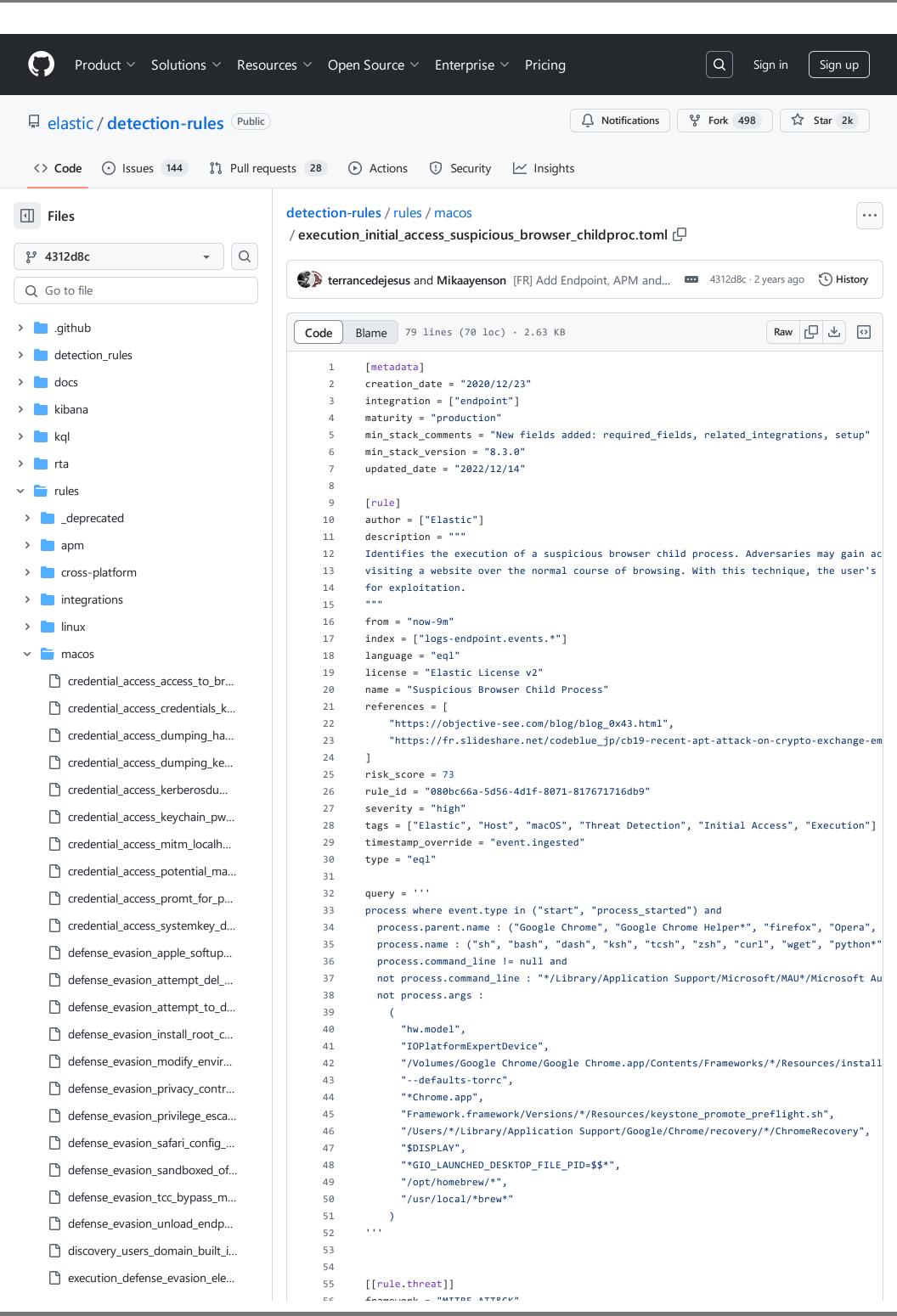
rules/blob/4312d8c9583be524578a14fe6295c3370b9a9307/rules/macos/execution initial access suspicious browser childproc.toml



rules/blob/4312d8c9583be524578a14fe6295c3370b9a9307/rules/macos/execution\_initial\_access\_suspicious\_browser\_childproc.toml

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

```
III alliework = PITINE ALLOCK
סכ
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]]
       framework = "MITRE ATT&CK"
68
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"
       reference = "https://attack.mitre.org/tactics/TA0001/"
```