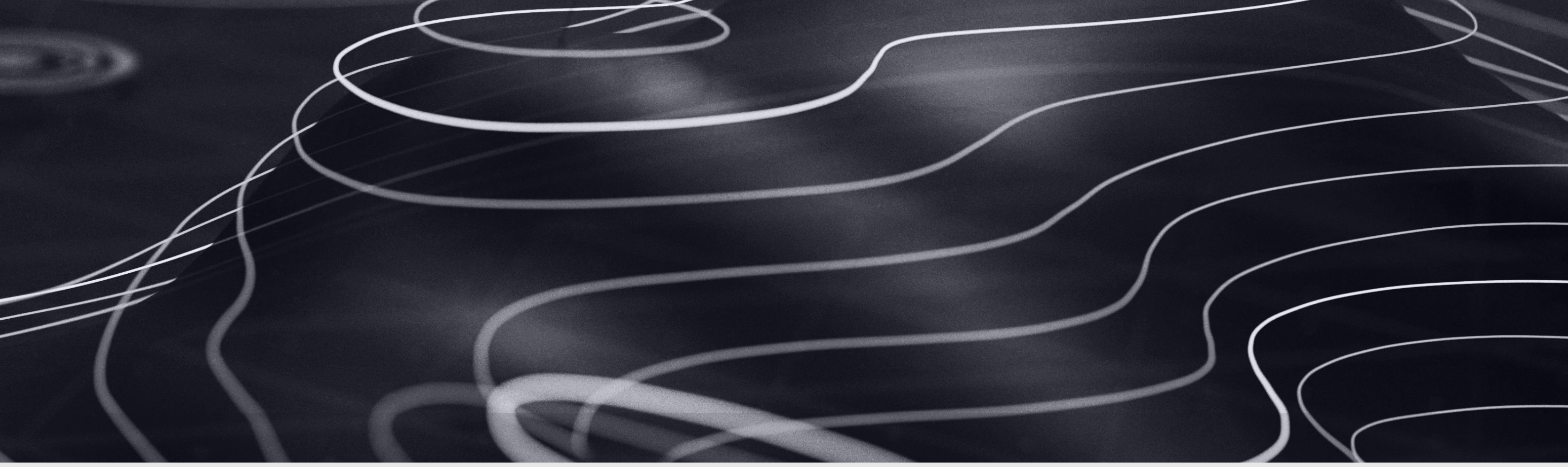
selling Network Access to very Big Bank

hit me up

selling to RANSOMWARE GANG high extortion

help me get buyer 20/70
DEAL

Figure 1: An Initial Access Broker advertises network access to a bank to ransomware operators on the dark web forum RaidForums.



PIVOTING TO THE THREAT ACTOR

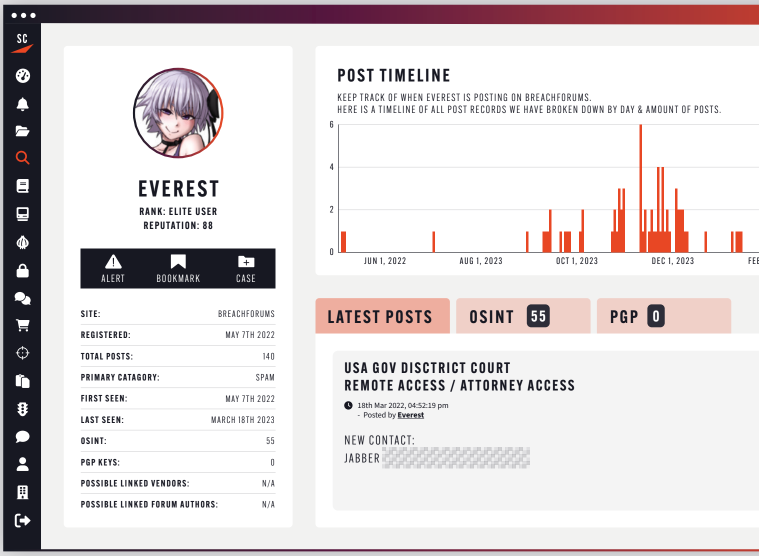
Another way that defenders can use Initial Access Broker posts is to analyze the capabilities and assess the threat of the actors posting and interacting with them. Reviewing previous posts linked to an actor, or associated profiles on other accounts, can provide valuable insight into the tactics the attacker uses, or the likelihood that the threat is genuine.

Modern day defenders are overwhelmed with alerts, data, and industry trends to keep up with - the last thing they need is to be chasing every single lead they have. Dark web intelligence can therefore provide a valuable opportunity to triage out any threat actors that may not be assessed as credible threats. For example, a threat actor posting on dark web forums asking what a webshell is might not be considered a credible threat worthy of investigation, even if they make big claims.

Meanwhile, a threat actor such as Everest - who have been observed increasingly selling initial access[2] - may be considered capable based on their previous activity as a ransomware operator. Therefore, any forum post from Everest advertising access to a company that matches your organization should be given high priority.

As well as the track record of the Initial Access Brokers, defenders can also identify other threat actors that are interacting with their posts - and are potentially looking to buy the access to orchestrate the attack. In many cases, by pivoting from an Initial Access Broker post to the actor who is interested, our threat intelligence team has been able to gather data on the specific tools used by a potential buyer - invaluable information that could allow a security team to harden their internal defenses and monitoring, even if the initial attack vector cannot be remediated.

In this section we have categorized some of the most common forms of initial access that we observe being sold against organizations in the banking sector.



EVEREST
RANK: ELITE USER
REPUTATION: 88

SITE:	BREACHFORUMS
REGISTERED:	MAY 7TH 2022
TOTAL POSTS:	140
PRIMARY CATAGORY:	SPAM
FIRST SEEN:	MAY 7TH 2022
LAST SEEN:	MARCH 18TH 2023
OSINT:	55
PGP KEYS:	0
POSSIBLE LINKED VENDORS:	N/A
POSSIBLE LINKED FORUM AUTHORS:	N/A

KEEP TRACK OF WHEN EVEREST IS POSTING ON BREACHFORUMS.
HERE IS A TIMELINE OF ALL POST RECORDS WE HAVE BROKEN DOWN BY DAY & AMOUNT OF POSTS.

USA GOV DISCTRICT COURT
REMOTE ACCESS / ATTORNEY ACCESS

18th Mar 2022, 04:52:19 pm
- Posted by Everest

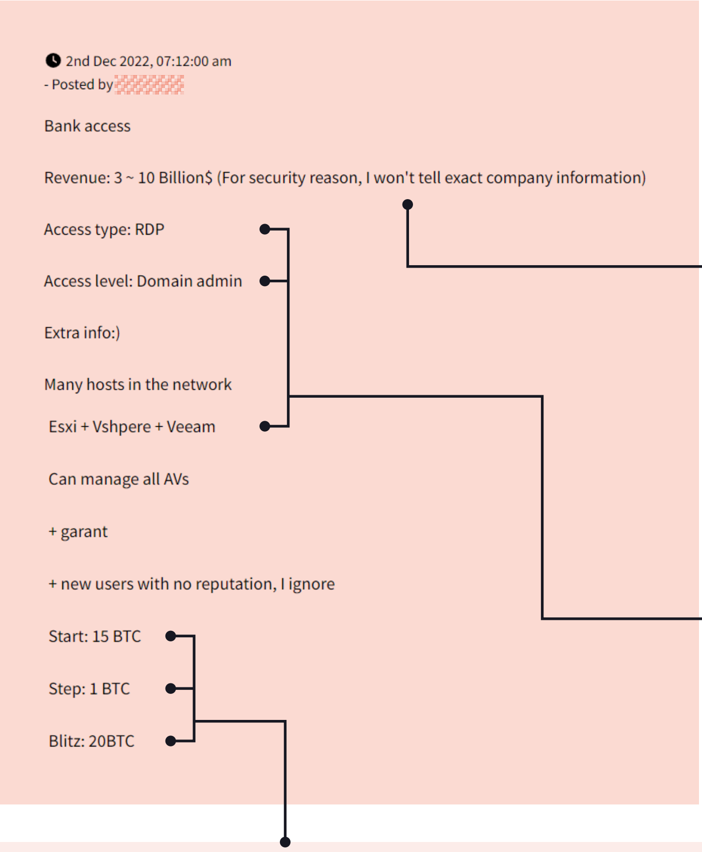
NEW CONTACT:
JABBER [redacted]

Figure 2: A sample of the information we have gathered on the threat actor Everest's activity on BreachForums, collated in our dark web investigation platform Cerberus.

[2] https://www.slcyber.io/everest-ransomware-group-increases-initial-access-broker-activity/

REMOTE NETWORK ACCESS

Remote network access is a large category in our observation of threat actors, which includes actors selling access to Remote Desktop Protocols (RDPs) and Virtual Private Networks (VPN). These technologies are common targets to hackers because of the "trusted" path they provide onto the infrastructure. **Figure 3** is a typical post and has some points worth noting:



2nd Dec 2022, 07:12:00 am
- Posted by [redacted]

Bank access

Revenue: 3 ~ 10 Billion$ (For security reason, I won't tell exact company information)

Access type: RDP

Access level: Domain admin

Extra info:)

Many hosts in the network

Esxi + Vshpere + Veeam

Can manage all AVs

+ garant

+ new users with no reputation, I ignore

Start: 15 BTC

Step: 1 BTC

Blitz: 20BTC

Figure 3: An Initial Access Broker auctions RDP access on the dark web forum Exploit.

THE ORGANIZATION IS NOT NAMED

This is common in Initial Access Broker posts so that the organization is not alerted to the fact that their network has been compromised. In this case, the threat actor explicitly says it is not naming the company for "security reasons". However, information on the revenue and technologies the organization uses could be enough for a security team to build a threat model on the hypothesis that it is their organization being targeted.

INFORMATION ON ACCESS

The threat actor provides technical detail on what they are selling, such as the system "RDP", the access level "Domain admin", and the technologies on the network "Esxi + Vshphere + Veeam".

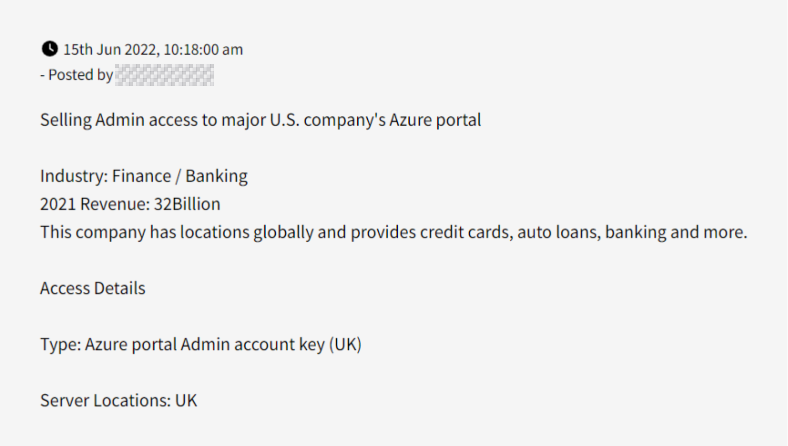
THE AUCTION PROCESS

The threat actor 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.

Cryptocurrency such as Bitcoin is often the payment method of choice for cybercriminals on the dark web because of the perception that it is more anonymous than traditional payment methods. The seller also indicates that he is not interested in buyers with "no reputation", which demonstrates that like all marketplaces the dark web is still run on trust.

Figure 4 is a slightly different case, where a threat actor is selling access to the Azure portal of a US financial institution through a compromised account key. As observed in many Initial Access Broker sales threads, the seller posts the revenue of the company, where it's based, and a description of their services - which may help a defending team identify whether it is likely that their organization has been targeted.

The threat actor explains that they are selling an administrator account key for the Azure servers, which could allow a buyer to access all of the services running within that Microsoft environment for the financial institution.



🕒 15th Jun 2022, 10:18:00 am
- Posted by [redacted]

Selling Admin access to major U.S. company's Azure portal

Industry: Finance / Banking
2021 Revenue: 32Billion
This company has locations globally and provides credit cards, auto loans, banking and more.

Access Details

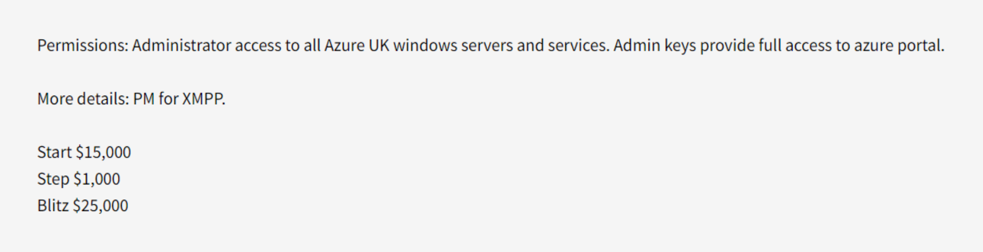
Type: Azure portal Admin account key (UK)

Server Locations: UK

Figure 4: An Initial Access Broker offers admin access to a major finance organization in the US on the dark web forum Exploit.

The exploitation of a privileged account is a serious incident, and could potentially lead to malware or ransomware being deployed on the system, control over the infrastructure operating for the organization, access to sensitive databases and file storage, and the harvesting of confidential information used to blackmail the victim into paying a ransom.

Once again, this Initial Access Broker provides the Start, Step, and Blitz prices for the auction further down the post (**Figure 5**). While $25,000 might sound like a lot of money, it is very little in comparison to the damage that could be done if a ransomware operator was able to successfully exploit the access. By point of comparison, researchers at Trend Micro used leaked data from the ransomware group Conti to estimate that the group had an annual income of at least $50,000,000 a year.[3]

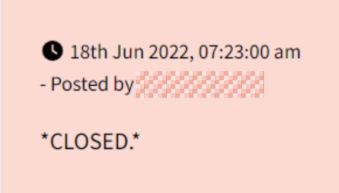


Permissions: Administrator access to all Azure UK windows servers and services. Admin keys provide full access to azure portal.

More details: PM for XMPP.

Start $15,000
Step $1,000
Blitz $25,000

Figure 5: The Initial Access Broker's post includes "Start", "Step", and "Blitz" prices for the auction.



🕒 18th Jun 2022, 07:23:00 am
- Posted by [redacted]

CLOSED.

Figure 6: Three days after the initial post the Initial Access Broker indicates the auction is closed.

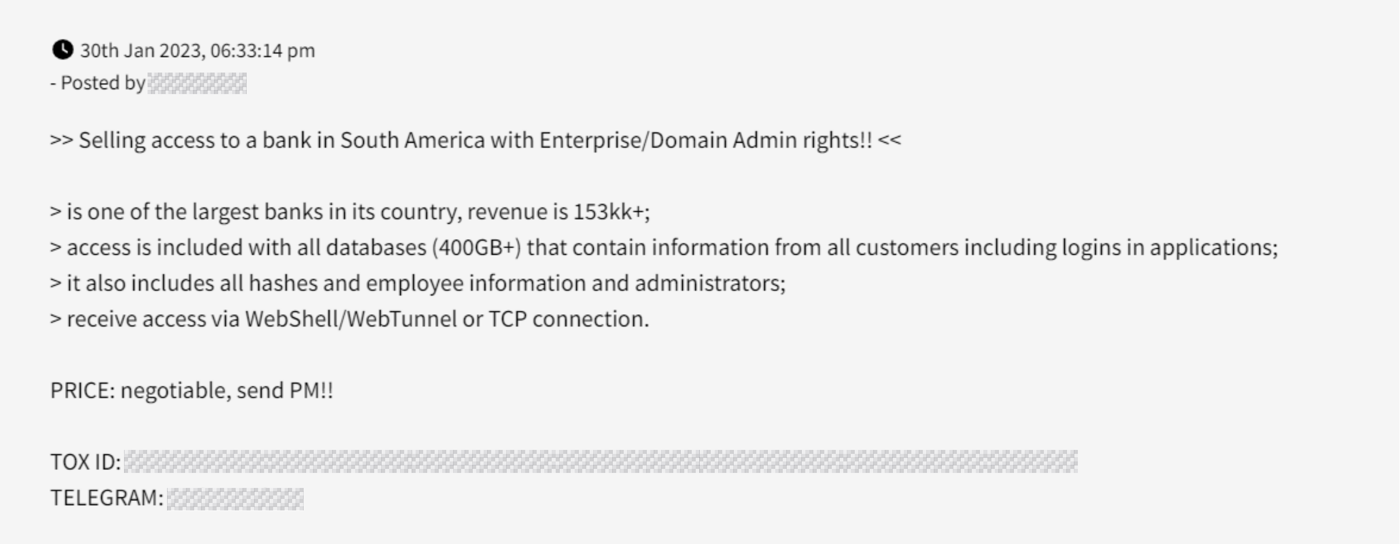
Several days after the post, the broker commented that the auction was closed (**Figure 6**), which is a strong indicator that - if a buyer was found - negotiations took place away from the forum. However, using dark web intelligence an analyst could track the Initial Access Broker, explore any similar attack vectors or sales, and identify who they may be communicating with to assess the exploitation tactics of a potential buyer.

[3] https://documents.trendmicro.com/assets/white_papers/wp-inside-the-halls-of-a-cybercrime-business.pdf

WEBSHELLS

A webshell is a malicious script used by threat actors to manipulate a web server from a remote location. Once the webshell is installed it can be used as a backdoor into the system that has been compromised. This backdoor allows the threat actor to return to the system to launch further attacks, with the ability to execute commands, upload and download files, or create new user accounts. Or in the Initial Access Broker cases we have observed - to sell the access for other cybercriminals to exploit.

In our research we observed a number of webshells for sale by Initial Access Brokers against targets in the banking sector. One such example (**Figure 7**) is the recent sale of a webshell for a South American bank on the hacking forum, BreachForums.



30th Jan 2023, 06:33:14 pm
- Posted by [redacted]

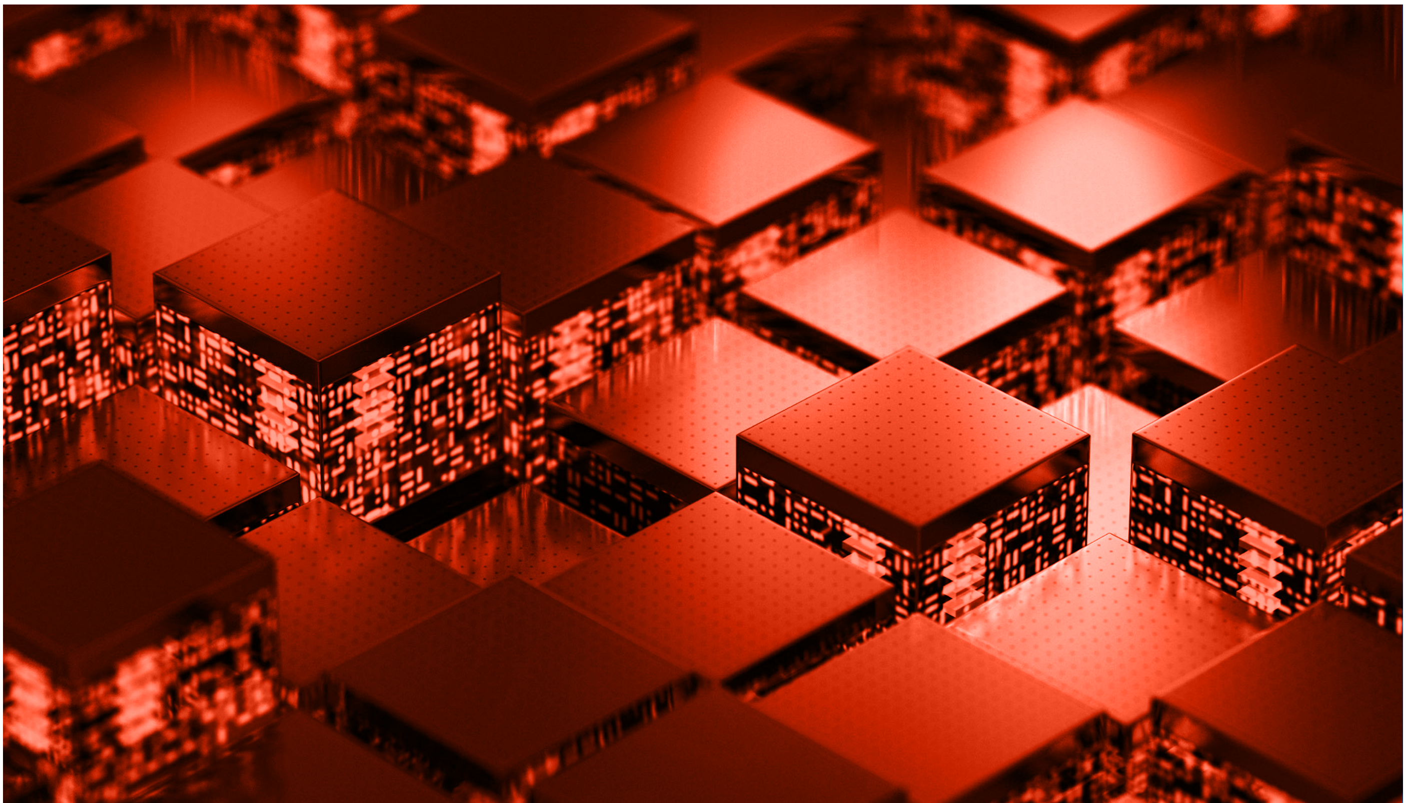
>> Selling access to a bank in South America with Enterprise/Domain Admin rights!! <<

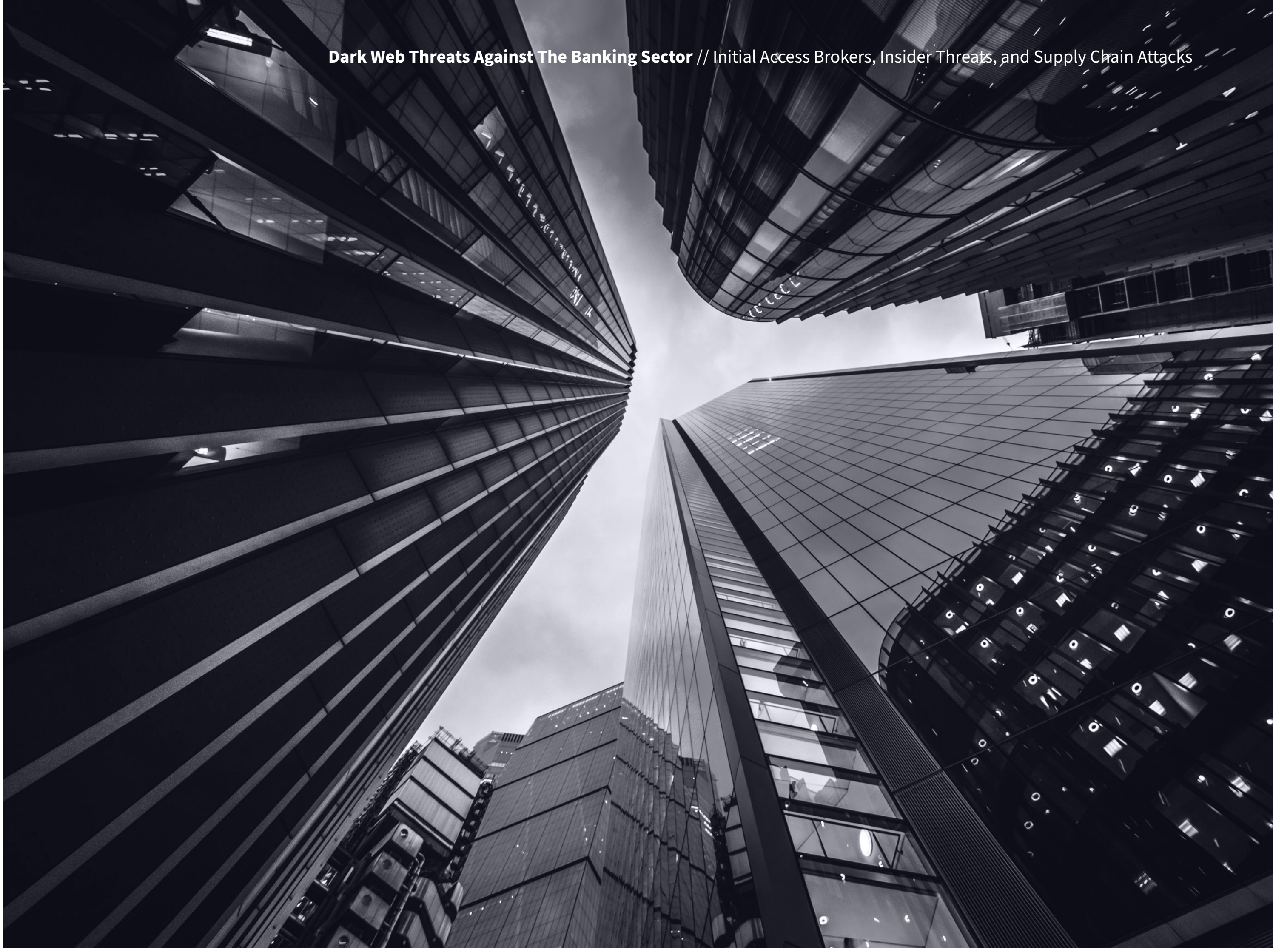
> is one of the largest banks in its country, revenue is 153kk+;
> access is included with all databases (400GB+) that contain information from all customers including logins in applications;
> it also includes all hashes and employee information and administrators;
> receive access via WebShell/WebTunnel or TCP connection.

PRICE: negotiable, send PM!!

TOX ID: [redacted]
TELEGRAM: [redacted]

Figure 7: An Initial Access Broker sells access to a South American bank via a webshell on BreachForums.





Alarmingly the webshell is posted for sale with domain admin rights - meaning a buyer could easily install malware or other malicious tools on the machine with relative ease in comparison to if the webshell was a low level user account.

As well as advertising it being a South American bank, the seller also posts other vital information about the bank including its revenue, which is a common sales tactic used by Initial Access Brokers to indicate the potential return a buyer could make through a cyberattack on the organization.

For cyber defenders tasked with proactively finding threat intelligence to protect their organizations, this information could prove critical in identifying an attack against their company, if it matches their profile.

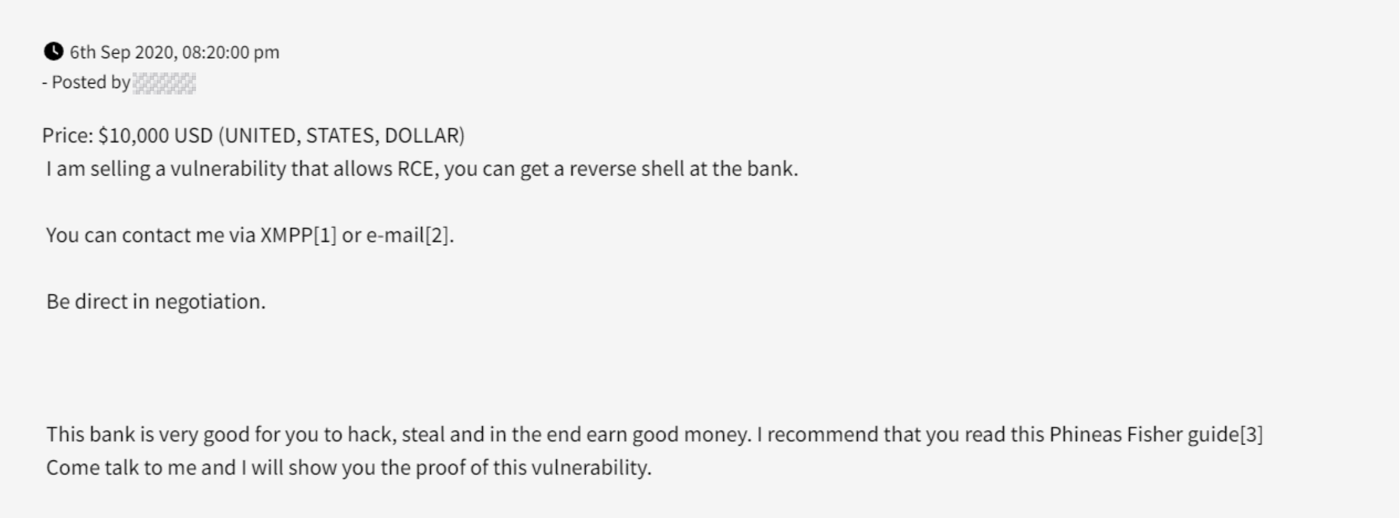
Having identified the post, a threat hunter could conduct an investigation into the actor in order to find additional intelligence - such as any linked accounts, email addresses, crypto-wallets, Telegram / TOX / Jabber accounts etc, but also information about how the actor operates, which may be vital to pinpointing where the vulnerability may be. For example, a threat actor who has posted frequently about hacking a particular Wordpress extension, or abusing a CVE in software running on a web server, this may be a good place to start threat hunting.

Using our dark web intelligence tools, Searchlight Cyber analysts were able to find a TOX ID, Telegram Channel, and multiple dark web accounts for this Initial Access Broker, who we track under the alias Magnetic Wolf. Though this by itself in isolation isn’t enough for solid attribution, it is a path to further intelligence on how the threat actor operates, which could be used to inform defenses.

REMOTE CODE EXECUTION

A remote code execution (RCE) is a classification of vulnerability that, when exploited, allows the attacker to make an application execute code they choose, rather than doing what the application should be doing. RCEs are no strangers to being sold on the dark web, and in fact these make up a good portion of our observed threats against the financial sector.

Taking one example of this, in **Figure 8** a threat actor is selling an RCE for a bank, which would allow a attacker to get a "reverse shell". This is a common type of hack where the target machine calls back to the hacker, instead of the hacker connecting to the target machine - which will allow the attacker to execute commands on the remote machine. This RCE is sold at a price of $10,000 and the broker asks to be contacted off-forum for negotiations.



6th Sep 2020, 08:20:00 pm
- Posted by [redacted]

Price: $10,000 USD (UNITED, STATES, DOLLAR)
I am selling a vulnerability that allows RCE, you can get a reverse shell at the bank.

You can contact me via XMPP[1] or e-mail[2].

Be direct in negotiation.

This bank is very good for you to hack, steal and in the end earn good money. I recommend that you read this Phineas Fisher guide[3]
Come talk to me and I will show you the proof of this vulnerability.

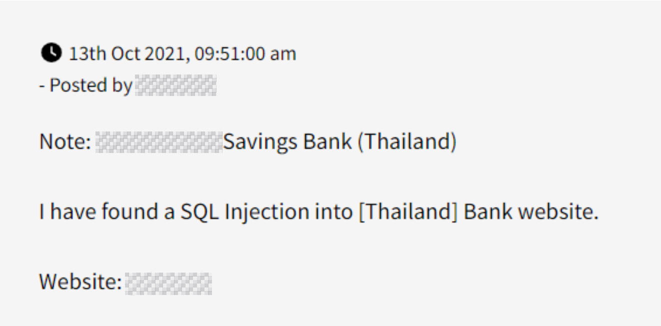
Figure 8: An Initial Access Broker advertises an RCE in a US bank on the hacking forum Exploit.

However, once again, the actor provides a number of details across their dark web forum posts that could be analyzed by defenders to build an arsenal of intelligence on that threat actor, potentially allowing them to remediate before a buyer is found.

SQL INJECTION

A Structured Query Language (SQL) injection is a type of hack whereby a threat actor is able to inject malicious code into a database query, which can often result in data being exposed or code being executed. SQL injections have long been established as an issue in cybersecurity and newer, well-built web applications are often less vulnerable to such flaws.

However, it is a vulnerability that continues to persist. For example, the recent MOVEit SQL vulnerability was estimated to have impacted hundreds of organizations and was exploited by the ransomware group Cl0p to orchestrate attacks at scale.[4]



13th Oct 2021, 09:51:00 am
- Posted by [redacted]

Note: [redacted] Savings Bank (Thailand)

I have found a SQL Injection into [Thailand] Bank website.

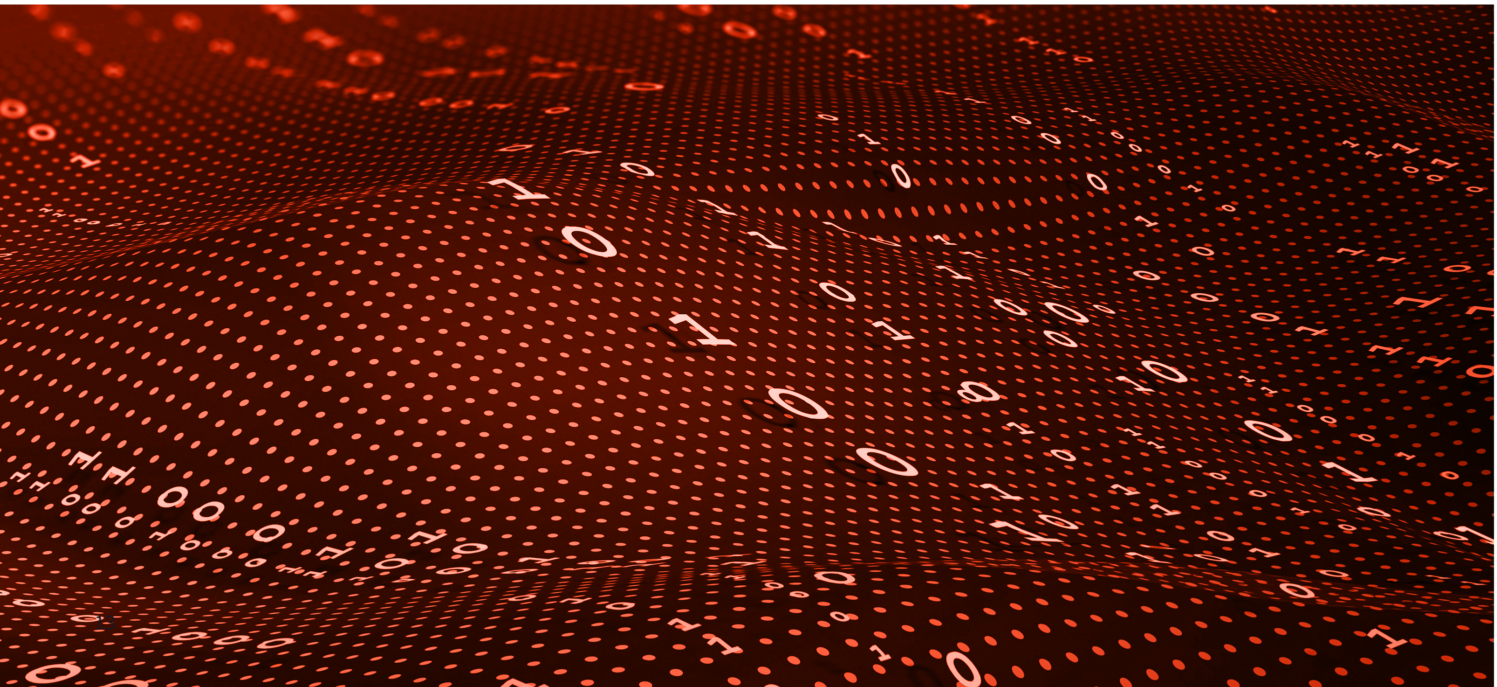
Website: [redacted]

Figure 9: An Initial Access Broker advertises an SQL injection into a Thai bank on the (now closed) hacking forum RaidForums.

In our research, Searchlight Cyber analysts observed a threat actor selling an SQL injection vulnerability for a bank, which has its website running on Wordpress (**Figure 9**). In this sale, the threat actor is selling the website administrator's account credentials, which would allow a threat actor to potentially install malicious extensions, and could even reveal database passwords or code handling requests, depending on the setup of the website and server.

Knowledge of this could then develop further to allow a sophisticated hacker, such as a well developed crime group or a state-backed group, to develop exploits against the bank, which could lead to huge financial losses as well as a data breach. This post received a lot of attention with the threat actor asking that potential buyers make them an offer via Telegram.

[4] https://www.darkreading.com/attacks-breaches/cl0p-claims-moveit-attack-how-gang-did-it



INSIDER THREAT

An insider threat is somebody within an organization - usually an employee, contractor, or third party with privileged access - who undermines the security of the company from within.

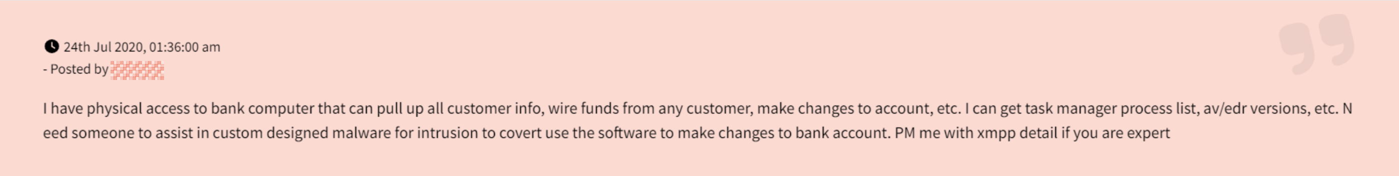
Insider threat is a broad category that usually includes employees that accidently compromise the security of the organization without malicious intent. For example, an employee who is the victim of a phishing attack or a staff member that takes confidential data off the network without recognising the consequences.

However, for the purposes of this report we are focusing on malicious insiders who are intentionally looking to compromise the organization from within, which we observe frequently for banking sector organizations.

There are two main opportunities to spot this type of insider threat activity outside of the organization's network: when employees with access advertise it on the web, or when threat actors try to recruit malicious insiders. We will examine examples of both in this section.

One caveat that does have to be provided at the outset is that individuals on the internet can engage in interactions, and even create whole personas, that are pure fantasy. Often individuals create fake accounts purporting to be somebody they are not for their own gratification and it is therefore possible that their claims of access or intention to abuse it are also inflated.

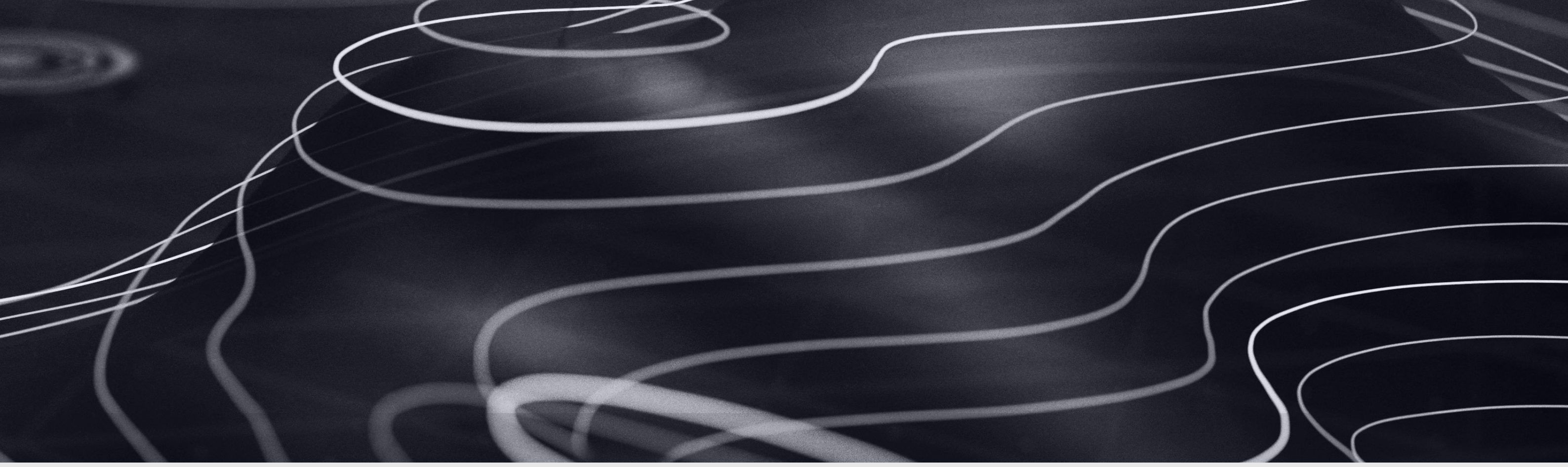
However, for a security team that has to consider malicious insiders with privileged access as part of their threat model, these posts do provide a valuable starting point to investigate and mitigate the risk of compromised employees. Armed with this intelligence, defenders can potentially find the malicious employee or at least the internal vulnerability they are exploiting, identify their activity within their network to prevent the breach, and take legal action where required.



24th Jul 2020, 01:36:00 am
- Posted by [redacted]

I have physical access to bank computer that can pull up all customer info, wire funds from any customer, make changes to account, etc. I can get task manager process list, av/edr versions, etc. N
eed someone to assist in custom designed malware for intrusion to covert use the software to make changes to bank account. PM me with xmpp detail if you are expert

Figure 10: A malicious insider asks for malware support on the dark web forum, Exploit.



CONNECTIONS TO TOR

Most of the examples used in this section of the report come from “clear web” hacking websites - i.e. sites that can be accessed via a regular browser, where individuals quite brazenly discuss cybercriminal activity. It is common for malicious insiders to use these websites or messaging services such as Telegram because they are not necessarily technical hackers themselves so they are looking to others on the forum for advice or to sell to. Similarly, cybercriminal recruiters use these sites to find malicious insiders who might not frequent the usual dark web forums where they operate.

However, security teams should also be aware of - and be monitoring for - employees using dark web networks such as Tor to communicate with the wider cybercriminal underworld or to leak data. In addition to monitoring dark web forums for malicious insiders, traffic between Tor and the company network can also be used as an early warning sign of a potential insider threat.

Many banks will have traffic coming *from* Tor *to* their network. This can be benign traffic, where people are visiting the bank’s website from the dark web. However, monitoring for anomalous traffic activity, such as a large number of connections, or inconsistencies in data request vs response can help security teams to identify if their network is being probed or attacked by threat actors from Tor. Where traffic is to non-browsable web content - i.e. access to VPN portals or login pages - the chance that this is malicious traffic increases. Ask yourself: why would an employee access your VPN portal via Tor?

In particular, connections *from* the company network *to* the Tor network are a very reliable data point for discovering insider threat because there is virtually no good reason why an employee would be connecting to the dark web in most organizations. Traffic going in this direction usually indicates one of only a few possibilities:

1 // An employee is engaging in illegal activity on the dark web, which is potentially putting the company at risk.

2 // An employee is deliberately engaging with cybercriminals through the dark web, which could include sharing data or providing access to the network.

3 // The network has already been compromised and the traffic leaving the corporate network is a beacon calling back to a command and control server.

Each of these justifies immediate investigation from the security team and should be seen as one of the clearest signals of malicious activity.

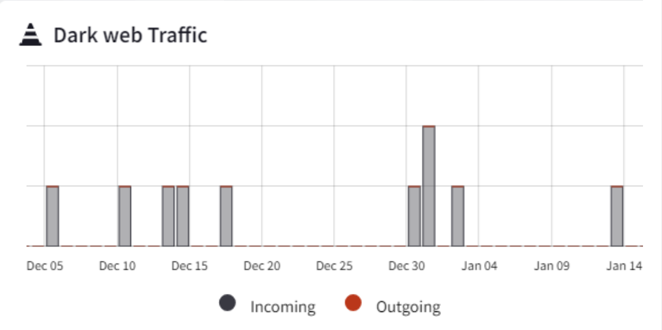
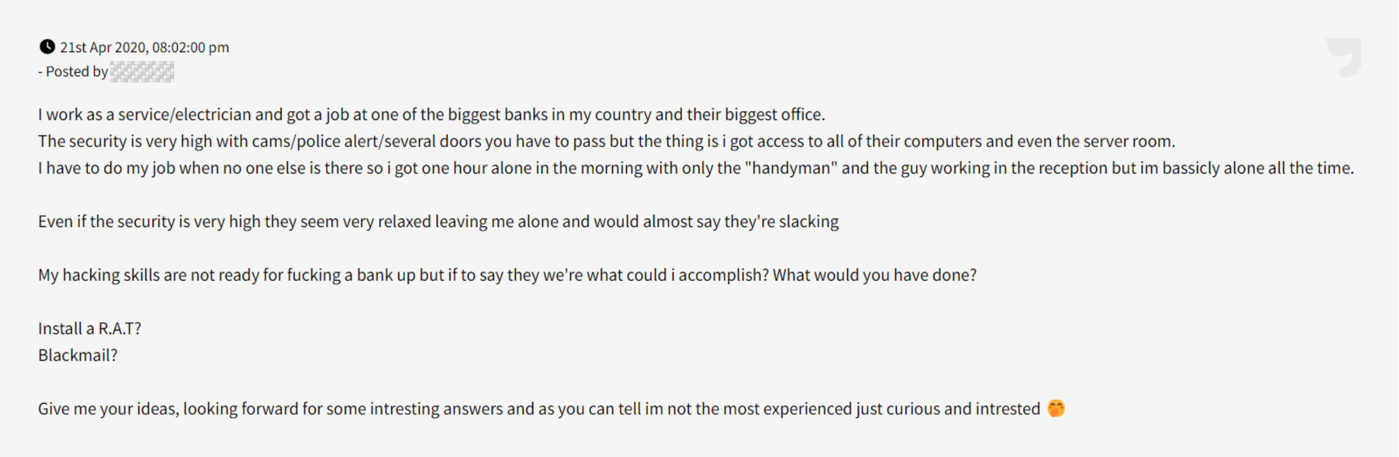


Figure 11: Tor traffic to and from a bank’s network, visualized through our dark web monitoring platform DarkIQ

A MALICIOUS EMPLOYEE

Figure 12 shows a forum user asking advice on how they can exploit their legitimate access to a bank's computers and server room. In particular, the individual - who claims to be an electrician - asks about installing a remote access trojan (RAT) or blackmailing the bank.



21st Apr 2020, 08:02:00 pm
- Posted by [redacted]

I work as a service/electrician and got a job at one of the biggest banks in my country and their biggest office.
The security is very high with cams/police alert/several doors you have to pass but the thing is i got access to all of their computers and even the server room.
I have to do my job when no one else is there so i got one hour alone in the morning with only the "handyman" and the guy working in the reception but im bassicly alone all the time.

Even if the security is very high they seem very relaxed leaving me alone and would almost say they're slacking

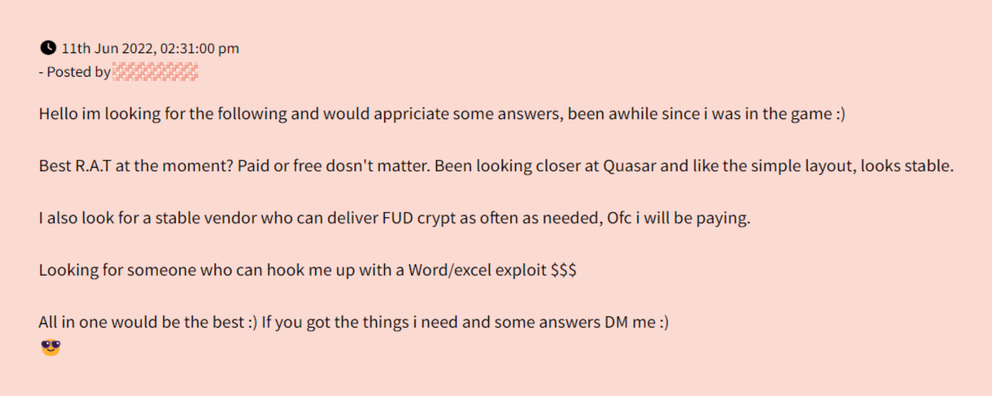
My hacking skills are not ready for fucking a bank up but if to say they we're what could i accomplish? What would you have done?

Install a R.A.T?
Blackmail?

Give me your ideas, looking forward for some intresting answers and as you can tell im not the most experienced just curious and intrested 🤭

Figure 12: An actor claiming to have access to "one of the biggest banks" in the country asks for ideas on a clear web hacking website.

While aspects of this post alone might suggest it is a fantasy, with the poster claiming they are just "curious and interested", in a later post (**Figure 13**) the same user asks for advice on the best RAT malware they can buy and even names one which they have specifically been looking into.



11th Jun 2022, 02:31:00 pm
- Posted by [redacted]

Hello im looking for the following and would appriciate some answers, been awhile since i was in the game :)

Best R.A.T at the moment? Paid or free dosn't matter. Been looking closer at Quasar and like the simple layout, looks stable.

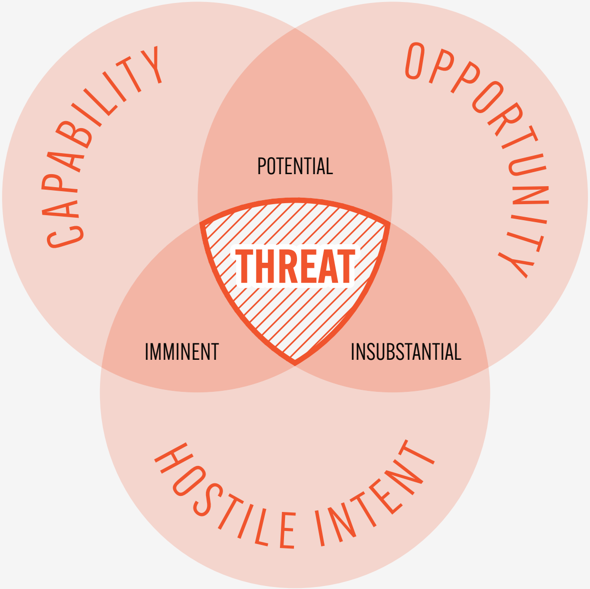
I also look for a stable vendor who can deliver FUD crypt as often as needed, Ofc i will be paying.

Looking for someone who can hook me up with a Word/excel exploit $$$

All in one would be the best :) If you got the things i need and some answers DM me :)
😎

Figure 13: The same actor asks for advice on Remote Access Trojans less than two months later.

The detail provided in this second post shows an increased risk of attack because the insider is now demonstrating the three components that constitute a threat:



OPPORTUNITY

The actor has already stated they have access to computers and the server room.

HOSTILE INTENT

Their posts are inquiring about ways to exploit the business.

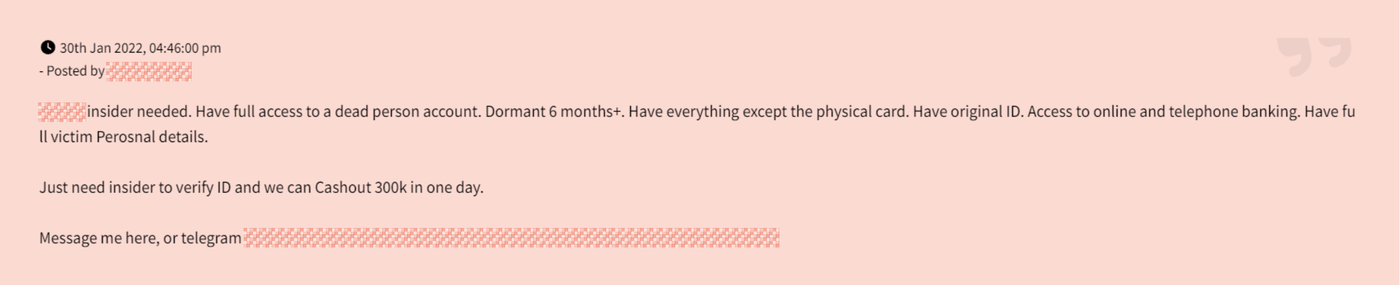
CAPABILITY

Finally, this latest post shows that the insider has technical knowledge and is looking for support from other criminals to build the capability to execute the attack.

A threat hunting team concerned about malicious insiders could pivot on the actor's profile to identify whether this is one of their employees and poses a potential threat. For example, by investigating unique strings, usernames and terms, we have been able to identify a number of email addresses associated with the actor. This information could be useful for a team of defenders in identifying any employees that have the email address or name of the email account holder.

RECRUITING

As well as insiders poised to inflict damage on their organization, cybercriminals are also stalking the internet trying to recruit people on the inside for their own criminal deeds. In one such case (**Figure 14**), an actor is trying to recruit a bank insider who will have access to the bank of a deceased individual in order to commit fraud.



30th Jan 2022, 04:46:00 pm
- Posted by [redacted]

[redacted] insider needed. Have full access to a dead person account. Dormant 6 months+. Have everything except the physical card. Have original ID. Access to online and telephone banking. Have full victim Perosnal details.

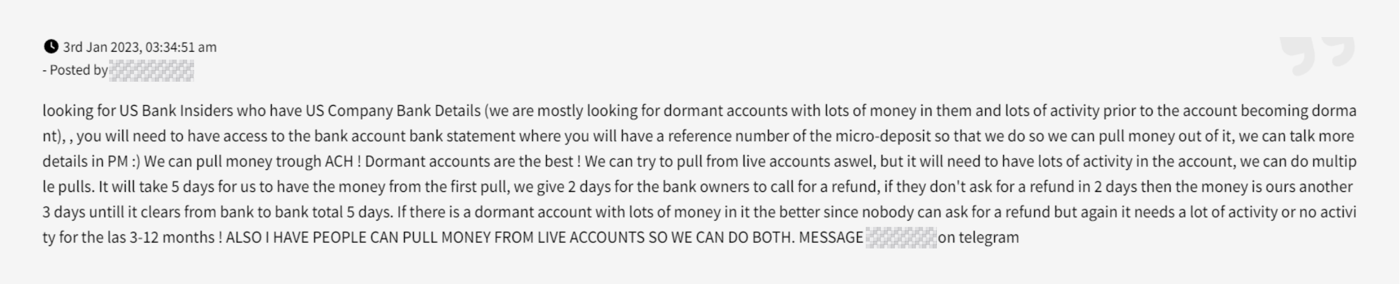
Just need insider to verify ID and we can Cashout 300k in one day.

Message me here, or telegram [redacted]

Figure 14: A user asks for an insider at a specific bank on a clear web hacking forum.

Though this is not a cyber threat to the bank itself, it is nevertheless encouraging bank insiders to commit cyber-enabled crimes. The target bank is named in the post (redacted by us), which means that this intelligence could be used by the organization to monitor for suspicious account activity or malicious employee behavior. At the very least, it should become a standing intelligence requirement to monitor for interactions with the post.

Another post (**Figure 15**) shows a threat actor looking to recruit insiders at US banks for a fraud scheme involving dormant accounts.



3rd Jan 2023, 03:34:51 am
- Posted by [redacted]

looking for US Bank Insiders who have US Company Bank Details (we are mostly looking for dormant accounts with lots of money in them and lots of activity prior to the account becoming dormant), , you will need to have access to the bank account bank statement where you will have a reference number of the micro-deposit so that we do so we can pull money out of it, we can talk more details in PM :) We can pull money trough ACH ! Dormant accounts are the best ! We can try to pull from live accounts aswel, but it will need to have lots of activity in the account, we can do multiple pulls. It will take 5 days for us to have the money from the first pull, we give 2 days for the bank owners to call for a refund, if they don't ask for a refund in 2 days then the money is ours another 3 days untill it clears from bank to bank total 5 days. If there is a dormant account with lots of money in it the better since nobody can ask for a refund but again it needs a lot of activity or no activity for the las 3-12 months ! ALSO I HAVE PEOPLE CAN PULL MONEY FROM LIVE ACCOUNTS SO WE CAN DO BOTH. MESSAGE [redacted] on telegram

Figure 15: A threat actor tries to recruit US bank insiders for a fraud scheme on a clear web hacking forum.

Once again, a defending team could pivot on the alias of the poster to try to determine the capability and therefore risk of the perpetrator, monitor the post for engagement to assess if their employees are interacting, or use the information the cybercriminal provides on their scheme to run an intelligence-led investigation into whether this type of fraud is taking place within their business.

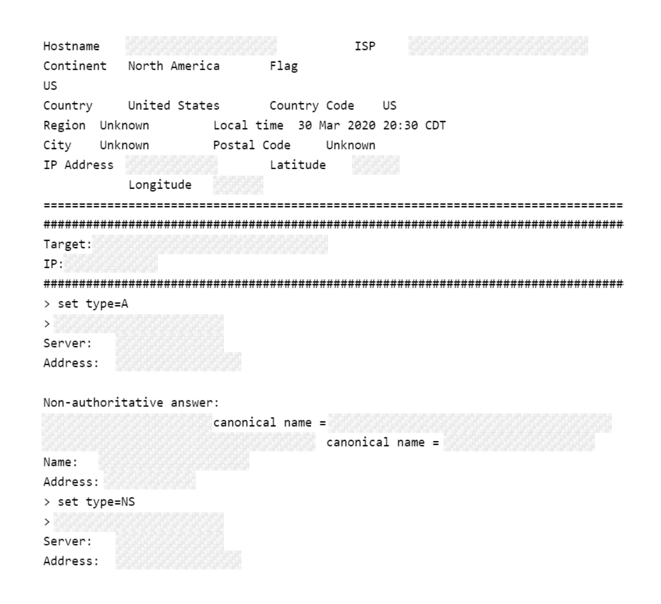
INFRASTRUCTURE RECONNAISSANCE

Threat actors also use the dark web to collaborate and plan their paths of attack. This activity is best defined by the MITRE ATT&CK framework as the two stages grouped in the PRE Matrix: Reconnaissance (TA0043) and Resource Development (TA0042):

RECONNAISSANCE	RESOURCE DEVELOPMENT
Techniques that involve adversaries actively or passively gathering information that can be used to support targeting, which may include details of the victim organization, infrastructure, or staff/personnel.	**Focused on an adversary trying to establish resources they can use to support operations, including techniques that involve adversaries creating, purchasing, or compromising/stealing resources that can be used to support targeting.**

These two tactics are significant because they are the only ones that focus on the period of time before the network is breached. This means that spotting activity at this stage gives security teams the best opportunity to actually stop a breach.

By way of example, (**Figure 16**) shows the start of a very long post, which lists an extensive amount of network and infrastructure information on a European national bank, based on various network scanning tools. This is the exact process that threat actors will go through in the Reconnaissance stage of an attack, gathering as much data as possible - including information about the network topology, operating systems and applications, and user accounts - to identify potential weaknesses and create an effective attack strategy.

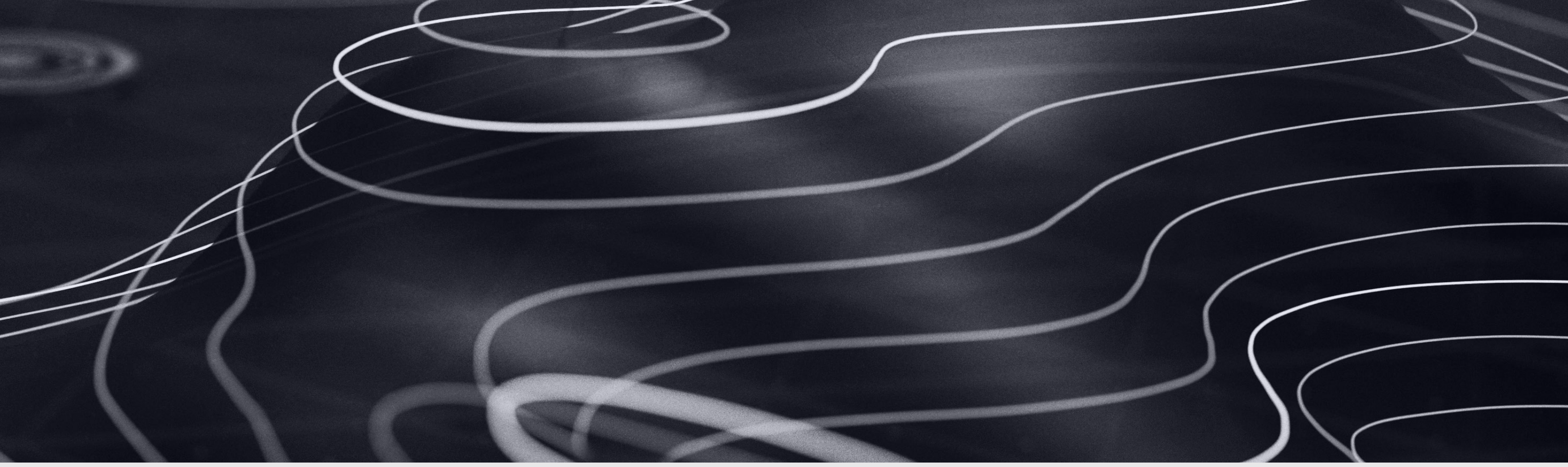


```
Hostname    [redacted]            ISP    [redacted]
Continent   North America      Flag
US
Country     United States      Country Code    US
Region  Unknown         Local time  30 Mar 2020 20:30 CDT
City    Unknown         Postal Code     Unknown
IP Address  [redacted]          Latitude    [redacted]
            Longitude  [redacted]
==================================================================================
##################################################################################
Target:[redacted]
IP:[redacted]
##################################################################################
> set type=A
> [redacted]
Server:
Address:

Non-authoritative answer:
[redacted]             canonical name = [redacted]
                                  canonical name = [redacted]
Name:
Address:
> set type=NS
> [redacted]
Server:
Address:
```

Figure 16: Redacted PasteBin post containing a vast amount of network information on a national European bank.

Armed with this intelligence that their infrastructure is being targeted and what is known by the attackers, the bank's security team could modify and enhance their defenses based on the most likely paths of attack.



SUPPLY CHAIN ATTACKS

Often threat actors' infrastructure reconnaissance leads them to an organization's supply chain as the initial point of compromise. Attackers have been targeting organizations' supply chains for a long time but there are very good reasons why it continues to persevere as a high risk attack vector for organizations.

Firstly, the reality is that most banks of any significant size will have very large and very complex supply chains. It is simply not possible for organizations to be across the security of every supplier, so they are reliant on security requirements and compliance to ensure their suppliers implement the correct security controls.

Secondly, organizations have extremely little visibility into the cybersecurity that their suppliers have in place because it is outside of their own infrastructure. It is impractical and - from a supplier's perspective, unreasonable - for a security team to gain access to their supplier's environment. This lack of visibility leaves organizations exposed to attack if they are unaware that their supplier has been compromised until it is too late to put security mitigations in place.

However, monitoring the dark web for the details of key suppliers can help organizations to gain visibility into potential threats by identifying when they are being targeted by threat actors.

For example, continuously searching for employee credentials, IP addresses, company datasets, devices, and software – can alert the enterprise to suspicious activity against their supplier that may indicate a potential attack. This gives the security team valuable time to warn their supplier and take their own defensive actions if they identify suspicious behavior.

Currently, this is a missed opportunity for many finance companies. In our recent survey of CISOs in the finance industry, 77 percent said that they would like to monitor for their suppliers being targeted on the dark web.[5] However, as of now, only 28 percent of those collecting dark web data are using it for that purpose.

Combined with implementing robust cybersecurity measures, conducting regular assessments, and collaborating with supply chain partners to ensure cybersecurity best practices - dark web monitoring can help organizations take a more proactive approach to their supply chain defense.

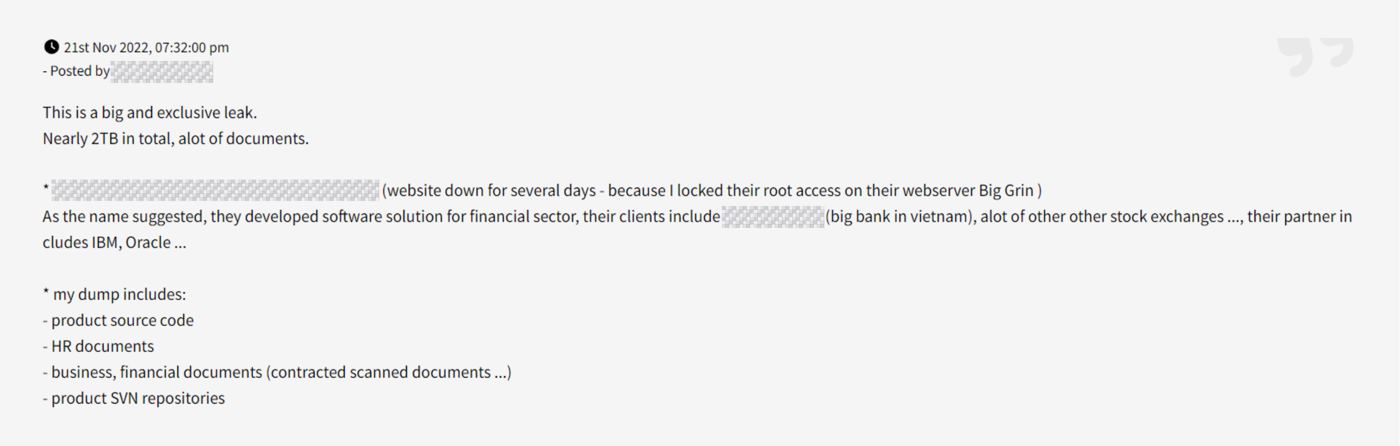
77% OF CISOS IN FINANCIAL SERVICES ORGANIZATIONS WANT TO MONITOR FOR THEIR SUPPLIERS BEING TARGETED ON THE DARK WEB.

ONLY **28%** OF THOSE COLLECTING DARK WEB DATA ARE CURRENTLY USING IT TO MONITOR FOR THREATS AGAINST THEIR SUPPLY CHAIN.

[5] https://www.slcyber.io/whitepapers-reports/proactive-defence-how-enterprises-are-using-dark-web-threat-intelligence/

SOURCE CODE SUPPLY CHAIN ATTACK

Figure 17 shows a threat actor selling data stolen from a financial services software supplier, including the source code of the product. The leak also includes financial records and HR documents but the source code in particular could allow hackers to find vulnerabilities which could, if exploited, lead to a data breach at one of the banks that uses the software.



21st Nov 2022, 07:32:00 pm
- Posted by [redacted]

This is a big and exclusive leak.
Nearly 2TB in total, alot of documents.

* [redacted] (website down for several days - because I locked their root access on their webserver Big Grin)
As the name suggested, they developed software solution for financial sector, their clients include [redacted] (big bank in vietnam), alot of other other stock exchanges ..., their partner in cludes IBM, Oracle ...

* my dump includes:
- product source code
- HR documents
- business, financial documents (contracted scanned documents ...)
- product SVN repositories

Figure 17: A threat actor advertises the sale of data stolen from a financial services software supplier, including source code.

In the post, the actor uses the name of the software supplier (redacted) and lists banks that the software is used by, clearly indicating the possibility to use this data in a supply chain attack.

However, from the perspective of a security team, this information could help them to quickly determine if their organization uses the supplier and whether they are vulnerable. In the scenario that they do use the supplier, they now have valuable time to put additional security measures in place before the source code is sold or a threat actor has time to use it to target their organization.

This information on a compromised supplier is invaluable intelligence for a security team and could be used to prevent an attack.

USING DARK WEB INTELLIGENCE FOR PROACTIVE CYBERSECURITY

Organizations in the banking sector are known to have some of the most comprehensive defensive measures in place. However, as this research has shown, that does not stop them from being targeted by cybercriminals. The barrier to entry is high for cybercriminals, but so is the return.

For banks, robust cyber tooling has to be combined with an intelligence-based approach to establish where the next attack is coming from, and what it might target. This is where dark web intelligence has a role to play.

Live data on dark web threats can support intelligence-driven investigations, allowing an organization to identify attacks against their sector before they are executed. These pre-attack warning signs provide valuable time for an organization to identify if they are at risk and to put the proper security controls in place to mitigate a potential incident.

Dark web data also allows intelligence-driven threat hunting within an organization's assets. Including, as this report has established, the human assets of the bank. This can help to identify vulnerabilities through threat modeling and a more proactive approach to security.

SEARCHLIGHT CYBER

COLLECT DARK WEB INTELLIGENCE WITH SEARCHLIGHT CYBER

Our dark web investigation and monitoring products give cybersecurity professionals unprecedented visibility into cybercriminal activity on hidden forums, marketplaces, and leak sites. Updated live, security teams can search and be alerted to threat actor activity that might indicate a group is in the reconnaissance stage of attack against their organization.

CERBERUS

DARK WEB INVESTIGATION

Cerberus provides security teams and threat hunters with the most comprehensive dark web dataset on the market, giving access to intelligence that was previously unobtainable.

EXTRACT THREAT INTELLIGENCE
Uncover activity of cybercriminals in the pre-attack phase and inform cyber defenses.

IDENTIFY THREAT ACTORS
Investigate individuals and groups with the ability to pivot on usernames, aliases, and connected accounts.

INTERROGATE HISTORIC DARK WEB DATA
Search an archive of more than 15 years of historic dark web data, including deleted posts and sites.

INVESTIGATE RANSOMWARE GROUPS
And spot ransomware attacks vs the finance sector, with the Ransomware Search & Insights module.

INFORM INCIDENT RESPONSE
Investigate the chain of events in the dark web that led to an attack to improve mitigation and response.

DARKIQ

DARK WEB MONITORING

DarkIQ continuously monitors the dark web for mentions of your organization, infrastructure components, staff credentials, supplier information, and more - to provide early warning signs of attack.

SPOT CRIMINAL RECONNAISSANCE
With our automated analyst continuously searching dark web marketplaces and forums.

MONITOR DARK WEB TRAFFIC
For early warning signs of anomalous activity that could indicate an external attack or insider threat.

ENHANCE SUPPLY CHAIN SECURITY
With visibility into the dark web exposure of suppliers and cybercriminals targeting third parties.

INCREASE SOC EFFICIENCY
Prioritize alerts based on dark web intelligence that indicates an imminent threat.

BUILD THREAT MODELS
With intelligence on who could be targeting your organization and with what capabilities.

SEARCHLIGHT CYBER

SLCYBER.IO

SEARCHLIGHT.
CYBER

VISIT **WWW.SLCYBER.IO** TO FIND
OUT MORE OR BOOK A DEMO NOW.

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