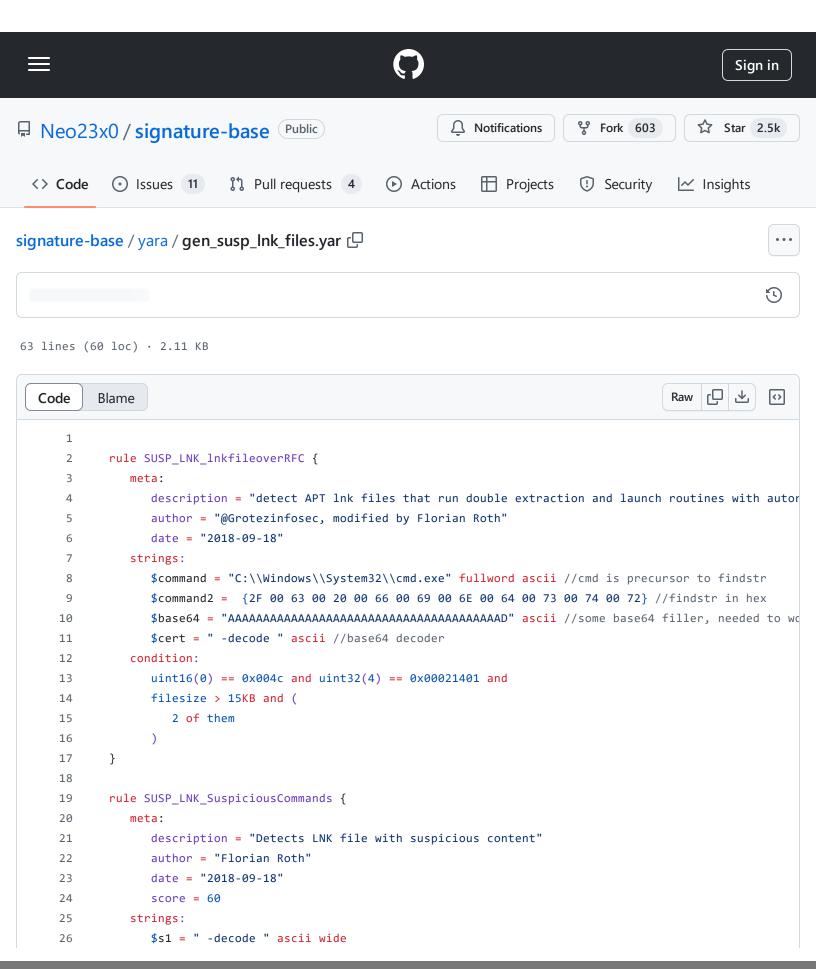
signature-base/yara/gen_susp_Ink_files.yar at 615bf1f6bac3c1bdc417025c40c073e6c2771a76 · Neo23x0/signature-base · GitHub - 31/10/2024 20:21 https://github.com/Neo23x0/signature-base/blob/615bf1f6bac3c1bdc417025c40c073e6c2771a76/yara/gen susp lnk files.yar#L19



```
27
             $s2 = " -enc " ascii wide
28
             $s3 = " -w hidden " ascii wide
             $s4 = " -ep bypass " ascii wide
29
             $s5 = " -noni " ascii nocase wide
30
             /* $s6 = " bypass " ascii wide */
31
             $s7 = " -noprofile " ascii wide
32
             $s8 = ".DownloadString(" ascii wide
33
             $s9 = ".DownloadFile(" ascii wide
34
             $s10 = "IEX(" ascii wide
35
             $s11 = "iex(" ascii wide
36
             $s12 = "WScript.shell" ascii wide fullword nocase
37
             $s13 = " -nop " ascii wide
38
             $s14 = "&tasklist>"
39
             $s15 = "setlocal EnableExtensions DisableDelayedExpansion"
40
             $s16 = "echo^ set^"
41
             $s17 = "del /f /q "
42
             $s18 = " echo | start "
43
             $s19 = "\&\& echo"
44
             $s20 = "&&set "
45
             $s21 = "%&&@echo off "
46
47
          condition:
             uint16(0) == 0x004c and 1 of them
48
49
       }
50
51
       rule SUSP_DOC_LNK_in_ZIP {
52
53
             description = "Detects suspicious .doc.lnk file in ZIP archive"
54
             author = "Florian Roth"
             reference = "https://twitter.com/RedDrip7/status/1145877272945025029"
55
             date = "2019-07-02"
56
57
             score = 50
             hash1 = "7ea4f77cac557044e72a8e280372a2abe072f2ad98b5a4fbed4e2229e780173a"
58
59
             $s1 = ".doc.lnk" fullword ascii
60
          condition:
61
             uint16(0) == 0x4b50 and 1 of them
62
63
       }
```