SideWinder

malpedia.caad.fkie.fraunhofer.de/details/win.sidewinder

win.sidewinder

There is no description at this point.

References

Medium (@CDSO_CyTec) DCSO CyTec

SideWinder

Malpedia Malpedia

SideWinder SideWinder

AlienVault Tom Hegel

8.t Dropper Koadic SideWinder

Trend Micro Joseph C Chen Jaromír Hořejší Ecular Xu

Meterpreter SideWinder SideWinder

AlienVault OTX AlienVault

SideWinder SideWinder

Qianxin Threat Intelligence Center

SideWinder

Qianxin Threat Intelligence Center

SideWinder

Tencent Tencent Yujian Threat Intelligence Center

SideWinder SideWinder

Medium Sebdraven Sébastien Larinier

SideWinder SideWinder

Tencent Tencent Mimi Threat Intelligence Center

SideWinder SideWinder

Yara Rules

```
rule win_sidewinder_auto {

    meta:
        author = "Felix Bilstein - yara-signator at cocacoding dot com"
        date = "2022-04-08"
        version = "1"
        description = "Detects win.sidewinder."
        info = "autogenerated rule brought to you by yara-signator"
        tool = "yara-signator v0.6.0"
        signator_config = "callsandjumps;datarefs;binvalue"
        malpedia_reference =
"https://malpedia.caad.fkie.fraunhofer.de/details/win.sidewinder"
        malpedia_rule_date = "20220405"
        malpedia_hash = "ecd38294bd47d5589be5cd5490dc8bb4804afc2a"
        malpedia_version = "20220411"
        malpedia_license = "CC BY-SA 4.0"
        malpedia_sharing = "TLP:WHITE"

    /* DISCLAIMER
     * The strings used in this rule have been automatically selected from the
     * disassembly of memory dumps and unpacked files, using YARA-Signator.
     * The code and documentation is published here:
     * https://github.com/fxb-cocacoding/yara-signator
     * As Malpedia is used as data source, please note that for a given
     * number of families, only single samples are documented.
     * This likely impacts the degree of generalization these rules will offer.
     * Take the described generation method also into consideration when you
     * apply the rules in your use cases and assign them confidence levels.
     */


    strings:
        $sequence_0 = { e8???????? 898510ffffff eb07 83a510ffffff00 8d4dc4
e8???????? e9???????? }
            // n = 7, score = 200
            //   e8????????           |
            //   898510ffffff         | mov                 dword ptr [ebp -
0xf0], eax
            //   eb07                 | jmp                 9
            //   83a510ffffff00       | and                 dword ptr [ebp -
0xf0], 0
            //   8d4dc4               | lea                 ecx, dword ptr [ebp -
0x3c]
            //   e8????????           |
            //   e9????????           |

        $sequence_1 = { 51 51 68???????? 64a100000000 50 64892500000000 6a28 }
            // n = 7, score = 200
            //   51                   | push                ecx
            //   51                   | push                ecx
            //   68????????           |
            //   64a100000000         | mov                 eax, dword ptr fs:[0]
            //   50                   | push                eax
            //   64892500000000       | mov                 dword ptr fs:[0], esp
            //   6a28                 | push                0x28

        $sequence_2 = { 6a78 68???????? ff75e4 ff75d0 e8???????? 89852cffffff
eb07 }
            // n = 7, score = 200
            //   6a78                 | push                0x78
            //   68????????           |
            //   ff75e4               | push                dword ptr [ebp -
```

```
0x1c]
            //   ff75d0              | push                dword ptr [ebp -
0x30]
            //   e8????????          |
            //   89852cffffff        | mov                 dword ptr [ebp -
0xd4], eax
            //   eb07                | jmp                 9

        $sequence_3 = { 89458c eb04 83658c00 8d45d4 50 8b45e8 }
            // n = 6, score = 200
            //   89458c              | mov                 dword ptr [ebp -
0x74], eax
            //   eb04                | jmp                 6
            //   83658c00            | and                 dword ptr [ebp -
0x74], 0
            //   8d45d4              | lea                 eax, dword ptr [ebp -
0x2c]
            //   50                  | push                eax
            //   8b45e8              | mov                 eax, dword ptr [ebp -
0x18]

        $sequence_4 = { 83a59cfdffff00 ff75d0 e8???????? 8bd0 8d4ddc e8????????
8d4dd0 }
            // n = 7, score = 200
            //   83a59cfdffff00      | and                 dword ptr [ebp -
0x264], 0
            //   ff75d0              | push                dword ptr [ebp -
0x30]
            //   e8????????          |
            //   8bd0                | mov                 edx, eax
            //   8d4ddc              | lea                 ecx, dword ptr [ebp -
0x24]
            //   e8????????          |
            //   8d4dd0              | lea                 ecx, dword ptr [ebp -
0x30]

        $sequence_5 = { 8bec 83ec14 68???????? 64a100000000 50 64892500000000
b8b8000000 }
            // n = 7, score = 200
            //   8bec                | mov                 ebp, esp
            //   83ec14              | sub                 esp, 0x14
            //   68????????          |
            //   64a100000000        | mov                 eax, dword ptr fs:[0]
            //   50                  | push                eax
            //   64892500000000      | mov                 dword ptr fs:[0], esp
            //   b8b8000000          | mov                 eax, 0xb8

        $sequence_6 = { 7d23 6890000000 68???????? ffb550ffffff ffb54cffffff
e8???????? 89859cfeffff }
            // n = 7, score = 200
            //   7d23                | jge                 0x25
            //   6890000000          | push                0x90
            //   68????????          |
            //   ffb550ffffff        | push                dword ptr [ebp -
0xb0]
            //   ffb54cffffff        | push                dword ptr [ebp -
0xb4]
            //   e8????????          |
            //   89859cfeffff        | mov                 dword ptr [ebp -
0x164], eax

        $sequence_7 = { 8d45d8 50 8b45c4 8b00 ff75c4 ff5024 dbe2 }
```

```
            // n = 7, score = 200
            //   8d45d8               | lea                 eax, dword ptr [ebp -
0x28]
            //   50                   | push                eax
            //   8b45c4               | mov                 eax, dword ptr [ebp -
0x3c]
            //   8b00                 | mov                 eax, dword ptr [eax]
            //   ff75c4               | push                dword ptr [ebp -
0x3c]
            //   ff5024               | call                dword ptr [eax +
0x24]
            //   dbe2                 | fnclex

        $sequence_8 = { 8b4508 6683603400 8b4508 8b00 ff7508 ff5044 e9???????? }
            // n = 7, score = 200
            //   8b4508               | mov                 eax, dword ptr [ebp +
8]
            //   6683603400           | and                 word ptr [eax +
0x34], 0
            //   8b4508               | mov                 eax, dword ptr [ebp +
8]
            //   8b00                 | mov                 eax, dword ptr [eax]
            //   ff7508               | push                dword ptr [ebp + 8]
            //   ff5044               | call                dword ptr [eax +
0x44]
            //   e9????????           |

        $sequence_9 = { eb07 83a560ffffff00 8d4dcc e8???????? 8d4dbc e8????????
e9???????? }
            // n = 7, score = 200
            //   eb07                 | jmp                 9
            //   83a560ffffff00       | and                 dword ptr [ebp -
0xa0], 0
            //   8d4dcc               | lea                 ecx, dword ptr [ebp -
0x34]
            //   e8????????           |
            //   8d4dbc               | lea                 ecx, dword ptr [ebp -
0x44]
            //   e8????????           |
            //   e9????????           |

    condition:
        7 of them and filesize < 679936
}
```

Download all Yara Rules