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

```
 1    rule MAL_REvil_Dec20 {
 2      meta:
 3        description = "Detects PowerShell invocation as used by REvil loader"
 4        author = "Florian Roth"
 5        date = "2020-12-02"
 6        reference = "https://app.any.run/tasks/b5146ffd-328f-4d6f-9bf7-c544d02f1d47/"
 7        score = 60
 8      strings:
 9        /* Encoded Command */
10        $ = " -Enc \"PAA" ascii
11
12        /* [Reflection.Assembly]::Load( */
13        $ = "WwBSAGUAZgBsAGUAYwB0AGkAbwBuAC4AQQBzAHMAZQBtAGIAbAB5AF0AOgA6AEwAbwBhAGQAKA" ascii
14        $ = "sAUgBlAGYAbABlAGMAdABpAG8AbgAuAEEAcwBzAGUAbQBiAGwAeQBdADoAOgBMAG8AYQBkACgA" ascii
15        $ = "bAFIAZQBmAGwAZQBjAHQAaQBvAG4ALgBBAHMAcwBlAG0AYgBsAHkAXQA6ADoATABvAGEAZAAoA" ascii
16
17        /* Win32_Shadowcopy | ForEach-Object */
18        $ = "VwBpAG4AMwAyAF8AUwBoAGEAZABvAHcAYwBvAHAAeQAgAHwAIABGAG8AcgBFAGEAYwBoAC0ATwBiAGoAZQBjAH
19        $ = "cAaQBuADMAMgBfAFMAaABhAGQQAbwB3AGMAbwBwAHkAIAB8ACAARgBvAHIARQBhAGMAaAAtAE8AYgBqAGUAYwB0
20        $ = "XAGkAbgAzADIAXwBTAGgAYQBkAG8AdwBjAG8AcAB5ACAAfAAgAEYAbwByAEUAYQBjAGgALQBPAGIAagBlAGMAd
21      condition:
22        1 of them
23    }
```