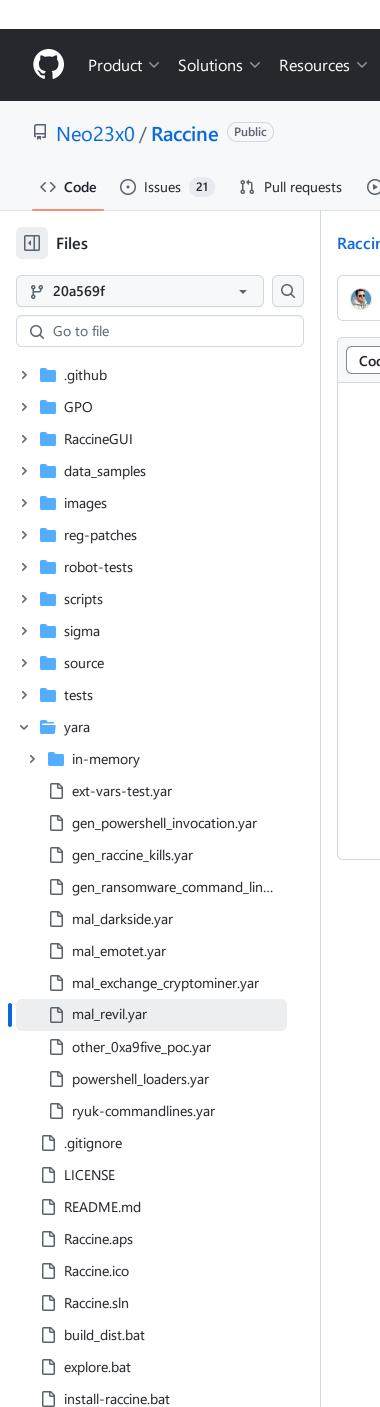
Open Source >



```
Actions
                  Security
                                ✓ Insights
Raccine / yara / mal_revil.yar 🖵
  Neo23x0 Update mal_revil.yar
                                                                        dc8b92d · 4 years ago
                                                                                           History
                    23 lines (21 loc) · 1.05 KB
                                                                                                 <>
   Code
           Blame
       1
             rule MAL_REvil_Dec20 {
       2
                meta:
       3
                   description = "Detects PowerShell invocation as used by REvil loader"
                   author = "Florian Roth"
                   date = "2020-12-02"
       5
                   reference = "https://app.any.run/tasks/b5146ffd-328f-4d6f-9bf7-c544d02f1d47/"
       6
                   score = 60
                strings:
       8
       9
                     /* Encoded Command */
      10
                     $ = " -Enc \"PAA" ascii
      11
      12
                     /* [Reflection.Assembly]::Load( */
                         "WwBSAGUAZgBsAGUAYwB0AGkAbwBuAC4AQQBzAHMAZQBtAGIAbAB5AF0AOgA6AEwAbwBhAGQAKA
      13
                         "sAUgBlAGYAbABlAGMAdABpAG8AbgAuAEEAcwBzAGUAbQBiAGwAeQBdADoAOgBMAG8AYQBkACgA
      14
                         "bAFIAZQBmAGwAZQBjAHQAaQBvAG4ALgBBAHMAcwBlAG0AYgBsAHkAXQA6ADoATABvAGEAZAAoA
      15
      16
      17
                     /* Win32_Shadowcopy | ForEach-Object */
                         "VwBpAG4AMwAyAF8AUwBoAGEAZABvAHcAYwBvAHAAeQAgAHwAIABGAG8AcgBFAGEAYwBoAC0ATw
      18
      19
                         "cAaQBuADMAMgBfAFMAaABhAGQAbwB3AGMAbwBwAHkAIAB8ACAARgBvAHIARQBhAGMAaAAtAE8A
      20
                         "XAGkAbgAzADIAXwBTAGgAYQBkAG8AdwBjAG8AcAB5ACAAfAAgAEYAbwByAEUAYQBjAGgALQBPA
      21
                condition:
      22
                   1 of them
      23
             }
```

Pricing

Notifications

Enterprise ~

Q

앟 Fork 122

Sign in

Sign up

☆ Star 945

Raccine/yara/mal_revil.yar at 20a569fa216250 https://github.com/Neo23x0/Raccine/blob/20a56	086433dcce8bb2765d0ea08dcb6 · Neo23x0/Rac 39fa21625086433dcce8bb2765d0ea08dcb6/yara/m	cine · GitHub - 02/11/2024 16:06 al_revil.yar