










 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_initial_access_suspicious_browser_childproc.toml 

 terrancedejesus and Mikaayenson [FR] Add Endpoint, APM and...

 4312d8c · 2 years ago

 History

CodeBlame79 lines (70 loc) · 2.63 KB

Raw







```
1  [metadata]
2  creation_date = "2020/12/23"
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 Identifies the execution of a suspicious browser child process. Adversaries may gain ac
13 visiting a website over the normal course of browsing. With this technique, the user's
14 for exploitation.
15 ""
16 from = "now-9m"
17 index = ["logs-endpoint.events.*"]
18 language = "eql"
19 license = "Elastic License v2"
20 name = "Suspicious Browser Child Process"
21 references = [
22     "https://objective-see.com/blog/blog_0x43.html",
23     "https://fr.slideshare.net/codeblue_jp/cb19-recent-apt-attack-on-crypto-exchange-em
24 ]
25 risk_score = 73
26 rule_id = "080bc66a-5d56-4d1f-8071-817671716db9"
27 severity = "high"
28 tags = ["Elastic", "Host", "macOS", "Threat Detection", "Initial Access", "Execution"]
29 timestamp_override = "event.ingested"
30 type = "eql"
31
32 query = '''
33 process where event.type in ("start", "process_started") and
34     process.parent.name : ("Google Chrome", "Google Chrome Helper*", "firefox", "Opera",
35     process.name : ("sh", "bash", "dash", "ksh", "tcsh", "zsh", "curl", "wget", "python*"
36     process.command_line != null and
37     not process.command_line : "*/Library/Application Support/Microsoft/MAU*/Microsoft Au
38     not process.args :
39         (
40             "hw.model",
41             "IOPlatformExpertDevice",
42             "/Volumes/Google Chrome/Google Chrome.app/Contents/Frameworks/*/Resources/install
43             "--defaults-torrc",
44             "*Chrome.app",
45             "Framework.framework/Versions/*/Resources/keystone_promote_preflight.sh",
46             "/Users/*/Library/Application Support/Google/Chrome/recovery/*/ChromeRecovery",
47             "$DISPLAY",
48             "*GIO_LAUNCHED_DESKTOP_FILE_PID=$$",
49             "/opt/homebrew/*",
50             "/usr/local/*brew*"
51         )
52     '''
53
54
55 [[rule.threat]]
56 framework = "MITRE ATTACK"
```

- 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 framework = "MITRE ATT&CK"
57 [[rule.threat.technique]]
58 id = "T1203"
59 name = "Exploitation for Client Execution"
60 reference = "https://attack.mitre.org/techniques/T1203/"
61
62
63 [rule.threat.tactic]
64 id = "TA0002"
65 name = "Execution"
66 reference = "https://attack.mitre.org/tactics/TA0002/"
67 [[rule.threat]]
68 framework = "MITRE ATT&CK"
69 [[rule.threat.technique]]
70 id = "T1189"
71 name = "Drive-by Compromise"
72 reference = "https://attack.mitre.org/techniques/T1189/"
73
74
75 [rule.threat.tactic]
76 id = "TA0001"
77 name = "Initial Access"
78 reference = "https://attack.mitre.org/tactics/TA0001/"
```