SEARCHLIGHT CYBER

DARK WEB THREATS AGAINST THE ENERGY INDUSTRY

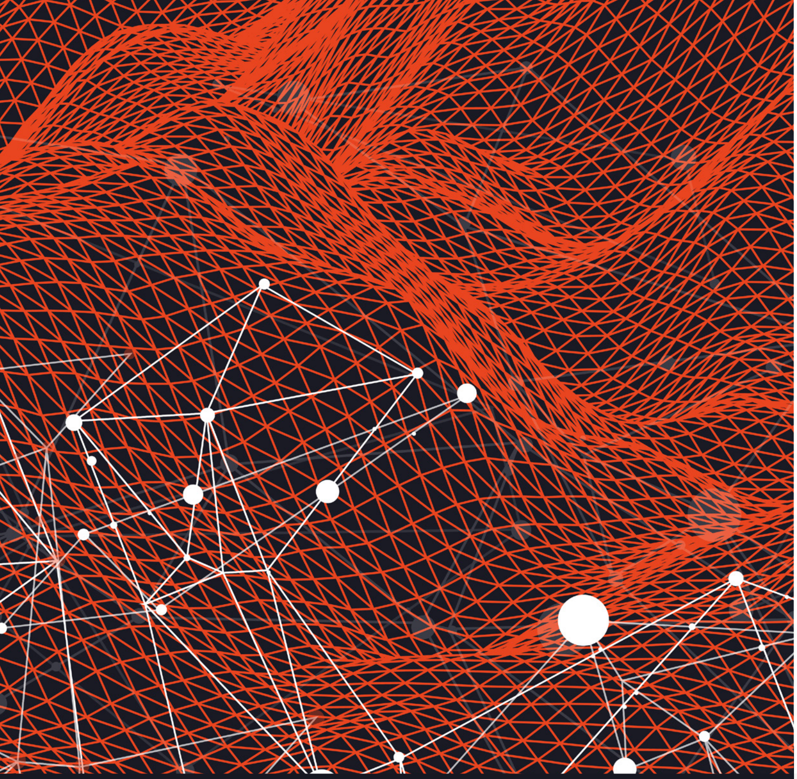
BUILDING A THREAT MODEL FOR ENERGY COMPANIES

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 professionals in every energy organization in the world are aware that they are being targeted by cybercriminals. This isn't news. However, what is sometimes harder to determine is exactly how they are being targeted.

That was the starting point for this research: to shed light on how energy organizations are being targeted on the dark web, the part of the internet that threat actors use to share techniques, build their resources, and plan their attacks. This report demonstrates that energy companies are routinely discussed on dark web forums - in particular - by threat actors auctioning initial access to remote software, VPNs, and stolen credentials. While they are primarily exploiting corporate infrastructure, Industrial Control Systems (ICS) and Operational Technology (OT) are also in the firing line.

Visibility into this cybercriminal reconnaissance can help security teams to identify likely paths of attack, inform defenses, and help them prioritize imminent threats. However, to do this they have to gather dark web intelligence.

Our recent survey[1] of CISOs found that 72 percent of oil and gas companies are gathering data from the dark web. While this is a promising start, it is notably less than comparable high risk industries such as financial services (85 percent), manufacturing (83 percent), and transportation (81 percent). Concerningly, more than a quarter (27 percent) of oil and gas CISOs still believe that activity on the dark web has no impact on their company.

Energy organizations may not have historically considered themselves the primary target for financially-motivated cyberattacks emanating from the dark web but the cybersecurity landscape has changed dramatically over the past few years. Cybercriminals are no longer just focusing on asset-rich organizations like banks and insurance companies. They are increasingly targeting enterprises in industries such as healthcare, oil and gas, and manufacturing, to leverage the critical nature of these companies and extort ransoms. This makes dark web intelligence vital.

The objective of this report is firstly, to demonstrate beyond a doubt that the activity on the dark web does impact energy companies and secondly - and most importantly - provide advice to security teams on what they can do about it. We have therefore combined the reconnaissance we have observed over the past year with insight into how to build threat models based on dark web intelligence. We hope this will be a useful resource for security professionals at energy companies to determine not just if they are being targeted, but also how they can use intelligence to fill crucial knowledge gaps and make the right strategic, operational, and tactical decisions.

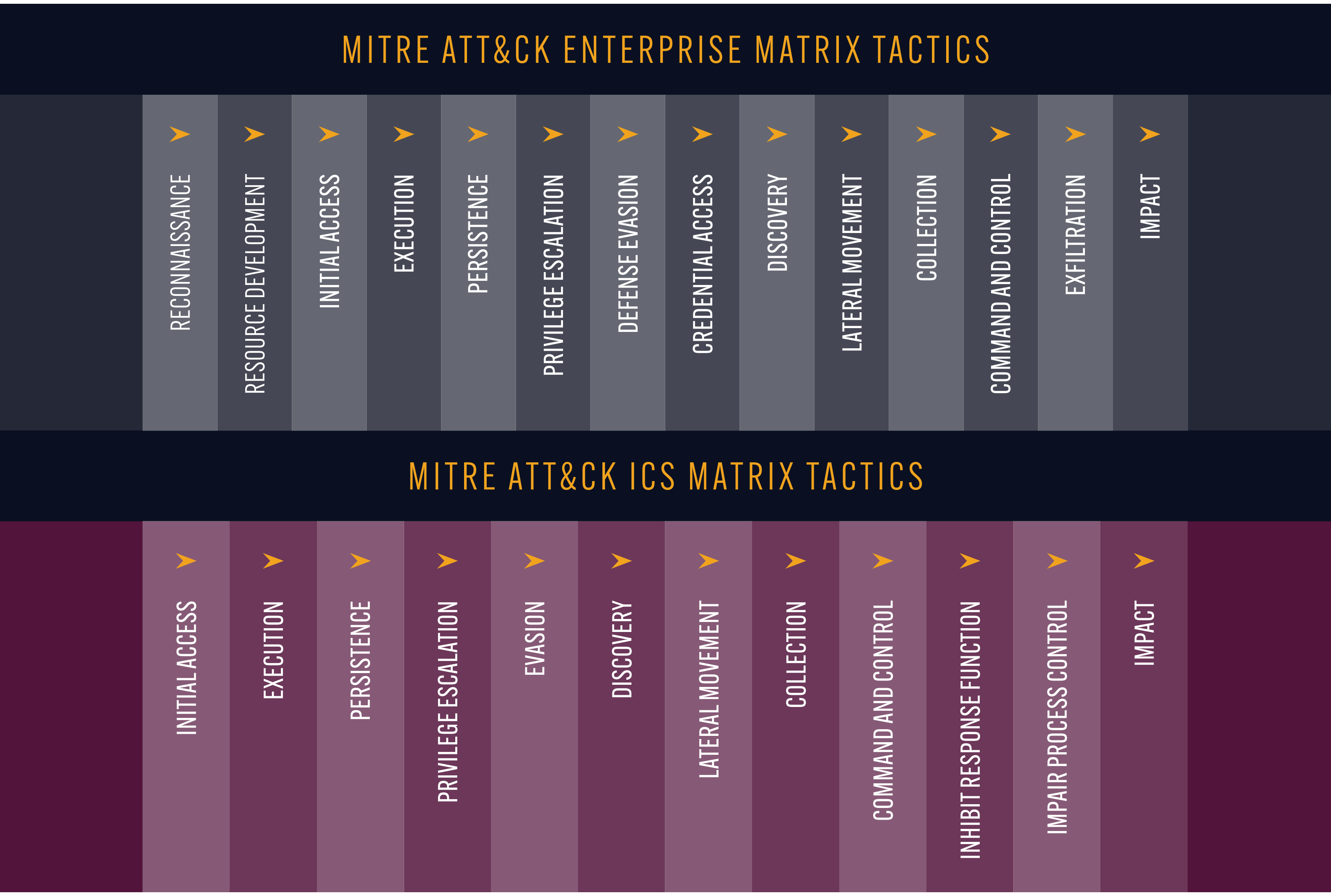
DR. GARETH OWENSON
CTO and Co-Founder
Searchlight Cyber

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

USING THE MITRE ATT&CK FRAMEWORK

In this report we have used MITRE ATT&CK as a common lexicon and taxonomy to illustrate how energy organizations can factor dark web intelligence into their defenses and build threat models (see more on page 18).

An open source knowledge base of adversary Tactics, Techniques and Procedures (TTPs), we have chosen the MITRE ATT&CK because it is already a popular tool with security professionals and creates a fantastic basis to build company-specific threat models on. There are two MITRE ATT&CK frameworks that energy companies should be aware of: the Enterprise and ICS matrices.



MITRE ATT&CK ENTERPRISE MATRIX TACTICS

- RECONNAISSANCE
- RESOURCE DEVELOPMENT
- INITIAL ACCESS
- EXECUTION
- PERSISTENCE
- PRIVILEGE ESCALATION
- DEFENSE EVASION
- CREDENTIAL ACCESS
- DISCOVERY
- LATERAL MOVEMENT
- COLLECTION
- COMMAND AND CONTROL
- EXFILTRATION
- IMPACT

MITRE ATT&CK ICS MATRIX TACTICS

- INITIAL ACCESS
- EXECUTION
- PERSISTENCE
- PRIVILEGE ESCALATION
- EVASION
- DISCOVERY
- LATERAL MOVEMENT
- COLLECTION
- COMMAND AND CONTROL
- INHIBIT RESPONSE FUNCTION
- IMPAIR PROCESS CONTROL
- IMPACT

Figure 1: The tactics of the MITRE ATT&CK Enterprise and ICS Matrices.

Where applicable, we have provided the MITRE ATT&CK codes for the attack techniques we have observed below, to demonstrate how this intelligence can practically be used by energy organizations to improve their understanding of - and defenses against - threat actors that are targeting them on the dark web.

DARK WEB INTELLIGENCE ON THREAT ACTOR RECONNAISSANCE

Our analysts focused on a 12 month period (February 2022 - February 2023) to collect a sample that is reflective of the types of threat actor activity that takes place on dark web sites, forums, and marketplaces, which energy organizations could factor into their threat models.

KEY FINDINGS

- The predominant activity we observe against the energy industry on the dark web are the "auctions" for initial access to energy companies that routinely take place on dark web forums.
- Threat actors often use the terms "Start", "Step" and "Blitz", which indicate the start price, the increments of the bids, and a "buy-it-now" price (blitz).
- Most of these auction posts list the access type along with the country of the organization, its industry, and its revenue. In some cases the name of the organization is also given.
- We observe listings for organizations in countries all over the world. The small sample in this report alone includes targets in the USA, Canada, UK, France, Italy, and Indonesia.
- Listings also include companies across the spectrum of the energy sector - upstream, midstream, and downstream - in traditional energy companies such as oil and gas but also renewable energy organizations.
- The dark web forum Exploit is the most popular site for these auctions but we have also observed activity on other forums such as RaidForums and BreachForums (now both closed).
- Some threat actors post multiple auctions impacting different organizations, suggesting that they are specialists in the initial access market.

JIM SIMPSON

DIRECTOR OF THREAT INTELLIGENCE

"While cybercriminals share this information with the intention of attracting buyers, visibility into auction activity on dark web forums offers security professionals with a valuable opportunity to determine if their organization is being targeted. With information on the revenue, location, and technology of the potential victim, security teams can identify if they fit the profile and take mitigative action. Even if they don't fit the exact profile of the victim, they know this is a tactic being used against other energy companies that they should factor into their threat modeling."

DARK WEB AUCTIONS

Our analysts have observed numerous instances of threat actors selling initial access to energy organizations around the world on popular dark web forums including Exploit, RaidForums, and BreachForums.

The screenshot in **Figure 2**, from the dark web forum Exploit, is a typical example of the format and content of these posts. From the information provided by the threat actor we can determine:

THE REVENUE OF THE ORGANIZATION

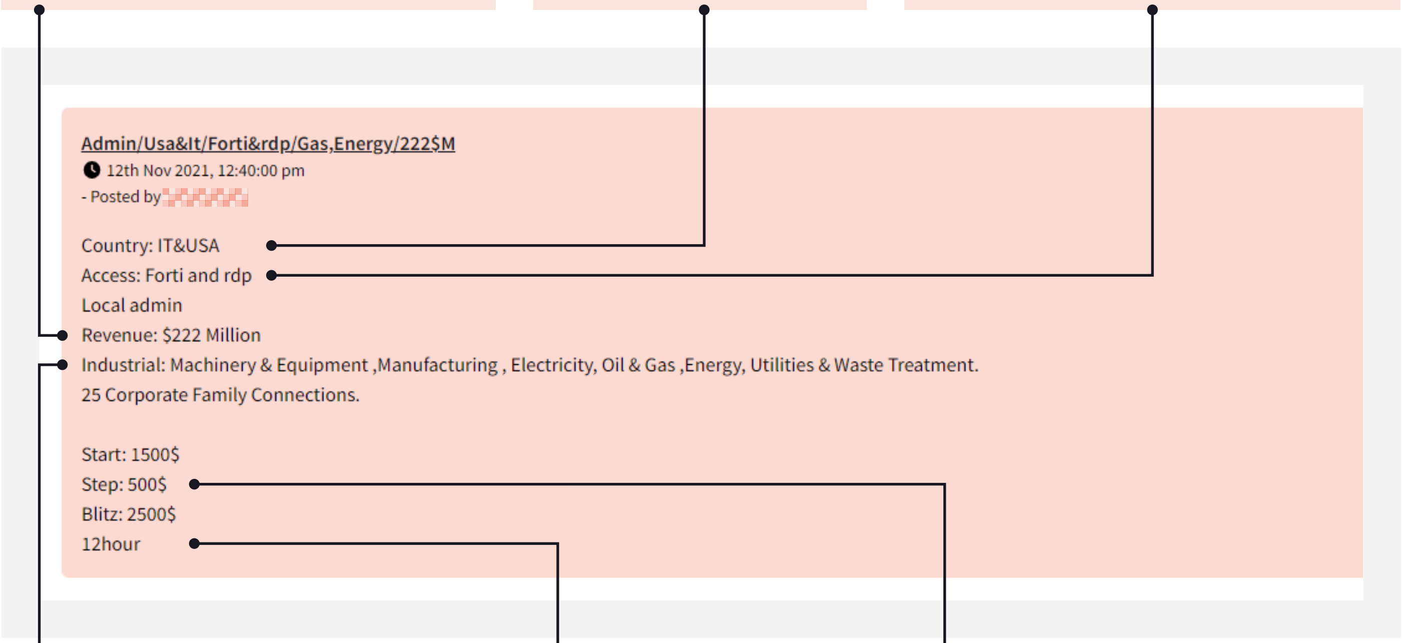
To provide buyers with an indication of the size of the organization, and therefore the potential earning potential.

THE GEOGRAPHY OF THE ORGANIZATION

Italy and the USA.

THE TYPE OF ACCESS THEY ARE SELLING

Local administrative access via a software vulnerability in "Forti" - likely referring to a Fortinet product - and Remote Desktop Protocol (RDP) (T1589.001)[2]



Admin/Usa&It/Forti&rdp/Gas,Energy/222$M

🕒 12th Nov 2021, 12:40:00 pm

- Posted by [redacted]

Country: IT&USA
Access: Forti and rdp
Local admin
Revenue: $222 Million
Industrial: Machinery & Equipment ,Manufacturing , Electricity, Oil & Gas ,Energy, Utilities & Waste Treatment.
25 Corporate Family Connections.

Start: 1500$
Step: 500$
Blitz: 2500$
12hour

THE INDUSTRY OF THE VICTIM ORGANIZATION

Labeled by the seller as "Industrial", including oil and gas, energy, and utilities.

THE DEADLINE ON THE AUCTION

In this case, 12 hours.

THE ASKING PRICE FOR THE INITIAL ACCESS

Indicated with the labels "Start, Step, and Blitz."

Figure 2: A threat actor auctions local admin access to an "Industrial" organization on the dark web forum Exploit.

[2] https://attack.mitre.org/techniques/T1589/001/

THE ASKING PRICE

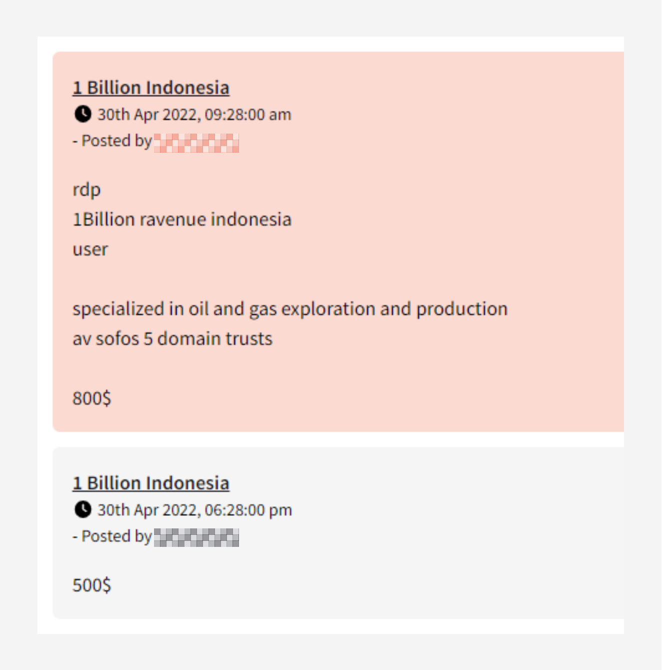
The "Start, Step, Blitz" terminology seen in **Figure 2** is a common approach to auctioning initial access on dark web forums. In this case, it means that bidding starts at $1500 and bids will be placed at increments of $500. However, if an individual wanted to purchase the access outright they could do so at the "blitz" price of $2500.

In other cases, such as in **Figure 3**, the threat actor will just provide a cost of the access (once again for RDP). Note, however, that the price quickly drops later that day to try and attract more interest. This indicates that these costs are always subject to demand and negotiation.

As we will see, the asking price of access varies. In the samples we have gathered, initial access is offered for as little as $20 and up to $2,500. The sellers almost always provide the revenue of the organization, presumably to indicate the size of the organization and therefore the "earning potential" for a prospective buyer.

However, as **Figure 2** and **Figure 3** demonstrate, the revenue and cost of access don't always correlate, which suggests other determiners of price. For example, the system being accessed, the geography of the organization, or the potential to compromise other organizations (ie. supply chain attacks). The latter may explain the higher asking price for **Figure 2** as the auctioneer very clearly indicates the "25 corporate family connections".

As **Figure 4** shows, the practice of offering a discount if the asking price is not met is also common. Initial access brokers' role in the cybercriminal ecosystem is to facilitate other criminals in undertaking bigger attacks. They operate at scale and are looking to make a quick, relatively risk-free profit from a large number of victims only by achieving access. This approach to pricing demonstrates the pragmatism of sellers in getting whatever funds they can for the access they have.



1 Billion Indonesia
30th Apr 2022, 09:28:00 am
- Posted by [redacted]

rdp
1Billion ravenue indonesia
user

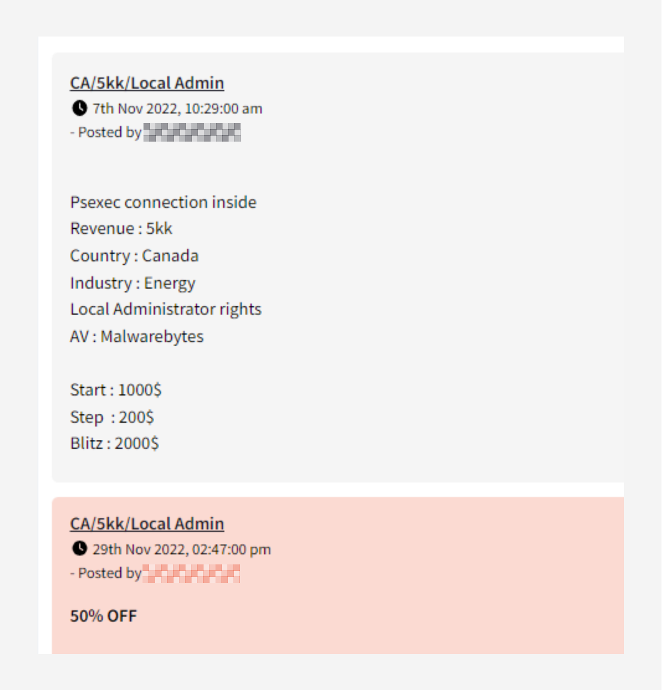
specialized in oil and gas exploration and production
av sofos 5 domain trusts

800$

1 Billion Indonesia
30th Apr 2022, 06:28:00 pm
- Posted by [redacted]

500$

Figure 3: A threat actor tries to sell initial access to an Indonesian oil and gas exploration company on the dark web forum Exploit.



CA/5kk/Local Admin
7th Nov 2022, 10:29:00 am
- Posted by [redacted]

Psexec connection inside
Revenue : 5kk
Country : Canada
Industry : Energy
Local Administrator rights
AV : Malwarebytes

Start : 1000$
Step : 200$
Blitz : 2000$

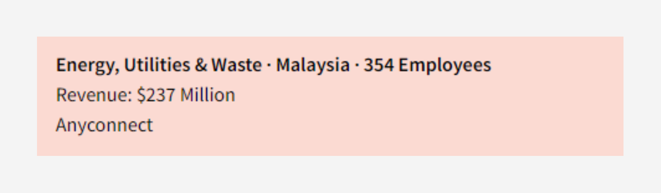
CA/5kk/Local Admin
29th Nov 2022, 02:47:00 pm
- Posted by [redacted]

50% OFF

Figure 4: A seller sets an initial auction for local administrator rights at a Canadian Energy company, then offers 50% off after two weeks.

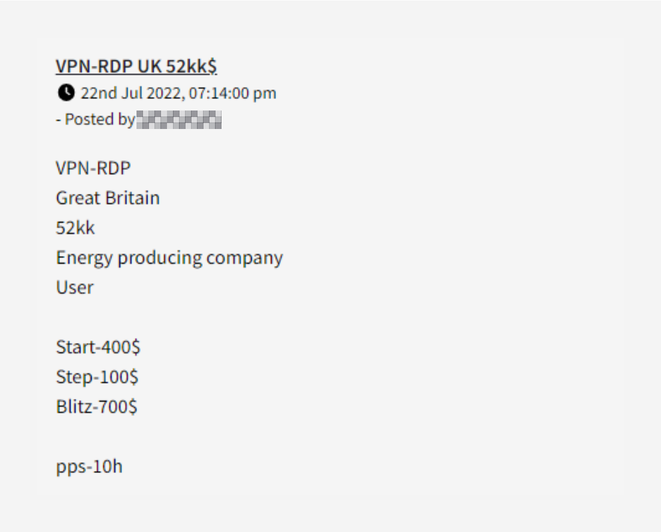
TYPES OF ACCESS FOR SALE

Figures 2, 3 and 4 - all for remote access software - already give us an indication of where energy companies are vulnerable. The sale of compromised VPNs is especially common, indicating that this is an attack vector that energy companies should be factoring into their threat models. For example, **Figures 5 & 6** show the sale of VPNs for Malaysian and UK energy companies.



Energy, Utilities & Waste · Malaysia · 354 Employees
Revenue: $237 Million
Anyconnect

Figure 5: A post on the dark web forum Exploit offering access to an energy, utilities, and waste company in Malaysia via the VPN AnyConnect.



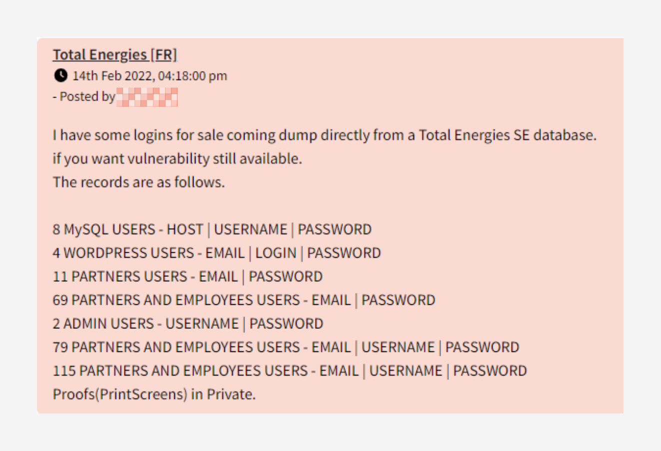
VPN-RDP UK 52kk$
22nd Jul 2022, 07:14:00 pm
- Posted by [redacted]

VPN-RDP
Great Britain
52kk
Energy producing company
User

Start-400$
Step-100$
Blitz-700$

pps-10h

Figure 6: A post on the dark web forum Exploit offering access to a UK "energy producing company" via VPN.



Total Energies [FR]
14th Feb 2022, 04:18:00 pm
- Posted by [redacted]

I have some logins for sale coming dump directly from a Total Energies SE database.
if you want vulnerability still available.
The records are as follows.

8 MySQL USERS - HOST | USERNAME | PASSWORD
4 WORDPRESS USERS - EMAIL | LOGIN | PASSWORD
11 PARTNERS USERS - EMAIL | PASSWORD
69 PARTNERS AND EMPLOYEES USERS - EMAIL | PASSWORD
2 ADMIN USERS - USERNAME | PASSWORD
79 PARTNERS AND EMPLOYEES USERS - EMAIL | USERNAME | PASSWORD
115 PARTNERS AND EMPLOYEES USERS - EMAIL | USERNAME | PASSWORD
Proofs(PrintScreens) in Private.

Figure 7: A post advertising logins for a french energy company on RaidForums.

IAN GARRATT

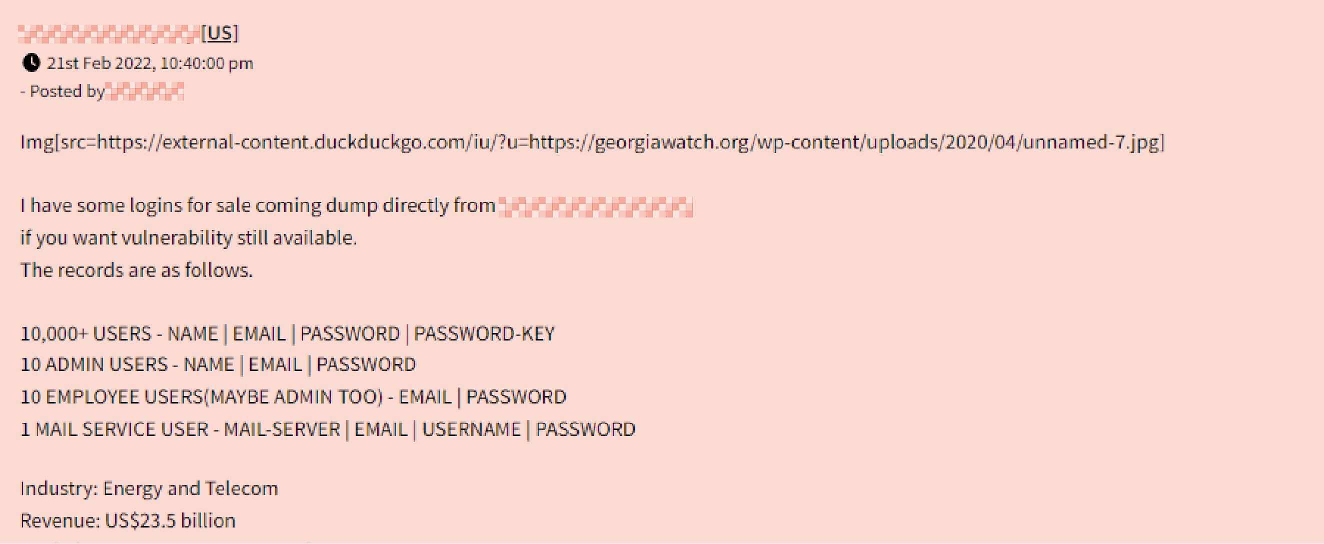
THREAT INTELLIGENCE ANALYST

"Some readers may recognize that a compromised VPN is the exact technique that the ransomware gang DarkSide used to breach Colonial Pipeline in the infamous 2021 attack. In that case, the oil pipeline was forced to shut for several days to reduce the risk of the ransomware attack spreading to the operational network, prompting the US president to declare a state of emergency. This remains a popular tactic with threat actors targeting the energy sector, which should prompt all organizations to pay special attention to the security of their VPNs and remote access software."

[3] https://attack.mitre.org/techniques/T1589/001/

Meanwhile, **Figures 7 & 8** demonstrate that the sale of corporate credentials (which our analysts observe for all industries) also impacts the energy industry (T1589.001).[3] Both of these posts are made by the same seller and in each case they are selling "combos" - i.e. not just email addresses but also passwords, usernames, and even password-keys to give the buyer everything they need to gain access to the systems.

The seller also offers "the vulnerability", indicating how he obtained the credentials and, once again, supporting our analysis that software vulnerabilities are a particular weak spot for energy organizations (T1588.005).[4]



[redacted][US]

21st Feb 2022, 10:40:00 pm

- Posted by[redacted]

Img[src=https://external-content.duckduckgo.com/iu/?u=https://georgiawatch.org/wp-content/uploads/2020/04/unnamed-7.jpg]

I have some logins for sale coming dump directly from[redacted]
if you want vulnerability still available.
The records are as follows.

10,000+ USERS - NAME | EMAIL | PASSWORD | PASSWORD-KEY
10 ADMIN USERS - NAME | EMAIL | PASSWORD
10 EMPLOYEE USERS(MAYBE ADMIN TOO) - EMAIL | PASSWORD
1 MAIL SERVICE USER - MAIL-SERVER | EMAIL | USERNAME | PASSWORD

Industry: Energy and Telecom
Revenue: US$23.5 billion

Figure 8: The same seller offers credential "combos" to an energy company in the USA in RaidForums later that month.

JIM SIMPSON

DIRECTOR OF THREAT INTELLIGENCE

"It is worth noting that in both of these posts the seller mentions the company name specifically, which we have redacted to protect the anonymity of the organizations. In most cases, energy companies monitoring these dark web forums would be able to see if they match the profile of the listed victims.

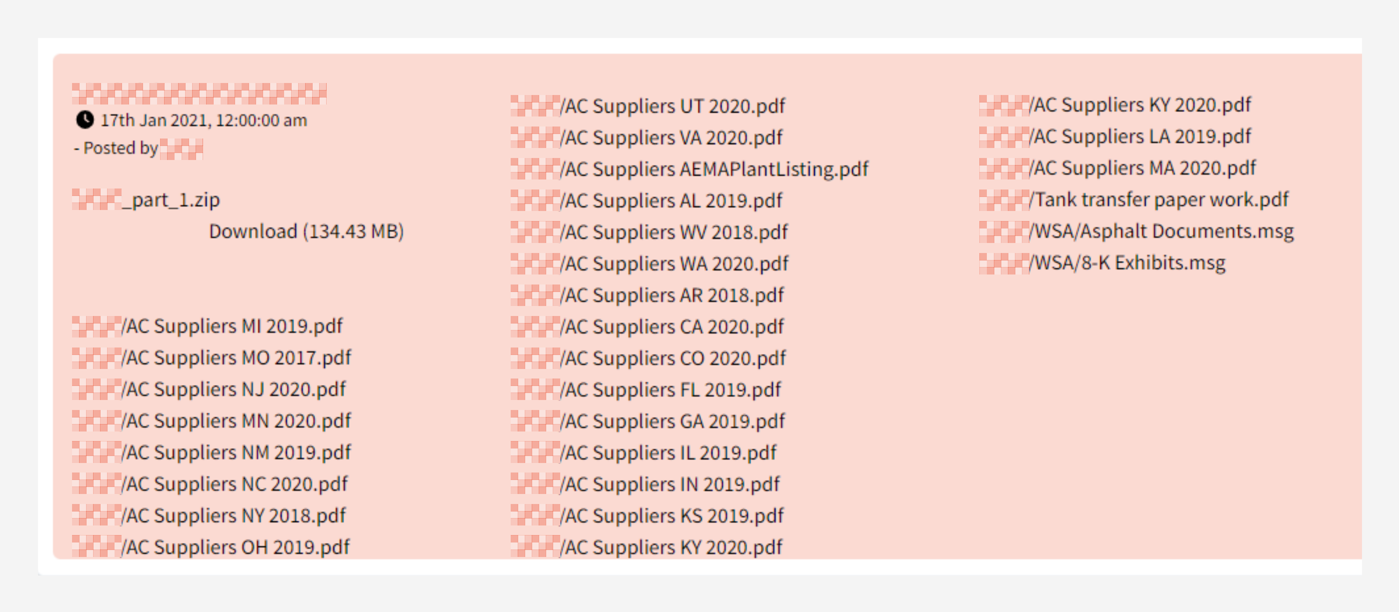
"However, in the situation where the company is named, if the organizations are monitoring the dark web their security teams would be able to immediately identify that they are being targeted and, potentially, that they have already been breached. This information could then be used to inform incident response."

[3] https://attack.mitre.org/techniques/T1589/001/
[4] https://attack.mitre.org/techniques/T1588/005/
[5] https://attack.mitre.org/techniques/T0883/

ATTACKS AGAINST ICS AND OT

While the previous examples appear to refer to the corporate systems of energy companies, our threat intelligence analysts do also observe threat actors discussing - and even publishing - access to ICS and OT.

While it falls outside of our research window, it is worth highlighting the post in **Figure 9** as an example of threat actors sharing what appears to be incredibly sensitive data related to ICS (T0883).[5] We have redacted the name of the organization, which was used in this case, but from the file names it is clear that this data refers to operational technology.



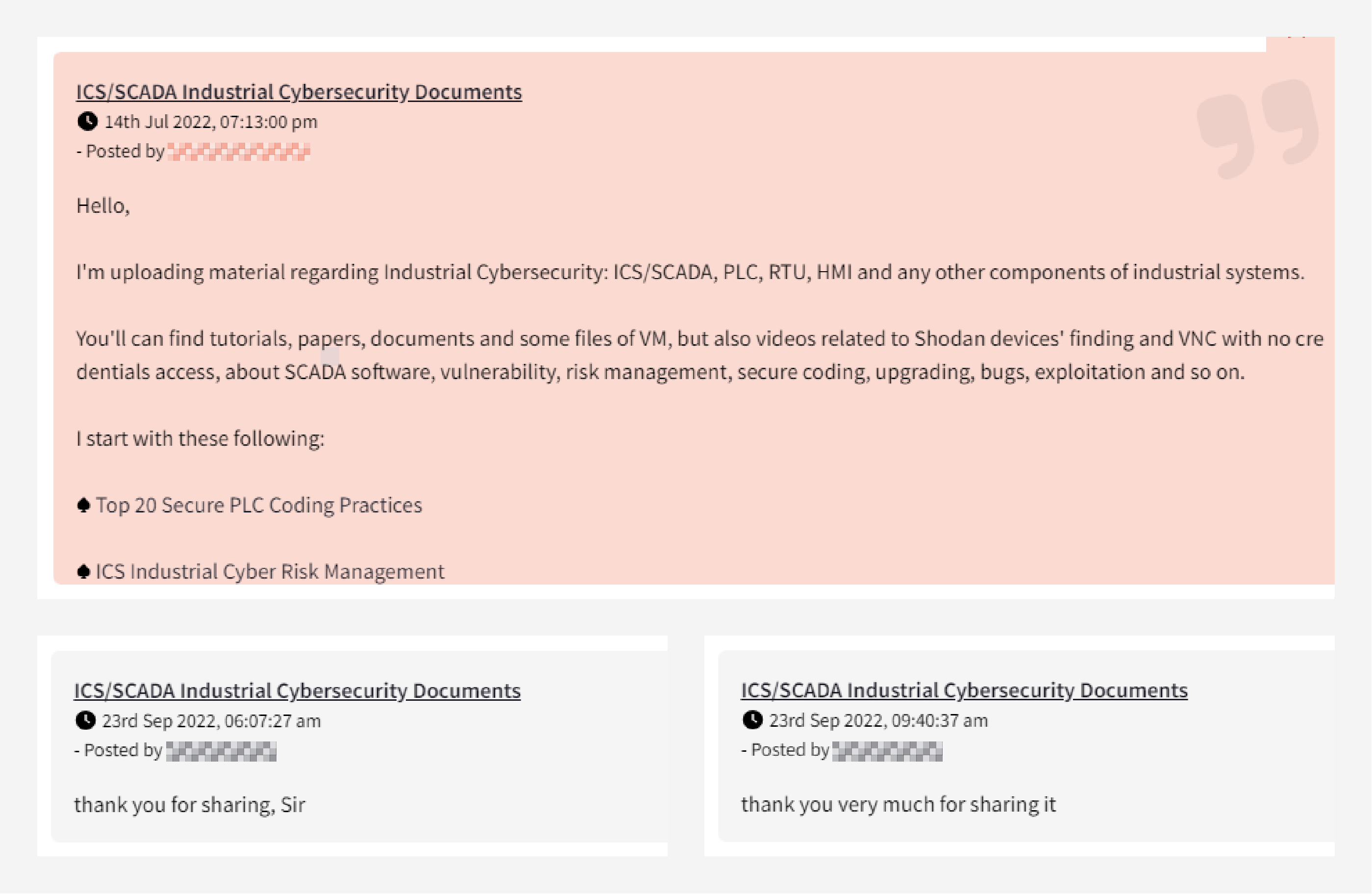
[redacted]
17th Jan 2021, 12:00:00 am
- Posted by [redacted]

[redacted]_part_1.zip
Download (134.43 MB)

[redacted]/AC Suppliers MI 2019.pdf
[redacted]/AC Suppliers MO 2017.pdf
[redacted]/AC Suppliers NJ 2020.pdf
[redacted]/AC Suppliers MN 2020.pdf
[redacted]/AC Suppliers NM 2019.pdf
[redacted]/AC Suppliers NC 2020.pdf
[redacted]/AC Suppliers NY 2018.pdf
[redacted]/AC Suppliers OH 2019.pdf
[redacted]/AC Suppliers UT 2020.pdf
[redacted]/AC Suppliers VA 2020.pdf
[redacted]/AC Suppliers AEMAPlantListing.pdf
[redacted]/AC Suppliers AL 2019.pdf
[redacted]/AC Suppliers WV 2018.pdf
[redacted]/AC Suppliers WA 2020.pdf
[redacted]/AC Suppliers AR 2018.pdf
[redacted]/AC Suppliers CA 2020.pdf
[redacted]/AC Suppliers CO 2020.pdf
[redacted]/AC Suppliers FL 2019.pdf
[redacted]/AC Suppliers GA 2019.pdf
[redacted]/AC Suppliers IL 2019.pdf
[redacted]/AC Suppliers IN 2019.pdf
[redacted]/AC Suppliers KS 2019.pdf
[redacted]/AC Suppliers KY 2020.pdf
[redacted]/AC Suppliers KY 2020.pdf
[redacted]/AC Suppliers LA 2019.pdf
[redacted]/AC Suppliers MA 2020.pdf
[redacted]/Tank transfer paper work.pdf
[redacted]/WSA/Asphalt Documents.msg
[redacted]/WSA/8-K Exhibits.msg

Figure 9: Files related to operational technology dumped on an onion site.

Our analysts also observe threat actors discussing ICS systems and sharing resources to help others conduct attacks (T0883[6] & T0866).[7] **Figure 10**, for example, shows a threat actor sharing “tutorials, papers, and documents, on “ICS/SCADA, PLC, RTU, HMI and any other components of industrial systems” on the dark web forum BreachForums. In the comments below, other forum users thank the poster for sharing.



ICS/SCADA Industrial Cybersecurity Documents

14th Jul 2022, 07:13:00 pm

- Posted by [redacted]

Hello,

I'm uploading material regarding Industrial Cybersecurity: ICS/SCADA, PLC, RTU, HMI and any other components of industrial systems.

You'll can find tutorials, papers, documents and some files of VM, but also videos related to Shodan devices' finding and VNC with no credentials access, about SCADA software, vulnerability, risk management, secure coding, upgrading, bugs, exploitation and so on.

I start with these following:

♠ Top 20 Secure PLC Coding Practices

♠ ICS Industrial Cyber Risk Management

ICS/SCADA Industrial Cybersecurity Documents

23rd Sep 2022, 06:07:27 am

- Posted by [redacted]

thank you for sharing, Sir

ICS/SCADA Industrial Cybersecurity Documents

23rd Sep 2022, 09:40:37 am

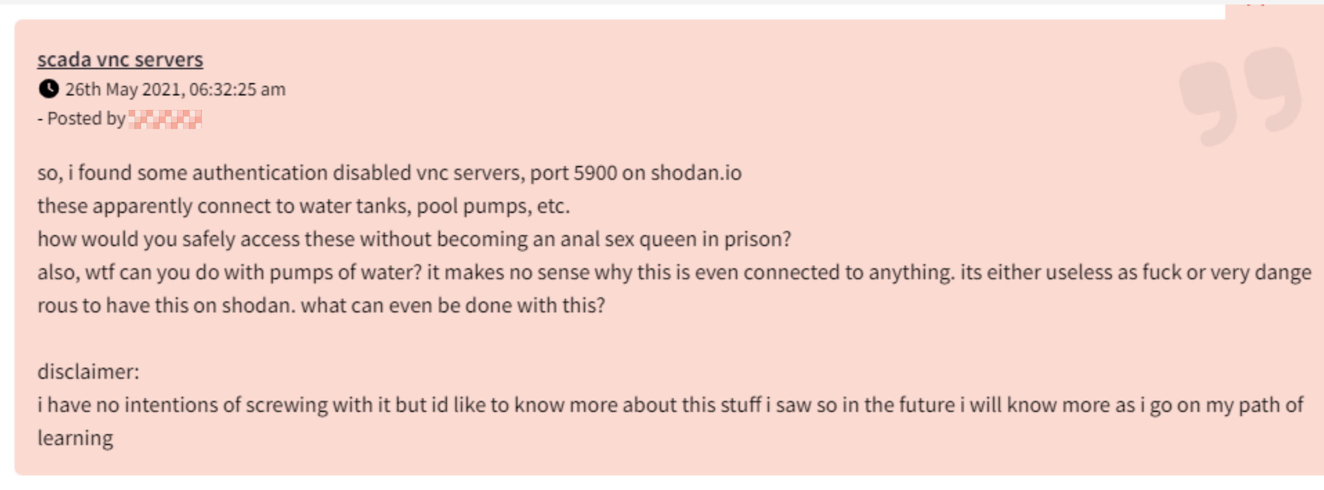
- Posted by [redacted]

thank you very much for sharing it

Figure 10: Users of the dark web forum BreachForums thank a threat actor for sharing resources on the cybersecurity of industrial components.

Perhaps even more concerning is the post in **Figure 11**, identified by our analysts on the CryptBB forum. Here, the poster claims to have “found” some authentication disabled VNC servers connected to “water tanks, pool pumps, etc.”, using the server search engine Shodan. While this individual says they have “no intention of screwing with it”, broadcasting this information on a dark web forum could alert malicious threat actors to the vulnerability, and security teams to check their own infrastructure.

[6] https://attack.mitre.org/techniques/T0883/
[7] https://attack.mitre.org/techniques/T0866/



scada vnc servers
26th May 2021, 06:32:25 am
- Posted by [redacted]

so, i found some authentication disabled vnc servers, port 5900 on shodan.io
these apparently connect to water tanks, pool pumps, etc.
how would you safely access these without becoming an anal sex queen in prison?
also, wtf can you do with pumps of water? it makes no sense why this is even connected to anything. its either useless as fuck or very dangerous to have this on shodan. what can even be done with this?

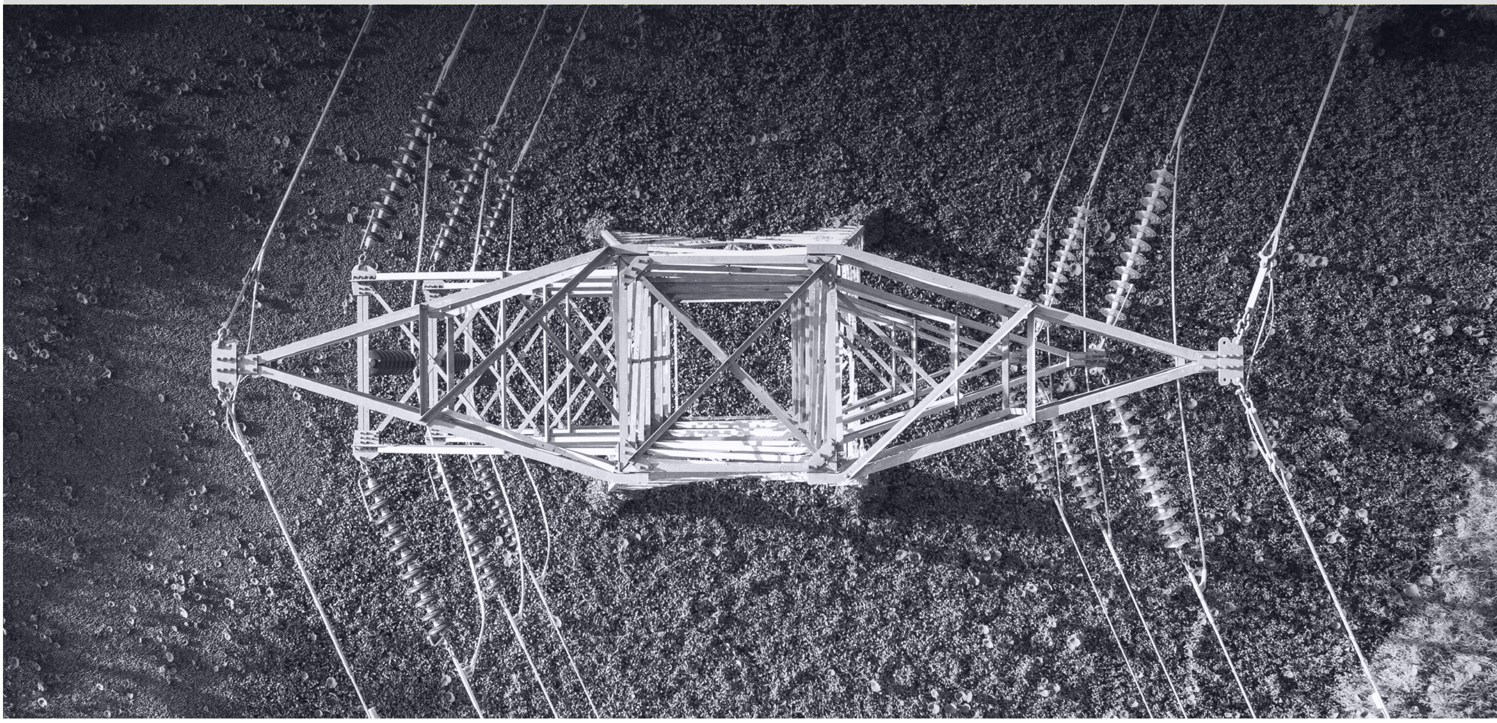
disclaimer:
i have no intentions of screwing with it but id like to know more about this stuff i saw so in the future i will know more as i go on my path of learning

Figure 11: An individual shares that they have found open VNC Servers on the dark web forum CryptBBcomponents.

IAN GARRATT

THREAT INTELLIGENCE ANALYST

“Access to ICS systems is undoubtedly the highest priority concern of security professionals at energy organizations and I imagine many will be concerned to see this technology openly discussed on dark web forums. It does however allow defenders to assess the capability of attackers with this information and monitor their evolution as credible threats overtime. This underlines the need to continuously monitor for evidence that their infrastructure - corporate or industrial - has been compromised. As the Colonial Pipeline demonstrated, even compromised corporate systems can be enough to bring operational activity to a halt.”



THE THREAT ACTORS

We have anonymized the name of the sellers throughout this report so as not to provide them with undue publicity. Therefore, what readers won't have necessarily realized, is that a number of the usernames recur in these posts, even across different forums. This suggests that some individuals (or possibly groups) specialize in targeting the energy industry. Energy organizations could potentially use this intelligence to better understand the capabilities of their likely adversaries, which is a key component of building a threat model (see page 18).

The profiles below demonstrate the intelligence that can be gathered on threat actors based on their dark web activity. We are actively tracking a number of persona and have changed the names they use in the adverts in line with our naming convention.

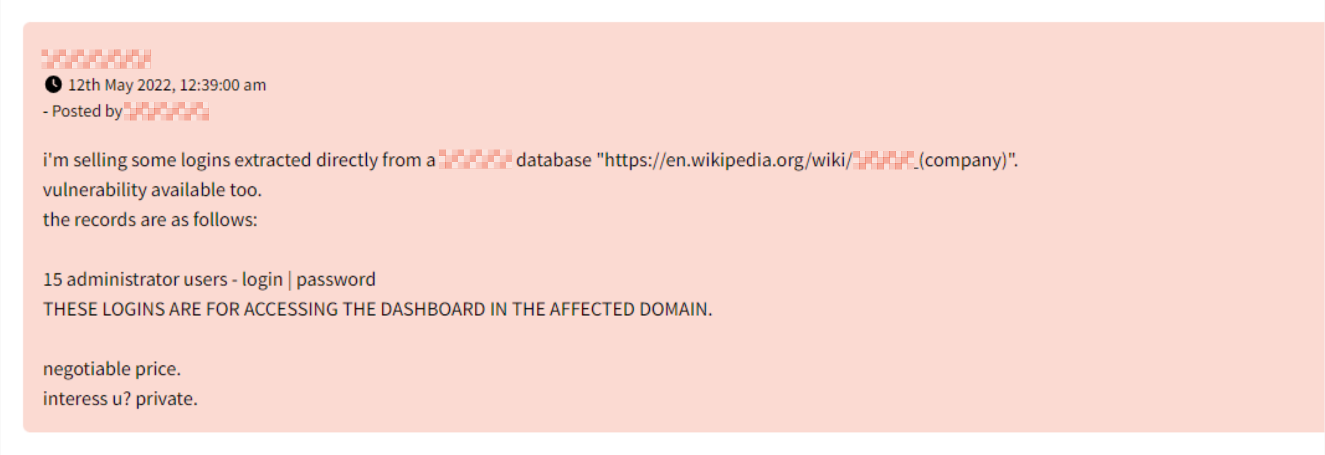
GREENHILLS

Figure 12 shows another post from the same threat actor we observed selling corporate credentials in **Figures 7 & 8**. This is what else we have learnt about the hacker from our dark web intelligence:

This actor appears to specialize in credential combos.

They often share the name of the affected organization.

As well as energy companies, they have posted access for telecoms companies, banks, manufacturing companies, a major US university, and even European Soccer clubs.



[redacted]

🕒 12th May 2022, 12:39:00 am

- Posted by [redacted]

i'm selling some logins extracted directly from a [redacted] database "https://en.wikipedia.org/wiki/[redacted]_(company)".
vulnerability available too.
the records are as follows:

15 administrator users - login | password
THESE LOGINS ARE FOR ACCESSING THE DASHBOARD IN THE AFFECTED DOMAIN.

negotiable price.
interess u? private.

They post in the English language.

They have been active on BreachForums since March 2011 and profiles with similar usernames appear on the dark web forums RaidForums and Xss.

Figure 12: The threat actor we track as GreenHills advertises credentials and a vulnerability for an electrical utility company in Italy.

PROFESSORCHARLIE

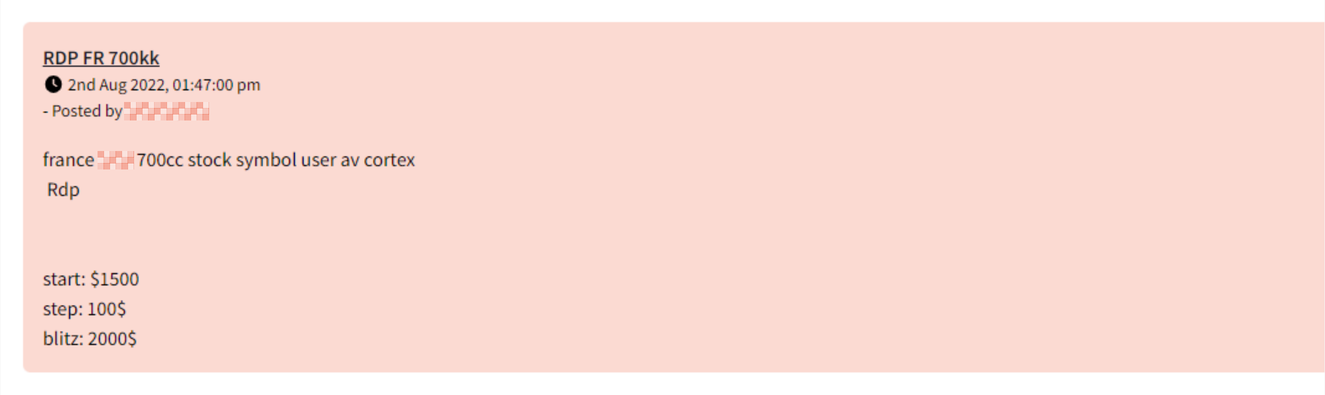
We observed this threat actor a number of times in our research, including in the post referenced in **Figure 3**. This is what we have learned about the actor:

They seem to specialize in selling access via RDP.

They post in Russian.

Their only known account is on Exploit, where they first appeared in March 2022.

As well as energy organizations, they also auction access to IT companies.



RDP FR 700kk

🕐 2nd Aug 2022, 01:47:00 pm

- Posted by [redacted]

france [redacted] 700cc stock symbol user av cortex
Rdp

start: $1500
step: 100$
blitz: 2000$

Figure 13: The threat actor we track as ProfessorCharlie auctions RDP access to a major energy company in France in the Exploit.

JIM SIMPSON

DIRECTOR OF THREAT INTELLIGENCE

“Dark web intelligence is a fantastic resource for informing an organization’s security posture, helping the security team spot early indicators of attack and feeding their threat models. However, the most proactive security teams can also use the data collected from the dark web to create hypotheses for determining what threat hunts to conduct. Even if companies aren’t resourced to conduct threat hunts, the data could be leveraged as inspiration for table top exercises, “What if our VPN had a vulnerability and an attacker leveraged that to gain credentials for a privileged user in R&D? How would we respond to this incident”. Knowing your game plan for when activity is identified is crucial - table top simulations are great for this.”

USING DARK WEB INTELLIGENCE FOR PROACTIVE CYBERSECURITY

In our recent survey, CISOs at oil and gas companies felt less confident that they understand the profile of their adversaries than their peers in other industries.[8] This can change.

The examples above account for just a fraction of the activity on the dark web and only provide a broad overview of what we observe against the energy sector. The real power of dark web intelligence comes from specificity and actionability. If their threat models are working correctly, energy organizations can use dark web data to identify activity that is likely to impact them and adjust their security procedures accordingly.

As we have demonstrated, this can often be determined by identifying if they match the profile of organizations being targeted - based on the geography, revenue, and software referenced in the listings. However, energy companies shouldn’t stop there. They should also be monitoring the dark web for the exposure of their suppliers, to identify if they are being targeted in the dark web, have exploits that are being discussed on dark web forums, and are leaving the company vulnerable to attack.

By building threat models, and feeding them with intelligence gathered from the dark web, energy organizations can identify threats against their organizations from right at the beginning of the Cyber Kill Chain, which allows their security posture to be much more responsive to emerging attacks.

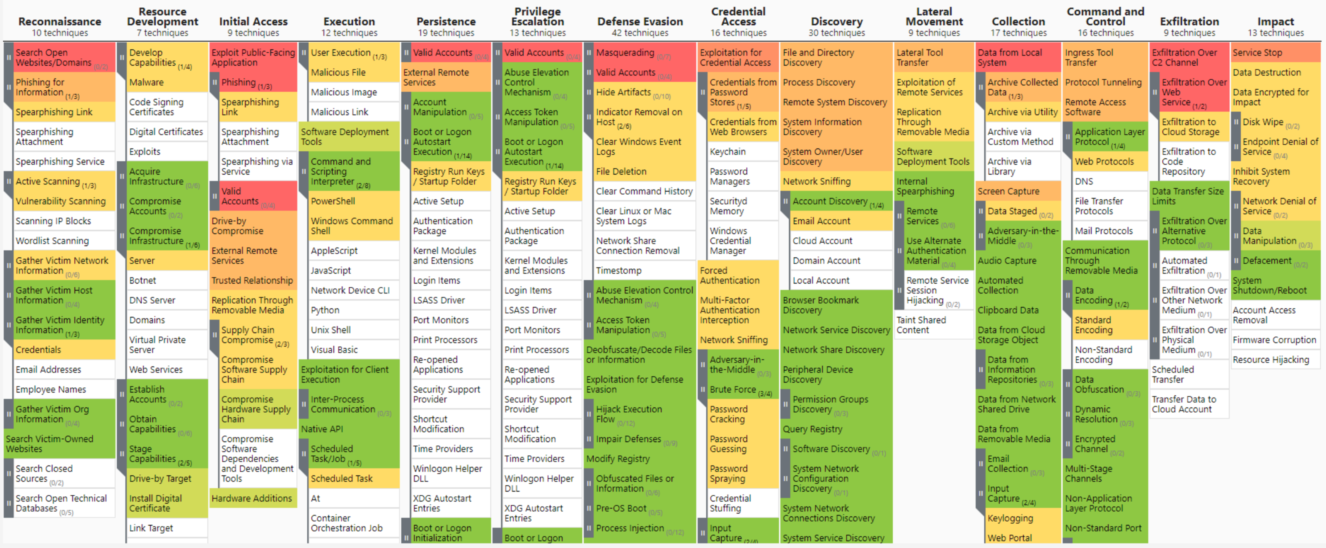
THREAT MODELING IN THE ENERGY INDUSTRY

Threat modeling is a process by which potential threats can be identified, enumerated, and prioritized – all from a hypothetical attacker's point of view. The intent is to provide defenders with a systematic analysis of the probable attacker's profile, most likely attack vectors, and the assets most desired by an attacker. Threat modeling aims to answer questions such as: "Where are my high-value assets?", "Where am I most vulnerable to attack?", "What are the most relevant threats to me?", and "Is there an attack vector that might go unnoticed?".

There are numerous advantages to threat modeling, including (but not limited to):

- Taking a more proactive approach to security by finding vulnerabilities while there is still time to fix them.
- Saving time, revenue, and the reputation of a company by preventing costly and embarrassing security breaches.
- Documenting all of the identified threats that the organization could face, to aid prioritization and risk assessment.
- Uncovering new intelligence and gaining awareness of the latest risks and vulnerabilities.

But where do security teams start?



Reconnaissance 10 techniques
- Search Open Websites/Domains (0/2)
- Phishing for Information (1/3)
  - Spearphishing Link
  - Spearphishing Attachment
  - Spearphishing Service
- Active Scanning (1/3)
  - Vulnerability Scanning
  - Scanning IP Blocks
  - Wordlist Scanning
- Gather Victim Network Information (0/6)
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (1/3)
  - Credentials
  - Email Addresses
  - Employee Names
- Gather Victim Org Information (0/4)
- Search Victim-Owned Websites
- Search Closed Sources (0/2)
- Search Open Technical Databases (0/5)

Resource Development 7 techniques
- Develop Capabilities (1/4)
  - Malware
  - Code Signing Certificates
  - Digital Certificates
  - Exploits
- Acquire Infrastructure (0/6)
- Compromise Accounts (0/2)
- Compromise Infrastructure (1/6)
  - Server
  - Botnet
  - DNS Server
  - Domains
  - Virtual Private Server
  - Web Services
- Establish Accounts (0/2)
- Obtain Capabilities (0/6)
- Stage Capabilities (2/5)
  - Drive-by Target
  - Install Digital Certificate
  - Link Target

Initial Access 9 techniques
- Exploit Public-Facing Application
- Phishing (1/3)
  - Spearphishing Link
  - Spearphishing Attachment
  - Spearphishing via Service
- Valid Accounts (0/4)
- Drive-by Compromise
- External Remote Services
- Trusted Relationship
- Replication Through Removable Media
- Supply Chain Compromise (2/3)
  - Compromise Software Supply Chain
  - Compromise Hardware Supply Chain
  - Compromise Software Dependencies and Development Tools
- Hardware Additions

Execution 12 techniques
- User Execution (1/3)
  - Malicious File
  - Malicious Image
  - Malicious Link
- Software Deployment Tools
- Command and Scripting Interpreter (2/8)
  - PowerShell
  - Windows Command Shell
  - AppleScript
  - JavaScript
  - Network Device CLI
  - Python
  - Unix Shell
  - Visual Basic
- Exploitation for Client Execution
- Inter-Process Communication (0/3)
- Native API
- Scheduled Task/Job (1/5)
  - Scheduled Task
  - At
  - Container Orchestration Job

Persistence 19 techniques
- Valid Accounts (0/4)
- External Remote Services
- Account Manipulation (0/5)
- Boot or Logon Autostart Execution (1/14)
  - Registry Run Keys / Startup Folder
  - Active Setup
  - Authentication Package
  - Kernel Modules and Extensions
  - Login Items
  - LSASS Driver
  - Port Monitors
  - Print Processors
  - Re-opened Applications
  - Security Support Provider
  - Shortcut Modification
  - Time Providers
  - Winlogon Helper DLL
  - XDG Autostart Entries
- Boot or Logon Initialization

Privilege Escalation 13 techniques
- Valid Accounts (0/4)
- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- Boot or Logon Autostart Execution (1/14)
  - Registry Run Keys / Startup Folder
  - Active Setup
  - Authentication Package
  - Kernel Modules and Extensions
  - Login Items
  - LSASS Driver
  - Port Monitors
  - Print Processors
  - Re-opened Applications
  - Security Support Provider
  - Shortcut Modification
  - Time Providers
  - Winlogon Helper DLL
  - XDG Autostart Entries
- Boot or Logon

Defense Evasion 42 techniques
- Masquerading (0/7)
- Valid Accounts (0/4)
- Hide Artifacts (0/10)
- Indicator Removal on Host (2/6)
  - Clear Windows Event Logs
  - File Deletion
  - Clear Command History
  - Clear Linux or Mac System Logs
  - Network Share Connection Removal
  - Timestomp
- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- Deobfuscate/Decode Files or Information
- Exploitation for Defense Evasion
- Hijack Execution Flow (0/12)
- Impair Defenses (0/9)
- Modify Registry
- Obfuscated Files or Information (0/6)
- Pre-OS Boot (0/5)
- Process Injection (0/12)

Credential Access 16 techniques
- Exploitation for Credential Access
- Credentials from Password Stores (1/5)
  - Credentials from Web Browsers
  - Keychain
  - Password Managers
  - Securityd Memory
  - Windows Credential Manager
- Forced Authentication
- Multi-Factor Authentication Interception
- Network Sniffing
- Adversary-in-the-Middle (0/3)
- Brute Force (3/4)
  - Password Cracking
  - Password Guessing
  - Password Spraying
  - Credential Stuffing
- Input Capture (2/4)

Discovery 30 techniques
- File and Directory Discovery
- Process Discovery
- Remote System Discovery
- System Information Discovery
- System Owner/User Discovery
- Network Sniffing
- Account Discovery (1/4)
  - Email Account
  - Cloud Account
  - Domain Account
  - Local Account
- Browser Bookmark Discovery
- Network Service Discovery
- Network Share Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (0/3)
- Query Registry
- Software Discovery (0/1)
- System Network Configuration Discovery (0/1)
- System Network Connections Discovery
- System Service Discovery

Lateral Movement 9 techniques
- Lateral Tool Transfer
- Exploitation of Remote Services
- Replication Through Removable Media
- Software Deployment Tools
- Internal Spearphishing
- Remote Services (0/6)
- Use Alternate Authentication Material (0/4)
- Remote Service Session Hijacking (0/2)
- Taint Shared Content

Collection 17 techniques
- Data from Local System
- Archive Collected Data (1/3)
  - Archive via Utility
  - Archive via Custom Method
  - Archive via Library
- Screen Capture
- Data Staged (0/2)
- Adversary-in-the-Middle (0/3)
- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Cloud Storage Object
- Data from Information Repositories (0/3)
- Data from Network Shared Drive
- Data from Removable Media
- Email Collection (0/3)
- Input Capture (2/4)
  - Keylogging
  - Web Portal

Command and Control 16 techniques
- Ingress Tool Transfer
- Protocol Tunneling
- Remote Access Software
- Application Layer Protocol (1/4)
  - Web Protocols
  - DNS
  - File Transfer Protocols
  - Mail Protocols
- Communication Through Removable Media
- Data Encoding (1/2)
  - Standard Encoding
  - Non-Standard Encoding
- Data Obfuscation (0/3)
- Dynamic Resolution (0/3)
- Encrypted Channel (0/2)
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port

Exfiltration 9 techniques
- Exfiltration Over C2 Channel
- Exfiltration Over Web Service (1/2)
  - Exfiltration to Cloud Storage
  - Exfiltration to Code Repository
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (0/3)
- Automated Exfiltration (0/1)
- Exfiltration Over Other Network Medium (0/1)
- Exfiltration Over Physical Medium (0/1)
- Scheduled Transfer
- Transfer Data to Cloud Account

Impact 13 techniques
- Service Stop
- Data Destruction
- Data Encrypted for Impact
- Disk Wipe (0/2)
- Endpoint Denial of Service (0/4)
- Inhibit System Recovery
- Network Denial of Service (0/2)
- Data Manipulation (0/3)
- Defacement (0/2)
- System Shutdown/Reboot
- Account Access Removal
- Firmware Corruption
- Resource Hijacking

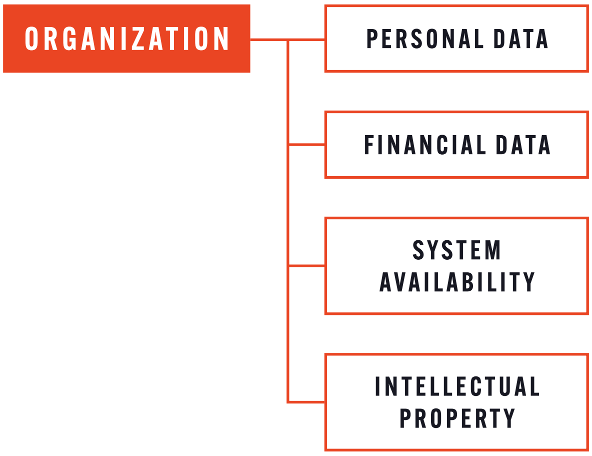
Figure 14: An example of the identified tactics, techniques and procedures (TTPs) identified used against the Energy Sector.

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

FIVE STEPS TO BUILDING A THREAT MODEL

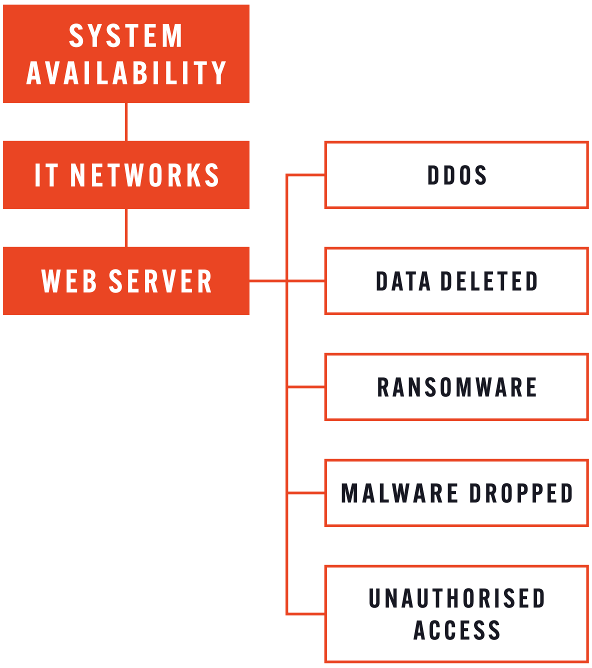
1. IDENTIFY THE ASSETS ADVERSARIES ARE LIKELY TO TARGET

To start threat modeling, security teams first have to identify the "crown jewels": the assets that need protecting. This is established by assessing the critical and sensitive systems and data within the business, and the assets that would be of most value to threat actors. For most companies, including energy organizations, this will include customer data, employee data, financial data, intellectual property, and IT network information. However, energy companies also need to consider their Industrial Control Systems (ICS), Operational Technology (OT) network information, and system availability.



2. PIVOT OFF THE TARGETED ASSETS TO IDENTIFY AREAS OF WEAKNESS AND POSSIBLE COUNTERMEASURES

Once the "target information" has been established, security teams can break down how each asset may be attacked. The example shown is not exhaustive of all attack types and this is an exercise that needs to be continuously re-run to keep pace with the changing threat landscape.



3. ESTABLISH THE ADVERSARIES THAT TARGET THE SECTOR

Security teams then need to establish the threat actors that are likely to target the organization and their industry sector, as well as the Tactics, Techniques, and Procedures (TTPs) they use.

A combination of first party collection (i.e. threat intelligence gathered by the security team) and third party collection (i.e. open source intelligence - OSINT) can help establish the threat landscape including known threat actors, recent campaigns, and the techniques used. The MITRE ATT&CK framework is a particularly valuable asset for security teams trying to establish an overall picture of the threat landscape, and can be used as the starting point for the threat model.

4. PIVOT OFF THE ADVERSARIES TO IDENTIFY TRIGGER EVENTS FOR THE ATTACK

All threats are a combination of three factors:

CAPABILITY

The tools and resources of the adversary.

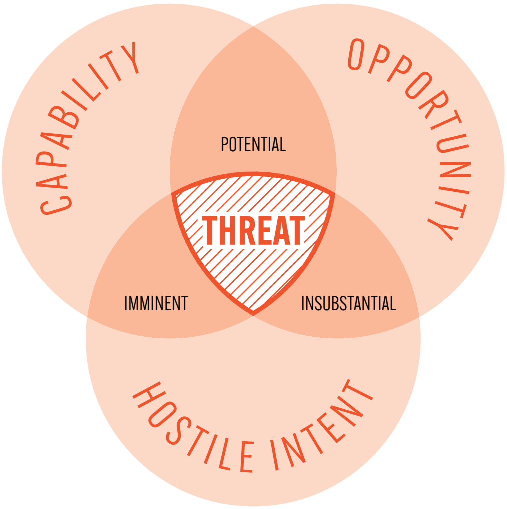
HOSTILE INTENT

The motive behind the attack (for example - political, financial, or destructive).

OPPORTUNITY

The ability for the threat actor to attack the organization at that time.

This stage of the threat model looks at the "Opportunity", or the "trigger event" that could lead a threat actor to initiate an attack. This may be the announcement of a new CVE in a software the organization uses, which provides the threat actor with a point of access. Or it might be tied to the "Hostile Intent", for example a threat actor choosing to target an energy company around the announcement of its financial results. Building these events into the threat model helps organizations establish when they are most vulnerable.



5. CREATE AN ATTACK MAP

Finally, an attack map should draw together all of the components above to provide a holistic visualization of the organization's specific threat landscape, including:

- The targeted Information;
- The types of attacks the organization is likely to face;
- The TTPs of the attackers;
- Detection opportunities with log sources that could be used to indicate any of the attacks you have determined might take place;
- And potential countermeasures that should be prioritized to prevent the most likely attacks.

Critically, threat modeling isn't a "one-and-done exercise" - attackers change what they are doing, new actors join the party, some actors aren't ever seen again. This means it is an ongoing requirement for security teams to gather threat intelligence (including from the dark web) and regularly (at least once a year) update the threat model to reflect how the threat landscape has evolved.

SEARCHLIGHT.
CYBER

DARK WEB INTELLIGENCE

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, with an archive of more than 15 years of historic data, 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

UNCOVER DARK WEB ACTIVITY

Cerberus uses proprietary techniques developed by world-leading researchers to deliver the most comprehensive dark web dataset on the market, providing access to intelligence that was previously unobtainable.

UNCOVER THE CYBERCRIMINAL UNDERWORLD

Understand the scale of criminal activity on the dark web to inform resourcing and investigation.

IDENTIFY ACTORS

Investigate individuals and groups with the ability to pivot on usernames, aliases, and historic activity.

EXTRACT THREAT INTELLIGENCE

Uncover the activity of cybercriminals in the pre-attack phase, to inform cyber defenses.

DARKIQ

DARK WEB MONITORING

SPOT CYBERATTACKS EARLIER

With DarkIQ, you can identify cybercriminals while they are still in the reconnaissance stage of their attack, so rather than just responding to attacks, you can prevent them from happening.

INCREASE SOC EFFICIENCY

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

BUILD THREAT MODELS

Based on dark web intelligence on the capability, opportunity, and intent of threat groups.

ENHANCE SUPPLY CHAIN SECURITY

With visibility into the dark web exposure of suppliers and cybercriminals targeting third parties.

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