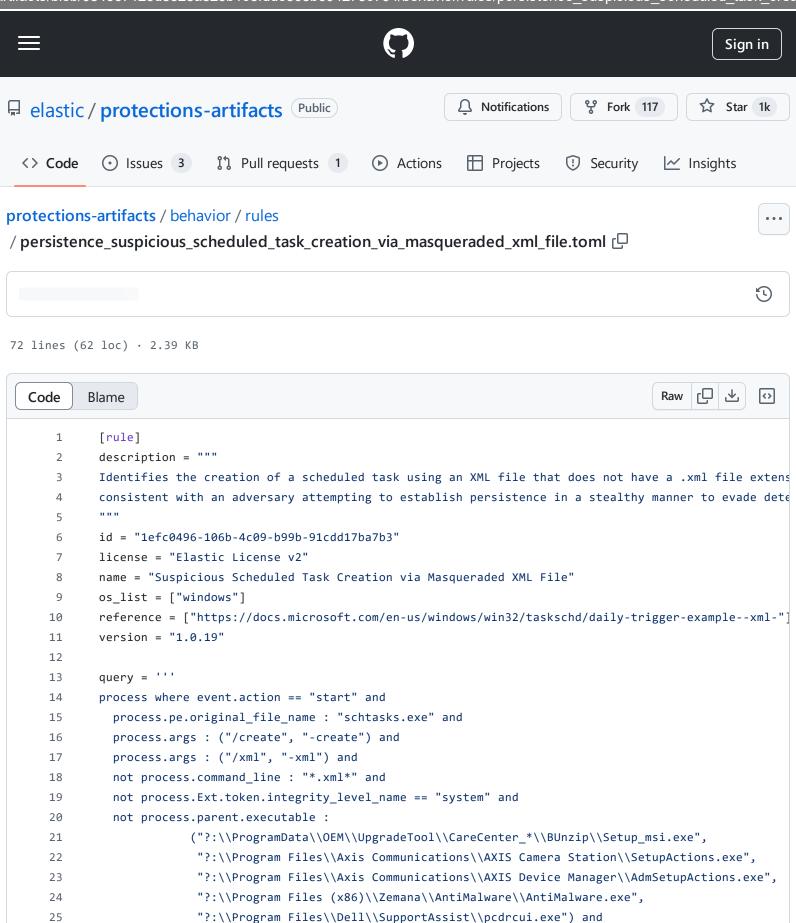
protections-

artifacts/behavior/rules/persistence\_suspicious\_scheduled\_task\_creation\_via\_masqueraded\_xml\_file.toml at 084067123d3328a823b1c3fdde305b694275c794 · elastic/protections-artifacts · GitHub - 31/10/2024 19:14 https://github.com/elastic/protections-

artifacts/blob/084067123d3328a823b1c3fdde305b694275c794/behavior/rules/persistence suspicious scheduled task creati



artifacts/behavior/rules/persistence\_suspicious\_scheduled\_task\_creation\_via\_masqueraded\_xml\_file.toml at 084067123d3328a823b1c3fdde305b694275c794 · elastic/protections-artifacts · GitHub - 31/10/2024 19:14

https://github.com/elastic/protections-

artifacts/blob/084067123d3328a823b1c3fdde305b694275c794/behavior/rules/persistence\_suspicious\_scheduled\_task\_creati

```
not (process.parent.name : "rundl132.exe" and process.parent.args : "?:\\WINDOWS\\Installer\\MSI*
27
28
29
       min_endpoint_version = "7.15.0"
       optional_actions = []
30
31
       [[actions]]
       action = "kill_process"
32
       field = "process.entity_id"
33
       state = 0
34
35
36
       [[threat]]
       framework = "MITRE ATT&CK"
37
38
       [[threat.technique]]
       id = "T1053"
39
40
       name = "Scheduled Task/Job"
       reference = "https://attack.mitre.org/techniques/T1053/"
41
42
       [[threat.technique.subtechnique]]
       id = "T1053.005"
43
       name = "Scheduled Task"
44
       reference = "https://attack.mitre.org/techniques/T1053/005/"
45
46
47
48
49
       [threat.tactic]
50
       id = "TA0003"
       name = "Persistence"
51
       reference = "https://attack.mitre.org/tactics/TA0003/"
52
53
       [[threat]]
       framework = "MITRE ATT&CK"
54
55
       [[threat.technique]]
       id = "T1036"
56
       name = "Masquerading"
57
       reference = "https://attack.mitre.org/techniques/T1036/"
58
59
       [[threat.technique.subtechnique]]
       id = "T1036.005"
60
       name = "Match Legitimate Name or Location"
61
62
       reference = "https://attack.mitre.org/techniques/T1036/005/"
63
64
65
       [threat.tactic]
66
       id = "TA0005"
67
       name = "Defense Evasion"
68
       reference = "https://attack.mitre.org/tactics/TA0005/"
69
70
71
       [internal]
```

## protections-

 $artifacts/behavior/rules/persistence\_suspicious\_scheduled\_task\_creation\_via\_masqueraded\_xml\_file.toml\ at \ 084067123d3328a823b1c3fdde305b694275c794 \cdot elastic/protections-artifacts \cdot GitHub - 31/10/2024\ 19:14$ 

https://github.com/elastic/protections-

artifacts/blob/084067123d3328a823b1c3fdde305b694275c794/behavior/rules/persistence\_suspicious\_scheduled\_task\_creati

72 min\_endpoint\_version = "7.15.0"