Shortcut File Written or Modified for Persistence | Elastic Security [7.17]

Archived: 2026-11-20 02:13:18 UTC

Shortcut File Written or Modified for Persistence

edit

Identifies files written to or modified in the startup folder by commonly abused processes. Adversaries may use this technique to maintain persistence.

Rule type: eql

Rule indices:

- winlogbeat-*
- logs-endpoint.events.*
- logs-windows.*

Severity: medium

Risk score: 47

Runs every: 5 minutes

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

Maximum alerts per execution: 100

Tags:

- Elastic
- Host
- Windows
- Threat Detection
- Persistence

Version: 3 (version history)

Added (Elastic Stack release): 7.11.0

Last modified (Elastic Stack release): 7.12.0

Rule authors: Elastic

Rule license: Elastic License v2

```
file where event.type != "deletion" and user.domain != "NT
AUTHORITY" and file.path :
("C:\\Users\\*\\AppData\\Roaming\\Microsoft\\Windows\\Start
Menu\\Programs\\Startup\\*",
"C:\\ProgramData\\Microsoft\\Windows\\Start
Menu\\Programs\\StartUp\\*") and process.name : ("cmd.exe",
"powershell.exe", "wmic.exe",
"mshta.exe", "pwsh.exe",
"cscript.exe", "wscript.exe",
"regsvr32.exe", "RegAsm.exe",
"rundll32.exe", "EQNEDT32.EXE",
"WINWORD.EXE", "EXCEL.EXE",
"POWERPNT.EXE", "MSPUB.EXE",
"MSACCESS.EXE", "iexplore.exe",
"InstallUtil.exe")
```

Framework: MITRE ATT&CK™

- Tactic:
  - Name: Persistence
  - ID: TA0003
  - Reference URL: https://attack.mitre.org/tactics/TA0003/
- Technique:
  - Name: Boot or Logon Autostart Execution
  - ID: T1547
  - Reference URL: https://attack.mitre.org/techniques/T1547/

Version 3 (7.12.0 release)

- Formatting only

Version 2 (7.11.2 release)

- Formatting only

Source: https://www.elastic.co/guide/en/security/7.17/shortcut-file-written-or-modified-for-persistence.html#shortcut-file-written-or-modified-for-persistence