Suspicious Cmd Execution via WMI

edit

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

```
process where host.os.type == "windows" and event.type == "start
 process.parent.name : "WmiPrvSE.exe" and process.name : "cmd.ex
 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 »