Product ▾Solutions ▾Resources ▾Open Source ▾Enterprise ▾Pricing

🔍

Sign in

Sign up

📄

Neo23x0 / signature-base

Public

🔔

Notifications

🍴

Fork

604

★

Star

2.5k

<>

Code

🔗

Issues

11

🔗

Pull requests

4

🔄

Actions

📁

Projects

🛡️

Security

📊

Insights

signature-base / yara / gen_susp_lnk_files.yar

...

Neo23x0 fix: FPs


88f3af3 · 3 years ago

🕒

History

📁

Files

615bf1f

🔍

🔍

Go to file

signature-base / yara / gen_susp_lnk_files.yar

↑ Top

Code

Blame

63 lines (60 loc) · 2.11 KB







Raw

📄

📥

🔗

```
5      author = "@GroteziNt0sec, modified by Florian Roth"
6      date = "2018-09-18"
7      strings:
8          $command = "C:\\Windows\\System32\\cmd.exe" fullword ascii //cmd is precursor to
9          $command2 = {2F 00 63 00 20 00 66 00 69 00 6E 00 64 00 73 00 74 00 72} //findstr
10         $base64 = "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAD" ascii //some base64 filler,
11         $cert = " -decode " ascii //base64 decoder
12     condition:
13         uint16(0) == 0x004c and uint32(4) == 0x00021401 and
14         filesize > 15KB and (
15             2 of them
16         )
17     }
18
19     ... rule SUSP_LNK_SuspiciousCommands {
20         meta:
21             description = "Detects LNK file with suspicious content"
22             author = "Florian Roth"
23             date = "2018-09-18"
24             score = 60
25         strings:
26             $s1 = " -decode " ascii wide
27             $s2 = " -enc " ascii wide
28             $s3 = " -w hidden " ascii wide
29             $s4 = " -ep bypass " ascii wide
30             $s5 = " -noni " ascii nocase wide
31             /* $s6 = " bypass " ascii wide */
32             $s7 = " -nopprofile " ascii wide
33             $s8 = ".DownloadString(" ascii wide
34             $s9 = ".DownloadFile(" ascii wide
35             $s10 = "IEX(" ascii wide
36             $s11 = "iex(" ascii wide
37             $s12 = "WScript.shell" ascii wide fullword nocase
38             $s13 = " -nop " ascii wide
39             $s14 = "&tasklist>"
40             $s15 = "setlocal EnableExtensions DisableDelayedExpansion"
41             $s16 = "echo^ set^"
42             $s17 = "del /f /q "
43             $s18 = " echo | start "
44             $s19 = "&& echo "
45             $s20 = "&&set "
46             $s21 = "%&&&echo off "
47         condition:
48             uint16(0) == 0x004c and 1 of them
49     }
50
51     rule SUSP_DOC_LNK_in_ZIP {
52         meta:
53             description = "Detects suspicious .doc.lnk file in ZIP archive"
54             author = "Florian Roth"
55             reference = "https://twitter.com/RedDrip7/status/1145877272945025029"
56             date = "2019-07-02"
57             score = 50
```

-  general_cloaking.yar
-  general_officemacros.yar
-  generic_anomalies.yar
-  generic_cryptors.yar
-  generic_dumps.yar
-  generic_exe2hex_payload.yar

```
57         score = 50
58         hash1 = "7ea4f77cac557044e72a8e280372a2abe072f2ad98b5a4fbed4e2229e780173a"
59         strings:
60             $s1 = ".doc.lnk" fullword ascii
61         condition:
62             uint16(0) == 0x4b50 and 1 of them
63     }
```