56 lines (47 loc) · 1.96 KB

Code Blame Raw

```
[metadata]
creation_date = "2020/11/24"
maturity = "production"
updated_date = "2022/03/31"
min_stack_comments = "Comprehensive timeline templates only available in 8.2+"
min_stack_version = "8.2"

[rule]
author = ["Elastic"]
description = """
Identifies the creation of a Local Security Authority Subsystem Service (lsass.exe) default memory
indicate a credential access attempt via trusted system utilities such as Task Manager (taskmgr.exe
(sqldumper.exe) or known pentesting tools such as Dumpert and AndrewSpecial.
"""
from = "now-9m"
index = ["winlogbeat-*", "logs-endpoint.events.*", "logs-windows.*"]
language = "eql"
license = "Elastic License v2"
name = "LSASS Memory Dump Creation"
note = """## Config

If enabling an EQL rule on a non-elastic-agent index (such as beats) for versions <8.2, events will
"""
references = ["https://github.com/outflanknl/Dumpert", "https://github.com/hoangprod/AndrewSpecial"
risk_score = 73
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/"
```