

Product ▾ Solutions ▾ Resources ▾ Open Source ▾ Enterprise ▾ Pricing

🔍

Sign in

Sign up

elastic / detection-rules Public

Notifications

Fork 498

Star 2k

<> Code

🔗 Issues 144

🔗 Pull requests 28

🔗 Actions

🔗 Security

🔗 Insights

Files

🔗 4312d8c 🔍

🔍 Go to file

> .github

> detection_rules

> docs

> kibana

> kql

> rta

> rules

- > _deprecated
- > apm
- > cross-platform
- > integrations
- > linux
- > macos
 - credential_access_access_to_br...
 - credential_access_credentials_k...
 - credential_access_dumping_ha...
 - credential_access_dumping_ke...
 - credential_access_kerberosdu...
 - credential_access_keychain_pw...
 - credential_access_mitm_localh...
 - credential_access_potential_ma...
 - credential_access_prompt_for_p...
 - credential_access_systemkey_d...
 - defense_evasion_apple_softup...
 - defense_evasion_attempt_del...
 - defense_evasion_attempt_to_d...
 - defense_evasion_install_root_c...
 - defense_evasion_modify_envir...
 - defense_evasion_privacy_contr...
 - defense_evasion_privilege_esca...
 - defense_evasion_safari_config...
 - defense_evasion_sandboxed_of...
 - defense_evasion_tcc_bypass_m...
 - defense_evasion_unload_endp...
 - discovery_users_domain_built_i...
 - execution_defense_evasion_ele...

detection-rules / rules / macos

/ execution_installer_package_spawned_network_event.toml 📄

terrancedejesus and Mikaayenson [FR] Add Endpoint, APM and... 4312d8c · 2 years ago 🕒 History

Code

Blame

81 lines (70 loc) · 2.79 KB

Raw

📄

📥

🔗

```
1  [metadata]
2  creation_date = "2021/02/23"
3  integration = ["endpoint"]
4  maturity = "production"
5  min_stack_comments = "New fields added: required_fields, related_integrations, setup"
6  min_stack_version = "8.3.0"
7  updated_date = "2022/12/14"
8
9  [rule]
10 author = ["Elastic"]
11 description = ""
12 Detects the execution of a MacOS installer package with an abnormal child process (e.g
13 network connection via a suspicious process (e.g curl). Threat actors will build and di
14 installer packages, which have a .pkg extension, many times imitating valid software in
15 their victims often using the package files (e.g pre/post install scripts etc.) to down
16 malicious software. If this rule fires it should indicate the installation of a malicio
17 ""
18 false_positives = [
19     ""
20     Custom organization-specific macOS packages that use .pkg files to run cURL could t
21     behavior is causing false positives, it can be excluded from the rule.
22     "",
23 ]
24 from = "now-9m"
25 index = ["logs-endpoint.events.*"]
26 language = "eql"
27 license = "Elastic License v2"
28 name = "MacOS Installer Package Spawns Network Event"
29 references = [
30     "https://redcanary.com/blog/clipping-silver-sparrows-wings",
31     "https://posts.specterops.io/introducing-mystikal-4fbd2f7ae520",
32     "https://github.com/D00MFist/Mystikal",
33 ]
34 risk_score = 47
35 rule_id = "99239e7d-b0d4-46e3-8609-acafcf99f68c"
36 severity = "medium"
37 tags = ["Elastic", "Host", "macOS", "Threat Detection", "Execution", "Command and Contr
38 type = "eql"
39
40 query = ''
41 sequence by host.id, user.id with maxspan=30s
42 [process where event.type == "start" and event.action == "exec" and process.parent.name
43 [network where event.type == "start" and process.name : ("curl", "osascript", "wget", "
44 ''
45
46
47 [[rule.threat]]
48 framework = "MITRE ATT&CK"
49 [[rule.threat.technique]]
50 id = "T1059"
51 name = "Command and Scripting Interpreter"
52 reference = "https://attack.mitre.org/techniques/T1059/"
53 [[rule.threat.technique.subtechnique]]
54 id = "T1059.007"
55 name = "JavaScript"
56 reference = "https://attack.mitre.org/techniques/T1059/007/"
```

Page 1 of 2

- execution_initial_access_suspici...
- execution_installer_package_sp...
- execution_script_via_automato...
- execution_scripting_osascript_e...
- execution_shell_execution_via_...
- initial access suspicious mac ...

```
56     reference = "https://attack.mitre.org/techniques/T1059/00/"
57
58
59
60     [rule.threat.tactic]
61     id = "TA0002"
62     name = "Execution"
63     reference = "https://attack.mitre.org/tactics/TA0002/"
64     [[rule.threat]]
65     framework = "MITRE ATT&CK"
66     [[rule.threat.technique]]
67     id = "T1071"
68     name = "Application Layer Protocol"
69     reference = "https://attack.mitre.org/techniques/T1071/"
70     [[rule.threat.technique.subtechnique]]
71     id = "T1071.001"
72     name = "Web Protocols"
73     reference = "https://attack.mitre.org/techniques/T1071/001/"
74
75
76
77     [rule.threat.tactic]
78     id = "TA0011"
79     name = "Command and Control"
80     reference = "https://attack.mitre.org/tactics/TA0011/"
```