Detection: Detect Renamed PSExec

By Author: Michael Haag, Splunk, Alex Oberkircher, Github Community

Published: 2026-02-25 · Archived: 2026-04-05 16:44:47 UTC

Description

The following analytic identifies instances where `PsExec.exe` has been renamed and executed on an endpoint. It leverages data from Endpoint Detection and Response (EDR) agents, focusing on process names and original file names. This activity is significant because renaming `PsExec.exe` is a common tactic to evade detection. If confirmed malicious, this could allow an attacker to execute commands remotely, potentially leading to unauthorized access, lateral movement, or further compromise of the network.

Search

```
 1
2| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time) as lastTime FROM datamodel=
3  WHERE (
4        Processes.process_name!=psexec.exe
5        AND
6        Processes.process_name!=psexec64.exe
7    )
8    AND Processes.original_file_name=psexec.c
9  BY Processes.action Processes.dest Processes.original_file_name
10     Processes.parent_process Processes.parent_process_exec Processes.parent_process_guid
11     Processes.parent_process_id Processes.parent_process_name Processes.parent_process_path
12     Processes.process Processes.process_exec Processes.process_guid
13     Processes.process_hash Processes.process_id Processes.process_integrity_level
14     Processes.process_name Processes.process_path Processes.user
15     Processes.user_id Processes.vendor_product
16
17| `drop_dm_object_name(Processes)`
18
19| `security_content_ctime(firstTime)`
20
21| `security_content_ctime(lastTime)`
22
23| `detect_renamed_psexec_filter`
```

...

spl

Data Source

Name	Platform	Sourcetype	Source
CrowdStrike ProcessRollup2	Other	`'crowdstrike:events:sensor'`	`'crowdstrike'`
Sysmon EventID 1	 Windows	`'XmlWinEventLog'`	`'XmlWinEventLog:Microsoft-Windows-Sysmon/Operational'`
Windows Event Log Security 4688	 Windows	`'XmlWinEventLog'`	`'XmlWinEventLog:Security'`

Macros Used

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

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

Annotations

ID	Technique	Tactic
T1569.002	Service Execution	Execution

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 * * * *`

Setting	Value
Earliest Time	`-70m@m`
Latest Time	`-10m@m`
Schedule Window	`auto`
Creates Risk Event	False

This configuration file applies to all detections of type hunting.

Implementation

The detection is based on data that originates from Endpoint Detection and Response (EDR) agents. These agents are designed to provide security-related telemetry from the endpoints where the agent is installed. To implement this search, you must ingest logs that contain the process GUID, process name, and parent process. Additionally, you must ingest complete command-line executions. These logs must be processed using the appropriate Splunk Technology Add-ons that are specific to the EDR product. The logs must also be mapped to the `Processes` node of the `Endpoint` data model. Use the Splunk Common Information Model (CIM) to normalize the field names and speed up the data modeling process.

Known False Positives

Limited false positives should be present. It is possible some third party applications may use older versions of PsExec, filter as needed.

Associated Analytic Story

- Active Directory Lateral Movement
- BlackByte Ransomware
- CISA AA22-320A
- Cactus Ransomware
- China-Nexus Threat Activity
- DHS Report TA18-074A
- DarkGate Malware
- DarkSide Ransomware
- HAFNIUM Group
- Medusa Ransomware

- Rhysida Ransomware
- Salt Typhoon
- SamSam Ransomware
- Sandworm Tools
- VanHelsing Ransomware

References

- https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1569.002/T1569.002.yaml
- https://redcanary.com/blog/threat-hunting-psexec-lateral-movement/

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: **16**
