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_relay_ntlm_auth_via_http_spoolss.toml

48 lines (41 loc) · 1.46 KB

Code Blame Raw

```toml
[metadata]
creation_date = "2022/04/30"
maturity = "production"
updated_date = "2022/04/30"

[rule]
author = ["Elastic"]
description = """
Identifies attempt to coerce a local NTLM authentication via HTTP using Printer Spooler service as
adversary may use this primitive in combination with other techniques to elevate privileges on a co
"""
from = "now-9m"
index = ["winlogbeat-*", "logs-endpoint.events.*", "logs-windows.*"]
language = "eql"
license = "Elastic License v2"
name = "Potential Local NTLM Relay via HTTP"
references = [
    "https://github.com/med0x2e/NTLMRelay2Self",
    "https://github.com/topotam/PetitPotam",
    "https://github.com/dirkjanm/krbrelayx/blob/master/printerbug.py",
]
risk_score = 73
rule_id = "4682fd2c-cfae-47ed-a543-9bed37657aa6"
severity = "high"
tags = ["Elastic", "Host", "Windows", "Threat Detection", "Credential Access"]
type = "eql"
```

```

query = '''
process where event.type in ("start", "process_started") and
  process.name : "rundll32.exe" and
  /* relay to HTTP via spoolss or srvsvc pipes */
  process.command_line : ("*davclnt.dll*http*spoolss*", "*davclnt.dll*http*pipe*srvsvc", "*davclnt.
'''


[[rule.threat]]
framework = "MITRE ATT&CK"
[[rule.threat.technique]]
id = "T1212"
name = "Exploitation for Credential Access"
reference = "https://attack.mitre.org/techniques/T1212/"


[rule.threat.tactic]
id = "TA0006"
name = "Credential Access"
reference = "https://attack.mitre.org/tactics/TA0006/"
```