

Q

8

Start free trial

Contact Sales

Platform Solutions Customers Resources Pricing Docs

Elastic Docs > Elastic Security Solution [8.15] > Detections and alerts > Prebuilt rule reference

Suspicious Cmd Execution via WMI



Identifies suspicious command execution (cmd) via Windows Management Instrumentation (WMI) on a remote host. This could be indicative of adversary lateral movement.

Rule type: eql

Rule indices:

- logs-endpoint.events.process-*
- winlogbeat-*
- logs-windows.forwarded*
- logs-windows.sysmon_operational-*
- endgame-*
- logs-system.security*
- logs-m365_defender.event-*
- logs-sentinel_one_cloud_funnel.*

Severity: medium

Risk score: 47

Runs every: 5m

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

Maximum alerts per execution: 100

References:

- https://www.elastic.co/security-labs/elastic-protectsagainst-data-wiper-malware-targeting-ukrainehermeticwiper
- https://www.elastic.co/security-labs/operation-bleedingbear

Tags:

Domain: Endpoint

OS: Windows

Use Case: Threat Detection

Tactic: Execution

• Data Source: Elastic Endgame

Data Source: Elastic Defend

• Data Source: System

• Data Source: Microsoft Defender for Endpoint

• Data Source: Sysmon

• Data Source: SentinelOne

Version: 313

Rule authors:

Elastic

Rule license: Elastic License v2

Rule query



process where host.os.type == "windows" and eventity
process.parent.name : "WmiPrvSE.exe" and process.nam
process.args : "\\\127.0.0.1*" and process.args

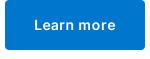
Framework: MITRE ATT&CKTM

- Tactic:
 - Name: Execution
 - ID: TA0002
 - Reference URL: https://attack.mitre.org/tactics/TA0002/
- Technique:
 - Name: Windows Management Instrumentation
 - ID: T1047
 - Reference URL: https://attack.mitre.org/techniques/T1047/
- Technique:
 - Name: Command and Scripting Interpreter
 - ID: T1059
 - Reference URL: https://attack.mitre.org/techniques/T1059/
- Sub-technique:
 - Name: Windows Command Shell
 - ID: T1059.003
 - Reference URL: https://attack.mitre.org/techniques/T1059/003/

« Suspicious Child Process of Adobe Suspicious Communication App Child Acrobat Reader Update Service Process »

ElasticON events are back!

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



Was this helpful?





The Search Al Company

Follow us











About us

About Elastic

Leadership

DE&I

Blog

Newsroom

Partners

Find a partner

Partner login

Request access

Become a partner

Trust & Security

Join us

Careers

Trust center

Career portal

EthicsPoint portal

ECCN report

Ethics email

Investor relations

Investor resources

Governance

Financials

Stock

EXCELLENCE AWARDS

Previous winners

ElasticON Tour

Become a sponsor

All events

<u>Trademarks</u> <u>Terms of Use</u> <u>Privacy</u> <u>Sitemap</u>

© 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.

Suspicious Cmd Execution via WMI Elastic Security Solution [8.15] Elastic - 31/10/2024 18:07 https://www.elastic.co/guide/en/security/current/suspicious-cmd-execution-via-wmi.html