

# Commit eea8326



**MHaggis** committed 3 weeks ago

Add 4 new drivers, 3 sample updates, and 2 data quality fixes from issue triage  
Triaged all 30 open GitHub issues. This PR covers the 9 actionable ones.

### New drivers:

- athpexnt.sys (AhnLab) - arbitrary physical memory r/w via IOCTL 0x81000000, 0/73 VT detection, VeriSign signed. Closes [#255](#)
- STProcessMonitor.sys (Safetica) - [CVE-2025-70795](#), process termination BYOVD, 18 VT execution parents showing active abuse. Closes [#268](#)
- shimano32.sys + shimano64.sys (HyperTech DNP CrackProof) - EPROCESS manipulation via IOCTLs, reported by Wack0. From Shimano E-TUBE bicycle management app. Closes [#163](#)
- tm\_filter.sys + tmfsdrv2.sys (Teramind) - kernel-level input capture drivers from employee monitoring software, abused for stealth keylogging. Closes [#243](#)

### Updated existing entries:

- AMDRyzenMasterDriverV17.sys v1.7.0 sample added to 13973a71, with [CVE-2023-20564](#) PoC link. Closes [#246](#)
- IOMap64.sys new sample (itm4n, CVE-2024-41498) added to f4990bdd. Closes [#201](#)
- WinRing0 entry updated with 2 new sample hashes and OpenHardwareMonitorLib.sys tag. Closes [#253](#), closes [#215](#)

### Data quality fixes:

- Removed non-vulnerable DBUtilDrv2.sys v2.7 (Dell's patched version was incorrectly listed as vulnerable). Closes [#270](#)
- Removed iqvw64e.sys v1.3.2.17 (post-patch version, CVE says before 1.3.1.0 are vulnerable). Closes [#223](#)

All samples downloaded from VT, metadata extracted with lief (Authentihash, TBS certs, Rich PE header, sections, imports). Driver binaries added via git LFS.

**main** (#279)

1 parent [03f48c4](#) commit eea8326

21 files changed

+1,766 -324

Filter files...



.gitattributes

drivers

- 1c57d067b9fc5e9ef9aeb14223481243.bin
- 3f9829071109fc051bd7f6b01a35ed46.bin
- 4da690ba853b12927fafd6b6387828cf.bin
- 5761bd63da03686fc480245da7bd1e9f.bin
- 6a4cced9a784369f50e618d85a16d234.bin
- 845af1ba23c8d5e64def61bcc441604c.bin
- 91717a70db6c7beabbc004bbd9544ae6.bin
- bf77a19e1396d6d36e32ff8d23eb5d3f.bin
- c047c92696e5cef5485a22df97e6646e.bin
- d104621c93213942b7b43d65b5d8d33e.bin
- d8d1c6cd663c9c5a457d8147e10c4e64.bin

yaml

- 0712c54c-69fd-41f2-950a-da678ac51246.yaml
- 13973a71-412f-4a18-a2a6-476d3853f8de.yaml
- 1d2cdef1-de44-4849-80e5-e2fa288df681.yaml
- 651d1cdc-3e13-405f-b8b3-65cc70cef5a8.yaml
- 7bb5ff05-25f8-410d-ae99-c8e8f082d24f.yaml
- 8d23f7e6-341a-431e-9dc1-bc797773d411.yaml
- bb808089-5857-4df2-8998-753a7106cb44.yaml
- f4990bdd-8821-4a3c-a11a-4651e645810c.yaml
- f4e00816-97a8-4c2d-b990-9812f16fe3d3.yaml



Search within code



```

.gitattributes
@@ -6,3 +6,13 @@ drivers/9e82ee5bde6b5d29281a3c280e6d1f2e.bin filter=lfs
diff=lfs merge=lfs -text
6 6 drivers/b96d75a000367c200958089728fc5cb8.bin filter=lfs diff=lfs merge=lfs -text

```

```

7 7 drivers/78fb9882e498d964f42169ce511f07fc.bin filter=-lfs diff=-lfs merge=-lfs -text
8 8 drivers/49d1002443655bc63b8d49fef0b584fd.bin filter=-lfs diff=-lfs merge=-lfs -text
9 + drivers/1c57d067b9fc5e9ef9aeb14223481243.bin filter=-lfs diff=-lfs merge=-lfs -text
10 + drivers/3f9829071109fc051bd7f6b01a35ed46.bin filter=-lfs diff=-lfs merge=-lfs -text
11 + drivers/4da690ba853b12927fafd6b6387828cf.bin filter=-lfs diff=-lfs merge=-lfs -text
12 + drivers/845af1ba23c8d5e64def61bcc441604c.bin filter=-lfs diff=-lfs merge=-lfs -text
13 + drivers/91717a70db6c7beabbc004bbd9544ae6.bin filter=-lfs diff=-lfs merge=-lfs -text
14 + drivers/5761bd63da03686fc480245da7bd1e9f.bin filter=-lfs diff=-lfs merge=-lfs -text
15 + drivers/6a4cced9a784369f50e618d85a16d234.bin filter=-lfs diff=-lfs merge=-lfs -text
16 + drivers/bf77a19e1396d6d36e32ff8d23eb5d3f.bin filter=-lfs diff=-lfs merge=-lfs -text
17 + drivers/c047c92696e5cef5485a22df97e6646e.bin filter=-lfs diff=-lfs merge=-lfs -text
18 + drivers/d8d1c6cd663c9c5a457d8147e10c4e64.bin filter=-lfs diff=-lfs merge=-lfs -text

```

▼ drivers/1c57d067b9fc5e9ef9aeb14223481243.bin ...

... @@ -0,0 +1,3 @@

```

1 + version https://git-lfs.github.com/spec/v1
2 + oid sha256:d5bca2ca464a6cc91344bd85e812a7bac6e7c67038c4929a29e0bc60c7eabe4d
3 + size 33176

```

▼ drivers/3f9829071109fc051bd7f6b01a35ed46.bin ...

... @@ -0,0 +1,3 @@

```

1 + version https://git-lfs.github.com/spec/v1
2 + oid sha256:e9fda504c9bdbe785c55a279ebb27e31783155570ab0c242e1de5bf79fbca6ed
3 + size 100712

```

▼ drivers/4da690ba853b12927fafd6b6387828cf.bin ...

... @@ -0,0 +1,3 @@

```

1 + version https://git-lfs.github.com/spec/v1
2 + oid sha256:e62d0c1353a3d913497e6016d0f48d7c9ef99e4026b94ccd873d6c7a9a54565
3 + size 54752

```

▼ drivers/5761bd63da03686fc480245da7bd1e9f.bin ...

... @@ -0,0 +1,3 @@

```

1 + version https://git-lfs.github.com/spec/v1
2 + oid sha256:5b4f59236a9b950bcd5191b35d19125f60cfb9e1a1e1aa2e4f914b6745dde9df
3 + size 37456

```

▼ drivers/6a4cced9a784369f50e618d85a16d234.bin ...

... @@ -0,0 +1,3 @@

1 + version https://git-lfs.github.com/spec/v1

2 + oid sha256:e8b1a0ddc7a4404eb3c46217e07b5ed91723f44464a6ef589634aeb4fb8f5666

3 + size 14336

▼ drivers/845af1ba23c8d5e64def61bcc441604c.bin ...

... @@ -0,0 +1,3 @@

1 + version https://git-lfs.github.com/spec/v1

2 + oid sha256:206ee7a7c3f4d9496f742ccb84718f556ecb4ba2a95fe7e0cdf3a003ffbe4597

3 + size 14416

▼ drivers/91717a70db6c7beabbc004bbd9544ae6.bin ...

... @@ -0,0 +1,3 @@

1 + version https://git-lfs.github.com/spec/v1

2 + oid sha256:4a0d0034f6deabb9369f553d4d9f3a7aa6f87fa8f2292be576d7b42897c686bb

3 + size 88880

▼ drivers/bf77a19e1396d6d36e32ff8d23eb5d3f.bin ...

... @@ -0,0 +1,3 @@

1 + version https://git-lfs.github.com/spec/v1

2 + oid sha256:fa0902daefbd9e716faaac8e854144ea0573e2a41192796f3b3138fe7a1d19f1

3 + size 14072

▼ drivers/c047c92696e5cef5485a22df97e6646e.bin ...

... @@ -0,0 +1,3 @@

1 + version https://git-lfs.github.com/spec/v1

2 + oid sha256:e3a1f0d967335c8a080a5b1e7e3a06a61f6cea39739cda3ebab11d2908713d80

3 + size 14848

▼ drivers/d104621c93213942b7b43d65b5d8d33e.bin ...

**Load Diff**

This file was deleted.

▼ drivers/d8d1c6cd663c9c5a457d8147e10c4e64.bin

... @@ -0,0 +1,3 @@

1 + version <https://git-lfs.github.com/spec/v1>

2 + oid sha256:2cea1a8d5d23a5ed2c2ac2a0c7c0d95da516aa355224cc707f86de8ade5880ef

3 + size 380264

▼ ...l/0712c54c-69fd-41f2-950a-da678ac51246.yaml

... @@ -0,0 +1,183 @@

1 + Id: 0712c54c-69fd-41f2-950a-da678ac51246

2 + Tags:

3 + - STProcessMonitor.sys

4 + Verified: 'TRUE'

5 + Author: Michael Haag

6 + Created: '2026-03-20'

7 + MitreID: T1562.001

8 + Category: vulnerable driver

9 + Commands:

10 + Command: sc.exe create STProcessMonitor

binPath=C:\windows\temp\STProcessMonitor.sys

11 + type=kernel &amp;&amp; sc.exe start STProcessMonitor

12 + Description: Safetica Technologies process monitoring kernel driver

vulnerable to

13 + BYOVD-style process termination via IOCTL. CVE-2025-70795. 18 execution parents

14 + observed in VirusTotal indicating active abuse by threat actors. 1/73 detections.

15 + Driver facilitates arbitrary process kill from kernel context, enabling EDR/AV

16 + bypass.

17 + Usecase: Disable security tools

18 + Privileges: kernel

19 + OperatingSystem: Windows 10

20 + Resources:

```
21 + - https://www.cve.org/CVERecord?id=CVE-2025-70795
22 + - https://github.com/magicsword-io/LOLDrivers/issues/268
23 + Detection: []
24 + Acknowledgement:
25 +   Person: ''
26 +   Handle: ''
27 + KnownVulnerableSamples:
28 + - Filename: STProcessMonitor.sys
29 +   MD5: 5761bd63da03686fc480245da7bd1e9f
30 +   SHA1: 68fec379f2ae76c3d2ce913f7be650cea1d06990
31 +   SHA256: 5b4f59236a9b950bcd5191b35d19125f60cfb9e1a1e1aa2e4f914b6745dde9df
32 + Signature:
33 + - Microsoft Windows Hardware Compatibility Publisher
34 + - Microsoft Windows Third Party Component CA 2012
35 + - Microsoft Root Certificate Authority 2010
36 + Date: '2026-02-04 12:24:39'
37 + Publisher: Microsoft Windows Hardware Compatibility Publisher
38 + Company: Safetica Technologies
39 + Description: ProcessMonitor Driver
40 + Product: Safetica
41 + ProductVersion: 11.26.18
42 + FileVersion: 11,26,18,0
43 + MachineType: AMD64
44 + OriginalFilename: ProcessMonitorDriver
45 + Authentihash:
46 +   MD5: 7590bc612d1cb940d6acf2d7ae384638
47 +   SHA1: 01bf6090818731e8121674a339a5f22cb18cf41d
48 +   SHA256: 0376d4554b4828a7e3721327cb4c9977301c02eb8c50d10d376d3be623d71e3a
49 + RichPEHeaderHash:
50 +   MD5: 6eb21f070cb73b6994e6b9aab3f72279
51 +   SHA1: ebe9c1483d5dc68041bbbf053dfd08c4651931e8
52 +   SHA256: a0b5c0bad77a66d6a25df16f7a2500b6df550eda8ba62333b5d1eccfeee7bf27
53 + InternalName: STProcessMonitor
54 + Copyright: Copyright (C) 2026, Safetica
55 + Imports:
56 + - FLTMGR.SYS
57 + - ntoskrnl.exe
58 + ImportedFunctions:
59 + - FltDeletePushLock
60 + - FltAcquirePushLockExclusiveEx
```

```
61 + - FltAcquirePushLockSharedEx
62 + - FltReleasePushLockEx
63 + - FltInitializePushLock
64 + - DbgPrintEx
65 + - KeGetCurrentIrql
66 + - ExFreePoolWithTag
67 + - ObfReferenceObject
68 + - ObfDereferenceObject
69 + - PsGetCurrentProcessId
70 + - PsGetCurrentThreadId
71 + - RtlInitUnicodeString
72 + - RtlCreateSecurityDescriptor
73 + - RtlSetDaclSecurityDescriptor
74 + - RtlGetVersion
75 + - KeSetEvent
76 + - KeEnterCriticalRegion
77 + - KeLeaveCriticalRegion
78 + - ExAllocatePoolWithTag
79 + - IoCompleteRequest
80 + - IoCreateDevice
81 + - IoCreateSymbolicLink
82 + - IoDeleteDevice
83 + - IoDeleteSymbolicLink
84 + - ObReferenceObjectByHandle
85 + - ZwClose
86 + - PsSetCreateProcessNotifyRoutineEx
87 + - ZwTerminateProcess
88 + - ZwOpenProcess
89 + - RtlCreateAcl
90 + - RtlAddAccessAllowedAce
91 + - ObOpenObjectByPointer
92 + - ZwSetSecurityObject
93 + - ExEventObjectType
94 + - SeExports
95 + - ZwSetInformationFile
96 + - KeLowerIrql
97 + - KfRaiseIrql
98 + - KeInitializeDpc
99 + - KeInsertQueueDpc
100 + - KeReleaseSemaphore
```

```
101 + - KeDelayExecutionThread
102 + - KeAcquireSpinLockRaiseToDpc
103 + - KeReleaseSpinLock
104 + - ExQueueWorkItem
105 + - ExReleaseResourceLite
106 + - ZwCreateFile
107 + - ZwWriteFile
108 + - ExAcquireResourceSharedLite
109 + - ZwOpenFile
110 + - _vsnwprintf
111 + ExportedFunctions:
112 + - _debugBootBuffer
113 + Sections:
114 + .text:
115 +     Entropy: 6.43
116 +     Virtual Size: '0x4746'
117 + .rdata:
118 +     Entropy: 3.58
119 +     Virtual Size: '0xa10'
120 + .data:
121 +     Entropy: 0.72
122 +     Virtual Size: '0x5b8'
123 + .pdata:
124 +     Entropy: 3.97
125 +     Virtual Size: '0x1ec'
126 + .edata:
127 +     Entropy: 3.88
128 +     Virtual Size: '0x5c'
129 + INIT:
130 +     Entropy: 5.12
131 +     Virtual Size: '0x6c4'
132 + .rsrc:
133 +     Entropy: 3.21
134 +     Virtual Size: '0x3d0'
135 + .reloc:
136 +     Entropy: 3.76
137 +     Virtual Size: '0x38'
138 + MagicHeader: 50 45 0 0
139 + CreationTimestamp: '2026-02-04 12:24:39'
140 + Imphash: 51777abf89572dc6d0ba931ade6ae5b9
```

```
141 + Signatures:
142 +   - CertificatesInfo: ''
143 +   SignerInfo: ''
144 +   Certificates:
145 +     - Subject: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
      CN=Microsoft
146 +       Windows Hardware Compatibility Publisher
147 +       ValidFrom: '2025-11-13 19:59:40'
148 +       ValidTo: '2026-11-10 19:59:40'
149 +       Signature:
      86e91c9dd77bcbe24e9c811c4ec9c47116d9d554243f04666bef14828edbfef665280fa10b643a5
      9d05c4db8b5f2bae0657af9a75457236e455f956ed7ba65f7e8019355d00e322f681ab15f14718b
      34bff1e50d8cde1217dc158c31a875b17fa45f015b4b2a30c471d43345257c729d83c2287716b3d
      19c177ed341da95687f8af92cfebc42e1e4439eb4304762e17feb85a09316afe8153e4783a98153
      d91249d29da0bca831ea6ccd93bace88fc284e82987df65bcd8ab0263a2da5e178e710c26e8abec
      12fe398782d1f1bc669ec9c5cbf3010f8e2600133a59fb8269daba61e5b2facee4f96ba19f9cfae
      f3fdb21e933a65c3245f6de70cb08f28f2c818
150 +       SignatureAlgorithmOID: 1.2.840.113549.1.1.11
151 +       IsCertificateAuthority: false
152 +       SerialNumber: 330000013c4a61fb3578d2b6dd00000000013c
153 +       Version: 3
154 +       CertificateType: Leaf (Code Signing)
155 +       IsCodeSigning: true
156 +       IsCA: false
157 +       TBS:
158 +         MD5: 93354b540685ae615b51e692ea0895de
159 +         SHA1: b38cd5d491c85bd55e9b111e98430171a01e9515
160 +         SHA256:
      037c041a283132dc57d29bc339b4d0d006787e32ac0a60afd7206c41c9fbf61f
161 +         SHA384:
      bbf5ad51ba2a76ba3f0e39459837c9533a56420db0da55814511346155922c98ae905d6541df5a
      79895ce1a51d53491
162 +     - Subject: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
      CN=Microsoft
163 +       Windows Third Party Component CA 2012
164 +       ValidFrom: '2012-04-18 23:48:38'
165 +       ValidTo: '2027-04-18 23:58:38'
166 +       Signature:
      5a8a67dacc5fd0d264177bf0a4678b4b3de12692b7723c2652f015fd203f461ba509d2e8c3972f
      36c3e6ab11e766decb7f382dcccbbc56970287366173f54abee011648c446d91b80ae813a8d0f79
```

```

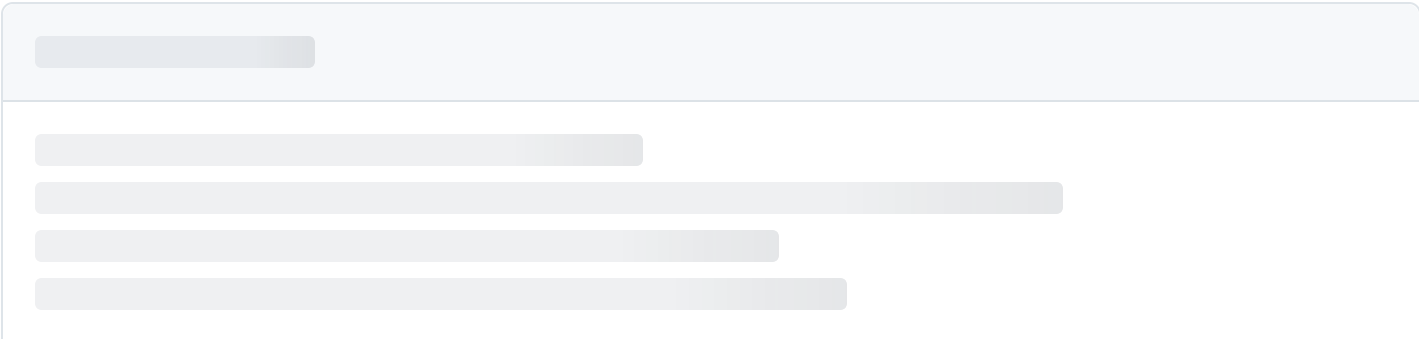
6d68b09eea2d3f39d3ca387ebd5e7c086e19dcc6c2f438336861e2524783e1000156d2bacb87820
5310a418b4ee77f5f5fed5fd3392d45eba213bffd1ec298417161165fc80a70257c59693124e471
e70abb0417f79f721ec9d2bb1abe3d02fe090cb243b4591a99539396215fe0d6b72601429536ac2
7fdbef48577683d18bdf4be98882211865216f345ec0397107087a37043713cdbc98603170cf573
5bc67de15c64edd7c548d7ed32e2d1aad3cfa7f6574e61f977eb67f288b3de00da038fd08a34373
e1dd862b8d2b1f3e12f8b723b81967c6ffcec667672601b24f2a0896d5b6d002eef28dd868705c2
b4b9e5be64c22af24a155c98e2c42785ff52e3627e0fb2020bd766c70ab2d33d200414503259830
a7d9bed5a38120152ba2f5e20728e4af1fde771028c3be107bec973f4dd47d8b4efb4a4b330b989
3e76cab90098567eabea8ab8a5d038ab6977130b142fe9aa411ff7babd3a2b348aee0aab63e663f
788248e200d2b3b9de3c24952ac9f1f0e393b5dd46e506ae67d523aaa7c3315290d265e0158a74e
a93d7a846f743f609fe4324f3600af6d71d33ea646655f8174f1fec171da4ca0415a82ddf11f

```

```

167 +   SignatureAlgorithmOID: 1.2.840.113549.1.1.11
168 +   IsCertificateAuthority: true
169 +   SerialNumber: 610baac1000000000009
170 +   Version: 3
171 +   CertificateType: CA
172 +   IsCodeSigning: false
173 +   IsCA: true
174 +   TBS:
175 +       MD5: a569061297e8e824767dbc3184a69bea
176 +       SHA1: adbb26a587a8f44b4fccaeceb306f980d1c55a150
177 +       SHA256:
178 +           cec1afd0e310c55c1dcc601ab8e172917706aa32fb5eaf826813547fdf02dd46
179 +           SHA384:
180 +               e947cac936803f5683196e4ff1b259096073395d0b908522ddce90d57597c9f7b57f7ddcbe021b
181 +               a863d843c340da8ba
182 +       Signer:
183 +           - SerialNumber: 330000013c4a61fb3578d2b6dd0000000013c
184 +           Issuer: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
185 +               CN=Microsoft
186 +           Windows Third Party Component CA 2012
187 +           Version: 1

```



**Comments** 0



Please [sign in](#) to comment.