Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

We use Splunk

But you don’t have to!
Agenda

 jugador Let’s tell a story
 jugador Oops, now I see where we went wrong
 jugador Pass go, collect 200 TTPs
So you’ve heard of this ATT&CK thing...

but how do you actually play use it?
We want to tell you a story...
“I don’t really know how we are defended and it makes me uncomfortable.”

- Grace Hoppy
CEO
“If it’s not an IP, how do I use it?
- Mallory Kraeusen
Threat Intel
“I’m drowning in meaningless alerts and my data isn’t helping me!”

- Alice Bluebird

Network Defender
“I’m not sure how I can help.”
- Kevin Lagerfield
Red Team
SS Hops and Ale

BREAKING NEWS
BEER TANKER THREATENED

19:25 HOPS PRICES PLUMET AS CONSUMERS CONSIDER "FROSE ALL DAY" OPTIONS
Iranians in my HOPS!

Grace Hoppy

Today, 8:47 PM
Mallory Kraeusen

Inbox

What the heck is going on over there! I turned on HOPSNN and found out there is cyberwarfare? Hops prices are affected!! I have a board meeting this week and I KNOW this is going to come up. I need to you find out how this going to impact us and if they are going to come after us next and how/if we are defended.

Regards,
Grace Hoppy
CEO
"Have a nice day!"
“I need to you to find out how this will impact us.... are we defended?”
How does Mallory find info on Iranian groups... ...and can ATT&CK help?
Groups - MITRE ATT&CK™ - The MITRE Corporation
https://attack.mitre.org/groups/

MuddyWater is an Iranian threat group that has primarily targeted Middle Eastern nations, and has also targeted European and North American nations. The group's victims are mainly in the telecommunications, government (IT services), and oil sectors.

APT28 · APT1 · APT3 · Threat Group-1314
<table>
<thead>
<tr>
<th>Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEODYMIUM</td>
<td>NEODYMIUM is an activity group that conducted a campaign in May 2016 and has heavily targeted Turkish victims. The group has demonstrated similarity to another activity group called PROMETHIUM due to overlapping victim and campaign characteristics. NEODYMIUM is reportedly associated closely with BlackOasis operations, but evidence that the group names are aliases has not been identified.</td>
</tr>
<tr>
<td>Night Dragon</td>
<td>Night Dragon is a campaign name for an activity involving a threat group that has conducted activity originating primarily in China.</td>
</tr>
<tr>
<td>OilRig</td>
<td>OilRig is a suspected Iranian threat group that has targeted Middle Eastern and international victims since at least 2014. The group has targeted a variety of industries, including financial, government, energy, chemical, and telecommunications, and has largely focused its operations within the Middle East. It appears the group carries out supply chain attacks, leveraging the trust relationship between organizations to attack their primary targets. FireEye assesses that the group works on behalf of the Iranian government based on infrastructure details that contain references to Iran, use of Iranian infrastructure, and targeting that aligns with nation-state interests. This group was previously tracked under two distinct groups, APT34 and OilRig, but was combined due to additional reporting giving higher confidence about the overlap of the activity.</td>
</tr>
<tr>
<td>Orangeworm</td>
<td>Orangeworm is a group that has targeted organizations in the healthcare sector in the United States, Europe, and Asia since at least 2015, likely for the purpose of corporate espionage.</td>
</tr>
<tr>
<td>Patchwork</td>
<td>Patchwork is a cyberespionage group that was first observed in December 2015. While the group has not been definitively attributed, circumstantial evidence suggests the group may be a pro-Indian or Indian entity. Patchwork has been seen targeting industries related to diplomatic and government agencies. Much of the code used by this group was copied and pasted from online forums. Patchwork was also seen operating spear phishing campaigns targeting U.S. think tank groups in March and April of 2018.</td>
</tr>
<tr>
<td>PittyTiger</td>
<td>PittyTiger is a threat group believed to operate out of China that uses multiple different types of malware to maintain command and control.</td>
</tr>
<tr>
<td>PLATINUM</td>
<td>PLATINUM is an activity group that has targeted victims since at least 2009. The group has focused on targets associated with governments and related organizations in South and Southeast Asia.</td>
</tr>
<tr>
<td>Poseidon Group</td>
<td>Poseidon Group is a Portuguese-speaking threat group that has been active since at least 2005. The group has a history of using information exfiltrated from victims to blackmail victim companies into contracting the Poseidon Group as a security firm.</td>
</tr>
<tr>
<td>PRAGUEKIN</td>
<td>PRAGUEKIN was a malware delivery or dropping tool campaign that started in 2016. The campaign has been associated with Chelk or Chelk-like malware families.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>OilRig</strong></td>
<td>is a suspected Iranian threat group that has targeted Middle Eastern and international victims since at least 2014. The group has targeted a variety of industries, including financial, government, energy, chemical, and telecommunications, and has largely focused its operations within the Middle East. It appears the group carries out supply chain attacks, leveraging the trust relationships between organizations to attack their primary targets. FireEye assesses the group on behalf of the Iranian government based on infrastructure details that contain characteristics of hacking tools used in the activity.</td>
</tr>
<tr>
<td>Patchwork</td>
<td>Dropping Elephant, Chinalstrats, MONSOON, Operation Hangover is a cyberespionage group that was first observed in December 2015. While the group has not been definitively attributed, circumstantial evidence suggests the group may be a pro-Indian or Indian entity. Patchwork has been seen targeting industries related to diplomatic and government agencies. Much of the code used by this group was copied and pasted from online forums. Patchwork was also seen operating spearphishing campaigns targeting U.S. think tank groups in March and April of 2018.</td>
</tr>
<tr>
<td>PittyTiger</td>
<td>is a threat group believed to operate out of China that uses multiple different types of malware to maintain command and control.</td>
</tr>
<tr>
<td>PLATINUM</td>
<td>is an activity group that has targeted victims since at least 2009. The group has focused on targets associated with governments and related organizations in South and Southeast Asia.</td>
</tr>
<tr>
<td>Poseidon Group</td>
<td>Poseidon Group is a Portuguese-speaking threat group that has been active since at least 2005. The group has a history of using information exfiltrated from victims to blackmail victim companies into contracting the Poseidon Group as a security firm.</td>
</tr>
<tr>
<td>PROTEUS</td>
<td>is associated with the FilePath Group, which operates in 2013. The group is said to be behind the 2013 “Blackout” malware campaign.</td>
</tr>
</tbody>
</table>
OilRig

OilRig is a suspected Iranian threat group that has targeted Middle Eastern and international victims since at least 2014. The group has targeted a variety of industries, including financial, government, energy, chemical, and telecommunications, and has largely focused its operations within the Middle East. It appears the group carries out supply chain attacks, leveraging the trust relationship between organizations to attack their primary targets. FireEye assesses that the group works on behalf of the Iranian government based on infrastructure details that contain references to Iran, use of Iranian infrastructure, and targeting that aligns with nation-state interests. [1][2][3][4][5][6][7][8][9] This group was previously tracked under two distinct groups, APT34 and OilRig, but was combined due to additional reporting giving higher confidence about the overlap of the activity.

Associated Group Descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IRN2</td>
<td>[1][4]</td>
</tr>
<tr>
<td>HELIX KITTEN</td>
<td>[7][14]</td>
</tr>
<tr>
<td>APT34</td>
<td>This group was previously tracked under two distinct groups, APT34 and OilRig, but was combined due to additional reporting giving higher confidence about the overlap of the activity. [7][14]</td>
</tr>
</tbody>
</table>

Techniques Used

<table>
<thead>
<tr>
<th>Domain</th>
<th>ID</th>
<th>Name</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise</td>
<td>T1087</td>
<td>Account Discovery</td>
<td>OilRig has run net user, net user /domain, net group &quot;domain admin&quot; /domain, and net group &quot;Exchange Trusted Subsystem&quot; /domain to get account listings on a victim. [2]</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1119</td>
<td>Automated Collection</td>
<td>OilRig has used automated collection. [3]</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1110</td>
<td>Brute Force</td>
<td>OilRig has used brute force techniques to obtain credentials. [9]</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1059</td>
<td>Command-Line Interface</td>
<td>OilRig has used the command-line interface for execution. [8][9][10]</td>
</tr>
</tbody>
</table>
OilRig

OilRig is a suspected Iranian threat group that has targeted Middle Eastern and international victims since at least 2014. The group has targeted a variety of industries, including financial, government, energy, chemical, and telecommunications, and has largely focused its operations within the Middle East. It appears the group carries out supply chain attacks, leveraging the trust relationship between organizations to attack their primary targets. FireEye assesses that the group works on behalf of the Iranian government based on infrastructure details that contain references to Iran, use of Iranian infrastructure, and targeting that aligns with nation-state interests. [1][2][3][4][5][6][7][8] This group was previously tracked under two distinct groups, APT34 and OilRig, but was combined due to additional reporting giving higher confidence about the overlap of the activity.

Associated Groups: IRN2, HELIX KITTEN, APT34
Contributors: Robert Falcone, Bryan Lee
Version: 1.1

Techniques Used

<table>
<thead>
<tr>
<th>Domain</th>
<th>ID</th>
<th>Name</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise</td>
<td>T1087</td>
<td>Account Discovery</td>
<td>OilRig has run net user, net user /domain, net group &quot;domain admin&quot; /domain, and net group &quot;Exchange Trusted Subsystem&quot; /domain to get account listings on a victim.[2]</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1119</td>
<td>Automated Collection</td>
<td>OilRig has used automated collection.[3]</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1110</td>
<td>Brute Force</td>
<td>OilRig has used brute force techniques to obtain credentials.[8]</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T0559</td>
<td>Command-Line Interface</td>
<td>OilRig has used the command-line interface for execution.[9][10]</td>
</tr>
<tr>
<td>S0075</td>
<td>Reg</td>
<td>[1][1]</td>
<td>Credentials In Registry, Modify Registry, Query Registry</td>
</tr>
<tr>
<td>-------</td>
<td>-----</td>
<td>--------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>S0258</td>
<td>RGDoor</td>
<td>[1][1]</td>
<td>Command-Line Interface, Data Encrypted, Deobfuscate/Decode Files or Information, Remote File Copy, Standard Application Layer Protocol, System Owner/User Discovery</td>
</tr>
<tr>
<td>S0096</td>
<td>Systeminfo</td>
<td>[6]</td>
<td>System Information Discovery</td>
</tr>
<tr>
<td>S0057</td>
<td>Tasklist</td>
<td>[5][5]</td>
<td>Process Discovery, Security Software Discovery, System Service Discovery</td>
</tr>
</tbody>
</table>

References

<table>
<thead>
<tr>
<th>ID</th>
<th>Technique</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S0075</td>
<td>Reg</td>
<td>Credentials in Registry, Modify Registry, Query Registry</td>
</tr>
<tr>
<td>S0258</td>
<td>RDDoor</td>
<td>Command-Line Interface, Data Encrypted, Deobfuscate/Decode Files or Information, Remote File Copy, Standard Application Layer Protocol, System Owner/User Discovery</td>
</tr>
<tr>
<td>S0185</td>
<td>SEASHARPEE</td>
<td>Command-Line Interface, Remote File Copy, Timestomp, Web Shell</td>
</tr>
<tr>
<td>S0096</td>
<td>SystemInfo</td>
<td>System Information Discovery</td>
</tr>
<tr>
<td>S0057</td>
<td>Tasklist</td>
<td>Process Discovery, Security Software Discovery, System Service Discovery</td>
</tr>
</tbody>
</table>

References

## ATT&CK Matrix for Enterprise

| Initial Access                  | Execution                  | Persistence                  | Privilege Escalation          | Defense Evasion               | Credential Access         | Discovery                        | Lateral Movement               | Collection                  | Command and Control | Exfiltration             | Impact              |
|--------------------------------|----------------------------|------------------------------|-------------------------------|-------------------------------|-----------------------------|----------------------------|-------------------------------|-------------------------------|---------------------------|------------------------|----------------------|---------------------|
| Drive-by Compromise             | AppleScript                | .bash_profile and .bashrc    | Access Token Manipulation     | Access Token Manipulation    | Account Manipulation        | Account Discovery            | Audio Capture                | Commonly Used Port        | Automated Exfiltration  | Data Destruction       |                     |
| Exploit Public-Facing Application | CMSTP                      | Accessibility Features       | Accessibility Features        | BITS Jobs                    | Bash History                | Application Window Discovery | Application Deployment Software | Communication Through Removable Media | Data Compressed          | Data Encrypted for Impact |                     |
| External Remote Services        | Command-Line Interface     | Account Manipulation         | AppCert DLLs                  | Binary Padding               | Brute Force                 | Browser Bookmark Discovery  | Distributed Component Object Model | Clipboard Data             | Connection Proxy         | Data Encrypted        | Defacement           |
| Hardware Additions              | Compiled HTML File          | AppCert DLLs                 | AppInit DLLs                  | Bypass User Account Control  | Credential Dumping          | Domain Trust Discovery      | Exploitation of Remote Services | Data Staged                | Custom Command and Control Protocol | Data Transfer Size Limits | Disk Content Wipe |
| Replication Through Removable Media | Control Panel Items        | AppInit DLLs                 | Application Shimming          | CMSTP                        | Credentials in Files        | File and Directory Discovery | Logon Scripts                | Data from Information Repositories | Custom Cryptographic Protocol | Exfiltration Over Alternative Protocol | Disk Structure Wipe |
| Spearphishing Attachment        | Dynamic Data Exchange      | Application Shimming         | Bypass User Account Control   | Clear Command History        | Credentials in Registry     | Network Service Scanning    | Pass the Hash                | Data from Local System     | Exfiltration Over Command and Control Channel | Endpoint Denial of Service |                     |
OilRig Indicators

Mallory Kraeusen

Today, 9:54 PM
Alice Bluebird

Sent Items

Alice,

Long story but basically I need you to block/action a bunch of OilRig/APT34 references at the bottom of this page that have indicators. Please do 30-day searches and also proactively block. Thanks in advance!

https://attack.mitre.org/groups/G0049/

Regards,
Mallory
“Plz block OilRig indicators.

(TTPs wha?)”
From: Alice Bluebird <Abluebird@froth.ly>
Sent: Wednesday, July 24, 2019 10:34 PM
To: Mallory Kraeusen <mkraeusen@froth.ly>
Subject: Re: OilRig Indicators

Mallory,
Okay, we didn’t have any hits and the indicators are all blocked. But what do we now? That doesn’t seem like it will be good enough for Grace. There are technique thingamabobs on that page too. Maybe we can do something with those?

Alice
Network Defender Extraordinaire
“No hits...but what do we do now? What are these techniques?”
How does Alice stop hoarding indicators and start detecting techniques?
<table>
<thead>
<tr>
<th>T1057</th>
<th>Process Discovery</th>
<th>OilRig has run <code>tasklist</code> on a victim's machine.</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1016</td>
<td>System Network Configuration Discovery</td>
<td>OilRig has run <code>ipconfig /all</code> on a victim.</td>
</tr>
<tr>
<td>T1049</td>
<td>System Network Connections Discovery</td>
<td>OilRig has used <code>netstat -an</code> on a victim to get a listing of network connections.</td>
</tr>
<tr>
<td>T1033</td>
<td>System Owner/User Discovery</td>
<td>OilRig has run <code>whoami</code> on a victim.</td>
</tr>
<tr>
<td>T1007</td>
<td>System Service Discovery</td>
<td>OilRig has used <code>sc query</code> on a victim to gather information about services.</td>
</tr>
</tbody>
</table>
Process Discovery

Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software running on systems within the network.

Windows
An example command that would obtain details on processes is "tasklist" using the Tasklist utility.

Mac and Linux
In Mac and Linux, this is accomplished with the `ps` command.
Process Discovery

Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software running on systems within the network.

Windows

An example command that would obtain process information is the Tasklist utility.

Mac and Linux

In Mac and Linux, this is accomplished with command-line parameters.

Data Sources:
Process monitoring, Process command-line parameters

ID: T1057
Tactic: Discovery
Platform: Linux, macOS, Windows
System Requirements: Administrator, SYSTEM may provide better process ownership details
Permissions Required: User, Administrator, SYSTEM
Data Sources: Process monitoring, Process command-line parameters
CAPEC ID: CAPEC-573
Version: 1.0
Correlation Search

Search Name *: Threat Activity Detected

App *: Enterprise Security

UI Dispatch Context *: Enterprise Security

Set an app to use for links such as the drill-down search in a notable event or links in an email adaptive response action. If None, uses the Application Context.

Description: Creating detection from ATT&CK for T1057 of tasklist.exe

Describes what kind of issues this search is intended to detect.

Mode: Guided, Manual

Search *:

```
index=* (source="*WinEventLog:Security" OR EventCode=4688) Tasklist.exe
```
Creating detection from ATT&CK for T1057 of tasklist.exe

Describes what kind of issues this search is intended to detect.

index="*
(source="*\WinEventLog:Security" OR EventCode=4688) Tasklist.exe
>>> Signature = 0
>>> OilRigTechniques = 41
>>> while Signature < OilRigTechniques:
...    print("Write or find more signatures")
...    Signature += 1
...
We’re good to go against OilRig, our #1 threat!

h/t to Kyle Rainey and Red Canary
How does Kevin test existing detections?
**T1057 - Process Discovery**

**Description from ATT&CK**

Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software running on systems within the network.

**Windows**

An example command that would obtain details on processes is "tasklist" using the Tasklist utility.

**Mac and Linux**

In Mac and Linux, this is accomplished with the **ps** command.

**Atomic Tests**

- **Atomic Test #1 - Process Discovery - ps**

**Atomic Test #1 - Process Discovery - ps**

Utilize ps to identify processes

**Supported Platforms:** macOS, CentOS, Ubuntu, Linux

**Inputs**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>output_file</td>
<td>path of output file</td>
<td>path</td>
<td>/tmp/loot.txt</td>
</tr>
</tbody>
</table>

Run it with **sh**!

```
ps >> #{output_file}
pseudo >> #{output_file}
```
<table>
<thead>
<tr>
<th>Time</th>
<th>Urgency</th>
<th>Security Domain</th>
<th>Title</th>
<th>Status</th>
<th>Risk Score</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>8/4/19 10:22:52.000 PM</td>
<td>Critical</td>
<td>Endpoint</td>
<td>Threat Activity Detected (Tasklist.exe)</td>
<td>New</td>
<td>0</td>
<td>▼</td>
</tr>
<tr>
<td>8/4/19 10:22:43.000 PM</td>
<td>Critical</td>
<td>Endpoint</td>
<td>Threat Activity Detected (Tasklist.exe)</td>
<td>New</td>
<td>0</td>
<td>▼</td>
</tr>
<tr>
<td>8/4/19 10:22:32.000 PM</td>
<td>Critical</td>
<td>Endpoint</td>
<td>Threat Activity Detected (ps)</td>
<td>New</td>
<td>0</td>
<td>▼</td>
</tr>
<tr>
<td>8/4/19 10:22:16.000 PM</td>
<td>Critical</td>
<td>Endpoint</td>
<td>Threat Activity Detected (Tasklist.exe)</td>
<td>New</td>
<td>0</td>
<td>▼</td>
</tr>
<tr>
<td>8/4/19 10:22:05.000 PM</td>
<td>Critical</td>
<td>Endpoint</td>
<td>Threat Activity Detected (Tasklist.exe)</td>
<td>New</td>
<td>0</td>
<td>▼</td>
</tr>
<tr>
<td>8/4/19 10:21:07.000 PM</td>
<td>Critical</td>
<td>Endpoint</td>
<td>Threat Activity Detected (Tasklist.exe)</td>
<td>New</td>
<td>0</td>
<td>▼</td>
</tr>
<tr>
<td>8/4/19 10:22:43.000 PM</td>
<td>Critical</td>
<td>Endpoint</td>
<td>Threat Activity Detected (Tasklist.exe)</td>
<td>New</td>
<td>0</td>
<td>▼</td>
</tr>
<tr>
<td>8/4/19 10:22:32.000 PM</td>
<td>Critical</td>
<td>Endpoint</td>
<td>Threat Activity Detected (ps)</td>
<td>New</td>
<td>0</td>
<td>▼</td>
</tr>
<tr>
<td>8/4/19 10:22:16.000 PM</td>
<td>Critical</td>
<td>Endpoint</td>
<td>Threat Activity Detected (Tasklist.exe)</td>
<td>New</td>
<td>0</td>
<td>▼</td>
</tr>
<tr>
<td>8/4/19 10:22:05.000 PM</td>
<td>Critical</td>
<td>Endpoint</td>
<td>Threat Activity Detected (Tasklist.exe)</td>
<td>New</td>
<td>0</td>
<td>▼</td>
</tr>
<tr>
<td>Time</td>
<td>Urgency</td>
<td>Security Domain</td>
<td>Title</td>
<td>Status</td>
<td>Risk Score</td>
<td>Action</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------</td>
<td>-----------------</td>
<td>------------------------------------------</td>
<td>--------</td>
<td>------------</td>
<td>--------</td>
</tr>
<tr>
<td>8/4/19 10:22:52.000 PM</td>
<td>Critical</td>
<td>Endpoint</td>
<td>Threat Activity Detected (Tasklist.exe)</td>
<td>New</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>8/4/19 10:22:43.000 PM</td>
<td>Critical</td>
<td>Endpoint</td>
<td>Threat Activity Detected (Tasklist.exe)</td>
<td>New</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>8/4/19 10:22:32.000 PM</td>
<td>Critical</td>
<td>Endpoint</td>
<td>Threat Activity Detected (ps)</td>
<td>New</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>8/4/19 10:22:16.000 PM</td>
<td>Critical</td>
<td>Endpoint</td>
<td>Threat Activity Detected (Tasklist.exe)</td>
<td>New</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>8/4/19 10:22:05.000 PM</td>
<td>Critical</td>
<td>Endpoint</td>
<td>Threat Activity Detected (Tasklist.exe)</td>
<td>New</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>8/4/19 10:22:32.000 PM</td>
<td>Critical</td>
<td>Endpoint</td>
<td>Threat Activity Detected (ps)</td>
<td>New</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>8/4/19 10:22:16.000 PM</td>
<td>Critical</td>
<td>Endpoint</td>
<td>Threat Activity Detected (Tasklist.exe)</td>
<td>New</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>8/4/19 10:22:05.000 PM</td>
<td>Critical</td>
<td>Endpoint</td>
<td>Threat Activity Detected (Tasklist.exe)</td>
<td>New</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>8/4/19 10:22:32.000 PM</td>
<td>Critical</td>
<td>Endpoint</td>
<td>Threat Activity Detected (ps)</td>
<td>New</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
We did all the things. This is fine. Everything is fine.
And then...
“Sorry, you’re pwned.”
BREAKING NEWS
FROTHLY HACKED BY TAEDONGGANG

1:12
DATA STOLEN! INSIDER THREAT? WILL THIS AFFECT THEIR IPO? WAS BOTS FOR NAUGHT...
WHY DID WE EVER USE ATTACK?
So you’ve “implemented” ATT&CK and you’re unhappy...now what?
What went wrong?
<table>
<thead>
<tr>
<th>CxO</th>
<th>CTI</th>
<th>Defender</th>
<th>Red Team</th>
</tr>
</thead>
<tbody>
<tr>
<td>Didn't test in depth or work with Blue Team</td>
<td>Couldn't follow up and action new threats</td>
<td>Had gaps in defenses but drowning in alerts</td>
<td>Had a false sense of security</td>
</tr>
</tbody>
</table>
Let’s get Frothly back on track
How can a CxO have a better understanding of their risk by using ATT&CK?
Communicate confidence level
<table>
<thead>
<tr>
<th>Color gradient by confidence in detections</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Color Gradient" /></td>
</tr>
</tbody>
</table>

h/t to Olaf Hartong
Integrate your teams
### MITRE ATT&CK Matrix

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution</th>
<th>Persistence</th>
<th>Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Discovery</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Exfiltration</th>
<th>Command and Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drive-by Compromise</td>
<td>AppleScript</td>
<td>.bash_profile and .bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>AppleScript</td>
<td>Audio Capture</td>
<td>Automated Exfiltration</td>
<td>Commonly Used Port</td>
</tr>
<tr>
<td>Exploit Public-Facing Application</td>
<td>CMSTP</td>
<td>Accessibility Features</td>
<td>Accessibility Features</td>
<td>BITS Jobs</td>
<td>Bash History</td>
<td>Application Window Discovery</td>
<td>Application Deployment Software</td>
<td>Data Compressed</td>
<td>Communication Through Removable Media</td>
<td></td>
</tr>
<tr>
<td>External Remote Services</td>
<td>Command-Line Interface</td>
<td>Account Manipulation</td>
<td>AppCert DLLs</td>
<td>Binary Padding</td>
<td>Brute Force</td>
<td>Browser Bookmark Discovery</td>
<td>Distributed Component Object Model</td>
<td>Data Staged</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>Hardware Additions</td>
<td>Compiled HTML File</td>
<td>AppInit DLLs</td>
<td>Application Shimming</td>
<td>CMSTP</td>
<td>Logon Scripts</td>
<td>Domain Trust Discovery</td>
<td>Exploitation of Remote Services</td>
<td>Data Encrypted</td>
<td>Custom Command and Protocol</td>
<td></td>
</tr>
<tr>
<td>Replication Through Removable Media</td>
<td>Control Panel Items</td>
<td>AppInit DLLs</td>
<td>Bypass User Account Control</td>
<td>Clear Command History</td>
<td>Exfiltration Over Alternative Protocol</td>
<td>Data from Information Repositories</td>
<td>Data Transfer</td>
<td>Data Over Command and Control Channel</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spearphishing Attachment</td>
<td>Dynamic Data Exchange</td>
<td>Application Shimming</td>
<td>DLL Search Order Hijacking</td>
<td>Code Signing</td>
<td>Exploitation for Credential Access</td>
<td>Network Share Discovery</td>
<td>Exfiltration Over Other Network Medium</td>
<td>Data Encoding</td>
<td>Data Over Obfuscation</td>
<td></td>
</tr>
<tr>
<td>Spearphishing Link</td>
<td>Execution through API</td>
<td>Authentication Package</td>
<td>DLL Search Order Hijacking</td>
<td>Exploitation for Credential Access</td>
<td>Network Share Discovery</td>
<td>Network Sniffing</td>
<td>Exfiltration Over Physical Medium</td>
<td>Email Collection</td>
<td>Remote File</td>
<td></td>
</tr>
<tr>
<td>Spearphishing via Service</td>
<td>Execution through Module Load</td>
<td>Bits Jobs</td>
<td>Dylib Hijacking</td>
<td>Compile After Delivery</td>
<td>Forced Authentication</td>
<td>Pass the Ticket</td>
<td>Data from Removable Media</td>
<td>Scheduled Transfer</td>
<td>Remote Desktop Protocol</td>
<td></td>
</tr>
<tr>
<td>Supply Chain Compromise</td>
<td>Exploitation for Client Exploitation</td>
<td>Compiled HTML File</td>
<td>Hooking</td>
<td>Password Policy Discovery</td>
<td>Exploitation for Credential Access</td>
<td>Network Share Discovery</td>
<td>Data from Network Medium</td>
<td>Domain Fronting</td>
<td>Domains Connection</td>
<td></td>
</tr>
</tbody>
</table>

**Active:** 1  
**Available:** 15  
**Needs data:** 1  
**Total:** 17  
**Selected:** 0  

**Threat Groups:** OilRig
How can a threat intel analyst action new threats?
Build your own threat library
Karkoff is a lightweight backdoor used by the DNSpionage group. According to SecureList researchers, its developers didn't obfuscate or include any defense measures to avoid the malware to be disassembled. The malware will persist as a service with the name "MSExchangeClient", mimicking a Microsoft legitimate tool.

<table>
<thead>
<tr>
<th>Campaign</th>
<th>Techniques</th>
<th>Tactics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNSpionage Upgraded</td>
<td>DTTT0008 - Environment Awareness</td>
<td>Defense Evasion</td>
<td>Karkoff uses the information collected from the local system in order to fingerprint the victims and avoid researchers or sandboxes.</td>
</tr>
<tr>
<td>Their Tool into Karkoff</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNSpionage Upgraded</td>
<td>DTTT0024 - File Management</td>
<td>Collection</td>
<td>Karkoff logs the executed command in a log file.</td>
</tr>
<tr>
<td>Their Tool into Karkoff</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNSpionage Upgraded</td>
<td>T1001 - Data Obfuscation</td>
<td>Command and Control</td>
<td>Karkoff uses base64 encoding to initially obfuscate C2 communications.</td>
</tr>
<tr>
<td>Their Tool into Karkoff</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNSpionage Upgraded</td>
<td>T1005 - Data from Local System</td>
<td>Collection</td>
<td>Karkoff collects data from the local system.</td>
</tr>
<tr>
<td>Their Tool into Karkoff</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Most Used Techniques (2019 sample)

<table>
<thead>
<tr>
<th>#</th>
<th>Technique Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>T1071 - Standard App Layer Protocol</td>
</tr>
<tr>
<td>2</td>
<td>T1082 - System Information Discovery</td>
</tr>
<tr>
<td>3</td>
<td>T1059 - Command-Line Interface</td>
</tr>
<tr>
<td>4</td>
<td>T1105 - Remote File Copy</td>
</tr>
<tr>
<td>5</td>
<td>T1083 - File and Directory Discovery</td>
</tr>
<tr>
<td>6</td>
<td>T1060 - Registry Run Keys / Start Folder</td>
</tr>
<tr>
<td>7</td>
<td>T1057 - Process Discovery</td>
</tr>
<tr>
<td>8</td>
<td>T1056 - Input Capture</td>
</tr>
<tr>
<td>9</td>
<td>T1113 - Screen Capture</td>
</tr>
<tr>
<td>10</td>
<td>T1107 - File Deletion</td>
</tr>
<tr>
<td>11</td>
<td>T1041 - Exfiltration Over C2 Channel</td>
</tr>
<tr>
<td>12</td>
<td>T1086 - PowerShell</td>
</tr>
<tr>
<td>13</td>
<td>T1193 - Spearphishing Attachment</td>
</tr>
<tr>
<td>14</td>
<td>T1016 - System Network Config Discovery</td>
</tr>
</tbody>
</table>
How can a **blue** teamer know what to detect and if she has the right data?
Map data to TTPs
Process Discovery

Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software running on systems within the network.

Windows
An example command that would obtain information about processes is the Tasklist utility.

Mac and Linux
In Mac and Linux, this is accomplished with similar commands and utilities.

Data Sources:
- Process monitoring
- Process command-line parameters
## scripts

This folder contains one-off scripts for working with ATT&CK content. These scripts are included either because they provide useful functionality or as demonstrations of how to fetch, parse or visualize ATT&CK content.

<table>
<thead>
<tr>
<th>script</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>techniques_from_data_source.py</td>
<td>Fetches the current ATT&amp;CK STIX 2.0 objects from the ATT&amp;CK TAXII server, prints all of the data sources listed in Enterprise ATT&amp;CK, and then lists all the Enterprise techniques containing a given data source. Run <code>python3 techniques_from_data_source.py -h</code> for usage instructions.</td>
</tr>
<tr>
<td>techniques_data_sources_vis.py</td>
<td>Generate the csv data used to create the &quot;Techniques Mapped to Data Sources&quot; visualization in the ATT&amp;CK roadmap. Run <code>python3 techniques_data_sources_vis.py -h</code> for usage instructions.</td>
</tr>
</tbody>
</table>

[https://github.com/mitre-attack/attack-scripts/tree/master/scripts](https://github.com/mitre-attack/attack-scripts/tree/master/scripts)
One Sig!=Complete TTP Coverage
Welcome to the Cyber Analytics Repository

The MITRE Cyber Analytics Repository (CAR) is a knowledge base of analytics developed by MITRE based on the MITRE ATT&CK adversary model.

If you want to start exploring, try viewing the Full Analytic List or use the CAR Exploration Tool (CARET). Also, check out the new ATT&CK Navigator Layer that captures the current set of ATT&CK tactics and techniques covered by CAR.

Analytics stored in CAR contain the following information:

- a hypothesis which explains the idea behind the analytic
- the information domain or the primary domain the analytic is designed to operate within (e.g. host, network, process, external)
- references to ATT&CK Techniques and Tactics that the analytic detects
- the Glossary
- a pseudocode description of how the analytic might be implemented
- a unit test which can be run to trigger the analytic

In addition to the analytics, CAR also contains a data model for observable data used to run the analytics and sensors that are used to collect that data.

https://car.mitre.org/
Description
This search will return a table of rare processes, the names of the systems running them, and the users who initiated each process.

Explain It Like I'm 5
This search first executes the subsearch and counts all of your processes to determine the 10 most rare (the limit set is 10). It then filters out whitelisted processes and outputs the first and last time a rare process was encountered, the destination where the process is running, the count of occurrences, and the users who initiated the processes.

Search
```
tstats `summariesonly` count values(Processes.dest) as dest values(Processes.user) as user min(_time) as firstTime max(_time) as lastTime from datamodel=Endpoint.Processes by Processes.process_name | rename Processes.process_name as process | rex field=user "(?<user_domain>.*)(?<<user_name>.*).*)" | `ctime(firstTime)` | `ctime(lastTime)` | search tstats count from datamodel=Endpoint.Processes by Processes.process_name | rare Processes.process_name limit=30 | rename Processes.process_name as process | `filter_rare_process_whitelist` | table process
```
Reduced Alerts

Incident Review

Urgency
- CRITICAL: 0
- HIGH: 0
- MEDIUM: 1
- LOW: 0
- INFO: 0

Status
- All

Correlation Search Name
- Select...

Owner
- All

Security Domain
- All

Tag
- Select...

Submit

Search

Format Timeline
- Zoom Out

1 event (8/3/19 10:00:00.000 PM to 8/4/19 10:37:29.000 PM)

Job

1 hour per column

8/4/19 8:05:47:000 AM
Access
- Brute Force Access Behavior Detected From 10.255.3.2
- Urgency: Medium
- Status: New
- Owner: unassigned

No investigation is currently loaded. Please create ▼ or load an existing one ▬.
How can a red teamer help improve defenses?
Small and highly portable detection tests based on MITRE's ATT&CK.

mitre  mitre-attack

1,241 commits  10 branches  0 releases  44 contributors

Branch: master  New pull request

CaseySmitc and MHAgs Fix t1138path (#513)

.circlici Only commit docs for non-PR branches because permissions.
github Create issue and pull request templates.
ARTifacts Chain Reaction - Qbot Infection (#508)
atomic_red_team Update ATT&CK icon for technique creation (#488)

Clone with HTTPS

https://github.com/redcanaryco/atomic

T1057-F.md  T1057.md  T1057.yml

/Users/jacob/Documents/Frothly_Atomics/atomics/T1057
notyobox:T1057  jacob $ ls
T1057-F.md  T1057.md  T1057.yml
<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution</th>
<th>Persistence</th>
<th>Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Discovery</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Command and Control</th>
<th>Exfiltration</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>AppLocker</td>
<td>local</td>
<td>User Interaction</td>
<td>Mimikatz</td>
<td>Domain Administrator</td>
<td>SMB Relay</td>
<td>Web Shell</td>
<td>Hybrid Agent</td>
<td>Silvermond DGA</td>
<td>Phishing</td>
<td>Evasion</td>
</tr>
<tr>
<td>Remote</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Go purple!**

**What blue detected**

**What red did that blue missed**
How do you (and Frothly) “Play at Home” with ATT&CK?
“How are we defended?”

“I can communicate about our defenses and make better decisions.”
“I’m tracking multiple threats and I’m a Pyramid of Pain master.”

“If it’s not an IP, how do I use it?”
“I’m drowning in alerts and missing data!”

“\textbf{I can prioritize} alerts and \textbf{use} the data I have.”
“I don’t know how to help!”

“...I know how to help defense get better.”
Takeaways

♟ ATT&CK is for everyone
♟ Start small and be realistic
♟ Collaborate and cooperate
Thank you!

♟ Blake Strom, Adam Pennington, and the whole MITRE ATT&CK Team
♟ Marty Pugliese
♟ Olaf Hartong
♟ Deloitte
♟ David Bianco
♟ Kyle Rainey and Red Canary
♟ David Veuve, Johan Bjerke, John Stoner, Dave Herrald
♟ Women’s Society of Cyberjutsu
References

https://github.com/mitre-attack/attack-navigator
https://github.com/redcanaryco/atomic-red-team
https://redcanary.com/blog/avoiding-common-attack-pitfalls/
https://splunkbase.splunk.com/app/3435
https://github.com/mitre-attack/attack-scripts/tree/master/scripts
https://nsacyber.github.io/unfetter/
https://github.com/rabobank-cdc/DeTTECT
https://github.com/krakow2600/atomic-threat-coverage
https://car.mitre.org/
https://github.com/Neo23x0/sigma/tree/master/rules
https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html
Thank you!

Katie Nickels
MITRE
@LiketheCoins

Ryan Kovar
Splunk
@meansec