

elastic / detection-rules

Public

Notifications

Fork 498

Star 2k

<> Code

Issues 144

Pull requests 28

Actions

Security

Insights

Files

dd224fb

Go to file

> .github

> detection_rules

> docs

> etc

> kibana

> kql

> rta

> rules

> _deprecated

> apm

> cross-platform

> integrations

> linux

> macos

> ml

> network

> promotions

> windows

collection_email_powershell_ex...

collection_posh_audio_capture....

collection_posh_keylogger.toml

collection_posh_screen_grabbe...

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_port_fo...

command_and_control_rdp_tu...

command_and_control_remote...

command_and_control_remote...

command_and_control_remote...

command_and_control_remote...

command_and_control_sunbur...

command_and_control_teamvi...

detection-rules / rules / windows

...

/ credential_access_relay_ntlm_auth_via_http_spoolss.toml

This commit does not belong to any branch on this repository, and may belong to a fork outside of the repository.

Samirbous [New Rule] Potential Local NTLM Relay via HTTP

dd224fb · 2 years ago

History

Code

Blame

48 lines (41 loc) · 1.46 KB

Raw

1 [metadata]

2 creation_date = "2022/04/30"

3 maturity = "production"

4 updated_date = "2022/04/30"

5

6 [rule]

7 author = ["Elastic"]

8 description = ""

9 Identifies attempt to coerce a local NTLM authentication via HTTP using Printer Spooler

10 adversary may use this primitive in combination with other techniques to elevate privil

11 ""

12 from = "now-9m"

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

14 language = "eql"

15 license = "Elastic License v2"

16 name = "Potential Local NTLM Relay via HTTP"

17 references = [

18 "https://github.com/med0x2e/NTLMRelay2Self",

19 "https://github.com/topotam/PetitPotam",

20 "https://github.com/dirkjanm/krbrelayx/blob/master/printerbug.py",

21]

22 risk_score = 73

23 rule_id = "4682fd2c-cfae-47ed-a543-9bed37657aa6"

24 severity = "high"

25 tags = ["Elastic", "Host", "Windows", "Threat Detection", "Credential Access"]

26 type = "eql"

27

28 query = '''

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

30 process.name : "rundll32.exe" and

31 /* relay to HTTP via spoolss or srvsvc pipes */

32 process.command_line : ("*davclnt.dll*http*spoolss*", "*davclnt.dll*http*pipe*srvsvc"

33 '''

34

35

36 [[rule.threat]]

37 framework = "MITRE ATT&CK"

38 [[rule.threat.technique]]

39 id = "T1212"

40 name = "Exploitation for Credential Access"

41 reference = "https://attack.mitre.org/techniques/T1212/"

42

43

44 [rule.threat.tactic]

45 id = "TA0006"

46 name = "Credential Access"

47 reference = "https://attack.mitre.org/tactics/TA0006/"

Page 1 of 2

- credential_access_cmdline_du...
- credential_access_copy_ntds_s...
- credential_access_credential_d...
- credential_access_dcsync_replic...
- credential_access_disable_kerb...
- credential access domain back...