OilRig Attack Graphs: Emulating the Iranian Threat Actor’s Global Campaigns

AttackIQ has released two new attack graphs that emulate different aspects of OilRig’s operations against multiple sectors around the globe. With these attack graphs, you can test and validate your defenses to improve cybersecurity readiness.

*Sectors Targeted: Government, Financial Services, Energy, Resources & Utilities, Manufacturing, Telecommunications and Technology*

OilRig, also known as APT34, is a likely state-sponsored Iranian adversary who was first identified in 2012 by [Symantec](https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=281521ea-2d18-4bf9-9e88-8b1dc41cfdb6&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments) during a wave of destructive attacks in the Middle East. The threat actor’s attacks have consistently aligned to Iran’s national interests and have targeted multiple sectors around the globe. OilRig’s victims have spanned the government, financial services, energy, resources and utilities, manufacturing, telecommunications, and technology industries.

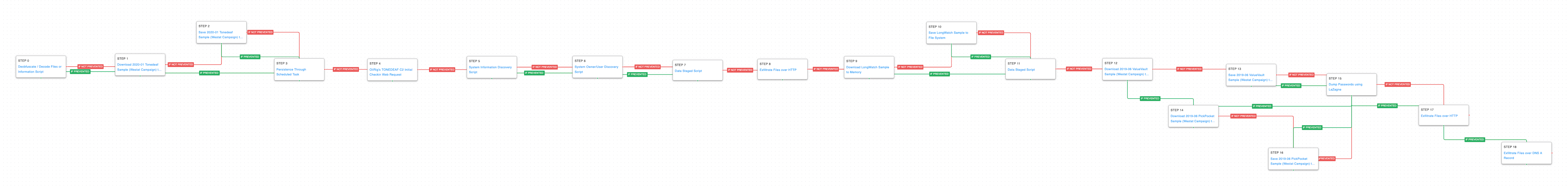
OilRig has shown proficiency in a wide range of attack vectors. They have conducted social engineering attacks through legitimate social networks like LinkedIn to deliver documents with fraudulent job offers from prominent organizations. They conducted destructive actions using wipers, such as the Disttrack malware family, during the Shamoon [attacks](https://unit42.paloaltonetworks.com/unit42-second-wave-shamoon-2-attacks-identified/). They also used supply chain compromises where the adversary exploited relationships of trust between organizations to reach their desired targets.

AttackIQ has released two new Attack Graphs that emulate different campaigns carried out by this adversary to help customers validate their security controls against OilRig.

Validating your security program performance against these specific threat actor behaviors is paramount in reducing risk. By using these new attack graphs in the AttackIQ Security Optimization Platform, security teams will be able to:

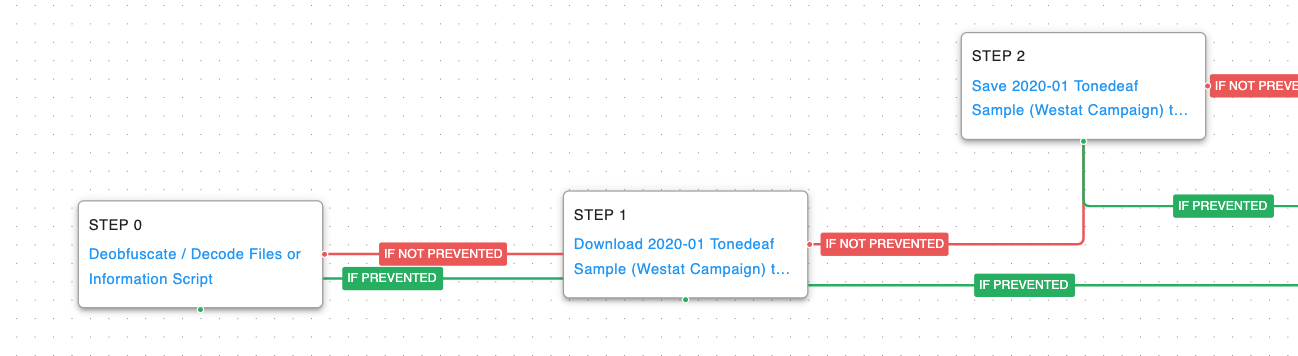
1. Evaluate security control performance against the same techniques a single threat actor utilized to be successful for years.
2. Assess security posture for attacks that are technically un-sophisticated but still allowed the actor to achieve their goals.
3. Continuously validate detection and prevention pipelines as your security controls and posture improve.

**OilRig – 2020-01 – Social Media Phishing Campaign**

[](https://attackiq.com/wp-content/uploads/2022/07/col-blg-0-0-attackgraph.png)

*Figure 1.0: Attack Graph (Click for Larger)*

This attack graph is based on reports from [Mandiant](https://www.mandiant.com/resources/hard-pass-declining-apt34-invite-to-join-their-professional-network) and [Intezer](https://www.intezer.com/blog/malware-analysis/new-iranian-campaign-tailored-to-us-companies-uses-updated-toolset/" \t "_blank) describing social engineering attacks against multiple organizations around the world conducted in 2020.

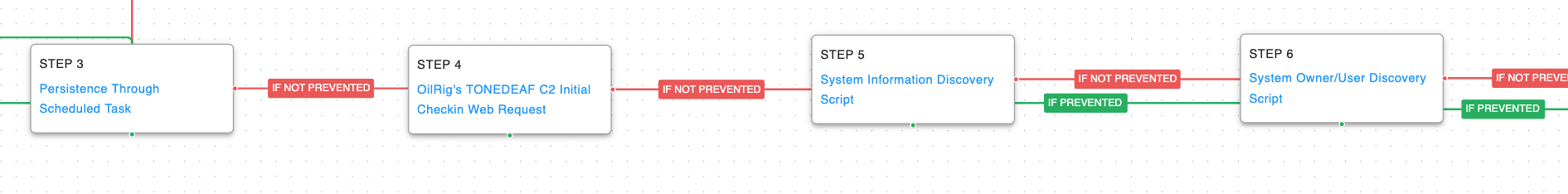
[](https://attackiq.com/wp-content/uploads/2022/07/col-blg-0-1-delivery.png)

*Figure 1.1: Delivery (Click for Larger)*

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**](https://attack.mitre.org/techniques/T1140/)**):** Use the legitimate “*certutil*” binary to decode a base64 encoded payload.

**Ingress Tool Transfer (**[**T1105**](https://attack.mitre.org/techniques/T1105/)**)**: Download and save the original sample of the actor’s Tonedeaf malware to test network and endpoint controls’ ability to prevent malicious files.

[](https://attackiq.com/wp-content/uploads/2022/07/col-blg-0-2-discovery.png)

*Figure 1.2: Discovery (Click for Larger)*

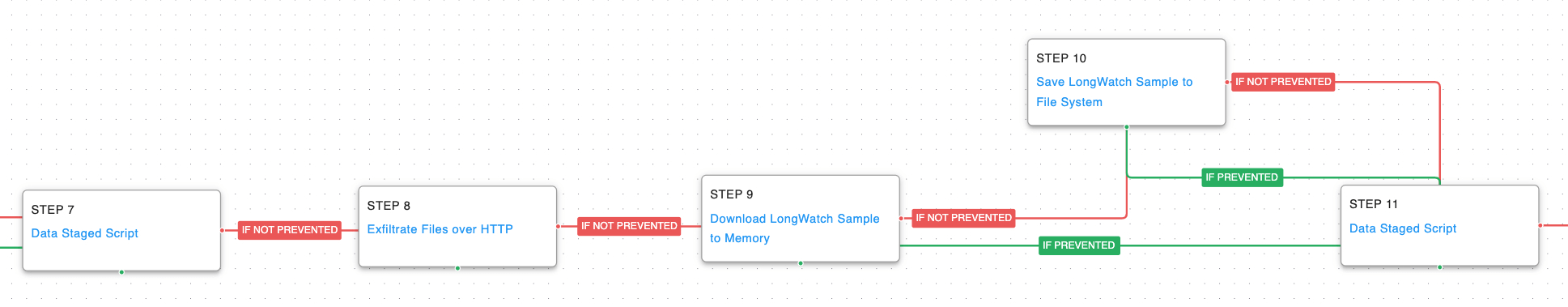
Once the malware was executed, the threat actor would establish persistence using a scheduled task, check-in with the command-and-control server, and perform initial discovery actions to learn more about the compromised environment.

**Scheduled Task (**[**T1053.005**](https://attack.mitre.org/techniques/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**](https://attack.mitre.org/techniques/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**](https://attack.mitre.org/techniques/T1082/)**):**Execute native commands like “*systeminfo*” or “*lshw*” to learn about the system hardware configuration.

**System Owner / User Discovery (**[**T1033**](https://attack.mitre.org/techniques/T1033/)**):** Live off the land by running “*whoami*” and “*users*” to gain details about the currently available accounts and permission groups.

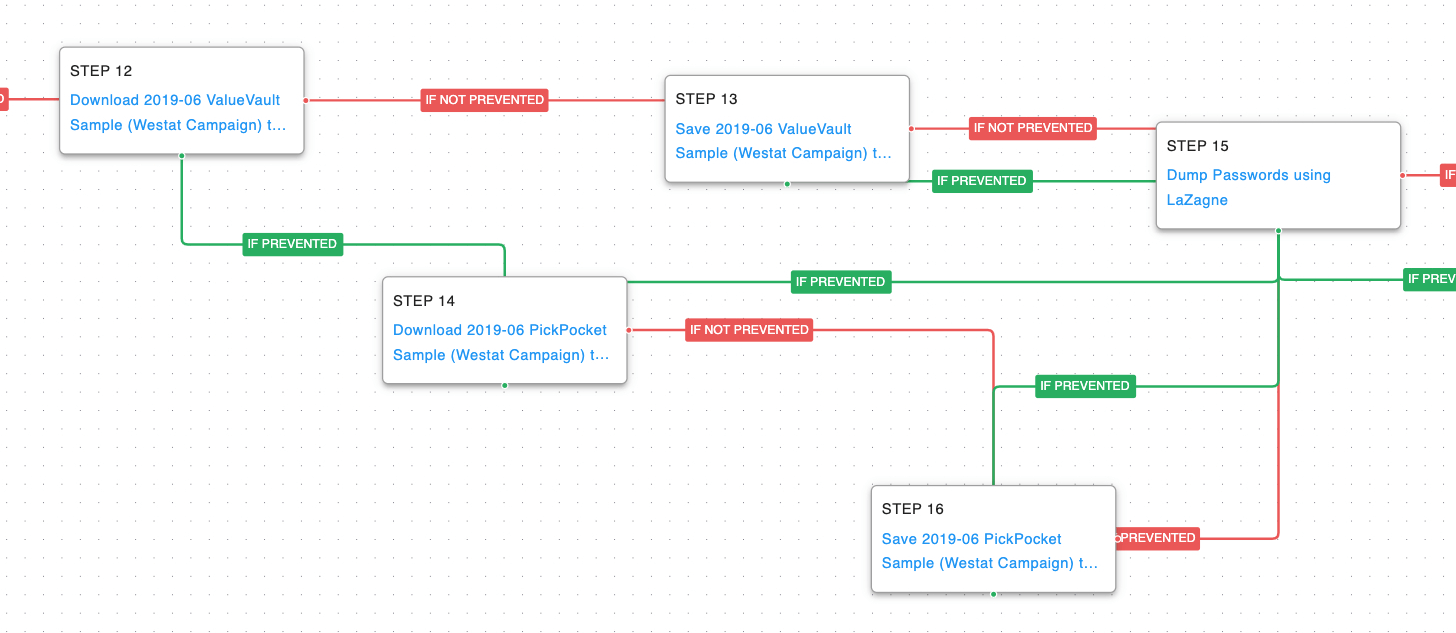
[](https://attackiq.com/wp-content/uploads/2022/07/col-blg-0-3-exfil-white.png)

*Figure 1.3: Exfiltration (Click for Larger)*

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**](https://attack.mitre.org/techniques/T1074/001/)**):**Files are collected and stored in a temporary directory so they can be exfiltrated later.

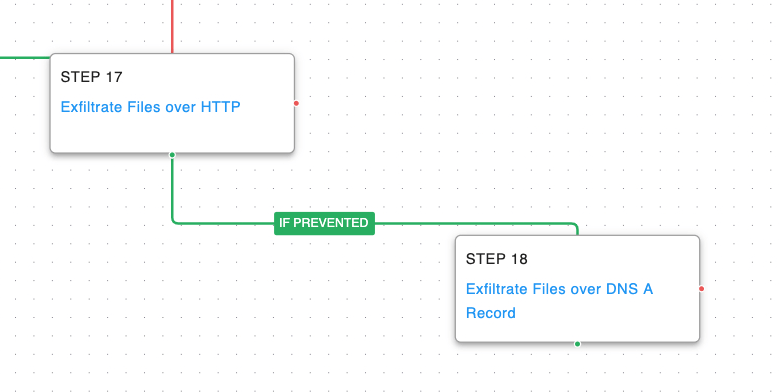
**Exfiltration Over C2 Channel (**[**T1041**](https://attack.mitre.org/techniques/T1041/)**):**Files are sent to an AttackIQ controlled server using HTTP POST requests.

[](https://attackiq.com/wp-content/uploads/2022/07/col-blg-0-4-passwords.png)

*Figure 1.4:Passwords (Click for Larger)*

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 isa browser credential-stealing tool.

**OS Credential Dumping (**[**T1003**](https://attack.mitre.org/techniques/T1003/)**):**The open source tool [LaZagne](https://github.com/AlessandroZ/LaZagne) is executed to dump all available credentials from the same sources ValueVault and PickPocket utilize.

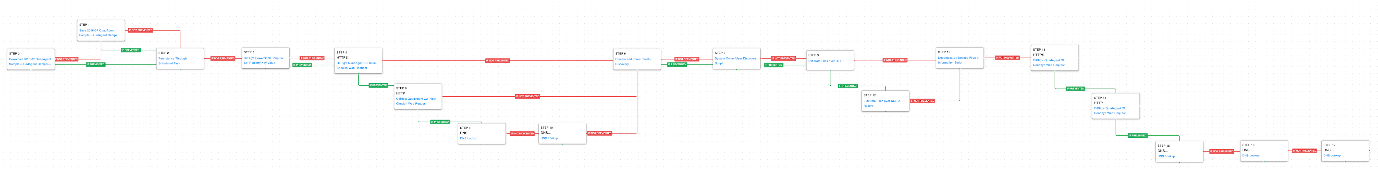
[](https://attackiq.com/wp-content/uploads/2022/07/col-blg-0-5-final.png)

*Figure 1.5: Exfiltration (Click for Larger)*

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**](https://attack.mitre.org/techniques/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**

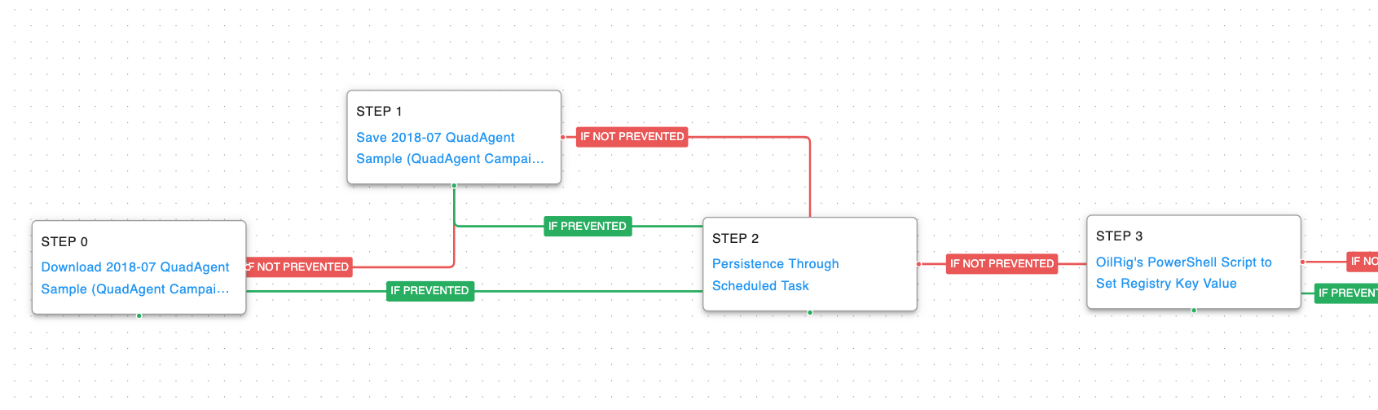
[](https://attackiq.com/wp-content/uploads/2022/07/1-0-AttackGraph.png)

*Figure 2.0: Attack Graph (Click for Larger)*

This Attack Graph is based on a 2018 Palo Alto Networks [report](https://unit42.paloaltonetworks.com/unit42-oilrig-targets-technology-service-provider-government-agency-quadagent/) where OilRig used a PowerShell-based backdoor known as QuadAgent against Technology Service providers and Government agencies.

Like the first attack graph, this one 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**](https://attack.mitre.org/techniques/T1112/)**):**This scenario sets the same registry key used by the actor by calling the “*New-ItemProperty*” cmdlet.

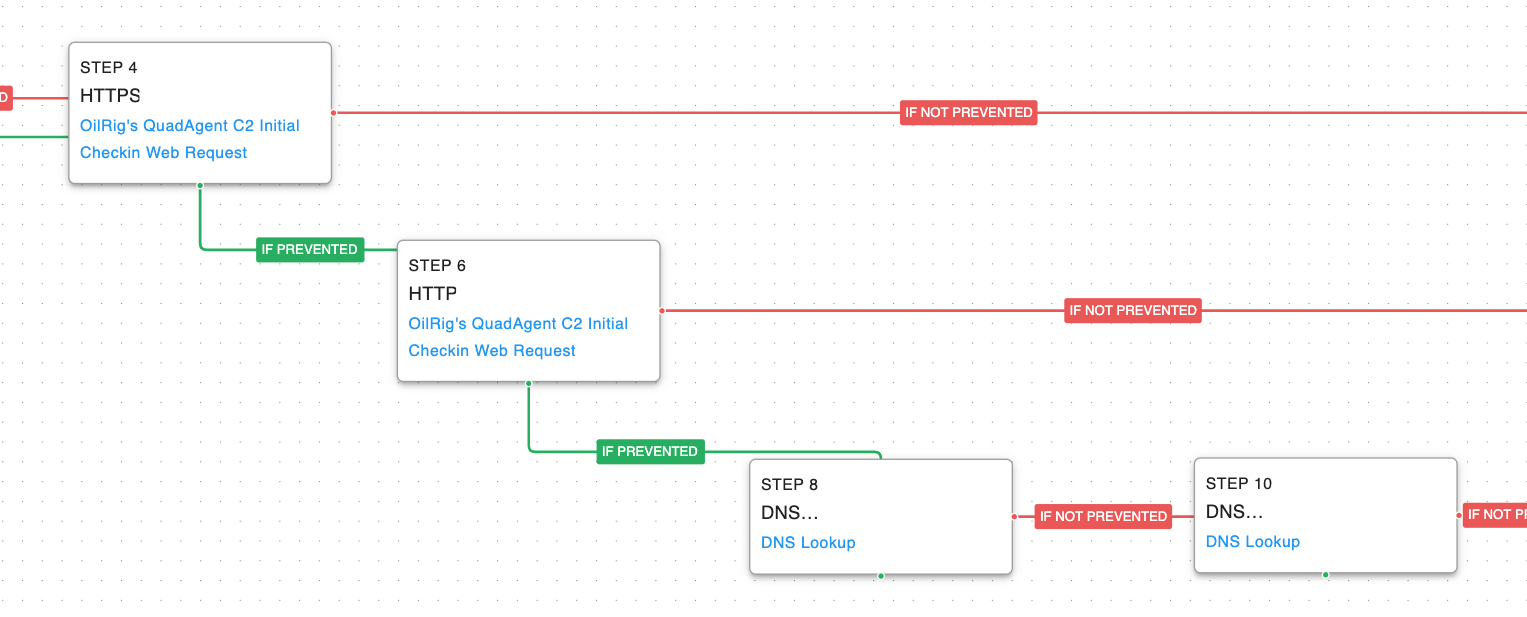
[](https://attackiq.com/wp-content/uploads/2022/07/col-blg-1-1-delivery.png)

*Figure 2.1:Delivery (Click for Larger)*

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**](https://attack.mitre.org/techniques/T1008/)**):** The attack graph will try each of the three possible communication protocols if the original tries are blocked.

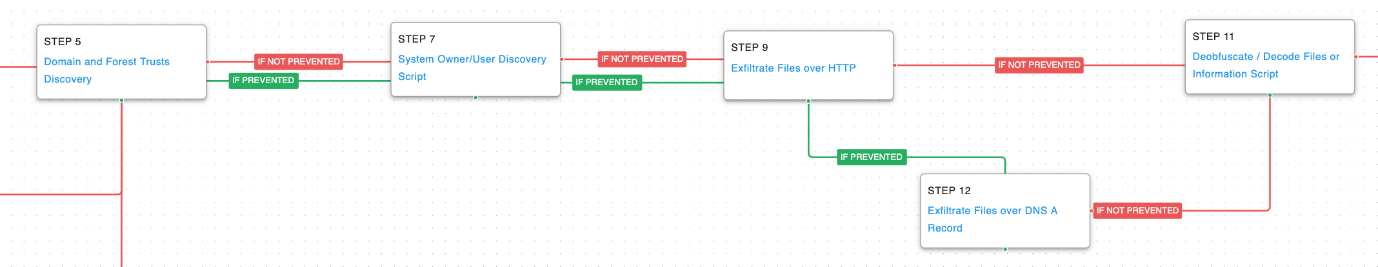
**Application Layer Protocol: DNS (**[**T1071.004**](https://attack.mitre.org/techniques/T1071/004/)**):**Two separate DNS requests are attempted, the first lets the actor know that they are going to be using the DNS protocol and the second is the initial check-in data.

[](https://attackiq.com/wp-content/uploads/2022/07/col-blg-1-2-c2.png)

*Figure 2.2: Command and Control (Click for Larger)*

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**](https://attack.mitre.org/techniques/T1482/)**):**PowerView is used to replace Window’s “net” commands that enumerate details on the connected domain and forests of the infected host.

[](https://attackiq.com/wp-content/uploads/2022/07/col-blg-1-3-discovery.png)

*Figure 2.3:Discovery (Click for Larger)*

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.

**Detection and Mitigation Opportunities**

With so many different techniques being utilized by threat actors, it can be difficult to know which to prioritize for prevention and detection opportunities. AttackIQ recommends first focusing on the following techniques emulated in our scenarios before moving on to the remaining techniques.

**1. Scheduled Task (**[**T1053.005**](https://attack.mitre.org/techniques/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.

*1a. Detections*

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”)

*1b. Mitigations*

MITRE’s mitigations for Scheduled Tasks ([T1053.005)](https://attack.mitre.org/techniques/T1053/005/)

* [M1047 – Audit](https://attack.mitre.org/mitigations/M1047/)
* [M1028 – Operating System Configuration](https://attack.mitre.org/mitigations/M1028/)
* [M1206 – Privileged Account Management](https://attack.mitre.org/mitigations/M1026/)
* [M1018 – User Account Management](https://attack.mitre.org/mitigations/M1018/)

**2. Application Layer Protocol: DNS (**[**T1071.004**](https://attack.mitre.org/techniques/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.

*2a. Detections*

As referenced per MITRE [Network Traffic Detection – DS0029](https://attack.mitre.org/datasources/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)).

**2b. Mitigations**

MITRE’s mitigations for Application Layer Protocol: DNS ([T1071.004)](https://attack.mitre.org/techniques/T1071/004/)

* [M1037 – Filter Network Traffic](https://attack.mitre.org/mitigations/M1037/)
* [M1031 – Network Intrusion Prevention](https://attack.mitre.org/mitigations/M1031/)

**Conclusion**

In summary, these two attack graphs will evaluate security and incident response processes and support the improvement of your security control posture against a nation-state actor who has been successful using common and unsophisticated measures.

With data generated from continuous testing and use of this attack graph, you can focus your teams on achieving key security outcomes, adjust your security controls, and work to elevate your total security program effectiveness against a known and dangerous threat.

AttackIQ stands at the ready to help security teams implement this attack graph and other aspects of the AttackIQ Security Optimization Platform, including through our co-managed security service, [AttackIQ Vanguard](https://attackiq.com/platform/attackiq-vanguard/).