GraphSteel

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

win.graphsteel

This malware was seen during the cyberattacks on Ukrainian state organizations. It is one of two used backdoors written in Go and attributed to UAC-0056 (SaintBear, UNC2589, TA471).

References

InQuest Will MacArthur Nick Chalard

CyclopsBlink Cobalt Strike GraphSteel GrimPlant HermeticWiper HermeticWizard MicroBackdoor PartyTicket Saint Bot Scieron WhisperGate

Malpedia Malpedia

GraphSteel SaintBear

Intezer Joakim Kennedy Nicole Fishbein

GraphSteel GrimPlant SaintBear

GovInfo Security Prajeet Nair

GraphSteel GrimPlant

Cert-UA Cert-UA

GraphSteel GrimPlant SaintBear

GOV.UA State Service of Special Communication and Information Protection of Ukraine (CIP)

Xloader Agent Tesla CaddyWiper Cobalt Strike DoubleZero GraphSteel GrimPlant HeaderTip HermeticWiper IsaacWiper MicroBackdoor Pandora

SentinelOne Amitai Ben Shushan Ehrlich

Cobalt Strike GraphSteel GrimPlant SaintBear

Yara Rules

```
rule win_graphsteel_auto {

    meta:
        author = "Felix Bilstein - yara-signator at cocacoding dot com"
        date = "2022-04-08"
        version = "1"
        description = "Detects win.graphsteel."
        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.graphsteel"
        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 = { 8b8c2484000000 8d42ff 85c9 0f49c1 498b4d00 80796100
4189c3 }
            // n = 7, score = 100
            //   8b8c2484000000       | pop                 edi
            //   8d42ff               | pop                 ebp
            //   85c9                 | ja                  0xca
            //   0f49c1               | dec                 eax
            //   498b4d00             | mov                 esi, 0x3e01
            //   80796100             | add                 eax, 0x48000003
            //   4189c3               | bt                  esi, edx

        $sequence_1 = { ff15???????? 48c7434000000000 ff15???????? 4c8b4b30
b90a180000 c74424202ab30000 894320 }
            // n = 7, score = 100
            //   ff15????????         |
            //   48c7434000000000     | lea                 eax, dword ptr
[0x3cc23b]
            //   ff15????????         |
            //   4c8b4b30             | dec                 eax
            //   b90a180000           | mov                 ebp, dword ptr [esp +
0xb8]
            //   c74424202ab30000     | dec                 eax
            //   894320               | add                 esp, 0xc0

        $sequence_2 = { eb0e 488d7848 488b4c2418 e8???????? 4889c3 488d05eebd4f00
488b6c2420 }
            // n = 7, score = 100
            //   eb0e                 | dec                 ecx
            //   488d7848             | mov                 ecx, dword ptr [edi +
0x50]
```

```
            //   488b4c2418           | mov                 eax, 2
            //   e8????????           |
            //   4889c3               | xor                 ebx, ebx
            //   488d05eebd4f00       | mov                 dword ptr [esp +
0x124], 0
            //   488b6c2420           | mov                 dword ptr [esp +
0xa0], 0

        $sequence_3 = { 8b430c 39f8 0f8fc5000000 c7430cffffffff 85ff 0f8efc000000
0f1f440000 }
            // n = 7, score = 100
            //   8b430c               | mov                 ecx, dword ptr [ebx +
0x10]
            //   39f8                 | dec                 eax
            //   0f8fc5000000         | mov                 ecx, dword ptr [ebx]
            //   c7430cffffffff       | dec                 esp
            //   85ff                 | lea                 eax, dword ptr [ebx +
0x28]
            //   0f8efc000000         | jne                 0x4a
            //   0f1f440000           | mov                 edx, 1

        $sequence_4 = { 8b8424f8000000 89742428 398424f0000000 8b442458 89442420
0f84fe080000 448b842488000000 }
            // n = 7, score = 100
            //   8b8424f8000000       | inc                 eax
            //   89742428             | movzx               edx, dh
            //   398424f0000000       | jmp                 0x351
            //   8b442458             | lea                 esi, dword ptr [edx -
0x41]
            //   89442420             | nop
            //   0f84fe080000         | inc                 eax
            //   448b842488000000     | cmp                 dh, 5

        $sequence_5 = { 754a 80b9a000000000 6690 753f 488d05d7153e00 e8????????
48c7400850000000 }
            // n = 7, score = 100
            //   754a                 | cmp                 byte ptr [edx], 0xa4
            //   80b9a000000000       | dec                 eax
            //   6690                 | mov                 ebx, edx
            //   753f                 | je                  0x1f37
            //   488d05d7153e00       | xor                 eax, eax
            //   e8????????           |
            //   48c7400850000000     | dec                 eax

        $sequence_6 = { 498b07 4c89f9 ff5020 4c89e2 4c89e9 4883c428 415c }
            // n = 7, score = 100
            //   498b07               | dec                 ebp
            //   4c89f9               | imul                eax, eax, 0xa6f7d
            //   ff5020               | dec                 esp
            //   4c89e2               | sub                 eax, eax
            //   4c89e9               | dec                 edi
            //   4883c428             | lea                 eax, dword ptr [edi]
            //   415c                 | dec                 ebp

        $sequence_7 = { 898424e8000000 85c0 0f8534010000 488b0b 448b7914 4585ff
0f89b4feffff }
            // n = 7, score = 100
            //   898424e8000000       | jne                 0x4d
            //   85c0                 | dec                 eax
            //   0f8534010000         | lea                 edx, dword ptr [esp +
0xd0]
            //   488b0b               | mov                 ecx, 4
```

```
            //   448b7914            | jne                 0x65
            //   4585ff              | inc                 esp
            //   0f89b4feffff        | movzx               eax, byte ptr [ecx +
1]

        $sequence_8 = { eb2d 4889c8 4889fb 4889d1 e8???????? 83f001 488b4c2450 }
            // n = 7, score = 100
            //   eb2d                | dec                 eax
            //   4889c8              | stosd               dword ptr es:[edi],
eax
            //   4889fb              | dec                 eax
            //   4889d1              | mov                 dword ptr [esp +
0x30], 0
            //   e8????????          |
            //   83f001              | dec                 eax
            //   488b4c2450          | mov                 dword ptr [esp +
0x38], 0

        $sequence_9 = { b981000000 e8???????? 488d05673d5c00 bb1e000000
e8???????? 90 4889442408 }
            // n = 7, score = 100
            //   b981000000          | cmp                 ecx, edx
            //   e8????????          |
            //   488d05673d5c00      | je                  0xf8b
            //   bb1e000000          | dec                 eax
            //   e8????????          |
            //   90                  | lea                 edx, dword ptr [ecx +
1]
            //   4889442408          | cmp                 dl, 0x2e

    condition:
        7 of them and filesize < 19812352
}
```

Download all Yara Rules