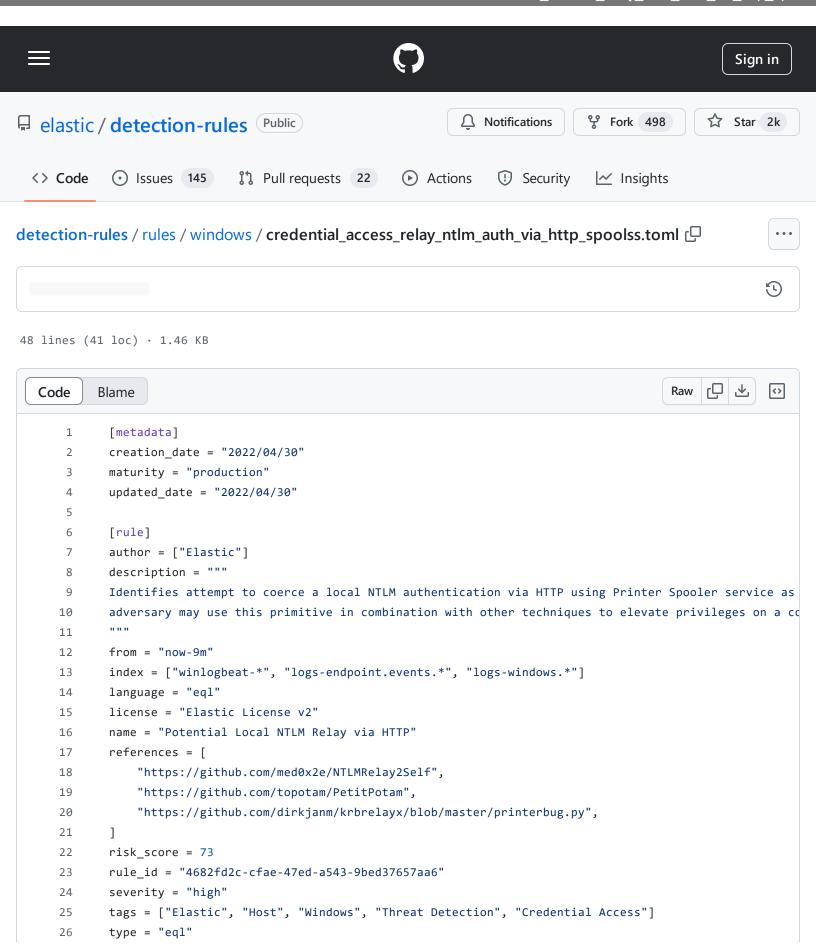
detection-rules/rules/windows/credential_access_relay_ntlm_auth_via_http_spoolss.toml at dd224fb3f81d0b4bf8593c5f02a029d647ba2b2d · elastic/detection-rules · GitHub - 31/10/2024 19:09 https://github.com/elastic/detection-

rules/blob/dd224fb3f81d0b4bf8593c5f02a029d647ba2b2d/rules/windows/credential access relay ntlm auth via http spools



detection-rules/rules/windows/credential_access_relay_ntlm_auth_via_http_spoolss.toml at dd224fb3f81d0b4bf8593c5f02a029d647ba2b2d · elastic/detection-rules · GitHub - 31/10/2024 19:09 https://github.com/elastic/detection-

rules/blob/dd224fb3f81d0b4bf8593c5f02a029d647ba2b2d/rules/windows/credential_access_relay_ntlm_auth_via_http_spools

```
27
28
       query = '''
       process where event.type in ("start", "process_started") and
29
         process.name : "rundll32.exe" and
30
31
         /* relay to HTTP via spoolss or srvsvc pipes */
         process.command_line : ("*davclnt.dll*http*spoolss*", "*davclnt.dll*http*pipe*srvsvc", "*davclnt.
32
       \mathbf{r}_{-1}, \mathbf{r}_{-1}
33
34
35
       [[rule.threat]]
36
37
       framework = "MITRE ATT&CK"
       [[rule.threat.technique]]
38
39
       id = "T1212"
       name = "Exploitation for Credential Access"
40
       reference = "https://attack.mitre.org/techniques/T1212/"
41
42
43
44
       [rule.threat.tactic]
       id = "TA0006"
45
46
       name = "Credential Access"
       reference = "https://attack.mitre.org/tactics/TA0006/"
47
```