in2al5dp3in4er Loader

Published: 2023-04-23 · Archived: 2026-04-05 15:54:25 UTC

Aurora Stealer

The extracted 2nd stage is the golang stealer sold as "Aurora Stealer" malpedia.

`21545028cac12fc9e8692a71247040718e6d640ee6117d1b19f4521f886586be` UnpacMe

Packer ID

We can make a simple yara rule based on the following

riid for `CreateDXGIFactory` call

```
EC 66 71 7B C7 21 AE 44 B2 1A C9 AE 32 1A E3 69
```

imports

`CreateDXGIFactory` from `DXGI.dll`

checks

```
 cmp     eax, 887A0002h
3D 02 00 7A 88
```

gfx whitelist ids

```
{29 9? 01 00}
```

Rule

```
 import "pe"
import "math"

rule riid_hunt {

    strings:
        $riid = { EC 66 71 7B C7 21 AE 44 B2 1A C9 AE 32 1A E3 69 }
        $embarcadero = "This program must be run under Win32" ascii
        $import = "CreateDXGIFactory" ascii wide
```

```
    condition:
        all of them and
        for any i in (0..(pe.number_of_sections)-1) :
        (
           pe.sections[i].name == ".data" and
            math.entropy(pe.sections[i].raw_data_offset, pe.sections[i].raw_data_size) >= 7
        )

}
```

```
 48 8D 05   9A 94 16 00                                  lea     rax, blob
48 B9   EE EE DE DD CD CC BB 0A                         mov     rcx, 0ABBCCCDDDDEEEEEh
48 BA   55 55 45 44 34 23 12 00                         mov     rdx, 12233444455555h
49 B8   CC CC B3 BB A2 1A 00 00                         mov     r8, 1AA2BBB3CCCCh
4C    63 4D E0                                          movsxd  r9, [rbp+var_20]
```

```
 48 8D 05   D1 93 16 00                                  lea     rax, blob
48 B9   81 FD A9 98 F6 50 00 00                         mov     rcx, 50F698A9FD81h
48 BA   1B 06 AC 5D DE F8 ED 00                         mov     rdx, 0EDF8DE5DAC061Bh
49 B8   04 68 7C AA 99 9D 0B 00                         mov     r8, 0B9D99AA7C6804h
4C   63 4D E8                                           movsxd  r9, [rbp+var_18]
```

Source: https://research.openanalysis.net/in2al5dp3in4er/loader/analysis/sandbox/invalid%20printer/2023/04/23/in2al5dp3in4er.html