SESSION ID: AIR-R02

MITRE ATT&CK - THE SEQUEL

Freddy Dezeure
CEO
Freddy Dezeure BV
@Fdezeure
www.freddydezeure.eu

Rich Struse
Director, Center for Threat-Informed Defense
MITRE Engenuity
@MITREattack
attack.mitre.org
The Sequel

- Presentation builds on our RSA2019 MITRE ATT&CK presentation
- Our goal is to provide real hands-on guidance
- Everything was built in cooperation with Munich Airport
Agenda

- Identify
- Protect
- Detect
- Update
- Share
Our Enterprise Is A Financial Service

- We process money for our clients
- Our main risks:
  - Financial loss
  - Business continuity
  - Brand damage
  - GDPR
- Our infrastructure is well protected (we think)
- We want to perform threat-informed defense
Our Infrastructure

“Win10”  “Win11”

Data Centre
Our Infrastructure

- Created in Detection Lab
  - Installed from GitHub
  - + One additional host
  - + Squid proxy
  - + Caldera

- We populated the logfiles by normal user behavior

- We executed our scenario and made screenshots
Identify

Our Assets, Our Infrastructure, Our Main Adversaries And Their TTPs
Identify **Our** Adversaries’ Objectives And Behavior

- Identify **our** Adversaries of interest
  - Open source and commercial threat intelligence
  - ISACs/ISAOs
  - NCICC/CERTs

- Identify which tactics/techniques they use
  - ATT&CK Navigator
Our Adversaries

Motives
Targets

Our Assets

Our Systems
Our Main Adversaries

- Cross-sector: targeted ransomware
  - Emotet
  - followed by Trickbot
  - Followed by Ryuk/LockerGoga...

- Sectoral: Fin7, Cobalt Group
Emotet

Emotet is a modular malware variant which is primarily used as a downloader for other malware variants such as TrickBot and IcedID. Emotet first emerged in June 2014 and has been primarily used to target the banking sector. [1]

Associated Software Descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Geodo</td>
<td>[7]</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>T110</td>
<td>Brute Force</td>
<td>Emotet has been observed using a hard coded list of passwords to brute force user accounts. [8]</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1059</td>
<td>Command-Line Interface</td>
<td>Emotet has used cmd.exe to run a PowerShell script. [9]</td>
</tr>
</tbody>
</table>
FIN7

FIN7 is a financially-motivated threat group that has primarily targeted the U.S. retail, restaurant, and hospitality sectors since mid-2015. They often use point-of-sale malware. A portion of FIN7 was run out of a front company called Combi Security. FIN7 is sometimes referred to as Carbanak Group, but these appear to be two groups using the same Carbanak malware and are therefore tracked separately.

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>T1138</td>
<td>Application Shimming</td>
<td>FIN7 has used application shim databases for persistence.</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1116</td>
<td>Code Signing</td>
<td>FIN7 has signed Carbanak payloads with legally purchased code signing certificates. FIN7 has also digitally signed their phishing documents, backdoors and other staging tools to bypass security controls.</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1059</td>
<td>Command-Line Interface</td>
<td>FIN7 used cmd.exe to launch commands on the victim's machine.</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1043</td>
<td>Commonly Used Port</td>
<td>FIN7 has used ports 53, 80, 443, and 8080 for C2.</td>
</tr>
</tbody>
</table>
Cobalt Group

Cobalt Group is a financially motivated threat group that has primarily targeted financial institutions. The group has conducted intrusions to steal money via targeting ATM systems, card processing, payment systems and SWIFT systems. Cobalt Group has mainly targeted banks in Eastern Europe, Central Asia, and Southeast Asia. One of the alleged leaders was arrested in Spain in early 2018, but the group still appears to be active. The group has been known to target organizations in order to use their access to then compromise additional victims. [1] [2] [3] [4] [6] [7] Reporting indicates there may be links between Cobalt Group and both the malware Carbanak and the group Carbanak. [8]

Associated Group Descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cobalt Gang</td>
<td>[1] [2][9]</td>
</tr>
<tr>
<td>Cobalt Spider</td>
<td>[12]</td>
</tr>
</tbody>
</table>

Techniques Used
We Built And Used A Realistic Exploit

- Word lure document with PowerShell macro connecting to api.ipify.org to grab external ip of our infrastructure and visualize it
Protect

Design And Validate Our Critical Controls
Design Our Controls

- Adversaries
  - Spear Phishing
  - PowerShell
- Assets
- Security Controls
# Mitigations For T1086 PowerShell

<table>
<thead>
<tr>
<th>Mitigation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code Signing</td>
<td>Set PowerShell execution policy to execute only signed scripts.</td>
</tr>
<tr>
<td>Disable or Remove Feature or Program</td>
<td>It may be possible to remove PowerShell from systems when not needed, but a review should be performed to assess the impact to an environment, since it could be in use for many legitimate purposes and administrative functions. Disable/restrict the WinRM Service to help prevent uses of PowerShell for remote execution.</td>
</tr>
<tr>
<td>Privileged Account Management</td>
<td>When PowerShell is necessary, restrict PowerShell execution policy to administrators. Be aware that there are methods of bypassing the PowerShell execution policy, depending on environment configuration.</td>
</tr>
</tbody>
</table>
Mitigation Guidance From The Community

CERT-EU Security Advisory 2019-021

Detecting and Preventing Emotet 2019 Campaign

September 30, 2019 — v1.0

CERT-EU Security Whitepaper 2019-001

PowerShell – Cybersecurity Perspective

PREVENT Legitimate Windows Executables To Be Used To Gain Initial Foothold In Your Infrastructure

Dimitris Margaritis Follow
Nov 24 · 4 min read
Implemented In Our Enterprise Environment

Without FW policy

“Win10”

“Win11”

With FW policy

Data Centre
Validate **Our** Controls In Our Lab

- Adversaries
- Spear Phishing PowerShell
- Security Controls
- Assets
Screenshot of the lure document
Result Of The Execution Of The Macro

Accept the following content:

You can use Microsoft Word until Friday, September 20, 2019.
After that date, most features of Microsoft Word will be disabled.

To accept and start Word, click Enable Editing and click Enable Content.
Visibility In Our Environment

- Screenshot in Splunk logs (Sysmon and proxy)

“Win10” (without FW rule)
Test Our Controls

Adversaries

Assets

Spear Phishing
PowerShell

Security Controls
Automated adversary emulation
- Safely replicate realistic adversary behavior
- Repeatable testing and verification of prevention/detection

Features
- Uses ATT&CK to create Adversary profiles
- Uses AI and modeling to make decisions about actions
- Self-cleans after operation completes
- Low install overhead
- Does not require extensive red team knowledge to operate
# Outcome Of Caldera With T1086 In Our Infrastructure

<table>
<thead>
<tr>
<th>Name</th>
<th>Adversary</th>
<th>Group</th>
<th>Steps</th>
<th>Planner</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Powershell Execution</strong></td>
<td><strong>Powershell Execution</strong></td>
<td><strong>my_group</strong></td>
<td><strong>14</strong></td>
<td><strong>Powershell Execution collected 6 tactics and used them to make decisions</strong></td>
</tr>
</tbody>
</table>

The operation lasted (not finished yet) with a random 4/8 second pause between steps.

<table>
<thead>
<tr>
<th>Att&amp;ck</th>
<th>Worked / Failed</th>
<th>Tactic</th>
<th>Technique ID</th>
<th>Technique name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>4 / 0</td>
<td>collection</td>
<td>T1086</td>
<td>PowerShell</td>
</tr>
<tr>
<td></td>
<td>5 / 3</td>
<td>execution</td>
<td>T1086</td>
<td>PowerShell</td>
</tr>
<tr>
<td></td>
<td>2 / 0</td>
<td>defense-evasion</td>
<td>T1086</td>
<td>PowerShell</td>
</tr>
</tbody>
</table>
Outcome On “Win11” (Protected With FW Policy)
Detect

Design And Validate Our Analytics
Design Our Detection

- Gain Visibility
  - Priorities in log collection

- Design Analytics
  - Write them with knowledge of Our Adversaries
  - Get them from the community

- Deploy
  - Detect / Hunt / Refine
SIGMA: A Language for Analytics

Sigma Format
Generic Signature Description

Sigma Converter
Applies Predefined and Custom Field Mapping

Elastic Search Queries
Splunk Searches
...

https://github.com/Neo23x0/sigma
SIGMA Community Rules Repository

Branch: master  sigma / rules / windows / powershell /

- powershell_data_compressed.yml Added UUIDs to rules  16 days ago
- powershell_downgrade_attack.yml Added UUIDs to rules  16 days ago
- powershell_exe_calling_ps.yml Added UUIDs to rules  16 days ago
- powershell_malicious_commandlets.yml Added UUIDs to rules  16 days ago
- powershell_malicious_keywords.yml Added UUIDs to rules  16 days ago
- powershell_ntfs_ads_access.yml Added UUIDs to rules  16 days ago
- powershell_prompt_credentials.yml Added UUIDs to rules  16 days ago
- powershell_psattack.yml Added UUIDs to rules  16 days ago
- powershell_shellcode_b64.yml Added UUIDs to rules  16 days ago
- powershell_suspicious_download.yml Added UUIDs to rules  16 days ago
- powershell_suspicious_invocation_generic.yml Added UUIDs to rules  16 days ago
- powershell_suspicious_invocation_specific.yml Added UUIDs to rules  16 days ago
- powershell_suspicious_keywords.yml Added UUIDs to rules  16 days ago
- powershell_winlogon_helper_dll.yml Added UUIDs to rules  16 days ago

Latest commit 0592cbb 16 days ago
Detecting Windows command line executable spawned from Microsoft Office
Detection With SIGMA Rules

- Splunk alerts detecting PowerShell spawned from Word
Detection With SIGMA Rules (2)

- Splunk alert detecting PowerShell communicating outside

Alert on “Win10” (without FW rule)
Detection With SIGMA Rules – Building Alerts (3)

- Splunk alerts built with identified SIGMA rules

<table>
<thead>
<tr>
<th>Time</th>
<th>Fixed alerts</th>
<th>App</th>
<th>Type</th>
<th>Severity</th>
<th>Media</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019-12-18 14:42:06 UTC</td>
<td>sysmon_powershell_network_connection</td>
<td>search</td>
<td>Real-time</td>
<td>Critical</td>
<td>Per Result</td>
<td>💡 View results</td>
</tr>
<tr>
<td>2019-12-18 14:41:34 UTC</td>
<td>win_office.shell</td>
<td>search</td>
<td>Real-time</td>
<td>Medium</td>
<td>Per Result</td>
<td>💡 View results</td>
</tr>
<tr>
<td>2019-12-18 14:41:29 UTC</td>
<td>win_office.shell</td>
<td>search</td>
<td>Real-time</td>
<td>Medium</td>
<td>Per Result</td>
<td>💡 View results</td>
</tr>
</tbody>
</table>

Critical alert on “Win10” (without FW rule)
## Alerts Triggered By Running Caldera With T1086

<table>
<thead>
<tr>
<th>Time</th>
<th>Fired alerts</th>
<th>App</th>
<th>Type</th>
<th>Severity</th>
<th>Mode</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019-12-20 13:19:50 UTC</td>
<td>sysmon_powershell_network_connection</td>
<td>search</td>
<td>Real-time</td>
<td>Critical</td>
<td>Per Result</td>
<td>View results</td>
</tr>
<tr>
<td>2019-12-20 13:19:41 UTC</td>
<td>sysmon_powershell_network_connection</td>
<td>search</td>
<td>Real-time</td>
<td>Critical</td>
<td>Per Result</td>
<td>View results</td>
</tr>
<tr>
<td>2019-12-20 13:19:40 UTC</td>
<td>sysmon_powershell_network_connection</td>
<td>search</td>
<td>Real-time</td>
<td>Critical</td>
<td>Per Result</td>
<td>View results</td>
</tr>
<tr>
<td>2019-12-20 13:19:39 UTC</td>
<td>sysmon_powershell_network_connection</td>
<td>search</td>
<td>Real-time</td>
<td>Critical</td>
<td>Per Result</td>
<td>View results</td>
</tr>
</tbody>
</table>

All alerts are on “Win10” (without FW rule)
Update on ATT&CK Developments

- ATT&CK for ICS, Cloud and more
- Subtechniques
- Threat Report ATT&CK Mapper (TRAM)
- MITRE ENGENUITY
Share

Contribute To The Community
Share Insights And Contribute

- The MITRE ATT&CK community is very active
- Sharing TTPs/SIGMA rules is easier and more useful than IOCs
  - Contribute to MITRE ATT&CK attack@mitre.org
  - Contribute to SIGMA https://github.com/Neo23x0/sigma/tree/master/rules
- Participate in the Community
  - MITRE ATT&CKcon
  - EU ATT&CK User Community
EU ATT&CK User Community

- Mailing list: opt in? -> email to info@circl.lu
- Next workshop in Brussels 18-19 May 2020
- The biggest ATT&CK event ever...

Workshop - EU ATT&CK Community

Next workshop - event for EU ATT&CK Community
“Apply” Slide

- Next week you should:
  - Consider Windows Firewall policy to mitigate PowerShell techniques

- In the first three months following this presentation you should:
  - Identify Your Adversaries
  - Identify and deploy at least three use cases in your organization

- Within six months you should:
  - Permeate your cyber defense using ATT&CK
  - Share your insights in the SIGMA community
Resources And Acknowledgements

- ATT&CK repository and ATT&CK Navigator
- How to use the MITRE ATT&CK Navigator
- PREVENT Legitimate Windows Executables To Be Used To Gain Initial Foothold In Your Infrastructure (@dmargaritis)
- SIGMA and SIGMA rule collection (Thomas Patzke, Florian Roth)
- CALDERA
- EU ATT&CK Community Workshop 18-19 May 2020
- Munich Airport Information Security Hub
- Center for Threat-Informed Defense
- Detection Lab