Sign in

Neo23x0 / Raccine Public

Notifications Fork 122 Star 945

Code Issues 21 Pull requests Actions Security Insights

Raccine / yara / mal_revil.yar

23 lines (21 loc) · 1.05 KB

Code Blame Raw

```
rule MAL_REvil_Dec20 {
   meta:
      description = "Detects PowerShell invocation as used by REvil loader"
      author = "Florian Roth"
      date = "2020-12-02"
      reference = "https://app.any.run/tasks/b5146ffd-328f-4d6f-9bf7-c544d02f1d47/"
      score = 60
   strings:
        /* Encoded Command */
        $ = " -Enc \"PAA" ascii

        /* [Reflection.Assembly]::Load( */
        $ = "WwBSAGUAZgBsAGUAYwB0AGkAbwBuAC4AQQBzAHMAZQBtAGIAbAB5AF0AOgA6AEwAbwBhAGQAKA" ascii
        $ = "sAUgBlAGYAbABlAGMAdABpAG8AbgAuAEEAcwBzAGUAbQBiAGwAeQBdADoAOgBMAG8AYQBkACgA" ascii
        $ = "bAFIAZQBmAGwAZQBjAHQAaQBvAG4ALgBBAHMAcwBlAG0AYgBsAHkAXQA6ADoATABvAGEAZAAoA" ascii

        /* Win32_Shadowcopy | ForEach-Object */
        $ = "VwBpAG4AMwAyAF8AUwBoAGEAZABvAHcAYwBvAHAAeQAgAHwAIABGAG8AcgBFAGEAYwBoAC0ATwBiAGoAZQBjA
        $ = "cAaQBuADMAMgBfAFMAaABhAGQAbwB3AGMAbwBwAHkAIAB8ACAARgBvAHIARQBhAGMAaAAtAE8AYgBqAGUAYwB
        $ = "XAGkAbgAzADIAXwBTAGgAYQBkAG8AdwBjAG8AcAB5ACAAfAAgAEYAbwByAEUAYQBjAGgALQBPAGIAagBlAGMA
   condition:
      1 of them
}
```