



Sign in

elastic / detection-rules Public

Notifications

Fork 498

Star 2k

[Code](#) [Issues 145](#) [Pull requests 22](#) [Actions](#) [Security](#) [Insights](#)

detection-rules / rules / windows / credential\_access\_lsass\_memdump\_file\_created.toml



56 lines (47 loc) · 1.96 KB

Code

Blame

Raw



```
1  [metadata]
2  creation_date = "2020/11/24"
3  maturity = "production"
4  updated_date = "2022/03/31"
5  min_stack_comments = "Comprehensive timeline templates only available in 8.2+"
6  min_stack_version = "8.2"
7
8  [rule]
9  author = ["Elastic"]
10 description = ""
11 Identifies the creation of a Local Security Authority Subsystem Service (lsass.exe) default memory
12 indicate a credential access attempt via trusted system utilities such as Task Manager (taskmgr.exe)
13 (sqldumper.exe) or known pentesting tools such as Dumpert and AndrewSpecial.
14 ""
15 from = "now-9m"
16 index = ["winlogbeat-*", "logs-endpoint.events.*", "logs-windows.*"]
17 language = "eql"
18 license = "Elastic License v2"
19 name = "LSASS Memory Dump Creation"
20 note = ""## Config
21
22 If enabling an EQL rule on a non-elastic-agent index (such as beats) for versions <8.2, events will
23 ""
24 references = ["https://github.com/outflanknl/Dumpert", "https://github.com/hoangprod/AndrewSpecial"]
25 risk_score = 73
26 rule_id = "f2f46686-6f3c-4724-bd7d-24e31c70f98f"
```

```
27     severity = "high"
28     tags = ["Elastic", "Host", "Windows", "Threat Detection", "Credential Access"]
29     timeline_id = "4d4c0b59-ea83-483f-b8c1-8c360ee53c5c"
30     timeline_title = "Comprehensive File Timeline"
31     timestamp_override = "event.ingested"
32     type = "eql"
33
34     query = '''
35     file where file.name : ("lsass*.dmp", "dumpert.dmp", "Andrew.dmp", "SQLDmpr*.mdmp", "Coredump.dmp")
36     '''
37
38
39     [[rule.threat]]
40     framework = "MITRE ATT&CK"
41     [[rule.threat.technique]]
42     id = "T1003"
43     name = "OS Credential Dumping"
44     reference = "https://attack.mitre.org/techniques/T1003/"
45     [[rule.threat.technique.subtechnique]]
46     id = "T1003.001"
47     name = "LSASS Memory"
48     reference = "https://attack.mitre.org/techniques/T1003/001/"
49
50
51
52     [[rule.threat.tactic]]
53     id = "TA0006"
54     name = "Credential Access"
55     reference = "https://attack.mitre.org/tactics/TA0006/"
```