Sign in

elastic / protections-artifacts Public

Notifications | Fork 117 | Star 1k

Code | Issues 3 | Pull requests 1 | Actions | Projects | Security | Insights

protections-artifacts / behavior / rules
/ persistence_suspicious_scheduled_task_creation_via_masqueraded_xml_file.toml

72 lines (62 loc) · 2.39 KB

Code | Blame | Raw

```
[rule]
description = """
Identifies the creation of a scheduled task using an XML file that does not have a .xml file extens
consistent with an adversary attempting to establish persistence in a stealthy manner to evade dete
"""
id = "1efc0496-106b-4c09-b99b-91cdd17ba7b3"
license = "Elastic License v2"
name = "Suspicious Scheduled Task Creation via Masqueraded XML File"
os_list = ["windows"]
reference = ["https://docs.microsoft.com/en-us/windows/win32/taskschd/daily-trigger-example--xml-"]
version = "1.0.19"

query = '''
process where event.action == "start" and
  process.pe.original_file_name : "schtasks.exe" and
  process.args : ("/create", "-create") and
  process.args : ("/xml", "-xml") and
  not process.command_line : "*.xml*" and
  not process.Ext.token.integrity_level_name == "system" and
  not process.parent.executable :
             ("?:\\ProgramData\\OEM\\UpgradeTool\\CareCenter_*\\BUnzip\\Setup_msi.exe",
              "?:\\Program Files\\Axis Communications\\AXIS Camera Station\\SetupActions.exe",
              "?:\\Program Files\\Axis Communications\\AXIS Device Manager\\AdmSetupActions.exe",
              "?:\\Program Files (x86)\\Zemana\\AntiMalware\\AntiMalware.exe",
              "?:\\Program Files\\Dell\\SupportAssist\\pcdrcui.exe") and
  not (process.parent.name : "rundll32.exe" and process.parent.args : "?:\\WINDOWS\\Installer\\MSI*
'''

min_endpoint_version = "7.15.0"
optional_actions = []
[[actions]]
action = "kill_process"
field = "process.entity_id"
state = 0

[[threat]]
framework = "MITRE ATT&CK"
[[threat.technique]]
id = "T1053"
name = "Scheduled Task/Job"
reference = "https://attack.mitre.org/techniques/T1053/"
[[threat.technique.subtechnique]]
id = "T1053.005"
name = "Scheduled Task"
reference = "https://attack.mitre.org/techniques/T1053/005/"



[threat.tactic]
id = "TA0003"
name = "Persistence"
reference = "https://attack.mitre.org/tactics/TA0003/"
[[threat]]
framework = "MITRE ATT&CK"
[[threat.technique]]
id = "T1036"
name = "Masquerading"
reference = "https://attack.mitre.org/techniques/T1036/"
[[threat.technique.subtechnique]]
id = "T1036.005"
name = "Match Legitimate Name or Location"
reference = "https://attack.mitre.org/techniques/T1036/005/"



[threat.tactic]
id = "TA0005"
name = "Defense Evasion"
reference = "https://attack.mitre.org/tactics/TA0005/"

[internal]
```

```
min_endpoint_version = "7.15.0"
```