Files

20a569f

Go to file

.github
GPO
RaccineGUI
data_samples
images
reg-patches
robot-tests
scripts
sigma
source
tests
yara
in-memory
ext-vars-test.yar
gen_powershell_invocation.yar
gen_raccine_kills.yar
gen_ransomware_command_lin...
mal_darkside.yar
mal_emotet.yar
mal_exchange_cryptominer.yar
mal_revil.yar
other_0xa9five_poc.yar
powershell_loaders.yar
ryuk-commandlines.yar
.gitignore
LICENSE
README.md
Raccine.aps
Raccine.ico
Raccine.sln
build_dist.bat
explore.bat
install-raccine.bat

Raccine / yara / mal_revil.yar

Neo23x0 Update mal_revil.yar dc8b92d · 4 years ago History

Code Blame 23 lines (21 loc) · 1.05 KB 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
14       $ = "sAUgBlAGYAbABlAGMAdABpAG8AbgAuAEEAcwBzAGUAbQBiAGwAeQBdADoAOgBMAG8AYQBkACgA
15       $ = "bAFIAZQBmAGwAZQBjAHQAaQBvAG4ALgBBAHMAcwBlAG0AYgBsAHkAXQA6ADoATABvAGEAZAAoA
16
17       /* Win32_Shadowcopy | ForEach-Object */
18       $ = "VwBpAG4AMwAyAF8AUwBoAGEAZABvAHcAYwBvAHAAeQAgAHwAIABGAG8AcgBFAGEAYwBoAC0ATw
19       $ = "cAaQBuADMAMgBfAFMAaABhAGQAbwB3AGMAbwBwAHkAIAB8ACAARgBvAHIARQBhAGMAaAAtAE8A
20       $ = "XAGkAbgAzADIAXwBTAGgAYQBkAG8AdwBjAG8AcAB5ACAAfAAgAEYAbwByAEUAYQBjAGgALQBPA
21    condition:
22       1 of them
23 }
```