ATTACKIQ®

White Paper

The CISO's Guide to MITRE ATT&CK® in the Energy Sector

Enabling threat-informed defense for a sector at high risk of cyberattack.

Notice

AttackIQ® publications are made available solely for general information purposes. The information contained in this publication is provided on an *"as is"* basis. Any additional developments or research since the date of publication will not be reflected in this report.

Table of Contents

Executive Summary

Securing an Industry at Risk

Operating in a critical infrastructure sector, energy companies are increasingly targeted by cybercriminals and nation-state actors either looking to secure a quick ransom or disable vital public services. As a result, it's more important than ever that chief information security officers (CISOs) and their teams can rely on the security controls they have in place. The credibility of their businesses and the resilience of their assets and networks depends on a robust security posture.

However, traditional approaches to security control validation and penetration testing are unsatisfactory. Red- and blue-team exercises are expensive and disruptive, and they often fail to test against real-world threats, let alone against a prioritized list of the biggest risks facing the energy industry.

Now, by leveraging the MITRE ATT&CK® framework — which records adversary tactics, techniques, and procedures from real-world attacks — and using it to fuel an automated approach to holistic, multi-stage threat emulation exercises and breach and attack simulations, CISOs can enable an always-on approach to security validation that's focused on the most important threats and designed to ensure that security controls are continually optimized.

This guide makes the case for threat-informed defense, discusses the benefits of automating security control validation, and outlines how multi-stage threat emulation is already helping energy companies stay ahead of the specific threats they face.

The Challenges of Cybersecurity in the Energy Sector

The cyberthreat profiles of organizations vary by sector according to their financial worth to criminals or their strategic worth to actors linked to nation states. Companies in the energy sector are particularly vulnerable, given the nature of their operations.

The energy sector includes enterprises that explore, produce, refine, market, store, and transport oil, gas, coal, and other consumable fuels, as well as those offering oil and gas equipment. Energy is a "critical infrastructure" sector, in that any disruption to its assets, systems, or networks would have a debilitating effect on security, national economic security, and/or national public health or safety.

The Growing Security Threat

Consequently, energy sector businesses are high-value targets to threat actors, and the opportunities to attack such companies are increasing as the digital transformation of the sector unfolds.

Already, energy companies have fallen victim to some of the highest profile and most damaging cyberattacks on record, such as the 2021 ransomware attack on Colonial Pipeline. As a result of the attack, the company was forced to shut its distribution operations and pay a ransom of $4.4 million. The attack also led to significant fuel shortages across multiple states.

Such incidents are set only to become more common. According to figures from IBM, the energy sector is one of the top four sectors in terms of attack volumes, behind only manufacturing, financial services, and professional services, and accounting for 8.2 percent of all observed attacks. Ransomware is the most common form of attack, totaling 25 percent of all attacks on the sector, followed by remote access trojan (RAT), DDoS, and business email compromise (BEC), which account for 17 percent each.

Getting Validation Right

In this context, it is vital that chief security officers (CISOs) at energy sector companies can trust the security tools and systems they invest in to protect their data and assets. The volume of successful attacks on energy companies and their infrastructure suggests that often energy sector companies are not as secure as they think.

One key challenge for CISOs in this respect is that the traditional approach to penetration testing is increasingly proving inadequate. Red-team/blue-team constructs are commonly used to mimic attacks on the network. Here, a red team charged with attacking the network will be countered by a blue team charged with defense. There are several drawbacks to this approach:

- **Cost.** Red-team/blue-team exercises demand a significant time commitment from the security team, driving up costs and disrupts business-as-usual.
- **Scale.** The goal of red teams is to discover a method to breach the network defenses, not to discover all the ways the network can be breached. This can mean significant security vulnerabilities remain even after an exercise.
- **Intermittency.** The resources required for red-team/blue-team penetration testing mean that they can only happen periodically, and therefore do not always reflect the true state of the enterprise at a given time.
- **Relevance.** Unless red teams are leveraging real-world threat intelligence in the way that they test corporate defenses, their approaches may have nothing in common with the real, industry-specific threats facing their businesses.
- **Depth.** Blue teams tend to track adversary behaviors atomically, focusing on one specific action at a time. They can therefore miss the bigger picture of a holistic attack sequence and, as a result, be ill prepared to defend against it.

To overcome these challenges, CISOs at energy sector companies should adopt a new approach to testing their security capabilities, one that leverages the real-world techniques and procedures outlined in the MITRE ATT&CK framework for a threat-informed defense, breach and attack simulation (BAS) platforms for process automation, and multi-stage attack emulation.

MITRE ATT&CK:

The Foundation of Threat-Informed Defense

MITRE ATT&CK is a knowledge base of adversary tactics, techniques, and procedures (TTPs) that have been observed in actual cyberattacks against organizations around the world. Globally accessible and based on real-world data, the ATT&CK knowledge base is fundamental to the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community. MITRE's stature in the cybersecurity community, as well as its objectivity, make it the ideal platform from which energy sector CISOs can objectively evaluate and measure the performance, risk, and capabilities of their cybersecurity controls.

Using the MITRE ATT&CK framework, security and compliance teams can assess the cybersecurity threats that their organization is likely to face and can create organization-specific models of these threats. They can then apply the models to simulate the threats in protected versions of their network environments. With frequent, comprehensive simulations, security teams can verify that their technology, staff, and processes can deliver appropriate defense and mitigation.

The Value of MITRE ATT&CK

MITRE ATT&CK is crucial in developing a program of threat-informed defense because it helps an organization's defenders focus on the threats likely to have the greatest impact on their institution. An energy company's security team can't protect its IT infrastructure against every threat it might someday face. Limited time and resources mean that even the most robust security program must focus on the subset of TTPs that pose the greatest risk.

A big part of MITRE ATT&CK's value lies in the collective and standardized nature of its threat intelligence gathering effort. Other threat intelligence communities often suffer from incoherence, as different contributors use different terminology to describe threats. The MITRE ATT&CK framework imposes a common vocabulary on all contributions, improving information quality. For instance, the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Energy (DOE) have collaborated around joint cybersecurity advisories to alert energy sector organizations to threats through the use of the descriptions provided in MITRE ATT&CK.

Beyond Atomic Threat Analysis

As mentioned above, blue teams moving towards a threat-informed defense leveraging MITRE ATT&CK often use an atomic analysis focus on a single TTP. Rather, the aim should be to bring together MITRE ATT&CK behaviors in attack "graphs" or "flows" that illustrate a multi-stage attack in the round.

MITRE ATT&CK now incorporates a repository of adversary tactics, techniques, and procedures that have been combined in attack graphs to emulate real-world adversaries with specificity and realism. Enumerating complete kill-chain sequences in this manner lays the foundation for a robust approach to security validation that is more realistic and revealing than anything used in the past.

But how should CISOs go about implementing a security control validation model that avoids the barriers outlined above (see "Getting Validation Right")?

Leveraging MITRE ATT&CK for Security Control Validation

Armed with the insights provides by the MITRE ATT&CK framework and its associated attack graphs, security teams at energy companies can map the defenses they currently have in place to the most problematic threats. This process presents an opportunity to identify clear gaps in coverage and to prioritize security investments that address the most glaring deficiencies in the institution's current state.

The end goal should be to develop an assessment program through which the security team can determine whether the measures they have in place — including technology, processes, and people — are working optimally.

When it comes to security control validation, one point is clear above all others: automation is vital.

Even the largest energy businesses struggle to staff red teams able to test protections against the full scope of threats to all their business groups and geographic locations. Testing should be ongoing and continuous against all the prioritized attack vectors the organization might be exposed to. Given the demand on time and budget, such an assessment regime is nearly impossible to deliver using human employees alone.

The Benefits of Automation

Automation enables continuous, low cost, and effective security control validation. Breach and attack simulation software can run assessments on a regular basis, making them a routine part of security operations. Leveraging a BAS platform can also make red team staff more productive. The team can leave routine tests to the software and take on more complex or one-off tests themselves, expanding the breadth of organizational activities that the assessment program can evaluate. A BAS platform that ties in with the MITRE ATT&CK framework can give a CISO a leg up in developing a cohesive, integrated assessment program.

The AttackIQ Security Optimization Platform provides scenarios that enable security teams to automatically assess security controls against specific TTPs in the MITRE ATT&CK framework. Security teams can leverage these attack simulation templates to test controls targeting their institution's most important threats. Once the tests are set up, they run automatically, and staff can launch them with the press of a button. This means that, even for a red team capable of performing some ongoing penetration testing internally, the AttackIQ Security Optimization Platform extends its reach by assessing the security infrastructure against a broader swath of threats and by testing more frequently.

Continuous Testing for Continuous Improvement

The ideal approach to control validation is to find gaps through testing, incrementally improve control effectiveness, retest, identify new opportunities for improvement, and then continue the cycle. Such a regime of continuous testing and improvement refines the security team's detection capabilities and enables an increasingly difficult set of scenarios, thereby continuously improving the institution's threat detection capabilities.

By leveraging MITRE ATT&CK in combination with an automated BAS platform, CISOs at energy companies cannot only hone their security infrastructures, but they can also gather the information they need to understand the return on investment on existing technology, make business cases for new investments, and provide thier boards and other stakeholders with clear answers regarding their organizations security posture.

Advanced Purple Teaming With Attack Graphs

For blue teams, attack graphs provide a schematic by which they can automatically test their cybersecurity defenses against real and relevant threats (i.e., those threats that history tells us are most likely to affect a given business in a given industry).

However, attack graphs are optimal in collaborative, purple team environments (i.e., where red and blue teams collaborate in highly communicative and supportive relationships across the functional boundary to better protect the enterprise). This is because the demands of guarding against rapidly evolving attacks have outstripped the ability of blue or red teams to understand and adapt to the complete threat landscape alone.

Purple teams focus first on reviewing attack variants and TTPs jointly, developing from there a prioritized list of attack graphs to investigate. Working together, red and blue teams can also better come up with mitigations to any flaws in their defenses identified by the attack graph, as well as the best approaches to break the kill chain in an attack.

Attack Graphs Applied: Case Studies From the Energy Sector

CASE STUDY #1: ATTACK GRAPH RESPONSE TO US-CERT AA22-083A: HISTORICAL RUSSIA-BASED ACTORS TARGETING THE ENERGY SECTOR

The HAVEX strain of malware first targeted energy companies between 2012 and 18. In March 2022, HAVEX was once again in the spotlight when the FBI, CISA, and DOE released a joint Cybersecurity Advisory (CSA) providing an overview of the TTPs used in these historic cases.

The TTPs employed by the Russia-based threat actors behind HAVEX are still relevant to today's threat landscape. AttackIQ has therefore issued a new attack graph, "[US-CERT AA22-083A] – TTPs of HAVEX Malware (2014-04) Used by Russian FSB Center 16 Cyber Operators Against Energy Sector 2012-2014," which emulates some of the key TTPs used in the first phase of the campaign. It is critical for energy company CISOs to validate their security program performance against these types of native techniques to ensure that their organizations are prepared.

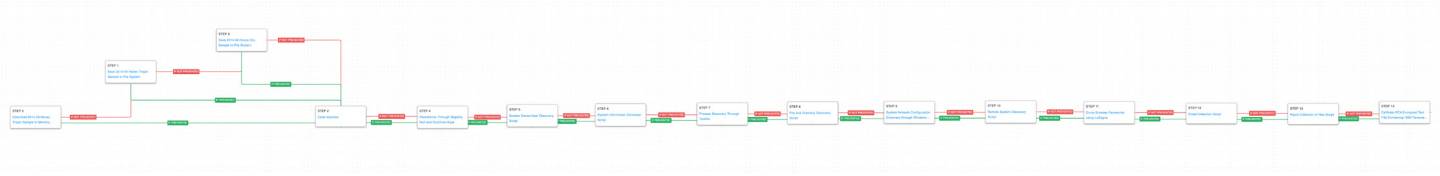

Figure 1: AttackIQ attack graph response to US-CERT AA22-083A, HAVEX malware targeting the energy sector.

Click for Larger View

The attack graph takes the following steps:

Scenario

Spearphishing Link (T1566.002): simulating when a user follows a link and attempts to download a malicious payload to disk.

One of the original trojanized ICS software installers are downloaded from a remote site over HTTP and then attempted to be written to disk. These are the atomic tests designed to test a security control's ability in preventing a well-known malicious file from being received or saved to disk.

Additionally, the final HAVEX DLL payload is also attempted to be written to disk.

Detection

EDR tools: attempt to build detections looking for Microsoft Office products invoking interpreters, as this is a sign a malicious macro may have been executed from a Microsoft document:

- `Parent Process Name == (winword.exe OR excel.exe OR powerpnt.exe)`
- `Process Name == (cmd.exe or powershell.exe)`

Add additional command line behavior indicating downloading/execution of a fileless attack:

- `Parent Process Name == (winword.exe OR excel.exe OR powerpnt.exe)`
- `Process Name == (cmd.exe or powershell.exe)`
- `Command Line CONTAINS ("DownloadString" AND ("IEX" OR "Invoke-Expression))`

Check for registry modifications to the following registry keys which could indicate a change that would enable macro execution:

- `HKEY_CURRENT_USER\Software\Microsoft\office\<OfficeVersion>\Word\security\VbaWarnings`
- `HKEY_CURRENT_USER\Software\Microsoft\office\<OfficeVersion>\Excel\security\VbaWarnings`
- `HKEY_CURRENT_USER\Software\Microsoft\office\<OfficeVersion>\PowerPoint\security\VbaWarnings`

Public Sigma rule for detecting via SIEM: Suspicious Double Extension

Mitigation

- Disable Office macros except in the specific apps where they are required.
- Utilize anti-phishing/email filtering software.
- Enforce user training on email and phishing awareness.

Scenario	Detection	Mitigation

Dynamic-link Library Injection (T1055.001): HAVEX injects itself into the running explorer.exe process. The actor uses this specific process to help evade detection via activity logging as all actions would appear to originate from the legitimate Explorer process. The scenario is initially configured to attempt injection of a custom AttackIQ DLL into the AttackIQ process, but advanced users can change the configuration to attempt the same injection into explorer.exe.	Using an EDR or SIEM product ingesting windows logs, attempt to identify instances where explorer.exe is loading in unsigned DLLs. Although this may be false positive prone, it will alert when explorer.exe is seen loading an abnormal DLL which could be an indicator of HAVEX.
	
	Public Sigma rule for detecting via SIEM:
	
	`title: Unsigned Image Loaded Into explorer Process`
	`id: 3BCDE80B-D74F-4E53-B35B-D24BDB790B75`
	`status: Experimental`
	`description: Loading unsigned image (DLL, EXE) into Explorer process`
	`author: Jackson Wells`
	`references:`
	`- https://www.slideshare.net/heirhabarov/hunting-for-credentials-dumping-in-windows-environment`
	`date: 2022/03/28`
	`modified: 2022/03/28`
	`logsource:`
	`category: image_load`
	`product: windows`
	`detection:`
	`selection:`
	`Image|endswith: '\explorer.exe'`
	`Signed: 'false'`
	`condition: selection`
	`level: medium`
	`tags:`
	`- attack.credential_access`
	`- attack.t1003.001`
		If possible, utilize EDR/EPP Products to block types of process injections based on sequences of behavior that occur during the injection process. https://attack.mitre.org/techniques/T1055/001/
		
		Additional documentation on proper mitigations to prevent DLL preloading attacks seen here: https://support.microsoft.com/en-us/topic/secure-loading-of-libraries-to-prevent-dll-preloading-attacks-d41303ec-0748-9211-f317-2edc819682e1

Registry Run Keys (T1547.001): The threat actors used common 'CurrentVersion\Run' registry keys to ensure HAVEX would continue to start up after every restart. Windows leverages many different registry keys for this purpose and the scenario tests two of the most commonly used keys:
 	
`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`
`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce`
	Using a SIEM or EDR Platform to see modifications to the Run and RunOnce keys will alert when unauthorized users or software makes modifications to "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run"
	
	`Process name: reg.exe`
	`Command Line Contains ("ADD" AND "Microsoft\Windows\CurrentVersion\Run" AND "/V")`
	
	Optionally you can include a search for users NOT IN to lower the chance of false positives.
		This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features. For best protection, ensure group policy is set to only allow specific users with need to utilize reg.exe as well as have anti-virus enabled to statically and dynamically scan files for possible malicious use of the registry.

Scenario	Detection	Mitigation

System Owner/User Discovery (T1033): The first local discovery step executed by the actors in this attack graph is to get details on the running users. This behavior is emulated using a command shell to run the "query user" command, which retrieves a list of Remote Desktop Sessions running on the host, and the "whoami" command to get the running user of the malicious process.	Although commands such as "query user" and "whoami" are utilized as administrators frequently, there should still be alerts in place when unexpected users are running these commands as they could be a sign of possible user enumeration and system discovery.
	
	With an EDR, if possible, look for the following details:
	
	`Process Name == (cmd.exe OR powershell.exe)`
	`Command Line CONTAINS ("Query User" OR "whoami")`
	`User != [<list of expected administrators to be issuing these commands>]`
	
	Additionally, "whoami" and "priv" is a command that should be monitored closely for typical end users. This command will show any permissions for token usage available and may give indicators if the user is exploitable to a Token Impersonation Attack.
		Ensure that group policy enforces only authorized users/administrators to be able to run cmd.exe or powershell.exe. These interpreters can be limited to lower privileged or unneeded users to prevent enumeration or abuse.

System Information Discovery (T1082): Threat actors commonly want to understand more about the host they have compromised. Understanding what version of the operating system is running, how much memory is installed, or how much disk space is available, will indicate if the actors have managed to access a server or client host. This scenario executes the native Windows command "systeminfo" through the command shell to receive detailed information about the computer.	`Process Name == (cmd.exe OR powershell.exe)`
	`Command Line CONTAINS "systeminfo"`
	`User NOT IN User != [<list of expected administrators to be issuing these commands>]`
		Ensure that Group Policy enforces only authorized users/administrators to be able to run cmd.exe or powershell.exe. These interpreters can be limited to lower privileged or unneeded users to prevent enumeration or abuse.

Process Discovery (T1057): A threat actor would want to understand what software is running on a specific host to either identify security software that may inhibit their actions or to illuminate targets of interest running ICS/SCADA applications. This is another scenario that uses a native Windows tool to achieve that end. Tasklist is executed as a command process and the results are saved to a temporary location.	Using an EDR or SIEM product, use the following parameters for identifying possible enumeration of system processes:
	
	`Process Name == ("cmd.exe" OR "powershell.exe")`
	`Command Line CONTAINS ("Tasklist" AND "/FO")`
	`User = [<list of expected administrators to be issuing these commands>]`
		Ensure application whitelisting is in place to allow only permitted users/administrators the right to run utility binaries such as cmd.exe, powershell.exe, tasklist.exe, and WMIC.exe.

Scenario	Detection	Mitigation
File and Directory Discovery (T1083): HAVEX performs many initial discovery and profiling activities on the host. The threat actors were interested in collecting information about available drives and files located in the Desktop, My Documents, and Program Files directories. This behavior is emulated by using the native Windows 'dir' command to list all files in those directories and record the results in a temporary text file.	File and Directory discovery typically utilizes living off the land binaries such as dir or ls to discover interesting directories of files that could be of use for the attacker. There is no excellent continuous way of monitoring this activity, but many actors use automated scripts to perform this activity to expedite the process. Look for excessive "dir" and "type" commands on a windows machine invoked possibly from a batch or VBS file which could indicate possible mass enumeration of file system.	Ensure sensitive files and directories have proper permissions assigned. Preventing non-need-to-know users access to configuration files or other sensitive user/system information could greatly reduce risk of malicious enumeration.

System Network Configuration Discovery (T1016): The HAVEX actors would want to understand how the existing host's network is configured to assist with future lateral movement. These details help the actor plan their future network scanning activity or identify which network shares and domain controllers could be targeted next. Continuing to live off the land, this scenario executes the following commands and collects the following data:
· Routing information: `route print`
· IP information: `ipconfig /all`
· Connected Domain Controller: `nltest /DSGETDC:`
· Network Shares: `net use`
· ARP information: `arp -a`
	Using an EDR or SIEM tool, you can monitor usage of windows network discovery tools. Keep in mind, these are binaries used rather frequently. we strongly recommend querying these commands with an "exclude user" option to limit false positives if that option is available in your EDR/SIEM product.
	`Process Name == ("cmd.exe" OR "powershell.exe")`
	`Command Line CONTAINS ("route print" OR "ipconfig /all" OR "nltest /DSGETDC" OR "net use" OR "arp -a")`
	`User NOT IN [<list of expected administrators to be issuing these commands>]`
		Ensure application whitelisting is in place to allow only permitted users/administrators the right to run utility binaries such as cmd.exe, powershell.exe, route.exe, ipconfig.exe, nltest.exe, net.exe, and arp.exe. Although some of these may be used on a day-to-day basis, only authorized users should have the right to run these executables to prevent misuse.

Remote System Discovery (T1018): Once the actor has collected what it needs from its initial entry point, they would shift their sights to identifying what other systems could be contacted for lateral movement. In this scenario, the "net view" command is executed and if a remote host is identified, a connection attempt is made.	Using an EDR or SIEM tool, you can monitor usage of windows network discovery tools. Keep in mind, these are binaries used rather frequently. We strongly recommend querying these commands with an "exclude user" option to limit false positives if that option is available in your EDR/SIEM product.
	`Process Name == ("cmd.exe" OR "powershell.exe")`
	`Command Line CONTAINS ("net view")`
	`User NOT IN [<list of expected administrators to be issuing these commands>]`
		Ensure application whitelisting is in place to allow only permitted users/administrators the right to run utility binaries such as cmd.exe, powershell.exe, route.exe, ipconfig.exe, nltest.exe, net.exe, and arp.exe. Although some of these may be used on a day-to-day basis, only authorized users should have the right to run these executables to prevent misuse.

Scenario	Detection	Mitigation

Credentials from Web Browsers (T1555.003): The HAVEX actors used a 3rd party tool to extract passwords from the infected browser. These credentials could include the username and passwords used to access internal resources or control ICS systems through web interfaces. This AttackIQ scenario uses a more modern tool, LaZagne, to perform credential harvesting from a selection of common Windows web browsers.	Tools such as Lazangne.exe and other password harvesting software look for browser directories for stored passwords. Looking for modifications (file copies) of locations such as "%APPDATA%\Local\Google\Chrome\User Data\Default\Login Data" would indicate that some process has taken action to copy or otherwise touch the location where browsers store encrypted passwords.
	
	Other than monitoring sensitive directories such as the one listed above, tools such as Lazangne.exe will have the following attributes when ran:
	
	`Process Name = ("cmd.exe" or "powershell.exe")`
	`Command Line CONTAINS ("browsers" AND "-oJ" AND "-output")`
		Ensure you configure browser settings to NOT store passwords on your behalf as the method is not secure. We recommend utilizing a password vault service to store and handle passwords.
		
		Additionally, utilize anti-virus product policies to look for browser-based attacks as well as any behavioral indicator engines to alert on possible browser password enumeration.

Local Email Collection (T1114.001): The Russian-based threat actors were interested in collecting local Outlook Address Book files. They could leverage this information for future phishing attacks to target other employees at the same company or their external connections. Having access to address book content would allow the actor to tailor their targeting based on job titles and locations provided by the contact records. The scenario in this attack graph takes it a little further by collecting all offline mail content on the host. A PowerShell script is used to search for PST and OST files located in the User or Program Files directories.	Malicious actors will attempt to pull email files (.PST and .OST) under Program Files, Users, and/or UsersProfile directories. Powershell scripts are the most common way these searches are performed, output to look for is as follows:
	
	`Process Name == ("powershell.exe" OR "cmd.exe")`
	`Command Line CONTAINS ("Get-ChildItem -Path" AND ("Users" OR "Programfiles" OR UserProfile") AND (".PST" OR ".OST"))`
		If possible, enforce encryption on these file locations. Use of encryption provides an added layer of security to sensitive information sent over email. Encryption using public key cryptography requires the adversary to obtain the private certificate along with an encryption key to decrypt messages. (https://attack.mitre.org/techniques/T1114/001/)
		
		Ensure application whitelisting is in place to allow only permitted users/administrators the right to run utility binaries such as cmd.exe and powershell.exe.

Automated Collection (T1119): Threat actors will commonly leverage file extension filters to automate data collection. By collecting everything that matches their rules instead of manually reviewing content during the intrusion, they are reducing the amount of time needed to find files of interest. There is a tradeoff though, as the actor will need to balance between speed and noise from mass collection activity. This scenario searches for all document file types and then collects them into a zip file stored in a temporary directory.	With automated collection, you should expect a wide array of files to be collected and zipped into a convenient folder for the attacker to utilize. Attempting to look for 100 or more of the files below being modified within one minute is a sign of some bulk automation that may need investigation if it was performed by an unexcepted user or time. `".doc, .xps, .xls, .ppt, .pps, .wps, .wpd, .ods, .odt, .lwp, .jtd, .pdf, .zip, .rar, .docx, .url, .xlsx, .pptx, .ppsx, .pst, .ost, psw, pass, login, admin, sifr, sifer, vpn, .jpg, .txt, *.lnk"`	Encryption and off-system storage of sensitive information may be one way to mitigate collection of files but may not stop an adversary from acquiring the information if an intrusion persists over an extended period of time and the adversary is able to discover and access the data through other means. Strong passwords should be used on certain encrypted documents that use them to prevent offline cracking through brute force techniques. (https://attack.mitre.org/techniques/T1114/001/) Additionally, utilizing a file integrity monitoring (FIM), data loss prevention (DLP), or endpoint detection and response (EDR) product with FIM or DLP may have policy settings to alert when these actions occur.

Scenario	Detection	Mitigation
Exfiltration Over Symmetric Encrypted Non-C2 Protocol (T1048.001): HAVEX used a combination of compression and encryption algorithms to encrypt and decrypt data sent to and from their command-and-control servers. The additional layers of obfuscation make it more difficult for detection as the commands and stolen data will not be visible as plain text even if advanced defensive techniques were utilized like SSL decryption. This scenario will exfiltrate an encrypted file containing personal data over HTTP, simulating the transfer of confidential data using layered encryption.		Enforce proxies and use dedicated servers for services such as DNS and only allow those systems to communicate over respective ports/protocols, instead of all systems within a network. (https://attack.mitre.org/techniques/T1048/001/) Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary command and control infrastructure and malware can be used to mitigate activity at the network level. (https://attack.mitre.org/techniques/T1048/001/) Follow best practices for network firewall configurations to allow only necessary ports and traffic to enter and exit the network (https://attack.mitre.org/techniques/T1048/001/)

CASE STUDIES #2 AND #3: OILRIG CAMPAIGNS

OilRig, also known as APT34, is likely a state-sponsored Iranian adversary who was first identified in 2012 by Symantec during a wave of destructive attacks in the Middle East. The threat actor's attacks have consistently aligned to Iran's national interests and target multiple sectors around the globe, including energy. OilRig has been behind two noteworthy campaigns: a 2020 social media phishing campaign and the 2018 QuadAgent campaign.

OilRig – 2020-01 – Social Media Phishing Campaign

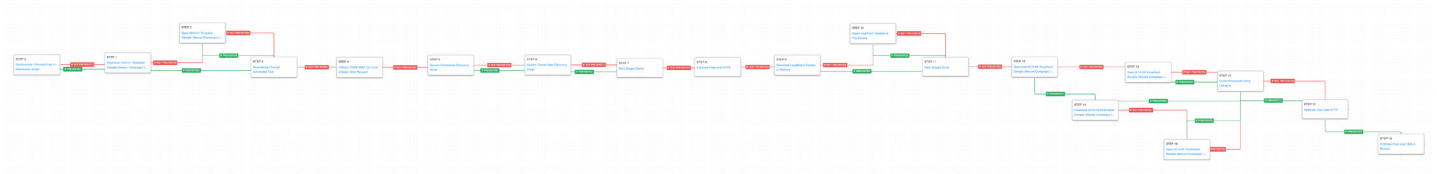

Figure 2: AttackIQ attack graph response to OilRig – 2020-01 – social media phishing campaign.

Click for Larger View

During this campaign, the adversaries impersonated members of various organizations to gain and exploit the trust of the victims. Malicious documents were distributed via LinkedIn that would lead to the delivery of the actor's bespoke Tonedeaf backdoor.

The first steps in this attack graph are emulating the delivery techniques used to download Tonedeaf to the victim's workstation.

- **Deobfuscate/Decode Files or Information (T1140):** Use the legitimate "certutil" binary to decode a base64 encoded payload.
- **Ingress Tool Transfer (T1105):** Download and save the original sample of the actor's Tonedeaf malware to test network and endpoint controls' ability to prevent malicious files.

Once the malware was executed, the threat actor would establish persistence using a scheduled task, check-in with the command-and-control server, and perform initial discovery actions to learn more about the compromised environment.

- **Scheduled Task (T1053.005):** The Windows Task Scheduler is used to create a task that will execute a command at startup.
- **Application Layer Protocol: Web Protocols (T1071.001):** A web request is made to AttackIQ controlled infrastructure that mimics the HTTP GET request the Tonedeaf malware uses when completing the initial check-in.
- **System Information Discovery (T1082):** Execute native commands like "systeminfo" or "lshw" to learn about the system hardware configuration.
- **System Owner/User Discovery (T1033):** Live off the land by running "whoami" and "users" to gain details about the currently available accounts and permission groups.

The data collected during the discovery phase is then staged and exfiltrated to the command-and-control server over HTTP. The actor then downloads LongWatch, a keylogger, that directs keystroke outputs to a file in the Windows Temp folder

- **Data Staged: Local Data Staging (T1074.001):** Files are collected and stored in a temporary directory so they can be exfiltrated later.
- **Exfiltration Over C2 Channel (T1041):** Files are sent to an AttackIQ controlled server using HTTP POST requests.

OilRig then brings down different password dumping utilities. The first attempt is for ValueVault, a Golang version of the credential-stealing tool known as "Windows Vault Password Dumper." If that attempt is prevented, then they will try to retrieve PickPocket which is a browser credential-stealing tool.

- **OS Credential Dumping (T1003):** The open source tool LaZagne is executed to dump all available credentials from the same sources ValueVault and PickPocket utilize.

Finally, passwords and any additional files of interest would be exfiltrated by the actor using fallback channels of HTTP and DNS.

- **Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol (T1048.003):** Data is broken up into small chunks and encoded into DNS requests sent to an AttackIQ controlled server.

OilRig – 2018-07 – QuadAgent Campaign

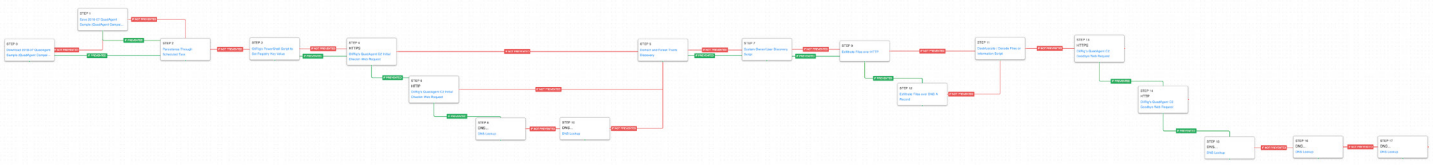

Figure 3: AttackIQ attack graph response to OilRig – 2018-07 – QuadAgent campaign.

Click for Larger View

As above, this attack graph starts with the delivery of the actor's custom PowerShell malware, QuadAgent, and creates persistence with a scheduled task. The actor then creates a unique victim identifier that is stored in a registry key. This value is later utilized when communicating with the command-and-control server for identification.

- **Modify Registry (T1112):** This scenario sets the same registry key used by the actor by calling the "New-ItemProperty" cmdlet.

The QuadAgent malware then communicates with the command-and-control server to let the actor know they are ready for tasking. The malware leverages fallback channels if it is unable to communicate with the actor's infrastructure. The first attempts are over SSL and if prevented revert to unencrypted HTTP requests. If those fail as well, the actor pivots to using DNS requests.

- **Fallback Channels (T1008):** The attack graph will try each of the three possible communication protocols if the original tries are blocked.
- **Application Layer Protocol: DNS (T1071.004):** Two separate DNS requests are attempted, the first lets the actor know that they are going to be using the DNS protocol and the second is the initial check-in data.

After communicating with the C2 server, the threat actor begins to perform discovery actions to learn more about the compromised environment. They begin by querying details around Active Directory configuration and then system owner information. Data is then exfiltrated either over HTTP or DNS depending on the previous network communications. Any data received from the actor is in the form of base64 data.

- **Domain Trust Discovery (T1482):** PowerView is used to replace Window's "net" commands that enumerate details on the connected domain and forests of the infected host.

The attack graph finishes by sending the good-bye requests made by QuadAgent before it receives any additional malware stages. Like the initial check-in messages, the actor leverages the same fallback channels of HTTPS, HTTP, and DNS.

The OilRig attack graphs set out the following:

Scenario	Detection	Mitigation

Scheduled Task (T1053.005): OilRig, like many actors, relies on Scheduled Tasks to maintain persistence in a victim's environment. Disrupting their ability to maintain their foothold will help prevent their immediate return when you initiate clean up actions.	Behavioral Detections can be utilized in EDR and SIEM products to detect and/or prevent malicious scheduling of tasks and creation of windows services:
	
	Scheduled Task Detection:
	
	`Process Name == (cmd.exe OR powershell.exe)`
	`Command Line CONTAINS ("schtasks" AND "/create" AND ("cmd" OR powershell") AND (".exe" OR ".bat") AND "/ru system")`
		MITRE's mitigations for Scheduled Tasks (T1053.005)
		
		· M1047 – Audit
		· M1028 – Operating System Configuration
		· M1206 – Privileged Account Management
		· M1018 – User Account Management

Scenario	Detection	Mitigation
Application Layer Protocol: DNS (T1071.004): The actor's use of command-and-control over DNS is common amongst many Iranian threat actors. The long and persistent amount of DNS requests involving hundreds or thousands of child domains with the same single parent domain can help identify potential use of this technique.	As referenced per MITRE Network Traffic Detection – DS0029 · Monitor and analyze traffic patterns and packet inspection associated to protocol(s), leveraging SSL/TLS inspection for DNSSEC traffic, that do not follow the expected protocol standards and traffic flows (e.g., extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated to traffic patterns (e.g., monitor anomalies in use of files that do not normally initiate connections for respective protocol(s)). · Monitor for DNS traffic to/from known-bad or suspicious domains and analyze traffic flows that do not follow the expected protocol standards and traffic flows (e.g., extraneous packets that do not belong to established flows, or gratuitous or anomalous traffic patterns). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated to traffic patterns (e.g., monitor anomalies in use of files that do not normally initiate connections for respective protocol(s)).	MITRE's mitigations for Application Layer Protocol: DNS (T1071.004) · M1037 – Filter Network Traffic · M1031 – Network Intrusion Prevention

Conclusion: Security Validation That's Fit for Purpose

"Know thy enemy and know yourself; in a hundred battles, you will never be defeated." Sun Tzu's famous quote is as relevant today as ever. In the digital age, "knowing your enemy" means taking a threat-informed defensive posture that draws on rich intelligence of how threat actors behave based on real-world activities. "Knowing yourself" means applying that intelligence to test your own security controls and ensure their effectiveness.

Thanks to advances in automation, particularly around breach and attack simulation, and deeper approaches to attack forensics that have led to the attack graphs, CISOs at energy companies have the tools they need to test repeatedly and holistically against their most important threats to ensure that their security controls are always optimized. In an industry where attacks are assured, a threat-informed defense provides the peace of mind CISOs and their business stakeholders need.

---

i Energy Sector, CFI
ii Critical Infrastructure Sectors, CISA
iii Colonial Pipeline boss confirms $4.4m ransom payment, BBC News, May 2021
iv X-Force Threat Intelligence Index 2022, IBM Security, February 2022
v Ibid
vi See Alert (AA22-083A), March 2022

ATTACKIQ
U.S. Headquarters
171 Main Street Suite 656
Los Altos, CA 94022
+1 (888) 588-9116
info@attackiq.com