Sign in

elastic / detection-rules Public

Notifications Fork 498 Star 2k

Code Issues 145 Pull requests 21 Actions Security Insights

detection-rules / rules / macos / execution_initial_access_suspicious_browser_childproc.toml

terrancedejesus and Mikaayenson [FR] Add Endpoint, APM and Windows Integration Tags t... 4312d8c · 2 years ago

79 lines (70 loc) · 2.63 KB

Code Blame Raw

```
[metadata]
creation_date = "2020/12/23"
integration = ["endpoint"]
maturity = "production"
min_stack_comments = "New fields added: required_fields, related_integrations, setup"
min_stack_version = "8.3.0"
updated_date = "2022/12/14"

[rule]
author = ["Elastic"]
description = """
Identifies the execution of a suspicious browser child process. Adversaries may gain access to a sy
visiting a website over the normal course of browsing. With this technique, the user's web browser
for exploitation.
"""
from = "now-9m"
index = ["logs-endpoint.events.*"]
language = "eql"
license = "Elastic License v2"
name = "Suspicious Browser Child Process"
references = [
    "https://objective-see.com/blog/blog_0x43.html",
    "https://fr.slideshare.net/codeblue_jp/cb19-recent-apt-attack-on-crypto-exchange-employees-by-h
]
risk_score = 73
```

```
rule_id = "080bc66a-5d56-4d1f-8071-817671716db9"
severity = "high"
tags = ["Elastic", "Host", "macOS", "Threat Detection", "Initial Access", "Execution"]
timestamp_override = "event.ingested"
type = "eql"

query = '''
process where event.type in ("start", "process_started") and
  process.parent.name : ("Google Chrome", "Google Chrome Helper*", "firefox", "Opera", "Safari", "c
  process.name : ("sh", "bash", "dash", "ksh", "tcsh", "zsh", "curl", "wget", "python*", "perl*", "
  process.command_line != null and
  not process.command_line : "*/Library/Application Support/Microsoft/MAU*/Microsoft AutoUpdate.app
  not process.args :
    (
      "hw.model",
      "IOPlatformExpertDevice",
      "/Volumes/Google Chrome/Google Chrome.app/Contents/Frameworks/*/Resources/install.sh",
      "--defaults-torrc",
      "*Chrome.app",
      "Framework.framework/Versions/*/Resources/keystone_promote_preflight.sh",
      "/Users/*/Library/Application Support/Google/Chrome/recovery/*/ChromeRecovery",
      "$DISPLAY",
      "*GIO_LAUNCHED_DESKTOP_FILE_PID=$$*",
      "/opt/homebrew/*",
      "/usr/local/*brew*"
    )
'''


[[rule.threat]]
framework = "MITRE ATT&CK"
[[rule.threat.technique]]
id = "T1203"
name = "Exploitation for Client Execution"
reference = "https://attack.mitre.org/techniques/T1203/"


[rule.threat.tactic]
id = "TA0002"
name = "Execution"
reference = "https://attack.mitre.org/tactics/TA0002/"
[[rule.threat]]
framework = "MITRE ATT&CK"
[[rule.threat.technique]]
id = "T1189"
name = "Drive-by Compromise"
```

```
reference = "https://attack.mitre.org/techniques/T1189/"


[rule.threat.tactic]
id = "TA0001"
name = "Initial Access"
reference = "https://attack.mitre.org/tactics/TA0001/"
```