

elastic / protections-artifacts

Public

Notifications

Fork 117

Star 1k

<> Code

Issues 3

Pull requests 1

Actions

Projects

Security

Insights

Files

0840671

Go to file

> .github

> behavior

> rules

command_and_control_conne...

command_and_control_conne...

command_and_control_conne...

command_and_control_conne...

command_and_control_curl_fr...

command_and_control_executi...

command_and_control_ingress...

command_and_control_ingress...

command_and_control_library...

command_and_control_netwir...

command_and_control_payloa...

command_and_control_potenti...

command_and_control_potenti...

command_and_control_potenti...

command_and_control_potenti...

command_and_control_potenti...

command_and_control_potenti...

command_and_control_potenti...

command_and_control_remcos...

command_and_control_shlayer...

command_and_control_suspici...

command_and_control_suspici...

command_and_control_suspici...

command_and_control_suspici...

command_and_control_suspici...

credential_access_access_to_wi...

credential_access_browser_deb...

credential_access_credential_ac...

credential_access_dumping_acc...

credential_access_failed_access...

credential_access_failed_attem...

credential_access_keychain_cre...

credential_access_keychain_du...

protections-artifacts / behavior / rules

/ persistence_suspicious_scheduled_task_creation_via_masqueraded_xml_file.toml

protectionsmachine Updating artifacts0840671 · last yearHistory

Code

Blame

72 lines (62 loc) · 2.39 KB

Raw

1

[rule]

2

description = ""

3

Identifies the creation of a scheduled task using an XML file that does not have a .xml

4

consistent with an adversary attempting to establish persistence in a stealthy manner t

5

""

6

id = "1efc0496-106b-4c09-b99b-91cdd17ba7b3"

7

license = "Elastic License v2"

8

name = "Suspicious Scheduled Task Creation via Masqueraded XML File"

9

os_list = ["windows"]

10

reference = ["https://docs.microsoft.com/en-us/windows/win32/taskschd/daily-trigger-exa

11

version = "1.0.19"

12

13

query = '''

14

process where event.action == "start" and

15

process.pe.original_file_name : "schtasks.exe" and

16

process.args : ("/create", "-create") and

17

process.args : ("/xml", "-xml") and

18

not process.command_line : "*.xml*" and

19

not process.Ext.token.integrity_level_name == "system" and

20

not process.parent.executable :

21

("?:\\ProgramData\\OEM\\UpgradeTool\\CareCenter_*\\BUnzip\\Setup_msi.exe",

22

"?:\\Program Files\\Axis Communications\\AXIS Camera Station\\SetupAction

23

"?:\\Program Files\\Axis Communications\\AXIS Device Manager\\AdmSetupAct

24

"?:\\Program Files (x86)\\Zemana\\AntiMalware\\AntiMalware.exe",

25

"?:\\Program Files\\Dell\\SupportAssist\\pcdrcui.exe") and

26

not (process.parent.name : "rundll32.exe" and process.parent.args : "?:\\WINDOWS\\Ins

27

'''

28

29

min_endpoint_version = "7.15.0"

30

optional_actions = []

31

[[actions]]

32

action = "kill_process"

33

field = "process.entity_id"

34

state = 0

35

36

[[threat]]

37

framework = "MITRE ATT&CK"

38

[[threat.technique]]

39

id = "T1053"

40

name = "Scheduled Task/Job"

41

reference = "https://attack.mitre.org/techniques/T1053/"

42

[[threat.technique.subtechnique]]

43

id = "T1053.005"

44

name = "Scheduled Task"

45

reference = "https://attack.mitre.org/techniques/T1053/005/"

46

47

48

49

[threat.tactic]

50

id = "TA0003"

51

name = "Persistence"

52

reference = "https://attack.mitre.org/tactics/TA0003/"

53

[[threat]]

54

framework = "MITRE ATT&CK"

55

[[threat.technique]]

56

id = "T1053"

Page 1 of 2

- credential_access_lsa_dump_vi...
- credential_access_lsa_dump_vi...
- credential_access_lsass_access_...
- credential_access_lsass_access_...
- credential_access_lsass_memor...
- credential access potential acc...

```
56     id = "T1036"
57     name = "Masquerading"
58     reference = "https://attack.mitre.org/techniques/T1036/"
59     [[threat.technique.subtechnique]]
60     id = "T1036.005"
61     name = "Match Legitimate Name or Location"
62     reference = "https://attack.mitre.org/techniques/T1036/005/"
63
64
65
66     [threat.tactic]
67     id = "TA0005"
68     name = "Defense Evasion"
69     reference = "https://attack.mitre.org/tactics/TA0005/"
70
71     [internal]
72     min_endpoint_version = "7.15.0"
```