

Notice

We and selected third parties use cookies or similar technologies for technical purposes and, with your consent, for other purposes as specified in the [cookie policy](#). Use the “Accept” button to consent. Use the “Reject” button to continue without accepting.

Learn more and customize

Reject

Accept

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-protects-against-data-wiper-malware-targeting-ukraine-hermeticwiper>
- <https://www.elastic.co/security-labs/operation-bleeding-bear>

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

ElasticON events are back!

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

Learn more

Was this helpful?



Notice

We and selected third parties use cookies or similar technologies for technical purposes and, with your consent, for other purposes as specified in the [cookie policy](#).
Use the “Accept” button to consent. Use the “Reject” button to continue without accepting.

```
process where host.os.type == "windows" and event.type == "start" and
process.parent.name : "WmiPrvSE.exe" and process.name : "cmd.exe" and
process.args : "\\127.0.0.1\*" and process.args : ("2>&1",
```

Framework: MITRE ATT&CK™

- 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 Acrobat Reader Update Service](#)

[Suspicious Communication App Child Process](#) »



Follow us



About us

- [About Elastic](#)
- [Leadership](#)
- [DE&I](#)
- [Blog](#)
- [Newsroom](#)

Join us

Partners

- [Find a partner](#)
- [Partner login](#)
- [Request access](#)
- [Become a partner](#)

Trust & Security

- [Trust center](#)

Notice

We and selected third parties use cookies or similar technologies for technical purposes and, with your consent, for other purposes as specified in the [cookie policy](#).
Use the “Accept” button to consent. Use the “Reject” button to continue without accepting.

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.