Sign in

elastic / **detection-rules** Public

Notifications Fork 498 Star 2k

Code Issues 145 Pull requests 20 Actions Security Insights

detection-rules / rules / macos / **execution_installer_package_spawned_network_event.toml**

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

81 lines (70 loc) · 2.79 KB

Code Blame Raw

```
[metadata]
creation_date = "2021/02/23"
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 = """
Detects the execution of a MacOS installer package with an abnormal child process (e.g bash) follow
network connection via a suspicious process (e.g curl). Threat actors will build and distribute mal
installer packages, which have a .pkg extension, many times imitating valid software in order to pe
their victims often using the package files (e.g pre/post install scripts etc.) to download additio
malicious software. If this rule fires it should indicate the installation of a malicious or suspic
"""
false_positives = [
    """
    Custom organization-specific macOS packages that use .pkg files to run cURL could trigger this
    behavior is causing false positives, it can be excluded from the rule.
    """,
]
from = "now-9m"
index = ["logs-endpoint.events.*"]
```

```
language = "eql"
license = "Elastic License v2"
name = "MacOS Installer Package Spawns Network Event"
references = [
    "https://redcanary.com/blog/clipping-silver-sparrows-wings",
    "https://posts.specterops.io/introducing-mystikal-4fbd2f7ae520",
    "https://github.com/D00MFist/Mystikal",
]
risk_score = 47
rule_id = "99239e7d-b0d4-46e3-8609-acafcf99f68c"
severity = "medium"
tags = ["Elastic", "Host", "macOS", "Threat Detection", "Execution", "Command and Control"]
type = "eql"

query = '''
sequence by host.id, user.id with maxspan=30s
[process where event.type == "start" and event.action == "exec" and process.parent.name : ("install
[network where event.type == "start" and process.name : ("curl", "osascript", "wget", "python")]
'''


[[rule.threat]]
framework = "MITRE ATT&CK"
[[rule.threat.technique]]
id = "T1059"
name = "Command and Scripting Interpreter"
reference = "https://attack.mitre.org/techniques/T1059/"
[[rule.threat.technique.subtechnique]]
id = "T1059.007"
name = "JavaScript"
reference = "https://attack.mitre.org/techniques/T1059/007/"



[rule.threat.tactic]
id = "TA0002"
name = "Execution"
reference = "https://attack.mitre.org/tactics/TA0002/"
[[rule.threat]]
framework = "MITRE ATT&CK"
[[rule.threat.technique]]
id = "T1071"
name = "Application Layer Protocol"
reference = "https://attack.mitre.org/techniques/T1071/"
[[rule.threat.technique.subtechnique]]
id = "T1071.001"
```

```toml
name = "Web Protocols"
reference = "https://attack.mitre.org/techniques/T1071/001/"



[rule.threat.tactic]
id = "TA0011"
name = "Command and Control"
reference = "https://attack.mitre.org/tactics/TA0011/"
```