Table of Contents

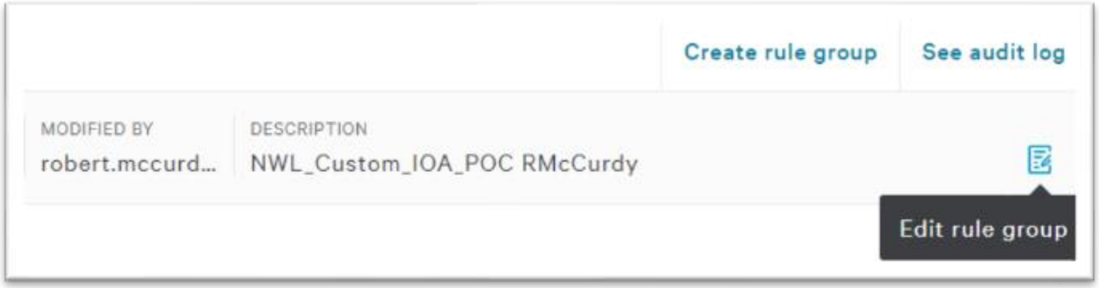
CS Custom IOA and ES

This section covers adding new Indicators of Attack (IOA) to CrowdStrike (CS) and Splunk Enterprise Security (ES)

Adding TTP to CS IOA

This section covers adding new TTPs to CS IOA. Take the defaults for all items where not specified in this document

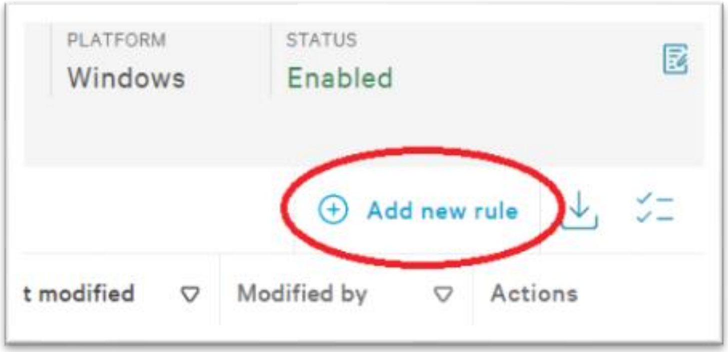
- Click EDIT on the desired ‘RULE GROUP NAME’ or create a new one : https://falcon.crowdstrike.com/configuration/custom-ioa-groups



MODIFIED BY robert.mccurd...

DESCRIPTION NWL_Custom_IOA_POC RMcCurdy

- Click ‘Add new rule’



PLATFORM Windows

STATUS Enabled

Rule Type

This section covers rule actions. This is what happens when I rule hits. Detect should be used for all new rules to allow for rule to be in place for N days before set to block. This can be escalated to tier 2 for review if block is need immediate.

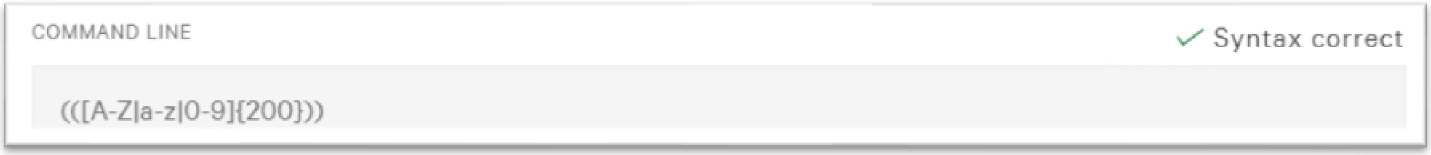
Process Creation

This rule type is designed to kill processes before they are executed. This should only be used when limiting rule to only processes. File Creation should be used normally as it covers not just execution but creation. See File Creation rule type below.

The ProcessRollup2 (PR2) event for certain processes now has a best-effort field called CreateProcessType added to it. This field can identify native process creation directly done through Ntdll.dll (such as NtCreateProcess), Win32 process creation through Kernel32.dll or Kernelbase.dll (such as CreateProcess), Shell process creation (ShellExecute), and CRT-based process creation (system).

File Creation

This rule type should normally be used for Regex Command Line. CS does not currently support \b and some other limitations.



COMMAND LINE

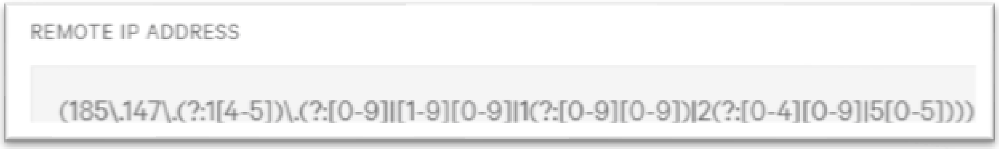
✓ Syntax correct

```
(([A-Z|a-z|0-9]{200}))
```

Network Connection

This rule type should contain regex with IP addresses or ranges.

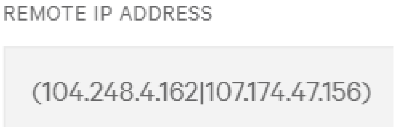
Regex Range:



REMOTE IP ADDRESS

```
(185\.147\.(?:1[4-5])\.(?:[0-9]|[1-9][0-9]|1(?:[0-9][0-9])|2(?:[0-4][0-9]|5[0-5])))
```

Regex List separated by pipe ‘|’ :

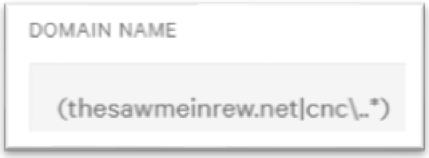


REMOTE IP ADDRESS

```
(104.248.4.162|107.174.47.156)
```

Domain

Regex/List separated by pipe ‘|’ Notice the . Is escaped. Otherwise anything starting with cnc would be blocked and not cnc. ‘.’ Matches any character except linebreaks. Equivalent to [^\n\r]. :

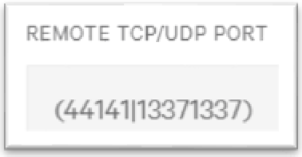


DOMAIN NAME

```
(thesawmeinrew.net|cnc\..*)
```

Remote TCP/UDP port

Normally obscure ports used by Command and Control processes (CnC).



REMOTE TCP/UDP PORT

(44141|13371337)

Action

This section covers rule actions. This is what happens when I rule hits.

Detect should be used for all new rules to allow for rule to be in place for N days before set to block. This can be escalated to tier 2 for review if block is need immediate

Severity

This section covers CS severity settings

Informational:

Not for malware of PUP. Reserved for tracking of events for reporting or used for correlation searches in ES. Where no analyst is required

Low:

Not for malware but Include PUP or Potentially Unwanted Programs not tracked by CS VNC Dropbox etc

Medium:

Include Command line-based attacks like LOL-bins (live off the land binaries) that should require SOC analyst to validate

High:

Include network-based rules IP or Domains. These should require SOC analyst to validate

Critical:

Only true positives that would go to SOC as active attacks. This does not include network only or Domain based rules

Rule Name

CS Rule Format: *(SOURCE COMPANY)_(ACTOR)_(MALWARE FAMILY)_(YYMMDD DISCLOSED)_(RULE OR PARTIAL RULE SYNTAX)*

Mcafee_Maze_Ransomeware_200326_185.147.14.0/23

Internal_Maze_Ransomeware_200526_199.

Rule description

Rule description should reference ticket number and Standard Change items.

Adding TTP to Splunk ES

These can be in the form of IP or Domain

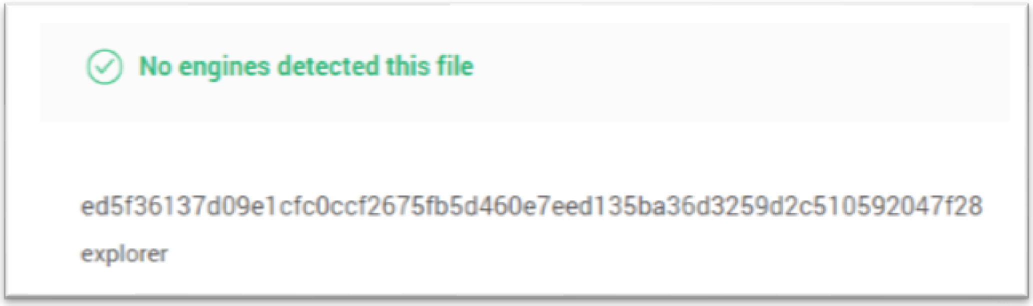
- Send IPs or domains list to ES SME to be added to "CS TTP" Alert
- Future state: Allow tier 1 to add new IPs or Domains to ES

Vetting

The vetting process helps ensure IOAs don't affect normal or legitimate businesses processes or block any required processes/connections

- Review any Hashes/IPs/Domains in VT before adding them

ieplorer.exe https://www.virustotal.com/gui/file/ed5f36137d09e1cfc0ccf2675fb5d460e7eed135ba36d3259d2c510592047f28/detection



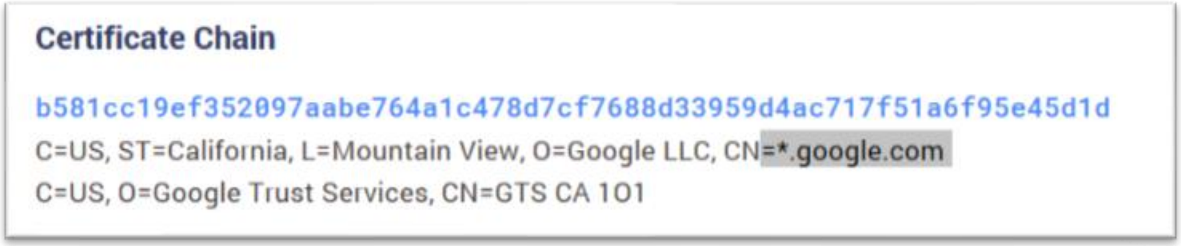
✓ No engines detected this file

ed5f36137d09e1cfc0ccf2675fb5d460e7eed135ba36d3259d2c510592047f28

explorer

- Review any Hashes/IPs/Domains in censys.io before adding them

https://censys.io/ipv4/**172.217.5.110** Review certificate and whois tab



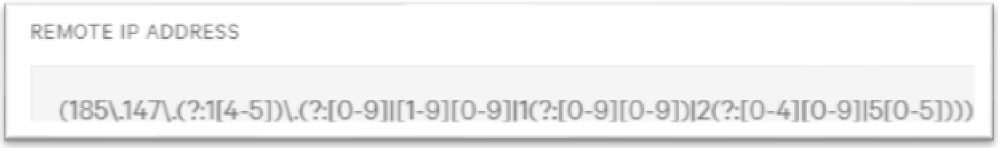
Certificate Chain

b581cc19ef352097aabe764a1c478d7cf7688d33959d4ac717f51a6f95e45d1d
C=US, ST=California, L=Mountain View, O=Google LLC, CN=*.google.com
C=US, O=Google Trust Services, CN=GTS CA 1O1

- If the TTP is a network range use https://d-fault.nl/CIDRtoRegEx to convert network range to regex.

    Be sure NOT to include the ^ and $ at the beginning and end of the regex. Zero-width assertions (\b, $, ^) not yet implemented

    - 185.147.14.0/23 becomes (185\.147\.(?:1[4-5])\.(?:[0-9]|[1-9][0-9]|1(?:[0-9][0-9])|2(?:[0-4][0-9]|5[0-5])))



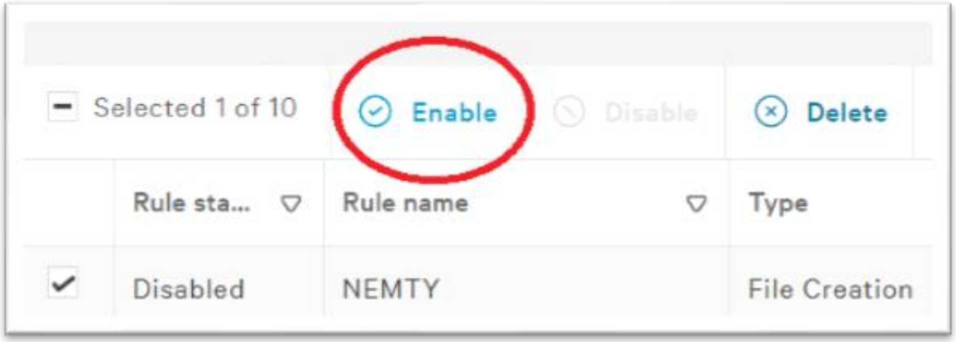
REMOTE IP ADDRESS

(185\.147\.(?:1[4-5])\.(?:[0-9]|[1-9][0-9]|1(?:[0-9][0-9])|2(?:[0-4][0-9]|5[0-5])))

Enabling New Rule / Set review Date

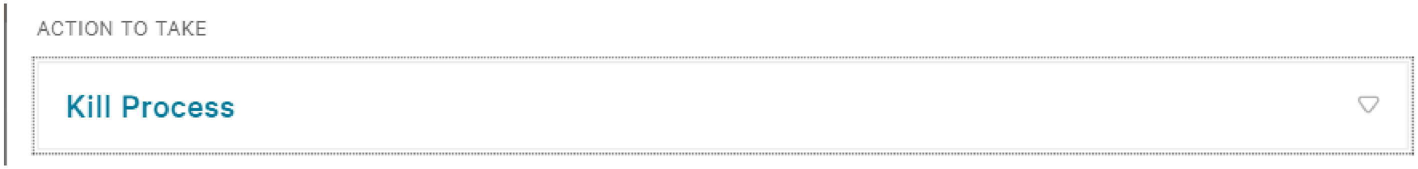
After a new rule is created and vetted it needs to be enabled. Analyst is responsible for setting it to Enable and setting review date N days after to set to the rule to block and ticket updated.

Enable Rule:



	Rule sta...	Rule name	Type
✓	Disabled	NEMTY	File Creation

Enable Block Rule:



ACTION TO TAKE

Kill Process

Standard Change

This is placeholder for requirements for Standard Change or ticket system. Each ticket can contain multiple TTP types.

- Date Disclosed: The Earliest Date the TTP was posted not when we received it
- Date Added: The date we added the new rule
- Source: Where did it come from (company/group /URL)
  - Mcafee_https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ransomware-maze/
  - VendorName_Internal_Use_Only
- Rule: What the rule or rules are
  - IP: 10.0.0.0/16
  - IP RANGE: (10\.0\.(?:[0-9]|[1-9][0-9]|1(?:[0-9][0-9])|2(?:[0-4][0-9]|5[0-5]))\.(?:[0-9]|[1-9][0-9]|1(?:[0-9][0-9])|2(?:[0-4][0-9]|5[0-5]))

Rule Maintenance

Rule review is scheduled for ever N days. If a rule has not hit in N days from modified date the rule should be reviewed and sent to tier 2 to be reviewed for removal by tier 1. This also includes relevant Splunk ES alerts. If tier 2 determines the rule should be removed it is set to disabled and end **YYMMDD_** prefix is added to the rule. If the rule is persistent the **FLast_** (First Last Name) prefix is added to the rule.

Audit Logs:

https://falcon.crowdstrike.com/configuration/custom-ioa-groups/audit-log

Disabled rule:

200601_ Mcafee_Maze_Ransomeware_200326_185.147.14.0/23

Persistent rule:

RMcCurdy_ Mcafee_Maze_Ransomeware_200326_185.147.14.0/23

Needed

- Severity levels need to ultimately bind to ES sev levels. IE Medium CS is Low in ES (ES SME/Managment)

- N days should be replaced with days ES SME/Managment)
- Process for tier 1 adding TTPs to Splunk ES (ES SME/Managment)
- Have invite sent for SOC Tier 1 to review / update current rules for proper formatting and tickets (all SOC members)

Version

Date Updated	Version	Name	Notes
20200511	1	Robert McCurdy	Original Draft Document