

Product Solutions Resources Open Source Enterprise Pricing

Search

Sign in

Sign up

elastic / detection-rules

Public

Notifications

Fork 498

Star 2k

<> Code

Issues 144

Pull requests 28

Actions

Security

Insights

Files

414d320

Go to file

.github

detection_rules

docs

etc

kibana

kql

rta

rules

_deprecated

apm

aws

azure

cross-platform

gcp

google-workspace

linux

macos

microsoft-365

ml

network

okta

promotions

windows

collection_email_powershell_ex...

collection_persistence_powersh...

collection_winrar_encryption.to...

command_and_control_certutil...

command_and_control_comm...

command_and_control_dns_tu...

command_and_control_encryp...

command_and_control_iexplor...

command_and_control_remote...

command_and_control_remote...

command_and_control_remote...

command_and_control_remote...

command_and_control_sunbur...

detection-rules / rules / windows / discovery_peripheral_device.toml

...

brokensound77 Update License to Elastic v2 (#944)

3fc34b8 · 3 years ago

History

CodeBlame43 lines (36 loc) · 1.16 KB

RawCopyDownloadCompare

1[metadata]

2creation_date = "2020/11/02"

3maturity = "production"

4updated_date = "2021/03/03"

5

6[rule]

7author = ["Elastic"]

8description = ""

9Identifies use of the Windows file system utility (fsutil.exe) to gather information a

10and components connected to a computer system.

11""

12from = "now-9m"

13index = ["winlogbeat-*", "logs-endpoint.events.*", "logs-windows.*"]

14language = "eql"

15license = "Elastic License v2"

16name = "Peripheral Device Discovery"

17risk_score = 21

18rule_id = "0c7ca5c2-728d-4ad9-b1c5-bbba83ecb1f4"

19severity = "low"

20tags = ["Elastic", "Host", "Windows", "Threat Detection", "Discovery"]

21timestamp_override = "event.ingested"

22type = "eql"

23

24query = '''

25process where event.type in ("start", "process_started") and

26(process.name : "fsutil.exe" or process.pe.original_file_name == "fsutil.exe") and

27process.args : "fsinfo" and process.args : "drives"

28'''

29

30

31[[rule.threat]]

32framework = "MITRE ATT&CK"

33[[rule.threat.technique]]

34id = "T1120"

35name = "Peripheral Device Discovery"

36reference = "https://attack.mitre.org/techniques/T1120/"

37

38







39[[rule.threat.tactic]]

40id = "TA0007"

41name = "Discovery"

42reference = "https://attack.mitre.org/tactics/TA0007/"

Page 1 of 2

-  command_and_control_teamvi...
-  credential_access_cmdline_du...
-  credential_access_copy_ntds_s...
-  credential_access_credential_d...
-  credential_access_domain_back...
-  credential access dump regist...