



Start free trial

Contact Sales

[Platform](#) [Solutions](#) [Customers](#) [Resources](#) [Pricing](#) [Docs](#)

[Elastic Docs](#) › [Elastic Security Solution \[8.15\]](#) › [Detections and alerts](#)  
› [Prebuilt rule reference](#)

# Volume Shadow Copy Deletion via PowerShell



Identifies the use of the Win32\_ShadowCopy class and related cmdlets to achieve shadow copy deletion. This commonly occurs in tandem with ransomware or other destructive attacks.

**Rule type:** eql

**Rule indices:**

- winlogbeat-\*
- logs-endpoint.events.process-\*
- logs-windows.forwarded\*
- logs-windows.sysmon\_operational-\*
- endgame-\*
- logs-system.security\*
- logs-m365\_defender.event-\*
- logs-sentinel\_one\_cloud\_funnel.\*

**Severity:** high

**Risk score:** 73

**Runs every:** 5m

**Searches indices from:** now-9m ([Date Math format](#), see also [Additional look-back time](#))

**Maximum alerts per execution:** 100

**References:**

- <https://docs.microsoft.com/en-us/previous-versions/windows/desktop/vsswmi/win32-shadowcopy>
- [https://powershell.one/wmi/root/cimv2/win32\\_shadowcopy](https://powershell.one/wmi/root/cimv2/win32_shadowcopy)
- <https://www.fortinet.com/blog/threat-research/stomping-shadow-copies-a-second-look-into-deletion-methods>

**Tags:**

- Domain: Endpoint
- OS: Windows
- Use Case: Threat Detection
- Tactic: Impact
- Tactic: Execution
- Resources: Investigation Guide
- Data Source: Elastic Endgame
- Data Source: Elastic Defend
- Data Source: System
- Data Source: Microsoft Defender for Endpoint
- Data Source: Sysmon
- Data Source: SentinelOne

**Version:** 312

**Rule authors:**

- Elastic
- Austin Songer

**Rule license:** Elastic License v2

# Investigation guide



## Triage and analysis

### Investigating Volume Shadow Copy Deletion via PowerShell

The Volume Shadow Copy Service (VSS) is a Windows feature that enables system administrators to take snapshots of volumes that can later be restored or mounted to recover specific files or folders.

A typical step in the playbook of an attacker attempting to deploy ransomware is to delete Volume Shadow Copies to ensure that victims have no alternative to paying the ransom, making any action that deletes shadow copies worth monitoring.

This rule monitors the execution of PowerShell cmdlets to interact with the Win32\_ShadowCopy WMI class, retrieve shadow copy objects, and delete them.

### Possible investigation steps

- Investigate the program execution chain (parent process tree).
- Check whether the account is authorized to perform this operation.
- Contact the account owner and confirm whether they are aware of this activity.
- Investigate other alerts associated with the user/host during the past 48 hours.
- If unsigned files are found on the process tree, retrieve them and determine if they are malicious:
- Use a private sandboxed malware analysis system to perform analysis.

- Observe and collect information about the following activities:
- Attempts to contact external domains and addresses.
- File and registry access, modification, and creation activities.
- Service creation and launch activities.
- Scheduled task creation.
- Use the PowerShell Get-FileHash cmdlet to get the files' SHA-256 hash values.
- Search for the existence and reputation of the hashes in resources like VirusTotal, Hybrid-Analysis, CISCO Talos, Any.run, etc.
- Use process name, command line, and file hash to search for occurrences in other hosts.
- Check if any files on the host machine have been encrypted.

### **False positive analysis**

- This rule has chances of producing benign true positives (B-TPs). If this activity is expected and noisy in your environment, consider adding exceptions — preferably with a combination of user and command line conditions.

### **Related rules**

- Volume Shadow Copy Deleted or Resized via VssAdmin - b5ea4bfe-a1b2-421f-9d47-22a75a6f2921
- Volume Shadow Copy Deletion via PowerShell - d99a037b-c8e2-47a5-97b9-170d076827c4

### **Response and remediation**

- Initiate the incident response process based on the outcome of the triage.
- Consider isolating the involved host to prevent destructive

behavior, which is commonly associated with this activity.

- Priority should be given due to the advanced stage of this activity on the attack.
- If the triage identified malware, search the environment for additional compromised hosts.
- Implement temporary network rules, procedures, and segmentation to contain the malware.
- Stop suspicious processes.
- Immediately block the identified indicators of compromise (IoCs).
- Inspect the affected systems for additional malware backdoors like reverse shells, reverse proxies, or droppers that attackers could use to reinfect the system.
- Remove and block malicious artifacts identified during triage.
- If data was encrypted, deleted, or modified, activate your data recovery plan.
- Investigate credential exposure on systems compromised or used by the attacker to ensure all compromised accounts are identified. Reset passwords for these accounts and other potentially compromised credentials, such as email, business systems, and web services.
- Perform data recovery locally or restore the backups from replicated copies (cloud, other servers, etc.).
- Run a full antimalware scan. This may reveal additional artifacts left in the system, persistence mechanisms, and malware components.
- Determine the initial vector abused by the attacker and take action to prevent reinfection through the same vector.
- Using the incident response data, update logging and audit policies to improve the mean time to detect (MTTD) and the mean time to respond (MTTR).

## Rule query



```
process where host.os.type == "windows" and event.type  
process.name : ("powershell.exe", "pwsh.exe", "pow  
process.args : ("*Get-WmiObject*", "*gwmi*", "*Get  
process.args : ("*Win32_ShadowCopy*") and  
process.args : ("*.Delete()*", "*Remove-WmiObject*
```

**Framework:** MITRE ATT&CK™

- Tactic:
  - Name: Impact
  - ID: TA0040
  - Reference URL:  
<https://attack.mitre.org/tactics/TA0040/>
- Technique:
  - Name: Inhibit System Recovery
  - ID: T1490
  - Reference URL:  
<https://attack.mitre.org/techniques/T1490/>
- Tactic:
  - Name: Execution
  - ID: TA0002
  - Reference URL:  
<https://attack.mitre.org/tactics/TA0002/>
- Technique:
  - Name: Command and Scripting Interpreter
  - ID: T1059
  - Reference URL:  
<https://attack.mitre.org/techniques/T1059/>
- Sub-technique:

- Name: PowerShell
- ID: T1059.001
- Reference URL:  
<https://attack.mitre.org/techniques/T1059/001/>

« [Volume Shadow Copy Deleted or Resized via VssAdmin](#)

[Volume Shadow Copy Deletion via WMIC](#) »

### ElasticON events are back!

Learn about the Elastic Search AI Platform from the experts at our live events.

[Learn more](#)

Was this helpful?



The Search AI Company

## Follow us



## About us

[About Elastic](#)

## Partners

[Find a partner](#)

Leadership

DE&I

Blog

Newsroom

# Join us

Careers

Career portal

Partner login

Request access

Become a partner

# Trust & Security

Trust center

EthicsPoint portal

ECCN report

Ethics email

# Investor relations

Investor resources

Governance

Financials

Stock

# EXCELLENCE AWARDS

Previous winners

ElasticON Tour

Become a sponsor

All events



[Trademarks](#) [Terms of Use](#) [Privacy](#) [Sitemap](#)

© 2024, Elasticsearch B.V. All Rights Reserved

Elastic, Elasticsearch and other related marks are trademarks, logos or registered trademarks of Elasticsearch B.V. in the United States and other countries.

Apache, Apache Lucene, Apache Hadoop, Hadoop, HDFS and the yellow elephant logo are trademarks of the Apache Software Foundation in the United States and/or other countries. All other brand names, product names, or trademarks belong to their respective owners.