

elastic / detection-rules

Public

Notifications

Fork 498

Star 2k

<> Code

Issues 144

Pull requests 28

Actions

Security

Insights

Files

2bc1795

Go to file

> .github

> detection_rules

> docs

> 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...

credential_access_cmdline_du...

detection-rules / rules / windows / credential_access_lsass_handle_via_malseclogon.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] 2bc1795 · 2 years ago History

Code

Blame

59 lines (48 loc) · 1.96 KB

Raw

1 [metadata]

2 creation_date = "2022/06/29"

3 maturity = "production"

4 updated_date = "2022/06/29"

5

6 [rule]

7 author = ["Elastic"]

8 description = ""

9 Identifies suspicious access to LSASS handle from a call trace pointing to seclogon.dll

10 value, this may indicate an attempt to leak an Lsass handle via abusing the Secondary L

11 credential access.

12 ""

13 from = "now-9m"

14 index = ["winlogbeat-*", "logs-windows.*"]

15 language = " eql "

16 license = "Elastic License v2"

17 name = "Suspicious LSASS Access via MalSecLogon"

18 note = ""### Config

19

20 If enabling an EQL rule on a non-elastic-agent index (such as beats) for versions <8.2,

21 ""

22 references = ["https://splintercod3.blogspot.com/p/the-hidden-side-of-seclogon-part-3.h

23 risk_score = 73

24 rule_id = "7ba58110-ae13-439b-8192-357b0fcfa9d7"

25 severity = "high"

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

27 timestamp_override = "event.ingested"

28 type = " eql "

29

30 query = '''

31 process where event.code == "10" and

32 winlog.event_data.TargetImage : "?:\\WINDOWS\\system32\\lsass.exe" and

33

34 /* seclogon service accessing lsass */

35 winlog.event_data.CallTrace : "*seclogon.dll*" and process.name : "svchost.exe" and

36

37 /* PROCESS_CREATE_PROCESS & PROCESS_DUP_HANDLE & PROCESS_QUERY_INFORMATION */

38 winlog.event_data.GrantedAccess == "0x14c0"

39 '''

40

41

42 [[rule.threat]]

43 framework = "MITRE ATT&CK"

44 [[rule.threat.technique]]

45 id = "T1003"

46 name = "OS Credential Dumping"

47 reference = "https://attack.mitre.org/techniques/T1003/"

48 [[rule.threat.technique.subtechnique]]

49 id = "T1003.001"

50 name = "LSASS Memory"

51 reference = "https://attack.mitre.org/techniques/T1003/001/"

Page 1 of 2

| | |
|--|---|
|  credential_access_copy_ntds_s... | 52 |
|  credential_access_credential_d... | 53 |
|  credential_access_dcsync_replic... | 54 |
|  credential_access_disable_kerb... | 55 [rule.threat.tactic] |
|  credential_access_domain_back... | 56 id = "TA0006" |
|  credential_access_dump regist... | 57 name = "Credential Access" |
| | 58 reference = "https://attack.mitre.org/tactics/TA0006/" |