Detection: Detect Regasm with Network Connection

Updated Date: 2024-08-14 | ID: 07921114-6db4-4e2e-ae58-3ea8a52ae93f | Author: Michael Haag, Splunk | Type: TTP

Product: Splunk Enterprise Security

Description

The following analytic detects the execution of regasm.exe establishing a network connection to a public IP address, excluding private IP ranges. This detection leverages Sysmon EventID 3 logs to identify such behavior. This activity is significant as regasm.exe is a legitimate Microsoft-signed binary that can be exploited to bypass application control mechanisms. If confirmed malicious, this behavior could indicate an adversary's attempt to establish a remote Command and Control (C2) channel, potentially leading to privilege escalation and further malicious actions within the environment.

Search

SPL

```
`sysmon` EventID=3 dest_ip!=10.0.0.0/8 dest_ip!=172.16.0.0/12 dest_ip!=192.168.0.0/16 process_name=regasm.exe
| stats count min(_time) as firstTime max(_time) as lastTime by dest, user, process_name, src_ip, dest_ip
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
| `detect_regasm_with_network_connection_filter`
```

Data Source

Name	Platform	Sourcetype	Source	Supported App
Sysmon EventID 3	Windows	'xmlwineventlog'	'XmlWinEventLog:Microsoft-Windows-Sysmon/Operational'	N/A

Macros Used

Name	Value
security_content_ctime	convert timeformat="%Y-%m-%dT%H:%M:%S" ctime($field$)
detect_regasm_with_network_connection_filter	search *

> `detect_regasm_with_network_connection_filter` is an empty macro by default. It allows the user to filter out any results (false positives) without editing the SPL.

Annotations

- MITRE ATT&CK + KILL CHAIN PHASES + NIST + CIS - THREAT ACTORS

ID	Technique	Tactic
T1218	System Binary Proxy Execution	Defense Evasion
T1218.009	Regsvcs/Regasm	Defense Evasion

LAZARUS GROUP

Default Configuration

This detection is configured by default in Splunk Enterprise Security to run with the following settings:

Setting	Value
Disabled	true
Cron Schedule	`0 * * * *`
Earliest Time	`-70m@m`
Latest Time	`-10m@m`
Schedule Window	`auto`
Creates Notable	Yes
Rule Title	`%name%`
Rule Description	`%description%`
Notable Event Fields	user, dest
Creates Risk Event	True

> This configuration file applies to all detections of type TTP. These detections will use Risk Based Alerting and generate Notable Events.

Implementation

To successfully implement this search, you need to be ingesting logs with the process name, parent process, and command-line executions from your endpoints. If you are using Sysmon, you must have at least version 6.0.4 of the Sysmon TA.

Known False Positives

Although unlikely, limited instances of regasm.exe with a network connection may cause a false positive. Filter based endpoint usage, command line arguments, or process lineage.

Associated Analytic Story

- Handala Wiper
- Living Off The Land
- Suspicious Regsvcs Regasm Activity

Risk Based Analytics (RBA)

Risk Message	Risk Score	Impact	Confidence
An instance of $process_name$ contacting a remote destination was identified on endpoint $dest$ by user $user$. This behavior is not normal for $process_name$.	80	80	100

> The Risk Score is calculated by the following formula: Risk Score = (Impact * Confidence/100). Initial Confidence and Impact is set by the analytic author.

References

- https://attack.mitre.org/techniques/T1218/009/

- https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1218.009/T1218.009.md
- https://lolbas-project.github.io/lolbas/Binaries/Regasm/

Detection Testing

Test Type	Status	Dataset	Source	Sourcetype
Validation	✅ Passing	N/A	N/A	N/A
Unit	✅ Passing	Dataset	`XmlWinEventLog:Microsoft-Windows-Sysmon/Operational`	`xmlwineventlog`
Integration	✅ Passing	Dataset	`XmlWinEventLog:Microsoft-Windows-Sysmon/Operational`	`xmlwineventlog`

Replay any dataset to Splunk Enterprise by using our `replay.py` tool or the UI. Alternatively you can replay a dataset into a Splunk Attack Range

---

Source: GitHub | Version: **5**

← Detection: Detect ...

Detection: Detect ... →