Introducing the Adversary Playbook: First up, OilRig

By Ryan Olson

Published: 2017-12-15 · Archived: 2026-04-05 16:01:58 UTC

Over the past few years, we've been tossing around the idea of an "Adversary Playbook." The idea is rather straightforward: just as we create offensive and defensive playbooks for sports, our adversaries also have offensive playbooks that they execute to compromise organizations. They may not write them down, but they exist. This year at Palo Alto Network's Ignite conference I spoke about how defenders could create a copy of an adversary's playbook through observation and data sharing, and then use that playbook to better defend their network with defensive playbooks.
Unit 42 has been working to refine the concept of the Adversary Playbook over the last few months. In this blog, I will explain how we've structured the content and will release the Playbook for the OilRig intrusion set.

What is a Playbook?
The goal of the Playbook is to organize the tools, techniques, and procedures that an adversary uses into a structured format, which can be shared with others, and built upon. To achieve this goal, we didn't want to develop a proprietary structure that would be exclusive to Palo Alto Networks. Instead, we identified two frameworks that would enable us to not only structure our data, but also enable us to share it with others.

Framework	**Description**
STIX 2.0	Structured Threat Information Expression (STIX™) is a language and serialization format used to exchange cyber threat intelligence (CTI).
ATT&CK	MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's lifecycle and the platforms they are known to target. ATT&CK is useful for understanding security risk against known adversary behavior, for planning security improvements, and verifying defenses work as expected.

STIX 2.0 is the latest iteration of the STIX format. It has been re-designed to simplify the creation of documents and uses JSON rather than XML. STIX 2.0 provides a list of objects to represent types of information typically generated for cyber threat intelligence (CTI). For instance, STIX includes objects for intrusion sets, malware, and indicators, among others. STIX standardizes the information and attributes stored within objects based on the object type, as well as the relationships available between the various object types. The standardized objects and their relationships between each other allows this intelligence to be sharable and easily consumable without having to write complicated parsing tools.
MITRE's ATT&CK framework provide names, descriptions, and links to examples of the high-level tactics adversaries' use during an operation, as well as the techniques the adversary uses to achieve them. For example, the ATT&CK framework has a tactic called 'Launch' that refers to an adversary attempting to penetrate a network. One technique associated with this tactic is called "Spear phishing messages with malicious attachments", which

describes how the adversary would launch an attack on the network. This provides common definitions and understandings of how a specific goal is accomplished by attackers.
To meld these frameworks together, we looked at how Mitre mapped their ATT&CK data to STIX 2.0 and then chose appropriate objects for additional Playbook components.

STIX 2.0 Object	Playbook Component
Intrusion Set	Adversary
Report	Playbook
Report	Play
Campaign	Campaign
Kill-Chain-Phase	ATT&CK Tactic
Attack-Pattern	ATT&CK Technique
Indicator	Indicator
Malware	Adversary Malware
Tool	Adversary Tool

Adversary STIX 2.0 to Playbook Object Mapping

With these mappings defined, we began mapping the activities of a particular adversary into the ATT&CK framework and storing the data and indicators in STIX JSON. The first adversary we choose to target is OilRig, a group that we've published multiple reports on in the last 18 months.

Overview of OilRig
OilRig is a threat group operating primarily in the Middle East by targeting organizations in this region that are in a variety of different industries; however, this group has occasionally targeted organizations outside of the Middle East as well. It also appears OilRig carries out supply chain attacks, where the threat group leverages the trust relationship between organizations to attack their primary targets.
OilRig is an active and organized threat group, which is evident based on their systematic targeting of specific organizations that appear to be carefully chosen for strategic purposes. Attacks attributed to this group primarily rely on social engineering to exploit the human rather than software vulnerabilities; however, on occasion this group has used recently patched vulnerabilities in the delivery phase of their attacks. The lack of software vulnerability exploitation does not necessarily suggest a lack of sophistication, as OilRig has shown maturity in other aspects of their operations. Such maturities involve:

- Organized evasion testing used during the development of their tools.
- Use of custom DNS Tunneling protocols for command and control (C2) and data exfiltration.
- Custom web-shells and backdoors used to persistently access servers.

OilRig relies on stolen account credentials for lateral movement. After OilRig gains access to a system, they use credential dumping tools, such as Mimikatz, to steal credentials to accounts logged into the compromised system. The group uses these credentials to access and to move laterally to other systems on the network. After obtaining credentials from a system, operators in this group prefer to use tools other than their backdoors to access the compromised systems, such as remote desktop and putty. OilRig also uses phishing sites to harvest credentials to individuals at targeted organizations to gain access to internet accessible resources, such as Outlook Web Access.

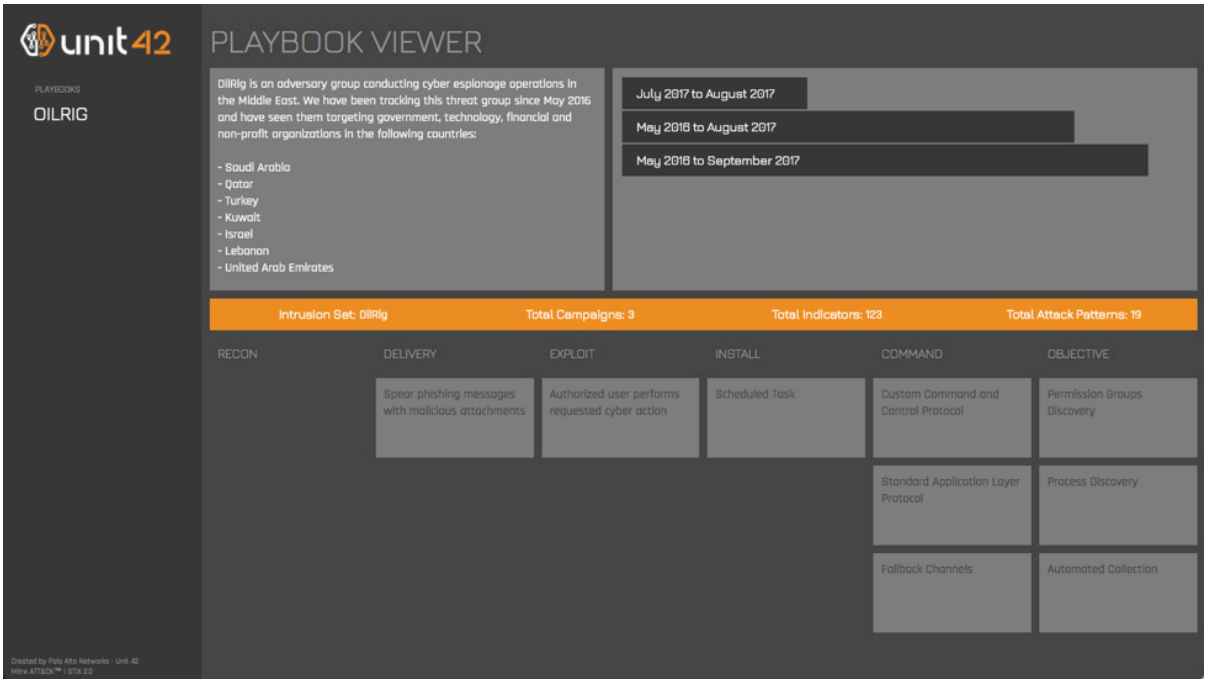
Previous reports on OilRig

- OilRig Performs Tests on the TwoFace Webshell
- OilRig Deploys "ALMA Communicator" – DNS Tunneling Trojan
- OilRig Group Steps Up Attacks with New Delivery Documents and New Injector Trojan
- Striking Oil: A Closer Look at Adversary Infrastructure
- OilRig Uses ISMDoor Variant; Possibly Linked to Greenbug Threat Group
- OilRig Actors Provide a Glimpse into Development and Testing Efforts
- OilRig Malware Campaign Updates Toolset and Expands Targets
- The OilRig Campaign: Attacks on Saudi Arabian Organizations Deliver Helminth Backdoor

The OilRig Playbook and Viewer

The OilRig Playbook is available here. It contains data on three campaigns conducted by OilRig spanning from May of 2016 to September of 2017. This includes 123 indicators that map to 19 different ATT&CK Techniques. This isn't everything we've learned about OilRig, but it's a starting point that we want to share with other members of the threat intelligence community.

In an ideal world, readers would download the JSON file and load it into their threat intelligence system. Unfortunately, there are few tools which can handle STIX 2 content at the moment, and none that would display the entire Playbook at once. To help remedy this, we're also releasing a simple tool to view the Playbook through a web interface. A screenshot of the viewer is below, and you can access the live version of it here: https://pan-unit42.github.io/playbook_viewer/



OilRig Playbook Viewed through Playbook Viewer

To start using the viewer, click on a Playbook in the left column. This reads the Playbook STIX JSON out of our GitHub repository and parses out the dated campaigns. You can then view specific campaigns by clicking on their date ranges, which will populate the attack life cycle phases in the bottom section.
If you click on a specific technique, the viewer displays a dialog (below) that includes a link to the relevant ATT&CK description as well as the STIX indicator patterns that indicate that technique. It's important to note that not every STIX indicator in the Playbook is indicative of malicious activity but simply that the behavior is present.

Indicators of an ATT&CK Technique in the Playbook Viewer

Final Thoughts
We believe that publishing Playbooks in this format will enable others to better evaluate how they can defend against a specific adversary. This is a living project, and we
intend to publish Playbooks for many of the adversaries we are currently tracking over the course of 2018, so please keep an eye out for updates through our blog.
If you have feedback on the Adversary Playbook, please leave a comment on this blog.
Thanks to the following organizations and individuals for their efforts to enable this project:

- Robert Falcone and Bryan Lee (Unit 42) for pulling together the details on OilRig and working on the Playbook Viewer
- Mitre for releasing ATT&CK and expanding its scope.
- The OASIS CTI Committee for all of their work to make STIX 2.0
- The members of the Cyber Threat Alliance for building a community of security vendors who share intelligence through automated means.
