# Commit eea8326

**MHaggis** committed 2 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 +1766 -324 lines changed

Top

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

**21 files changed** +1766 -324 lines changed

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:e62d0c1353a3d913497e6016d0f48d7cf9ef99e4026b94ccd873d6c7a9a54565
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 @@
+ version https://git-lfs.github.com/spec/v1
+ oid sha256:2cea1a8d5d23a5ed2c2ac2a0c7c0d95da516aa355224cc707f86de8ade5880ef
+ size 380264
```

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

```
@@ -0,0 +1,183 @@
+ Id: 0712c54c-69fd-41f2-950a-da678ac51246
+ Tags:
+ - STProcessMonitor.sys
+ Verified: 'TRUE'
+ Author: Michael Haag
+ Created: '2026-03-20'
+ MitreID: T1562.001
+ Category: vulnerable driver
+ Commands:
+   Command: sc.exe create STProcessMonitor binPath=C:\windows\temp\STProcessMonitor.sys
+     type=kernel && sc.exe start STProcessMonitor
+   Description: Safetica Technologies process monitoring kernel driver vulnerable to
+     BYOVD-style process termination via IOCTL. CVE-2025-70795. 18 execution parents
+     observed in VirusTotal indicating active abuse by threat actors. 1/73 detections.
+     Driver facilitates arbitrary process kill from kernel context, enabling EDR/AV
+     bypass.
+   Usecase: Disable security tools
+   Privileges: kernel
+   OperatingSystem: Windows 10
+ Resources:
+ - https://www.cve.org/CVERecord?id=CVE-2025-70795
+ - https://github.com/magicsword-io/LOLDrivers/issues/268
+ Detection: []
+ Acknowledgement:
+   Person: ''
+   Handle: ''
+ KnownVulnerableSamples:
+ - 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  +    - IofCompleteRequest
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
```

```
+   - ZwOpenFile
+   - _vsnwprintf
+   ExportedFunctions:
+   - _debugBootBuffer
+   Sections:
+     .text:
+       Entropy: 6.43
+       Virtual Size: '0x4746'
+     .rdata:
+       Entropy: 3.58
+       Virtual Size: '0xa10'
+     .data:
+       Entropy: 0.72
+       Virtual Size: '0x5b8'
+     .pdata:
+       Entropy: 3.97
+       Virtual Size: '0x1ec'
+     .edata:
+       Entropy: 3.88
+       Virtual Size: '0x5c'
+     INIT:
+       Entropy: 5.12
+       Virtual Size: '0x6c4'
+     .rsrc:
+       Entropy: 3.21
+       Virtual Size: '0x3d0'
+     .reloc:
+       Entropy: 3.76
+       Virtual Size: '0x38'
+   MagicHeader: 50 45 0 0
+   CreationTimestamp: '2026-02-04 12:24:39'
+   Imphash: 51777abf89572dc6d0ba931ade6ae5b9
+   Signatures:
+   - CertificatesInfo: ''
+     SignerInfo: ''
+     Certificates:
+     - Subject: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
  CN=Microsoft
+         Windows Hardware Compatibility Publisher
+       ValidFrom: '2025-11-13 19:59:40'
```

```
148 +       ValidTo: '2026-11-10 19:59:40'
149 +       Signature:
      86e91c9dd77bcbe24e9c811c4ec9c47116d9d554243f04666bef14828edbfeb665280fa10b643a5
      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:
      bbef5ad51ba2a76ba3f0e39459837c9533a56420db0da55814511346155922c98ae905d6541df5a
      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:
      5a8a67daccd5fd0d264177bf0a4678b4b3de12692b7723c2652f015fd203f461ba509d2e8c3972f
      36c3e6ab11e766decb7f382dcccbbc56970287366173f54ebee011648c446d91b80ae813a8d0f79
      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: adbb26a587a8f44b4fccaecb306f980d1c55a150
177 +         SHA256:
cec1afd0e310c55c1dcc601ab8e172917706aa32fb5eaf826813547fdf02dd46
178 +         SHA384:
e947cac936803f5683196e4ff1b259096073395d0b908522ddce90d57597c9f7b57f7ddcdbe021b
a863d843c340da8ba
179 +     Signer:
180 +     - SerialNumber: 330000013c4a61fb3578d2b6dd00000000013c
181 +       Issuer: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
CN=Microsoft
182 +         Windows Third Party Component CA 2012
183 +       Version: 1
```

...l/13973a71-412f-4a18-a2a6-476d3853f8de.yaml

```
@@ -16,6 +16,7 @@ Commands:
16  16    Resources:
17  17    - Internal Research
18  18    - https://github.com/elastic/protections-artifacts/search?
q=AMDRyzenMasterDriver
    19  + - https://github.com/NtGabrielGomes/CVE-2023-20564
19  20    Detection:
20  21    - type: yara_signature
21  22      value: https://github.com/magicsword-
io/LOLDrivers/blob/main/detections/yara/yara-
rules_vuln_drivers_strict_renamed.yar
@@ -1496,3 +1497,208 @@ KnownVulnerableSamples:
1496 1497      CreationTimestamp: '2019-05-13 04:14:16'
```

```
1497  1498      Imphash: 8bbc742eaed888736a715757f0584fb6
1498  1499      LoadsDespiteHVCI: 'FALSE'
      1500  + - Filename: AMDRyzenMasterDriver.sys
      1501  +   MD5: 91717a70db6c7beabbc004bbd9544ae6
      1502  +   SHA1: 8f1623af2bb00cb5e75e4a4134244e6e1b5ad83c
      1503  +   SHA256: 4a0d0034f6deabb9369f553d4d9f3a7aa6f87fa8f2292be576d7b42897c686bb
      1504  +   Authentihash:
      1505  +     MD5: 7961069ec3254ffe292120e3746bddf4
      1506  +     SHA1: 07417968cd500098780bf72547817d2ee724e5b6
      1507  +     SHA256: 45799bfaea64e065a9b0c97f9f10f42c830d26e55fdcb354e39179d0993e9c7d
      1508  +   Description: AMD Ryzen Master Service Driver
      1509  +   Company: Advanced Micro Devices
      1510  +   InternalName: AMDRyzenMasterDriver.sys
      1511  +   OriginalFilename: AMDRyzenMasterDriver.sys
      1512  +   FileVersion: 1.7.0.0
      1513  +   Product: AMD Ryzen Master Service Driver
      1514  +   ProductVersion: 1.7.0.0
      1515  +   Copyright: "Copyright \xA9 2020 AMD, Inc."
      1516  +   MachineType: AMD64
      1517  +   Imports:
      1518  +   - ntoskrnl.exe
      1519  +   - HAL.dll
      1520  +   - WDFLDR.SYS
      1521  +   ExportedFunctions: ''
      1522  +   ImportedFunctions:
      1523  +   - KeLeaveCriticalRegion
      1524  +   - IofCompleteRequest
      1525  +   - IoCreateSymbolicLink
      1526  +   - IoDeleteDevice
      1527  +   - IoDeleteSymbolicLink
      1528  +   - MmBuildMdlForNonPagedPool
      1529  +   - MmMapLockedPagesSpecifyCache
      1530  +   - MmUnmapLockedPages
      1531  +   - MmMapIoSpace
      1532  +   - MmUnmapIoSpace
      1533  +   - IoAllocateMdl
      1534  +   - IoFreeMdl
      1535  +   - MmGetSystemRoutineAddress
      1536  +   - ZwClose
      1537  +   - ZwSetSecurityObject
```

```
1538 +    - IoDeviceObjectType
1539 +    - IoCreateDevice
1540 +    - KeEnterCriticalRegion
1541 +    - RtlGetDaclSecurityDescriptor
1542 +    - RtlGetGroupSecurityDescriptor
1543 +    - RtlGetOwnerSecurityDescriptor
1544 +    - RtlGetSaclSecurityDescriptor
1545 +    - SeCaptureSecurityDescriptor
1546 +    - _snwprintf
1547 +    - RtlLengthSecurityDescriptor
1548 +    - SeExports
1549 +    - RtlCreateSecurityDescriptor
1550 +    - _wcsnicmp
1551 +    - wcschr
1552 +    - RtlAbsoluteToSelfRelativeSD
1553 +    - RtlAddAccessAllowedAce
1554 +    - RtlLengthSid
1555 +    - IoIsWdmVersionAvailable
1556 +    - RtlSetDaclSecurityDescriptor
1557 +    - ZwOpenKey
1558 +    - ZwSetValueKey
1559 +    - ZwQueryValueKey
1560 +    - ZwCreateKey
1561 +    - RtlFreeUnicodeString
1562 +    - KeDelayExecutionThread
1563 +    - RtlGetVersion
1564 +    - DbgPrint
1565 +    - RtlCopyUnicodeString
1566 +    - RtlInitUnicodeString
1567 +    - ExFreePoolWithTag
1568 +    - ExAllocatePoolWithTag
1569 +    - ObOpenObjectByPointer
1570 +    - strncmp
1571 +    - HalSetBusDataByOffset
1572 +    - HalGetBusDataByOffset
1573 +    - WdfVersionBind
1574 +    - WdfVersionUnbind
1575 +    - WdfVersionBindClass
1576 +    - WdfVersionUnbindClass
1577 +   Signatures:
```

```
1578 +   - CertificatesInfo: ''
1579 +     SignerInfo: ''
1580 +     Certificates:
1581 +     - Subject: C=US, O=Symantec Corporation, CN=Symantec Time Stamping
       Services CA
1582 +         , G2
1583 +       ValidFrom: '2012-12-21 00:00:00'
1584 +       ValidTo: '2020-12-30 23:59:59'
1585 +       Signature:
       03099b8f79ef7f5930aaef68b5fae3091dbb4f82065d375fa6529f168dea1c9209446ef56deb5
       87c30e8f9698d23730b126f47a9ae3911f82ab19bb01ac38eeb599600adce0c4db2d031a6085c
       2a7afce27a1d574ca86518e979406225966ec7c7376a8321088e41eaddd9573f1d7749872a160
       65ea6386a2212a35119837eb6
1586 +       SignatureAlgorithmOID: 1.2.840.113549.1.1.5
1587 +       IsCertificateAuthority: true
1588 +       SerialNumber: 7e93ebfb7cc64e59ea4b9a77d406fc3b
1589 +       Version: 3
1590 +       CertificateType: CA
1591 +       IsCodeSigning: false
1592 +       IsCA: true
1593 +       TBS:
1594 +         MD5: d0785ad36e427c92b19f6826ab1e8020
1595 +         SHA1: 365b7a9c21bd9373e49052c3e7b3e4646ddd4d43
1596 +         SHA256:
       c2abb7484da91a658548de089d52436175fdb760a1387d225611dc0613a1e2ff
1597 +         SHA384:
       eab4fe5ef90e0de4a6aa3a27769a5e879f588df5e4785aa4104debd1f81e19ea56d33e3a16e5f
       acf99f68b5d8e3d287b
1598 +     - Subject: C=US, O=Symantec Corporation, CN=Symantec Time Stamping
       Services Signer
1599 +         , G4
1600 +       ValidFrom: '2012-10-18 00:00:00'
1601 +       ValidTo: '2020-12-29 23:59:59'
1602 +       Signature:
       783bb4912a004cf08f62303778a38427076f18b2de25dca0d49403aa864e259f9a40031cddcee
       379cb216806dab632b46dbff42c266333e449646d0de6c3670ef705a4356c7c8916c6e9b2dfb2
       e9dd20c6710fcd9574dcb65cdebd371f4378e678b5cd280420a3aaf14bc48829910e80d111fcd
       d5c766e4f5e0e4546416e0db0ea389ab13ada097110fc1c79b4807bac69f4fd9cb60c162bf17f
       5b093d9b5be216ca13816d002e380da8298f2ce1b2f45aa901af159c2c2f491bdb22bbc3fe789
```

```
                451c386b182885df03db451a179332b2e7bb9dc20091371eb6a195bcfe8a530572c89493fb9cf
                7fc9bf3e226863539abd6974acc51d3c7f92e0c3bc1cd80475
1603  +       SignatureAlgorithmOID: 1.2.840.113549.1.1.5
1604  +       IsCertificateAuthority: false
1605  +       SerialNumber: 0ecff438c8febf356e04d86a981b1a50
1606  +       Version: 3
1607  +       CertificateType: Intermediate
1608  +       IsCodeSigning: false
1609  +       IsCA: false
1610  +       TBS:
1611  +         MD5: e9d38360b914c8863f6cba3ee58764d3
1612  +         SHA1: 4cba8eae47b6bf76f20b3504b98b8f062694a89b
1613  +         SHA256:
                88901d86a4cc1f1bb193d08e1fb63d27452e63f83e228c657ab1a92e4ade3976
1614  +         SHA384:
                e9f2a75334a9e336c5a4712eadee88d0374b0fdc273262f4e65c9040ad2793067cc076696db52
                79a478773485e285652
1615  +     - Subject: C=US, ST=California, L=Santa Clara, O=Advanced Micro Devices
                INC.,
1616  +         CN=Advanced Micro Devices INC.
1617  +       ValidFrom: '2019-02-13 00:00:00'
1618  +       ValidTo: '2022-02-13 23:59:59'
1619  +       Signature:
                8c521a9a934b3e45eaccd7ed8e301606b9e25215b4914181c8dfb5226b0e0e96df11e24e5d598
                5637b0ed21b121b6b46cc448cea697a0cb62faccc7cd5ec515797e424cf9e28634da84b95fa2e
                ef52f8b9cc0752b6a161bae0be9f4924d7fd9a8fe5443177f16025dbf020287184581d3b1eed6
                7fa369b80eb66cb70050089965da0bf36d68dd303738ac99edff5b7943ce863c4f3b2833a0457
                6e6a28555c630d91bd4ea9f0ca41c0d97b07240c1059bc4a6cbe58276fede21f22de0ec57efe2
                0b33ee4b2bb35cbfb1e5590193aa35368e728a09d27c3bf8e84815c66e092b91e63d025665756
                aa8e73f847b5506e6b118dde05bf7d72547ec2146d8b9dec80
1620  +       SignatureAlgorithmOID: 1.2.840.113549.1.1.11
1621  +       IsCertificateAuthority: false
1622  +       SerialNumber: 1885b7e188d8fafd38a43d48967d7488
1623  +       Version: 3
1624  +       CertificateType: Leaf (Code Signing)
1625  +       IsCodeSigning: true
1626  +       IsCA: false
1627  +       TBS:
1628  +         MD5: 7383bf699bcb229fcf33802fe77d95fc
1629  +         SHA1: 9b497b4a98173e0e91517daae8e47ca0fce3ff21
```

```
1630 +         SHA256:
     79ea901ff84d0e090348148fd3b9be496ee45e0e852ec8582b27c6d46f11b5b0
1631 +         SHA384:
     dc879c437e176bfe1e9de208ba3cef533290598e81031e9210f2a8c0f79a15415106632a881a3
     d24aadf385c2c6861c6
1632 +     - Subject: C=US, O=Symantec Corporation, OU=Symantec Trust Network,
     CN=Symantec
1633 +         Class 3 SHA256 Code Signing CA
1634 +       ValidFrom: '2013-12-10 00:00:00'
1635 +       ValidTo: '2023-12-09 23:59:59'
1636 +       Signature:
     13851a1e69a937f7a0bda4af7e1d6153fe9d8c5e0ca6751e781723ddfdec1a035539fb7195c76
     55aa78e30d2445a61db706fda2105c22e73ba49f1d193fe5dc9cd5e03e0899e3f741ed7f7388b
     a9d6cfbb352f3358a89256d1c84d3b82e6798416fc28b0b147f31da23eee87d9a67fa456a53fa
     d842e29de7cbca8aaa33d0401eaba93a20e502229174c87e43a115fd6a425899b056b2fb4c901
     4c277b0bac190522a060153fdac9fb4d4c8ffb726777fd2794c7ba350e8849fe8dfd28af4a12b
     d0db39705de440c15fa362b03dcc15001f1a1115d14e5e2bd274b54be2b845e0fa6c374050aef
     97c38922b11f77f3bdcd43d4f14ca93fb58b84af64f2d01421
1637 +       SignatureAlgorithmOID: 1.2.840.113549.1.1.11
1638 +       IsCertificateAuthority: true
1639 +       SerialNumber: 3d78d7f9764960b2617df4f01eca862a
1640 +       Version: 3
1641 +       CertificateType: CA
1642 +       IsCodeSigning: true
1643 +       IsCA: true
1644 +       TBS:
1645 +         MD5: 1f056ff7d5f874984dc605402b7cb042
1646 +         SHA1: bdb348353a2203deb4b767914fa1bd7248dd728b
1647 +         SHA256:
     a08e79c386083d875014c409c13d144e0a24386132980df11ff59737c8489eb1
1648 +         SHA384:
     fa2729064b49e0d77540c1ee95d5f74acaf8eaf55197851a3a40383335f8113e51190bc48b552
     196edf8ac5cf0c89278
1649 +     - Subject: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 2006
     VeriSign,
1650 +         Inc. , For authorized use only, CN=VeriSign Class 3 Public Primary
     Certification
1651 +         Authority , G5
1652 +       ValidFrom: '2011-02-22 19:25:17'
1653 +       ValidTo: '2021-02-22 19:35:17'
```

```
1654 +       Signature:
       812a82168c34672be503eb347b8ca2a3508af45586f11e8c8eae7dee0319ce72951848ad6211f
       d20fd3f4706015ae2e06f8c152c4e3c6a506c0b36a3cf7a0d9c42bc5cf819d560e369e6e22341
       678c6883762b8f93a32ab57fbe59fba9c9b2268fcaa2f3821b983e919527978661ee5b5d076bc
       d86a8e26580a8e215e2b2be23056aba0cf347934daca48c077939c061123a050d89a3ec9f5789
       84fbecca7c47661491d8b60f195de6b84aacbc47c8714396e63220a5dc7786fd3ce38b71db7b9
       b03fcb71d3264eb1652a043a3fa2ead59924e7cc7f233424838513a7c38c71b242228401e1a46
       1f17db18f7f027356cb863d9cdb9645d2ba55eefc629b4f2c7f821cc04ba57fd01b6abc667f9e
       7d3997ff4f522fa72f5fdff3a1c423aa1f98018a5ee8d1cd4669e4501feaaeefffb178f30f7f1
       cd29c59decb5d549003d85b8cbbb933a276a49c030ae66c9f723283276f9a48356c848ce5a96a
       aa0cc0cc47fb48e97af6de35427c39f86c0d6e473089705dbd054625e0348c2d59f7fa7668cd0
       9db04fd4d3985f4b7ac97fb22952d01280c70f54b61e67cdc6a06c110384d34875e72afeb03b6
       e0a3aa66b769905a3f177686133144706fc537f52bd92145c4a246a678caf8d90aad0f679211b
       93267cc3ce1ebd883892ae45c6196a4950b305f8ae59378a6a250394b1598150e8ba8380b7233
       5f476b9671d5918ad208d94
1655 +       SignatureAlgorithmOID: 1.2.840.113549.1.1.5
1656 +       IsCertificateAuthority: true
1657 +       SerialNumber: 611993e400000000001c
1658 +       Version: 3
1659 +       CertificateType: CA
1660 +       IsCodeSigning: false
1661 +       IsCA: true
1662 +       TBS:
1663 +         MD5: 78a717e082dcc1cda3458d917e677d14
1664 +         SHA1: 4a872e0e51f9b304469cd1dedb496ee9b8b983a4
1665 +         SHA256:
       317fa1d234ebc49040ebc5e8746f8997471496051b185a91bdd9dfbb23fab5f8
1666 +         SHA384:
       b71052da4eb9157c8c1a5d7f55df19d69b9128598b72fcca608e5b7cc7d64c43c5504b9c86355
       a6dc22ee40c88cc385c
1667 +     Signer:
1668 +     - SerialNumber: 1885b7e188d8fafd38a43d48967d7488
1669 +       Issuer: C=US, O=Symantec Corporation, OU=Symantec Trust Network,
       CN=Symantec
1670 +         Class 3 SHA256 Code Signing CA
1671 +       Version: 1
1672 +   RichPEHeaderHash:
1673 +     MD5: 6d6b8554188fb7411ca051ba2dff2781
1674 +     SHA1: e72511c1833327ca1c8a601928d34423474dc29f
1675 +     SHA256: 627de079d57aa0a30e00513bea298e3d0d1da718e568f8e13520afe3762f3aff
```

```
1676 +   Sections:
1677 +     .text:
1678 +       Entropy: 6.06
1679 +       Virtual Size: '0x899a'
1680 +     .rdata:
1681 +       Entropy: 4.67
1682 +       Virtual Size: '0xbac'
1683 +     .data:
1684 +       Entropy: 2.37
1685 +       Virtual Size: '0x207a8'
1686 +     .pdata:
1687 +       Entropy: 4.59
1688 +       Virtual Size: '0x4f8'
1689 +     PAGE:
1690 +       Entropy: 6.28
1691 +       Virtual Size: '0x1b94'
1692 +     INIT:
1693 +       Entropy: 5.17
1694 +       Virtual Size: '0x6fe'
1695 +     .rsrc:
1696 +       Entropy: 3.27
1697 +       Virtual Size: '0x3c8'
1698 +     .reloc:
1699 +       Entropy: 3.46
1700 +       Virtual Size: '0x34'
1701 +   MagicHeader: 50 45 0 0
1702 +   CreationTimestamp: '2020-09-18 02:22:51'
1703 +   Imphash: 3152fa00add1f466d28c7e78ed54fdea
1704 +   LoadsDespiteHVCI: 'FALSE'
```

...l/1d2cdef1-de44-4849-80e5-e2fa288df681.yaml

```
@@ -54,207 +54,6 @@ Acknowledgement:
54 54     Handle: ''
55 55     Person: ''
56 56   KnownVulnerableSamples:
57    - - Filename: iQVW64.SYS
58    -   MD5: 69ba501a268f09f694ff0e8e208aa20e
59    -   SHA1: 3d6d53b0f1cc908b898610227b9f1b9352137aba
60    -   SHA256: 37c637a74bf20d7630281581a8fae124200920df11ad7cd68c14c26cc12c5ec9
61    -   Signature: ''
```

```
-   Date: ''
-   Publisher: ''
-   Company: 'Intel Corporation '
-   Description: Intel(R) Network Adapter Diagnostic Driver
-   Product: Intel(R) iQVW64.SYS
-   ProductVersion: 1.3.2.17
-   FileVersion: '1.3.2.17 built by: WinDDK'
-   MachineType: AMD64
-   OriginalFilename: iQVW64.SYS
-   Imphash: 2cf48a541dc193e91bb2a831adcf278e
-   Authentihash:
-     MD5: 61c9bc2fd776b341f21b71fb1891eb5a
-     SHA1: 9af173db51828d2a3c64d34e9120f1fd129a2359
-     SHA256: ecd6e879e5521ca4053a59ef6682a95d97f6d9ba75f313b87bd133afe5267852
-   RichPEHeaderHash:
-     MD5: 84dfb7245aa6b7f3efec05cfa6559636
-     SHA1: 695bd45c0e89dcb58253e90c9a43400b03ae2202
-     SHA256: 3ff178ffbb2c17ce7c3a02ef5943ddf3b580e3e28f6cc59775c5369062a0b9ab
-   Sections:
-     .text:
-       Entropy: 6.2614381305981635
-       Virtual Size: '0x4945'
-     .rdata:
-       Entropy: 4.781156413274236
-       Virtual Size: '0xed0'
-     .data:
-       Entropy: 1.1262035268835313
-       Virtual Size: '0x5ca0a0'
-     .pdata:
-       Entropy: 4.658699009524359
-       Virtual Size: '0x678'
-     PAGE:
-       Entropy: 6.1261566082145595
-       Virtual Size: '0x1b71'
-     INIT:
-       Entropy: 5.7698100081018655
-       Virtual Size: '0xb4c'
-     .rsrc:
-       Entropy: 3.4436811351467087
-       Virtual Size: '0x3f8'
```

```
-      .reloc:
-        Entropy: 1.2072398645622464
-        Virtual Size: '0x60'
-    MagicHeader: 50 45 0 0
-    CreationTimestamp: '2018-09-17 05:18:08'
-    InternalName: iQVW64.SYS
-    Copyright: Copyright (C) 2002-2018 Intel Corporation All Rights Reserved.
-    Imports:
-    - ntoskrnl.exe
-    - HAL.dll
-    ExportedFunctions: ''
-    ImportedFunctions:
-    - IoCreateSymbolicLink
-    - IofCompleteRequest
-    - MmIsAddressValid
-    - ExAllocatePoolWithTag
-    - ExFreePoolWithTag
-    - MmGetPhysicalAddress
-    - DbgPrint
-    - strncpy
-    - vsprintf
-    - IoFreeMdl
-    - MmMapLockedPagesSpecifyCache
-    - MmBuildMdlForNonPagedPool
-    - IoAllocateMdl
-    - MmUnmapIoSpace
-    - MmUnmapLockedPages
-    - MmAllocateContiguousMemory
-    - MmFreeContiguousMemory
-    - MmMapIoSpace
-    - RtlInitUnicodeString
-    - KeWaitForSingleObject
-    - IofCallDriver
-    - IoBuildSynchronousFsdRequest
-    - KeInitializeEvent
-    - ZwClose
-    - RtlFreeAnsiString
-    - strstr
-    - RtlUnicodeStringToAnsiString
-    - ZwEnumerateValueKey
```

```
142 -    - ZwOpenKey
143 -    - wcsncpy
144 -    - IoGetDeviceObjectPointer
145 -    - IoGetDeviceInterfaces
146 -    - ObReferenceObjectByPointer
147 -    - MmAllocateNonCachedMemory
148 -    - MmFreeNonCachedMemory
149 -    - KeBugCheckEx
150 -    - IoDeleteSymbolicLink
151 -    - ObfDereferenceObject
152 -    - IoDeleteDevice
153 -    - MmGetSystemRoutineAddress
154 -    - ZwSetSecurityObject
155 -    - ObOpenObjectByPointer
156 -    - IoDeviceObjectType
157 -    - IoCreateDevice
158 -    - RtlGetDaclSecurityDescriptor
159 -    - RtlGetSaclSecurityDescriptor
160 -    - RtlGetGroupSecurityDescriptor
161 -    - RtlGetOwnerSecurityDescriptor
162 -    - _snwprintf
163 -    - RtlLengthSecurityDescriptor
164 -    - SeCaptureSecurityDescriptor
165 -    - SeExports
166 -    - IoIsWdmVersionAvailable
167 -    - _wcsnicmp
168 -    - RtlAddAccessAllowedAce
169 -    - RtlLengthSid
170 -    - wcschr
171 -    - RtlAbsoluteToSelfRelativeSD
172 -    - RtlSetDaclSecurityDescriptor
173 -    - RtlCreateSecurityDescriptor
174 -    - ZwCreateKey
175 -    - ZwQueryValueKey
176 -    - ZwSetValueKey
177 -    - RtlFreeUnicodeString
178 -    - KeStallExecutionProcessor
179 -    - KeQueryPerformanceCounter
180 -   Signatures:
181 -    - CertificatesInfo: ''
```

```
182 -     SignerInfo: ''
183 -     Certificates:
184 -     - Subject: C=SE, O=AddTrust AB, OU=AddTrust External TTP Network,
      CN=AddTrust
185 -         External CA Root
186 -       ValidFrom: '2013-08-15 20:26:30'
187 -       ValidTo: '2023-08-15 20:36:30'
188 -       Signature:
      362ba2f2e1331fe493f7f26985c6640ec99b632fe4703798fd94ec7bcff8a14246f9ed6a4e8d346
      93605557a1ebbad8c99429606e925a82684bec1bf16a97caa5b04b7fdd1c0f402be28edf577c79b
      fe3af6e8c17bd382abfa144ecf2bcfe5d5b54840b1a38f838bad2b2553aba634cef243f74f2ce9d
      d1e4e5ab6bae83b10992400bc50fd78f6e523a8899493f7b74130374a57b7e644d9c9df9905aa44
      fc74af8264cc07cb01b609c32ee3e832a7b49f4178c7a184365462f2ec150ac8ead084f8f1e06bf
      456125f95e0fcddb77693fe294a25e90400f1b4110ec9849edb177df51ea58e3629193a6d6c464b
      d7ab7024288d05a3d9d524f2f8a0d13c8239d4a8820e693a8109fc06f0c75933843693064191232
      c22a5a7012b50b428aedb46b0591b86b39b87e8494e390b6d14df4c03301e1f5f74aef55b590353
      ec9816e0d06235751b48b87d13e57a48b87752a40798253b069b7a4e6a6f44864f144f2779273d5
      073414c9c413edd290c73b1c7fb1f760c176504ebd25010924149ece4067d3615446f89bf697df9
      4d40c13a98b6a07e31d2b5aecafb53d53f5086cd5e933b6d5d7c9a3f3ff7a9255884dd114900a2c
      7c89e37dd778e6d718be05b81345d54baccf59347886de7ef5be228e4801b40e40f2ad17f231565
      5aac9994433f465526d6c4fa8895e2919aa32d0b85deac8ce0f967709f71790231f761a229c4
189 -       SignatureAlgorithmOID: 1.2.840.113549.1.1.5
190 -       IsCertificateAuthority: true
191 -       SerialNumber: 3300000035d8d5595b0671412b000000000035
192 -       Version: 3
193 -       CertificateType: CA
194 -       IsCodeSigning: true
195 -       IsCA: true
196 -       TBS:
197 -         MD5: 3d488d41aaeb5661974952080abef2fd
198 -         SHA1: df01e35e6befc7d65625319f17397b861e618d56
199 -         SHA256:
      3d6ef38b5d26773dc77392e415e88b3a744b30ea9f2081e2a992b5818db2f0c4
200 -         SHA384:
      ac7c06916fe4a00307834b2499f12799d3fe463c2e63d1881df669a2786745beeee2b3a7d87cd6b
      c9e4fe293c22e5a59
201 -     - Subject: C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited,
      CN=COMODO
202 -         RSA Certification Authority
203 -       ValidFrom: '2000-05-30 10:48:38'
```

```
204 -       ValidTo: '2020-05-30 10:48:38'
205 -       Signature:
      64bf83f15f9a85d0cdb8a129570de85af7d1e93ef276046ef15270bb1e3cff4d0d746acc818225d
      3c3a02a5d4cf5ba8ba16dc4540975c7e3270e5d847937401377f5b4ac1cd03bab1712d6ef34187e
      2be979d3ab57450caf28fad0dbe5509588bbdf8557697d92d852ca7381bf1cf3e6b86e661105b31
      e942d7f91959259f14ccea391714c7c470c3b0b19f6a1b16c863e5caac42e82cbf90796ba484d90
      f294c8a973a2eb067b239ddea2f34d559f7a6145981868c75e406b23f5797aef8cb56b8bb76f46f
      47bf13d4b04d89380595ae041241db28f15605847dbef6e46fd15f5d95f9ab3dbd8b8e440b3cd97
      39ae85bb1d8ebcdc879bd1a6eff13b6f10386f
206 -       SignatureAlgorithmOID: 1.2.840.113549.1.1.12
207 -       IsCertificateAuthority: true
208 -       SerialNumber: 2766ee56eb49f38eabd770a2fc84de22
209 -       Version: 3
210 -       CertificateType: CA
211 -       IsCodeSigning: false
212 -       IsCA: true
213 -       TBS:
214 -         MD5: be5bfbe77379139ac5cdcbcc8d4d3b34
215 -         SHA1: 606b701bc9f448ddbfe6fa63ccb8061b838ee254
216 -         SHA256:
      0d73a614eef7596cf5a34733f74daf2ccfe4df7b4a40069bf43c43e428264177
217 -         SHA384:
      7ce102d63c57cb48f80a65d1a5e9b350a7a618482aa5a36775323ca933ddfcb00def83796a6340d
      ec5ebf7596cfd8e5d
218 -     - Subject: C=US, ST=CA, L=Santa Clara, O=Intel Corporation, OU=ND,
      CN=Intel(R)
219 -         INTELND1820
220 -       ValidFrom: '2018-08-09 21:34:08'
221 -       ValidTo: '2020-08-08 21:34:08'
222 -       Signature:
      714c055fff1a2bd770c1b7103eb47360ca789a29c9e4a59a9050dd5f9b20d559fa927bd5a6a7bb8
      e90be3324862edbe148f96f164427cd86b7c99ef8e972368a3aad8789e77ad0787ca5361a940ece
      b6b575a78655040f4104ddc57610bb1045c9aa03f3044b67c067a57c1d2dcf6be9969ce946684d1
      31c1f8e750ddde70bf6740ea6c912945b8aea873d8a2653180e02fa8cd0803d617f6bc1a432d3dd
      39ee49cb520959cffcab34bf6deba98ce8a8eba46eec31a34a075e1269c8cf68fe8d70b17e72c83
      206ca40797c51997ee0521ed3ebf4f20fb5a8c48c93722362f65ffb68f49325f479e30b398938d8
      b87a8adfe0d8c1e68b0be9de1d11dca8aca582ba3a568c0f94b344c0cc5acd6b13870baf515fe16
      9110c33d54f5e475272e485e949bf8f6dd4c7306bc32859dbbcde89228d1f92a7b9a0b20dd88097
      f76a19e6149afa28fb25574f9885252460aadb51be7695a59f13fe307a8346f4cf54f36b94dd1d8
      d082747f9869da38daed9301a20e728f7562dd789b52e11d061800bf8eb5bfce47c114b939ed078
```

```
7760bb530a86585de6b79927216dfadc3b6ab3234b94e3069feedfcac8adfa9ab3f910104f32fb1
8a44c90a8b9dab58915cccf8ce134bcb39a9eb4ddc158607cccbce0cfb7f23506fc40b99d3c79b6
de258c7c1734e29abae3a2330cf45871fc0dd444abbe8057a27b67cb4467f5bfd199d4ddedb7
223 -       SignatureAlgorithmOID: 1.2.840.113549.1.1.11
224 -       IsCertificateAuthority: false
225 -       SerialNumber: 560000077b478c76c9afcafcaf00000000077b
226 -       Version: 3
227 -       CertificateType: Leaf (Code Signing)
228 -       IsCodeSigning: true
229 -       IsCA: false
230 -       TBS:
231 -         MD5: f3eba8fe0d2dd1bc861e0b0e6e23d96e
232 -         SHA1: bce46695d618b69de8a4bb5ebede302378c1aebb
233 -         SHA256:
5de689926c95c269de72cd6edf9cad152c5ce41729dfc7835607b9b1182fe66e
234 -         SHA384:
348401b8898e24fd502451c161739c56eecd8f5a8159045b1fc312dd636174aba96273060253877
36bf478ade2b773a0
235 -     - Subject: C=US, ST=CA, L=Santa Clara, O=Intel Corporation, CN=Intel
External
236 -         Issuing CA 7B
237 -       ValidFrom: '2015-10-28 00:00:00'
238 -       ValidTo: '2021-06-17 23:59:59'
239 -       Signature:
35bb03eacc9b601a13d075528e8095454e9ebf6ec0bb64aac36eb1021d465e2fe82f48cc8410f7a
d993bfffa856829b0d37c31e21ab47bc166e2a53bc729189835ae6301a845209561db104db90d6b
d39964ce5f8bb86c1346a06e5a0d3ee790ebb731a121f58dde3b7b6936f10800b9aabf1c566156d
7cc923f29d4d96bd8222f0e56f56ad146e8808f397a923c6748b7e2fa190f3767e2df292d02aa43
282eae2c464224be6dbb6a8849a64c20dfe5654ffae1c1be71d5f85ef59d6692b23b64e1e8aeac9
95517bddb1bdfa0934f3f56f23b83d5d2b7c1085a524042e33e9120f735b491f04de134694879c0
ed30c9931a84d572198f6d8039f459ab2016d8f9ff7026237becc50033227c3d203aedb428bc7a8
10ce70bc13f7c300c4e50b8670fd76417b7c3c52085ca8fced5262a1254b9ff22f8a8273cca0e85
3714ee02e52f66156263876a5ecf29d3b89178b76172177bc119a6180822dad09125f606090926b
02dac808874335fc7e044c1309976d877b14701ef69922bedae582963a0358ee41db704f1da3ab2
3280b1c8bcf0e70f71007a333a06e8a4d879d9d953cd9bfeb2685b8884856b0771d04f930a07600
33408d273bf141adfe3c7041b2d999e931c95b38798425a1c916352398a8f4a2ac24c7b70693a3c
f1fb2fff0e0a8794e4016acf9bb41fa30ea9ea2adcaf2b8c4401fd3a587d3278a219d5c974c5
240 -       SignatureAlgorithmOID: 1.2.840.113549.1.1.12
241 -       IsCertificateAuthority: true
242 -       SerialNumber: 069b5e99277284c8767f1368a7deb0f3
```

```
243         -       Version: 3
244         -       CertificateType: CA
245         -       IsCodeSigning: true
246         -       IsCA: true
247         -       TBS:
248         -         MD5: 5578c7331db18bb448db403ad32c94ee
249         -         SHA1: dfcfe5d6087cf830513d705aa701ff957d960298
250         -         SHA256:
              5b619f82064ace7ecf48d26ce8ae6fa3b52671915fa81ee81cddbe740dd8698b
251         -         SHA384:
              5fa042c979faba67de861093b4aca808ae4be0fcedf123cb8afe126856c0b6ac3451393048211db
              8993914c5ff410bd8
252         -     Signer:
253         -     - SerialNumber: 560000077b478c76c9afcafcaf00000000077b
254         -       Issuer: C=US, ST=CA, L=Santa Clara, O=Intel Corporation, CN=Intel
              External Issuing
255         -         CA 7B
256         -       Version: 1
257         -   LoadsDespiteHVCI: 'FALSE'
258   57      - Authentihash:
259   58          MD5: 1789a16d20ca2b55f491ad71848166a2
260   59          SHA1: 2cbfe4ad0e1231ff3e19c19ca9311d952ce170b7
```

...l/651d1cdc-3e13-405f-b8b3-65cc70cef5a8.yaml

**Load Diff**

Large diffs are not rendered by default.

...l/7bb5ff05-25f8-410d-ae99-c8e8f082d24f.yaml

**Load Diff**

Large diffs are not rendered by default.

...l/8d23f7e6-341a-431e-9dc1-bc797773d411.yaml

```
@@ -0,0 +1,238 @@
+ Id: 8d23f7e6-341a-431e-9dc1-bc797773d411
+ Tags:
+ - shimano32.sys
+ - shimano64.sys
+ Verified: 'TRUE'
+ Author: Michael Haag
+ Created: '2026-03-20'
+ MitreID: T1068
+ Category: vulnerable driver
+ Commands:
+   Command: sc.exe create shimano binPath=C:\windows\temp\shimano64.sys type=kernel
+     && sc.exe start shimano
+   Description: HyperTech DNP CrackProof DRM kernel drivers (32-bit and 64-bit variants)
+     from Shimano E-TUBE Project. Expose EPROCESS manipulation IOCTLs (0xAA013880,
+     0xAA013884, 0xAA013888) similar to capcom.sys exploitation technique. Device
+     accessible at \\.\Htsysm4EFB. Zero detections (0/72 and 0/73) on VirusTotal.
+     Signed by Microsoft WHCP via HyperTech DNP CrackProof (Japanese DRM vendor).
+   Usecase: Elevate privileges
+   Privileges: kernel
+   OperatingSystem: Windows 10
+ Resources:
+ - https://github.com/magicsword-io/LOLDrivers/issues/163
+ Detection: []
+ Acknowledgement:
+   Person: Wack0
+   Handle: '@Wack0'
+ KnownVulnerableSamples:
+ - Filename: shimano32.sys
+   MD5: 6a4cced9a784369f50e618d85a16d234
+   SHA1: ae47836896e8e996d3dd6f860c63b95d011ee741
+   SHA256: e8b1a0ddc7a4404eb3c46217e07b5ed91723f44464a6ef589634aeb4fb8f5666
```

```
+   Signature:
+   - Microsoft Windows Hardware Compatibility Publisher
+   - Microsoft Windows Third Party Component CA 2014
+   - Microsoft Root Certificate Authority 2010
+   Date: '2021-10-01 00:11:36'
+   Publisher: Microsoft Windows Hardware Compatibility Publisher
+   Company: ''
+   Description: ''
+   Product: ''
+   ProductVersion: ''
+   FileVersion: ''
+   MachineType: I386
+   OriginalFilename: ''
+   Authentihash:
+     MD5: edadfe645e5fb9d921f81aa383b6fcac
+     SHA1: 632b17a46a046ee021b0d4e77c50c1cc0601865d
+     SHA256: 41011afde89ff9727fbd0380ec2d5cc733e1e0289d1f45d5bd45b7b1aa963aea
+   RichPEHeaderHash:
+     MD5: 9e8b6394a353fa378bfb1ecdec27cd1f
+     SHA1: bd28d0459b13b937ff9fafdf0aa0715553046d7a
+     SHA256: 139a965a13022e02329daa44012c9037fba79bb05b21e4f0d783cea2e0fa9aff
+   InternalName: ''
+   Copyright: ''
+   Imports:
+   - ntoskrnl.exe
+   ImportedFunctions:
+   - wcscat
+   - wcscpy
+   - IoDeleteDevice
+   - IoDeleteSymbolicLink
+   - RtlInitUnicodeString
+   - IofCompleteRequest
+   - KeQuerySystemTime
+   - PsGetCurrentProcessId
+   - IoGetCurrentProcess
+   - IoCreateSymbolicLink
+   - IoCreateDevice
+   ExportedFunctions: ''
+   Sections:
+     .text:
```

```
+       Entropy: 6.39
+       Virtual Size: '0x5a9'
+     .rdata:
+       Entropy: 2.57
+       Virtual Size: '0x9e'
+     .data:
+       Entropy: 0.26
+       Virtual Size: '0xd0'
+     .info:
+       Entropy: 1.65
+       Virtual Size: '0xa0'
+     INIT:
+       Entropy: 4.61
+       Virtual Size: '0x13e'
+     .reloc:
+       Entropy: 2.92
+       Virtual Size: '0x7e'
+   MagicHeader: 50 45 0 0
+   CreationTimestamp: '2021-10-01 00:11:36'
+   Imphash: df3935786e2f33563e5ace152d5d7517
+   Signatures:
+   - CertificatesInfo: ''
+     SignerInfo: ''
+     Certificates:
+     - Subject: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
  CN=Microsoft
+         Windows Hardware Compatibility Publisher
+       ValidFrom: '2020-12-15 22:25:28'
+       ValidTo: '2021-12-02 22:25:28'
+       Signature:
  3a8e15af3660c47a1def4303906af38b6ca69186409b4f44ebe8106ece701f6e00e734fe1d0bb29
  0d1496c3f17859e1f9ff1f31080dd8bfd2bb5013956c2f49ffe73916654f04c35b9df2fb27c55a7
  1df3d8e1f25185d398abed244b42e27741c0b1c953c139c011b801f00e80ea992005a1305dd65bc
  b2032790b0d87636b75d2fb8f431546cd906ab0a55083a26d2649d822871b6aacd1b4d8c74ea236
  6903eeb318e7826db64e3a858d6377cf2f9a628f21d6ef65279603c18d25d365dd370cef1a45527
  deec589a331a221c909a8b0d2010d078970678c648d62168056e3b775233eac20e50cc039a85900
  749f627a419e8959fcf21efc89da76426107e43261ccdcaebad659b89abfdd5d1a78e9d438868b9
  ff58cac5176bddff8c8dd11008ed72ed249bb7d78af559b04561e6b44aae7846b103d2db8c0e31a
  5f661851f97acba0757b474c1caa49cf8eed86de15a4118743a418b6b415e7770265801ba51061b
  5d32125ed5ba1e27fe83ac795f9cc868949b14d59eb4f596763da9102f9e6ae8fe92de61d68af67
```

```
a906e0be424f5c81dcecd4d190953a66384c3b5fe33f7b402a0934c2befd4a51b2f2850ef05e156
fc4e1460eab2f67e3cbc999db761f57970ccafbc49040e999965f5306c1f5c90ce172d889a3aa63
ec502a60020b2a7b4fff562b9dc5c50a8e06bc52f04ff0fe535591e2e6b7325239666152819a
+       SignatureAlgorithmOID: 1.2.840.113549.1.1.11
+       IsCertificateAuthority: false
+       SerialNumber: 33000000433a68189e33902987000000000043
+       Version: 3
+       CertificateType: Leaf (Code Signing)
+       IsCodeSigning: true
+       IsCA: false
+       TBS:
+         MD5: 3d790bd5602e84a4aa8560133ced0a41
+         SHA1: 909e31e3e3808ab55d508fc0ba47e0132a57d7ab
+         SHA256:
ac1acbcba260f10270527c3762457c1b96818466df9da51dfec3b147c90db453
+         SHA384:
c548f472f381df2da149c036e2f47be20293838eb23adce5e1b0ad1ba1fe8c33f688528452146c8
7dcb26070a2a23ced
+     - Subject: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
CN=Microsoft
+         Windows Third Party Component CA 2014
+       ValidFrom: '2014-10-15 20:31:27'
+       ValidTo: '2029-10-15 20:41:27'
+       Signature:
96b5c33b31f27b6ba11f59dd742c3764b1bca093f9f33347e9f95df21d89f4579ee33f10a359501
8053b142941b6a70e5b81a2ccbd8442c1c4bed184c2c4bd0c8c47bcbd8886fb5a0896ae2c2fdfbf
9366a32b20ca848a6945273f732332936a23e9fffdd918edceffbd6b41738d579cf8b46d499805e
6a335a9f07e6e86c06ba8086725afc0998cdba7064d4093188ba959e69914b912178144ac57c3ae
8eae947bcb3b8edd7ab4715bba2bc3c7d085234b371277a54a2f7f1ab763b94459ed9230cce47c0
99212111f52f51e0291a4d7d7e58f8047ff189b7fd19c0671dcf376197790d52a0fbc6c12c4c50c
2066f50e2f5093d8cafb7fe556ed09d8a753b1c72a6978dcf05fe74b20b6af63b5e1b15c804e9c7
aa91d4df72846782106954d32dd6042e4b61ac4f24636de357302c1b5e55fb92b59457a9243d7c4
e963dd368f76c728caa8441be8321a66cde5485c4a0a602b469206609698dcd933d721777f886da
c4772daa2466eab64682bd24e98fb35cc7fec3f136d11e5db77edc1c37e1f6a4a14f8b4a721c671
866770cdd819a35d1fa09b9a7cc55d4d728e74077fa74d00fcdd682412772a557527cda92c1d8e7
c19ee692c9f7425338208db38cc7cc74f6c3a6bc237117872fe55596460333e2edfc42de72cd7fb
0a82256fb8d70c84a5e1c4746e2a95329ea0fecdb4188fd33bad32b2b19ab86d0543fbff0d0f
+       SignatureAlgorithmOID: 1.2.840.113549.1.1.11
+       IsCertificateAuthority: true
+       SerialNumber: 330000000d690d5d7893d076df00000000000d
```

```
121 +       Version: 3
122 +       CertificateType: CA
123 +       IsCodeSigning: false
124 +       IsCA: true
125 +       TBS:
126 +         MD5: 83f69422963f11c3c340b81712eef319
127 +         SHA1: 0c5e5f24590b53bc291e28583acb78e5adc95601
128 +         SHA256:
    d8be9e4d9074088ef818bc6f6fb64955e90378b2754155126feebbbd969cf0ae
129 +         SHA384:
    260ad59ba706420f68ba212931153bd89f760c464b21be55fba9d014fff322407859d4ebfb78ea9
    a3330f60dc9821a63
130 +     Signer:
131 +     - SerialNumber: 33000000433a68189e33902987000000000043
132 +       Issuer: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
    CN=Microsoft
133 +         Windows Third Party Component CA 2014
134 +       Version: 1
135 + - Filename: shimano64.sys
136 +   MD5: c047c92696e5cef5485a22df97e6646e
137 +   SHA1: 37de60ae6adc042b596a90446ce12d53030c5db2
138 +   SHA256: e3a1f0d967335c8a080a5b1e7e3a06a61f6cea39739cda3ebab11d2908713d80
139 +   Signature:
140 +   - Microsoft Windows Hardware Compatibility Publisher
141 +   - Microsoft Windows Third Party Component CA 2014
142 +   - Microsoft Root Certificate Authority 2010
143 +   Date: '2021-10-01 00:11:36'
144 +   Publisher: Microsoft Windows Hardware Compatibility Publisher
145 +   Company: ''
146 +   Description: ''
147 +   Product: ''
148 +   ProductVersion: ''
149 +   FileVersion: ''
150 +   MachineType: AMD64
151 +   OriginalFilename: ''
152 +   Authentihash:
153 +     MD5: 08bbf3b41df7fb7629edf67fb9206e0c
154 +     SHA1: 06a02e1ec8d9fd2f25770706f0034e7d70d8290b
155 +     SHA256: bf8734d83d2b8bc9798ba931794504af791e9a0d913266fa39d41b574ce53d88
156 +   RichPEHeaderHash:
```

```
157 +     MD5: 1cae7fcf3f9627d90b3aa959faa5495d
158 +     SHA1: a6fdd5b1bebd1c134a1ff6e613d9694d2ad2f81d
159 +     SHA256: 46e9b36f8db362f22fa5d1fcd13371e9cd34ee5302ea3a7be320d7cf07815bbd
160 +   InternalName: ''
161 +   Copyright: ''
162 +   Imports:
163 +   - ntoskrnl.exe
164 +   ImportedFunctions:
165 +   - IoDeleteDevice
166 +   - IoDeleteSymbolicLink
167 +   - RtlInitUnicodeString
168 +   - IofCompleteRequest
169 +   - PsGetCurrentProcessId
170 +   - IoGetCurrentProcess
171 +   - IoCreateSymbolicLink
172 +   - IoCreateDevice
173 +   ExportedFunctions: ''
174 +   Sections:
175 +     .text:
176 +       Entropy: 6.38
177 +       Virtual Size: '0x677'
178 +     .rdata:
179 +       Entropy: 3.2
180 +       Virtual Size: '0x120'
181 +     .data:
182 +       Entropy: 0.18
183 +       Virtual Size: '0xd0'
184 +     .pdata:
185 +       Entropy: 3.26
186 +       Virtual Size: '0x6c'
187 +     .info:
188 +       Entropy: 1.67
189 +       Virtual Size: '0xa0'
190 +     INIT:
191 +       Entropy: 4.1
192 +       Virtual Size: '0x12e'
193 +   MagicHeader: 50 45 0 0
194 +   CreationTimestamp: '2021-10-01 00:11:36'
195 +   Imphash: df43355c636583e56e92142dcc69cc58
196 +   Signatures:
```

```
197 +   - CertificatesInfo: ''
198 +     SignerInfo: ''
199 +     Certificates:
200 +     - Subject: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
      CN=Microsoft
201 +         Windows Hardware Compatibility Publisher
202 +       ValidFrom: '2020-12-15 22:25:28'
203 +       ValidTo: '2021-12-02 22:25:28'
204 +       Signature:
      3a8e15af3660c47a1def4303906af38b6ca69186409b4f44ebe8106ece701f6e00e734fe1d0bb29
      0d1496c3f17859e1f9ff1f31080dd8bfd2bb5013956c2f49ffe73916654f04c35b9df2fb27c55a7
      1df3d8e1f25185d398abed244b42e27741c0b1c953c139c011b801f00e80ea992005a1305dd65bc
      b2032790b0d87636b75d2fb8f431546cd906ab0a55083a26d2649d822871b6aacd1b4d8c74ea236
      6903eeb318e7826db64e3a858d6377cf2f9a628f21d6ef65279603c18d25d365dd370cef1a45527
      deec589a331a221c909a8b0d2010d078970678c648d62168056e3b775233eac20e50cc039a85900
      749f627a419e8959fcf21efc89da76426107e43261ccdcaebad659b89abfdd5d1a78e9d438868b9
      ff58cac5176bddff8c8dd11008ed72ed249bb7d78af559b04561e6b44aae7846b103d2db8c0e31a
      5f661851f97acba0757b474c1caa49cf8eed86de15a4118743a418b6b415e7770265801ba51061b
      5d32125ed5ba1e27fe83ac795f9cc868949b14d59eb4f596763da9102f9e6ae8fe92de61d68af67
      a906e0be424f5c81dcecd4d190953a66384c3b5fe33f7b402a0934c2befd4a51b2f2850ef05e156
      fc4e1460eab2f67e3cbc999db761f57970ccafbc49040e999965f5306c1f5c90ce172d889a3aa63
      ec502a60020b2a7b4fff562b9dc5c50a8e06bc52f04ff0fe535591e2e6b7325239666152819a
205 +       SignatureAlgorithmOID: 1.2.840.113549.1.1.11
206 +       IsCertificateAuthority: false
207 +       SerialNumber: 33000000433a68189e33902987000000000043
208 +       Version: 3
209 +       CertificateType: Leaf (Code Signing)
210 +       IsCodeSigning: true
211 +       IsCA: false
212 +       TBS:
213 +         MD5: 3d790bd5602e84a4aa8560133ced0a41
214 +         SHA1: 909e31e3e3808ab55d508fc0ba47e0132a57d7ab
215 +         SHA256:
      ac1acbcba260f10270527c3762457c1b96818466df9da51dfec3b147c90db453
216 +         SHA384:
      c548f472f381df2da149c036e2f47be20293838eb23adce5e1b0ad1ba1fe8c33f688528452146c8
      7dcb26070a2a23ced
217 +     - Subject: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
      CN=Microsoft
218 +         Windows Third Party Component CA 2014
```

```
+       ValidFrom: '2014-10-15 20:31:27'
+       ValidTo: '2029-10-15 20:41:27'
+       Signature:
  96b5c33b31f27b6ba11f59dd742c3764b1bca093f9f33347e9f95df21d89f4579ee33f10a359501
  8053b142941b6a70e5b81a2ccbd8442c1c4bed184c2c4bd0c8c47bcbd8886fb5a0896ae2c2fdfbf
  9366a32b20ca848a6945273f732332936a23e9fffdd918edceffbd6b41738d579cf8b46d499805e
  6a335a9f07e6e86c06ba8086725afc0998cdba7064d4093188ba959e69914b912178144ac57c3ae
  8eae947bcb3b8edd7ab4715bba2bc3c7d085234b371277a54a2f7f1ab763b94459ed9230cce47c0
  99212111f52f51e0291a4d7d7e58f8047ff189b7fd19c0671dcf376197790d52a0fbc6c12c4c50c
  2066f50e2f5093d8cafb7fe556ed09d8a753b1c72a6978dcf05fe74b20b6af63b5e1b15c804e9c7
  aa91d4df72846782106954d32dd6042e4b61ac4f24636de357302c1b5e55fb92b59457a9243d7c4
  e963dd368f76c728caa8441be8321a66cde5485c4a0a602b469206609698dcd933d721777f886da
  c4772daa2466eab64682bd24e98fb35cc7fec3f136d11e5db77edc1c37e1f6a4a14f8b4a721c671
  866770cdd819a35d1fa09b9a7cc55d4d728e74077fa74d00fcdd682412772a557527cda92c1d8e7
  c19ee692c9f7425338208db38cc7cc74f6c3a6bc237117872fe55596460333e2edfc42de72cd7fb
  0a82256fb8d70c84a5e1c4746e2a95329ea0fecdb4188fd33bad32b2b19ab86d0543fbff0d0f
+       SignatureAlgorithmOID: 1.2.840.113549.1.1.11
+       IsCertificateAuthority: true
+       SerialNumber: 330000000d690d5d7893d076df00000000000d
+       Version: 3
+       CertificateType: CA
+       IsCodeSigning: false
+       IsCA: true
+       TBS:
+         MD5: 83f69422963f11c3c340b81712eef319
+         SHA1: 0c5e5f24590b53bc291e28583acb78e5adc95601
+         SHA256:
  d8be9e4d9074088ef818bc6f6fb64955e90378b2754155126feebbbd969cf0ae
+         SHA384:
  260ad59ba706420f68ba212931153bd89f760c464b21be55fba9d014fff322407859d4ebfb78ea9
  a3330f60dc9821a63
+     Signer:
+     - SerialNumber: 33000000433a68189e33902987000000000043
+       Issuer: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
  CN=Microsoft
+         Windows Third Party Component CA 2014
+       Version: 1
```

...l/bb808089-5857-4df2-8998-753a7106cb44.yaml

```
@@ -162,123 +162,3 @@ KnownVulnerableSamples:
```

```
162 162         Version: 1
163 163       Imphash: f138fdbc6c7fbf73e135717c7d7eac27
164 164       LoadsDespiteHVCI: 'TRUE'
165     - - Authentihash:
166     -     MD5: 1e96108c0938d4c34d7072f04bc8b951
167     -     SHA1: d46ae9bcc746ca408fbb55fb0d61b638720a8f25
168     -     SHA256: 7bacb353363cc29f7f3815a9d01e85cd86202d92378d1ab1b11df1ab2f42f40a
169     -   Company: Dell
170     -   Copyright: "\xA9 2021 Dell Inc. All Rights Reserved. "
171     -   CreationTimestamp: '2021-05-06 19:20:18'
172     -   Date: ''
173     -   Description: DBUtil
174     -   ExportedFunctions: ''
175     -   FileVersion: ''
176     -   Filename: DBUtilDrv2.sys
177     -   ImportedFunctions:
178     -   - MmMapIoSpace
179     -   - MmUnmapIoSpace
180     -   - MmAllocateContiguousMemorySpecifyCache
181     -   - KeSetPriorityThread
182     -   - MmGetPhysicalAddress
183     -   - KeBugCheckEx
184     -   - KeInsertQueueDpc
185     -   - RtlCopyUnicodeString
186     -   - IoWMIRegistrationControl
187     -   - MmGetSystemRoutineAddress
188     -   - MmFreeContiguousMemorySpecifyCache
189     -   - RtlInitUnicodeString
190     -   - WdfVersionBind
191     -   - WdfVersionUnbind
192     -   - WdfVersionUnbindClass
193     -   - WdfVersionBindClass
194     -   Imports:
195     -   - ntoskrnl.exe
196     -   - WDFLDR.SYS
197     -   InternalName: ''
198     -   MD5: d104621c93213942b7b43d65b5d8d33e
199     -   MachineType: AMD64
200     -   MagicHeader: 50 45 0 0
201     -   OriginalFilename: ''
```

```
-   Product: DBUtil
-   ProductVersion: 2.7.0.0
-   Publisher: ''
-   RichPEHeaderHash:
-     MD5: 55da99917deafbd2428eba37ab352764
-     SHA1: 72420433a55e6c3b3dd02e90ad238c5f5f632344
-     SHA256: 7c8e32c30b6f8a981e4b54696e979a23cc9662b6440c2c8833494bc6d17cd9fe
-   SHA1: b03b1996a40bfea72e4584b82f6b845c503a9748
-   SHA256: 71fe5af0f1564dc187eea8d59c0fbc897712afa07d18316d2080330ba17cf009
-   Sections:
-     .text:
-       Entropy: 6.230478937617782
-       Virtual Size: '0x1039'
-     .rdata:
-       Entropy: 4.642223343654196
-       Virtual Size: '0x754'
-     .data:
-       Entropy: 0.808730421176234
-       Virtual Size: '0xfe0'
-     .pdata:
-       Entropy: 3.9589762468524823
-       Virtual Size: '0x1bc'
-     PAGE:
-       Entropy: 6.243717098384845
-       Virtual Size: '0x118c'
-     INIT:
-       Entropy: 5.874007861559603
-       Virtual Size: '0x47a'
-     .rsrc:
-       Entropy: 3.174963077143067
-       Virtual Size: '0x2c0'
-     .reloc:
-       Entropy: 3.2464393446710145
-       Virtual Size: '0x28'
-   Signature:
-   - Microsoft Windows Hardware Compatibility Publisher
-   - Microsoft Windows Third Party Component CA 2012
-   - Microsoft Root Certificate Authority 2010
-   Signatures:
-   - CertificatesInfo: ''
```

```
242 -     SignerInfo: ''
243 -     Certificates:
244 -     - Subject: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
      CN=Microsoft
245 -         Windows Hardware Compatibility Publisher
246 -       ValidFrom: '2020-12-15 22:15:33'
247 -       ValidTo: '2021-12-02 22:15:33'
248 -       Signature:
      0d2d53cd15a8feddcb17e2df1bf7dc1aef21e98c6cd220f58b593824849c134a0f1add59ce42ef8
      0ddf47860273013604d9568ec5894a797bd4e571432a9aaf10ab04dd1c038b26ab7c5ca3a9c88d0
      09267fab56254525546a0a055fb37b9cd8029c7d501809fc8b11482c7a4347b3ad29f35427c9570
      e87117db52cc94864259274b9e2e758f918a3af1fdb9f9d40ffa3ae2e2ae012fb97a436258642a2
      a4223dc6690db88103a6e5220646bd8afb3d12eb894ac28b527396a1965408487f6ab878b3c474b
      8c960842861ae8e799a3d2a8d6f918f50f8e26bb1ed6ced47be36e447574e8568582964ff31cd28
      8b9c7f8d7e6a46d6c3d92f5c101fe1522a720c
249 -       SignatureAlgorithmOID: 1.2.840.113549.1.1.11
250 -       IsCertificateAuthority: false
251 -       SerialNumber: 33000000b5213fca1e4aa03de40000000000b5
252 -       Version: 3
253 -       CertificateType: Leaf (Code Signing)
254 -       IsCodeSigning: true
255 -       IsCA: false
256 -       TBS:
257 -         MD5: a0dd89c33c4973bf6758331e200fb6de
258 -         SHA1: 65ff7fa429c0f08f8a8bf30509e8ca2919d9edb5
259 -         SHA256:
      29a7b646af062aee3bf37d1ba190211365116db7d7aa4cb87ba268843262ae47
260 -         SHA384:
      a7ac729302762483ea304ff2660a2ce2f5fa67cbbfc3f6df32a8feafa3852812c9bb8f705014007
      9aad1dec8119ee88e
261 -     - Subject: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
      CN=Microsoft
262 -         Windows Third Party Component CA 2012
263 -       ValidFrom: '2012-04-18 23:48:38'
264 -       ValidTo: '2027-04-18 23:58:38'
265 -       Signature:
      5a8a67daccd5fd0d264177bf0a4678b4b3de12692b7723c2652f015fd203f461ba509d2e8c3972f
      36c3e6ab11e766decb7f382dcccbbc56970287366173f54ebee011648c446d91b80ae813a8d0f79
      6d68b09eea2d3f39d3ca387ebd5e7c086e19dcc6c2f438336861e2524783e1000156d2bacb87820
      5310a418b4ee77f5f5fed5fd3392d45eba213bffd1ec298417161165fc80a70257c59693124e471
```

```
e70abb0417f79f721ec9d2bb1abe3d02fe090cb243b4591a99539396215fe0d6b72601429536ac2
7fdbef48577683d18bdf4be98882211865216f345ec0397107087a37043713cdbc98603170cf573
5bc67de15c64edd7c548d7ed32e2d1aad3cfa7f6574e61f977eb67f288b3de00da038fd08a34373
e1dd862b8d2b1f3e12f8b723b81967c6ffcec667672601b24f2a0896d5b6d002eef28dd868705c2
b4b9e5be64c22af24a155c98e2c42785ff52e3627e0fb2020bd766c70ab2d33d200414503259830
a7d9bed5a38120152ba2f5e20728e4af1fde771028c3be107bec973f4dd47d8b4efb4a4b330b989
3e76cab90098567eabea8ab8a5d038ab6977130b142fe9aa411ff7babd3a2b348aee0aab63e663f
788248e200d2b3b9de3c24952ac9f1f0e393b5dd46e506ae67d523aaa7c3315290d265e0158a74e
a93d7a846f743f609fe4324f3600af6d71d33ea646655f8174f1fec171da4ca0415a82ddf11f
- SignatureAlgorithmOID: 1.2.840.113549.1.1.11
- IsCertificateAuthority: true
- SerialNumber: 610baac1000000000009
- Version: 3
- CertificateType: CA
- IsCodeSigning: false
- IsCA: true
- TBS:
-   MD5: a569061297e8e824767dbc3184a69bea
-   SHA1: adbb26a587a8f44b4fccaecb306f980d1c55a150
-   SHA256:
cec1afd0e310c55c1dcc601ab8e172917706aa32fb5eaf826813547fdf02dd46
-   SHA384:
e947cac936803f5683196e4ff1b259096073395d0b908522ddce90d57597c9f7b57f7ddcdbe021b
a863d843c340da8ba
-  Signer:
-  - SerialNumber: 33000000b5213fca1e4aa03de40000000000b5
-    Issuer: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
CN=Microsoft
-      Windows Third Party Component CA 2012
-    Version: 1
-  Imphash: 506a31d768aec26b297c45b50026c820
-  LoadsDespiteHVCI: 'TRUE'
```

...l/f4990bdd-8821-4a3c-a11a-4651e645810c.yaml

```
@@ -5,6 +5,8 @@ Verified: 'TRUE'
5  5  Author: Michael Haag
6  6  Created: '2023-01-09'
7  7  MitreID: T1068
   8  + CVE:
   9  + - CVE-2024-41498
```

```
 8  10    Category: vulnerable driver
 9  11    Commands:
10  12      Command: sc.exe create IOMap64.sys binPath=C:\windows\temp\IOMap64.sys
          type=kernel
          @@ -15,6 +17,7 @@ Commands:
15  17      Usecase: Elevate privileges
16  18    Resources:
17  19    - https://github.com/elastic/protections-artifacts/search?q=VulnDriver
    20  + - https://www.asus.com/content/asus-product-security-advisory/
18  21    Detection:
19  22    - type: yara_signature
20  23      value: https://github.com/magicsword-
          io/LOLDrivers/blob/main/detections/yara/ea85bbe63d6f66f7efee7007e770af820d57f91
          4c7f179c5fee3ef2845f19c41.yara
          @@ -209,3 +212,147 @@ KnownVulnerableSamples:
209 212          Version: 1
210 213      Imphash: 9928d53dbe860aba1b7c891831680629
211 214      LoadsDespiteHVCI: 'FALSE'
    215  + - Filename: IOMap64.sys
    216  +   MD5: 4da690ba853b12927fafd6b6387828cf
    217  +   SHA1: 849bcfd80ecfe74e5344238d5ea219ee8e2bcf14
    218  +   SHA256: e62d0c1353a3d913497e6016d0f48d7cf9ef99e4026b94ccd873d6c7a9a54565
    219  +   Authentihash:
    220  +     MD5: 7651960891e16982932b8036cb8cbd34
    221  +     SHA1: b4b275af4ab6fcddebc68948c103ba5882c7b1e2
    222  +     SHA256: e6d1017bb3ef8198ab693b8a3cecb14263d7d132678610348440ce64e147cf3a
    223  +   Description: 'ASUS Kernel Mode Driver for NT '
    224  +   Company: ASUSTeK Computer Inc.
    225  +   InternalName: IOMap.sys
    226  +   OriginalFilename: IOMap.sys
    227  +   FileVersion: '2.50'
    228  +   Product: ASUS Kernel Mode Driver for Windows
    229  +   ProductVersion: '2.50'
    230  +   Copyright: Copyright 2023 ASUSTeK Computer Inc.
    231  +   MachineType: AMD64
    232  +   Imports:
    233  +   - ntoskrnl.exe
    234  +   - HAL.dll
    235  +   ExportedFunctions: ''
```

```
236 +   ImportedFunctions:
237 +   - ExAllocatePoolWithTag
238 +   - ExFreePoolWithTag
239 +   - MmMapIoSpace
240 +   - MmUnmapIoSpace
241 +   - IofCompleteRequest
242 +   - IoCreateSymbolicLink
243 +   - KeInitializeMutex
244 +   - IoDeleteSymbolicLink
245 +   - PoCallDriver
246 +   - PoStartNextPowerIrp
247 +   - KeReleaseMutex
248 +   - KeWaitForSingleObject
249 +   - KeBugCheckEx
250 +   - ZwCreateKey
251 +   - RtlInitUnicodeString
252 +   - IoDeleteDevice
253 +   - __C_specific_handler
254 +   - MmGetSystemRoutineAddress
255 +   - ZwClose
256 +   - ZwSetSecurityObject
257 +   - IoDeviceObjectType
258 +   - IoCreateDevice
259 +   - ObOpenObjectByPointer
260 +   - RtlGetDaclSecurityDescriptor
261 +   - RtlGetGroupSecurityDescriptor
262 +   - RtlGetOwnerSecurityDescriptor
263 +   - RtlGetSaclSecurityDescriptor
264 +   - SeCaptureSecurityDescriptor
265 +   - _snwprintf
266 +   - RtlLengthSecurityDescriptor
267 +   - SeExports
268 +   - RtlCreateSecurityDescriptor
269 +   - _wcsnicmp
270 +   - wcschr
271 +   - RtlAbsoluteToSelfRelativeSD
272 +   - RtlAddAccessAllowedAce
273 +   - RtlLengthSid
274 +   - IoIsWdmVersionAvailable
275 +   - RtlSetDaclSecurityDescriptor
```

```
276 +    - ZwOpenKey
277 +    - ZwSetValueKey
278 +    - ZwQueryValueKey
279 +    - RtlFreeUnicodeString
280 +    - KeStallExecutionProcessor
281 +    - HalTranslateBusAddress
282 +   Signatures:
283 +    - CertificatesInfo: ''
284 +      SignerInfo: ''
285 +      Certificates:
286 +      - Subject: C=US, O=DigiCert, Inc., CN=DigiCert Trusted G4 Code Signing
      RSA4096
287 +          SHA384 2021 CA1
288 +        ValidFrom: '2021-04-29 00:00:00'
289 +        ValidTo: '2036-04-28 23:59:59'
290 +        Signature:
      3a23443d8d0876ee8fbc3a99d356e0021aa5f84834f32cb6e67466f79472b100caaf6c302713129
      e90449f4bfd9ea37c26d537bc3a5d486d95d53f49f427bb16814550fd9cbdb685e0767e3771cb22
      f75aaa90cff5936ae3eb20d1d55079889a8a8ac1b6bda148187edcd8801a111918cd61998156f6c
      9e376e7c4e41b5f43f83e94ff76393d9ed499cf4add28eb5f26a1955848d51afed7273ffd90d176
      86dd1cb0605cf30da8eee089a1bd39e1384eda6ebb369dfbe521535ac3cae96af1a23edb43b833c
      84f38149299f5ddce546dd95d02141f40337c03e295b2c221757352cb46d8c4341ca2a54b8dcd6f
      76372c853f1ace26e918be9007b0437f9588208270f0cccaeffd29355c1f893855f7378a8b09a1c
      b0be9311aff2e195c3971e1be9ca70a06d62667b792e64e5fde7aac49cf2ea47492addb3ca49c86
      1fe3c1561b2b23ff8fb5ea887b706be6a0bafd3a3f45a6c4e81691528b41c048844b964dab4440e
      38df01528ceedf11856072a2f10c40c08643c338fae288c3ccb8f880b0dbf3bf4ce1e7b8eefb5eb
      cbb7f07713e6e7283fac12aea52f226c41f9825c1566cc6c0ecac586c3f626330c074ba0d307026
      a6a4030484b34a85120bbad1b8508e2590d6dca05502bea4a1c9ea5fda0a71f0674e7f2d65290fd
      af854821f9573bb49c03ed8645f4b4616ebf68e2266086eac8afa9fe941de7631b3a8656784e
291 +        SignatureAlgorithmOID: 1.2.840.113549.1.1.12
292 +        IsCertificateAuthority: true
293 +        SerialNumber: 08ad40b260d29c4c9f5ecda9bd93aed9
294 +        Version: 3
295 +        CertificateType: CA
296 +        IsCodeSigning: true
297 +        IsCA: true
298 +        TBS:
299 +          MD5: 5d8003a64dfa5a4d88365da1566038cb
300 +          SHA1: 79465b56bc7ad55a37bdf633943da8bfc84db228
```

```
301 +         SHA256:
    84bdc82e2f2a7f7aaa782667dac556ffcb2b33240c1f9c0a00a3264526a98332
302 +         SHA384:
    65b1d4076a89ae273f57e6eeedecb3eae129b4168f76fa7671914cdf461d542255c59d9b85b916a
    e0ca6fc0fcf7a8e64
303 +     - Subject: JURISDICTION_OF_INCORPORATION_C=TW, BUSINESS_CATEGORY=Private
    Organization,
304 +         serialNumber=23638777, C=TW, ST=Taipei City, L=Beitou District,
    O=ASUSTeK
305 +         COMPUTER INC., CN=ASUSTeK COMPUTER INC.
306 +       ValidFrom: '2022-04-08 00:00:00'
307 +       ValidTo: '2025-03-27 23:59:59'
308 +       Signature:
    937c645145253f3315a6d3da886d6ee5f03621a74b2266721cc6d71f96dbc73b7b0e9ce33a2a887
    118c3282c254f2d3686d322edc371b3845b542efecf88f147532486206aa7e887e71d296535fc03
    4117402f30740b99f9f12edc3328e8ce2f6ca4544bcb475e0893206bec0bb5f9948fef5c677d9c0
    56be02531ee23d35f5933de8bcd98650d722d445a797d0278cc990f0102999307cade1d224bc7c7
    f46cd5c12130a5e1b6eb8849b6f00a994c575ba29baa67e850d85d8488916e2ae52565ee22bbe71
    b7e3d3fa623e9f228879a679b1c538a676b4b79475ddb5b78da076197d294fb90a5cc8036611aa1
    d6809ea85ccf5e6e5473537812eaaeab322951447fcf35a1be2ba84f31b264e4bb61b4382a97862
    7632f9155d62560a11e5210d5888b31faa79bb71a51201e281c1ac36380f5e8fa2a87df33396991
    2400ac7a6bbe93592e28726a9688585c44f030917615e1bd11f7c3aa863eb05e30831fff9a624db
    6a1233db9ac2b46ec1fc8bb7a8104ff049621d9ef61be13d76eda0a573de6a370d185fc7ce4c522
    f2450b26b4cf5a9d804778c4ad05e0c782502187dd7c090c18c3b001d60a21e89f76be044d1ce40
    cd6e7ff40fd9d9ec8557fe275cea2d78b5bdc8b0359a9f4403c9923385dd5fdf865e6fff883ecdb
    5b12d185691411e2fb37077571f738b95736ce34a7fc276a1462a25f521bf5c9091a5941911f
309 +       SignatureAlgorithmOID: 1.2.840.113549.1.1.11
310 +       IsCertificateAuthority: false
311 +       SerialNumber: 0414dcf7ac18be7b0e5d1db9a3fee469
312 +       Version: 3
313 +       CertificateType: Leaf (Code Signing)
314 +       IsCodeSigning: true
315 +       IsCA: false
316 +       TBS:
317 +         MD5: 57dbc9dba7e9561f375fcc5b9033b319
318 +         SHA1: f85e6de5d479506c2a3dabab8491d9e0bba33603
319 +         SHA256:
    86107afeccad1c24431c5ed73b3621705c4eaaf93ab68fa9360ff50c44e94a4a
320 +         SHA384:
    6450ff6a38ec387a2c2ab23e327a0d7e735fee3e6c4be5e07e4453f9705005967a6c4ee5b1d98d9
```

```
    284b94b6e5675d975
321 +     Signer:
322 +     - SerialNumber: 0414dcf7ac18be7b0e5d1db9a3fee469
323 +       Issuer: C=US, O=DigiCert, Inc., CN=DigiCert Trusted G4 Code Signing
    RSA4096
324 +         SHA384 2021 CA1
325 +       Version: 1
326 +   RichPEHeaderHash:
327 +     MD5: 07d607cfdadf931605cb55702c16b391
328 +     SHA1: bcb28f8f7a4ed0f3020b572e8190e3e04a527ea8
329 +     SHA256: 9a774274259d13fecb0eee265a4b312954a4fc61cf54e932eff813cc7c432d48
330 +   Sections:
331 +     .text:
332 +       Entropy: 6.28
333 +       Virtual Size: '0x32d8'
334 +     .rdata:
335 +       Entropy: 4.42
336 +       Virtual Size: '0x124c'
337 +     .data:
338 +       Entropy: 1.27
339 +       Virtual Size: '0x4d6'
340 +     .pdata:
341 +       Entropy: 4.37
342 +       Virtual Size: '0x48c'
343 +     PAGE:
344 +       Entropy: 6.23
345 +       Virtual Size: '0x1c8c'
346 +     INIT:
347 +       Entropy: 5.25
348 +       Virtual Size: '0x63a'
349 +     .rsrc:
350 +       Entropy: 3.29
351 +       Virtual Size: '0x418'
352 +     .reloc:
353 +       Entropy: 3.81
354 +       Virtual Size: '0x38'
355 +   MagicHeader: 50 45 0 0
356 +   CreationTimestamp: '2023-01-18 23:35:19'
357 +   Imphash: 892a0ac24a43307d5efc9e8365227577
358 +   LoadsDespiteHVCI: 'FALSE'
```

...l/f4e00816-97a8-4c2d-b990-9812f16fe3d3.yaml

```
@@ -0,0 +1,190 @@
+ Id: f4e00816-97a8-4c2d-b990-9812f16fe3d3
+ Tags:
+ - athpexnt.sys
+ Verified: 'TRUE'
+ Author: Michael Haag
+ Created: '2026-03-20'
+ MitreID: T1068
+ Category: vulnerable driver
+ Commands:
+   Command: sc.exe create ATHpExNt binPath=C:\windows\temp\ATHpExNt.sys type=kernel
+     && sc.exe start ATHpExNt
+   Description: AhnLab kernel driver exposing arbitrary physical memory read/write
+     via IOCTL 0x81000000. Device accessible at \\.\ATHpEx. Signed by AhnLab Inc.
+     with VeriSign certificate (first seen 2014). Zero detections (0/73) on VirusTotal
+     but exploitable for privilege escalation by mapping attacker-controlled physical
+     memory into kernel address space.
+   Usecase: Elevate privileges
+   Privileges: kernel
+   OperatingSystem: Windows 10
+ Resources:
+ - https://github.com/magicsword-io/LOLDrivers/issues/255
+ Detection: []
+ Acknowledgement:
+   Person: ''
+   Handle: ''
+ KnownVulnerableSamples:
+ - Filename: ATHpExNt.sys
+   MD5: bf77a19e1396d6d36e32ff8d23eb5d3f
+   SHA1: e630a14b4c74264cbe702999f78750ec49359ca4
+   SHA256: fa0902daefbd9e716faaac8e854144ea0573e2a41192796f3b3138fe7a1d19f1
+   Signature:
+   - AhnLab, Inc.
```

```
+   - VeriSign Class 3 Code Signing 2010 CA
+   - VeriSign Class 3 Public Primary Certification Authority - G5
+   Date: '2012-04-29 20:42:46'
+   Publisher: AhnLab, Inc.
+   Company: AhnLab, Inc.
+   Description: Sample Driver (AMD64)
+   Product: AhnLab Security Product
+   ProductVersion: 7.0.0.0
+   FileVersion: 1,0,0,2
+   MachineType: AMD64
+   OriginalFilename: ATHpExNt.sys
+   Authentihash:
+     MD5: 2beabc796f5ba54d9cb08c6db2aa2490
+     SHA1: 4cd5fa8a875644fc803013dc4bfb116b13d70dc1
+     SHA256: fc22650cae4722a174da31addbaf088a04ad4f8b2460191da946b3de529f6a0a
+   RichPEHeaderHash:
+     MD5: f24fecff070d6de48f8452f084ca59a2
+     SHA1: f5a1c90789bff98da7f5b31dfbe4eedcb430f7c6
+     SHA256: 71626f35f23efa838db49ff74d9788a1f7784ebdae11b7885c3994eb4365fe3b
+   InternalName: ATHpExNt.sys
+   Copyright: Copyright(C) 2005 AhnLab, Inc.
+   Imports:
+   - ntoskrnl.exe
+   ImportedFunctions:
+   - IoDeleteDevice
+   - IoDeleteSymbolicLink
+   - RtlInitUnicodeString
+   - IofCompleteRequest
+   - IoCreateSymbolicLink
+   - IoCreateDevice
+   - __C_specific_handler
+   - MmUnmapIoSpace
+   - MmMapIoSpace
+   - MmGetPhysicalAddress
+   - MmUnlockPages
+   - MmMapLockedPagesSpecifyCache
+   - IoFreeMdl
+   - MmProbeAndLockPages
+   - IoAllocateMdl
+   ExportedFunctions: ''
```

```
+   Sections:
+     .text:
+       Entropy: 5.01
+       Virtual Size: '0x74e'
+     .rdata:
+       Entropy: 4.09
+       Virtual Size: '0x150'
+     .data:
+       Entropy: 0.7
+       Virtual Size: '0x128'
+     .pdata:
+       Entropy: 3.21
+       Virtual Size: '0x60'
+     INIT:
+       Entropy: 4.88
+       Virtual Size: '0x25c'
+     .rsrc:
+       Entropy: 3.32
+       Virtual Size: '0x368'
+   MagicHeader: 50 45 0 0
+   CreationTimestamp: '2012-04-29 20:42:46'
+   Imphash: 3bac3002e583d000a28f76a62f67bfed
+   Signatures:
+   - CertificatesInfo: ''
+     SignerInfo: ''
+     Certificates:
+     - Subject: C=US, O=VeriSign, Inc., CN=VeriSign Time Stamping Services
  Signer
+         , G2
+       ValidFrom: '2007-06-15 00:00:00'
+       ValidTo: '2012-06-14 23:59:59'
+       Signature:
  50c54bc82480dfe40d24c2de1ab1a102a1a6822d0c831581370a820e2cb05a1761b5d805fe88dbf
  19191b3561a40a6eb92be3839b07536743a984fe437ba9989ca95421db0b9c7a08d57e0fad56404
  42354e01d133a217c84daa27c7f2e1864c02384d8378c6fc53e0ebe00687dda4969e5e0c98e2a5b
  ebf8285c360e1dfad28d8c7a54b64dac71b5bbdac3908d53822a1338b2f8a9aebbc07213f444109
  07b5651c24bc48d34480eba1cfc902b414cf54c716a3805cf9793e5d727d88179e2c43a2ca53ce7
  d3df62a3ab84f9400a56d0a835df95e53f418b3570f70c3fbf5ad95a00e17dec4168060c90f2b6e
  8604f1ebf47827d105c5ee345b5eb94932f233
+       SignatureAlgorithmOID: 1.2.840.113549.1.1.5
```

```
105 +       IsCertificateAuthority: false
106 +       SerialNumber: 3825d7faf861af9ef490e726b5d65ad5
107 +       Version: 3
108 +       CertificateType: Intermediate
109 +       IsCodeSigning: false
110 +       IsCA: false
111 +       TBS:
112 +         MD5: d6c7684e9aaa508cf268335f83afe040
113 +         SHA1: 18066d20ad92409c567cdfde745279ff71c75226
114 +         SHA256:
    a612fb22ce8be6dab75e47c98508f98496583e79c9c97b936a8caee9ea9f3fff
115 +         SHA384:
    35c249d6ad0261a6229b2a727067ac6ba32a5d24b30b9249051f748c7735fbe2ec2ef26a702c50d
    f1790fbe32a65aee7
116 +     - Subject: C=US, O=VeriSign, Inc., CN=VeriSign Time Stamping Services CA
117 +       ValidFrom: '2003-12-04 00:00:00'
118 +       ValidTo: '2013-12-03 23:59:59'
119 +       Signature:
    4a6bf9ea58c2441c318979992b96bf82ac01d61c4ccdb08a586edf0829a35ec8ca9313e704520de
    f47272f0038b0e4c9934e9ad4226215f73f37214f703180f18b3887b3e8e89700fecf55964e24d2
    a9274e7aaeb76141f32acee7c9d95eddbb2b853eb59db5d9e157ffbeb4c57ef5cf0c9ef097fe2bd
    33b521b1b3827f73f4a
120 +       SignatureAlgorithmOID: 1.2.840.113549.1.1.5
121 +       IsCertificateAuthority: true
122 +       SerialNumber: 47bf1995df8d524643f7db6d480d31a4
123 +       Version: 3
124 +       CertificateType: CA
125 +       IsCodeSigning: false
126 +       IsCA: true
127 +       TBS:
128 +         MD5: 518d2ea8a21e879c942d504824ac211c
129 +         SHA1: 21ce87d827077e61abddf2beba69fde5432ea031
130 +         SHA256:
    1ec3b4f02e03930a470020e0e48d24b84678bb558f46182888d870541f5e25c7
131 +         SHA384:
    53e346bbde23779a5d116cc9d86fdd71c97b1f1b343439f8a11aa1d3c87af63864bb8488a5aeb2d
    0c26a6a1e0b15f03f
132 +     - Subject: C=KR, ST=Seoul, L=Yeongdeungpo,gu, O=AhnLab, Inc., OU=Digital ID
133 +         Class 3 , Microsoft Software Validation v2, CN=AhnLab, Inc.
134 +       ValidFrom: '2011-05-23 00:00:00'
```

```
135 +       ValidTo: '2012-05-22 23:59:59'
136 +       Signature:
      42cadb90fbd3c01da180632af9ad044a8b07bd46aa56506d4cc2cb88d088b3ebfdf28ff7fa466f5
      b8babfef6756d6c7e963dde652f6ebfbd60ae934ea33345c73b69060ed933a4a60d3de858428273
      2ee977244b4ece00ab67463db80c0c9e06fbc57cb57527fa776668636d5478122facaba4216ad93
      261ab4d922a12812548a43d5c4a736d7fba599fa24f333814c44994ad02f045775356abad733dd5
      705c0b5b278274617d271f52dd6cbf91b19612447b8a0e620a34d983d6f4987abc6d36c39276b0d
      9638e855b17ffa591368c63660ef9265158cc042a22b593acf9091b9599218ae41434e7f00254ba
      ea83d97475f45f87be7463b18ae5664d37240f
137 +       SignatureAlgorithmOID: 1.2.840.113549.1.1.5
138 +       IsCertificateAuthority: false
139 +       SerialNumber: 2badad20ccbc170164bdec8fbca06924
140 +       Version: 3
141 +       CertificateType: Leaf (Code Signing)
142 +       IsCodeSigning: true
143 +       IsCA: false
144 +       TBS:
145 +         MD5: 560c013af6edf1b1088644c0290c64ed
146 +         SHA1: 8626a75b2e1ab18ccb06bb8d0c544e516a8e177b
147 +         SHA256:
      5592c238b5ecae534db714f6225e5b949406476f96259893b701c931e0a5c9b5
148 +         SHA384:
      5cbde52a7702edb411ecc34feda6f93fa20f0662fe6539f081586fc626b9f806883d6d7ee979765
      ca6a34cd78875dd0c
149 +     - Subject: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 2006
      VeriSign,
150 +         Inc. , For authorized use only, CN=VeriSign Class 3 Public Primary
      Certification
151 +         Authority , G5
152 +       ValidFrom: '2011-02-22 19:25:17'
153 +       ValidTo: '2021-02-22 19:35:17'
154 +       Signature:
      812a82168c34672be503eb347b8ca2a3508af45586f11e8c8eae7dee0319ce72951848ad6211fd2
      0fd3f4706015ae2e06f8c152c4e3c6a506c0b36a3cf7a0d9c42bc5cf819d560e369e6e22341678c
      6883762b8f93a32ab57fbe59fba9c9b2268fcaa2f3821b983e919527978661ee5b5d076bcd86a8e
      26580a8e215e2b2be23056aba0cf347934daca48c077939c061123a050d89a3ec9f578984fbecca
      7c47661491d8b60f195de6b84aacbc47c8714396e63220a5dc7786fd3ce38b71db7b9b03fcb71d3
      264eb1652a043a3fa2ead59924e7cc7f233424838513a7c38c71b242228401e1a461f17db18f7f0
      27356cb863d9cdb9645d2ba55eefc629b4f2c7f821cc04ba57fd01b6abc667f9e7d3997ff4f522f
      a72f5fdff3a1c423aa1f98018a5ee8d1cd4669e4501feaaeefffb178f30f7f1cd29c59decb5d549
```

```
003d85b8cbbb933a276a49c030ae66c9f723283276f9a48356c848ce5a96aaa0cc0cc47fb48e97a
f6de35427c39f86c0d6e473089705dbd054625e0348c2d59f7fa7668cd09db04fd4d3985f4b7ac9
7fb22952d01280c70f54b61e67cdc6a06c110384d34875e72afeb03b6e0a3aa66b769905a3f1776
86133144706fc537f52bd92145c4a246a678caf8d90aad0f679211b93267cc3ce1ebd883892ae45
c6196a4950b305f8ae59378a6a250394b1598150e8ba8380b72335f476b9671d5918ad208d94
155 +       SignatureAlgorithmOID: 1.2.840.113549.1.1.5
156 +       IsCertificateAuthority: true
157 +       SerialNumber: 611993e400000000001c
158 +       Version: 3
159 +       CertificateType: CA
160 +       IsCodeSigning: false
161 +       IsCA: true
162 +       TBS:
163 +         MD5: 78a717e082dcc1cda3458d917e677d14
164 +         SHA1: 4a872e0e51f9b304469cd1dedb496ee9b8b983a4
165 +         SHA256:
317fa1d234ebc49040ebc5e8746f8997471496051b185a91bdd9dfbb23fab5f8
166 +         SHA384:
b71052da4eb9157c8c1a5d7f55df19d69b9128598b72fcca608e5b7cc7d64c43c5504b9c86355a6
dc22ee40c88cc385c
167 +     - Subject: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=Terms of
use
168 +         at https://www.verisign.com/rpa (c)10, CN=VeriSign Class 3 Code Signing
2010
169 +         CA
170 +       ValidFrom: '2010-02-08 00:00:00'
171 +       ValidTo: '2020-02-07 23:59:59'
172 +       Signature:
5622e634a4c461cb48b901ad56a8640fd98c91c4bbcc0ce5ad7aa0227fdf47384a2d6cd17f711a7
cec70a9b1f04fe40f0c53fa155efe749849248581261c911447b04c638cbba134d4c645e80d8526
7303d0a98c646ddc7192e645056015595139fc58146bfed4a4ed796b080c4172e737220609be23e
93f449a1ee9619dccb1905cfc3dd28dac423d6536d4b43d40288f9b10cf2326cc4b20cb901f5d8c
4c34ca3cd8e537d66fa520bd34eb26d9ae0de7c59af7a1b42191336f86e858bb257c740e58fe751
b633fce317c9b8f1b969ec55376845b9cad91faaced93ba5dc82153c2825363af120d5087111b3d
5452968a2c9c3d921a089a052ec793a54891d3
173 +       SignatureAlgorithmOID: 1.2.840.113549.1.1.5
174 +       IsCertificateAuthority: true
175 +       SerialNumber: 5200e5aa2556fc1a86ed96c9d44b33c7
176 +       Version: 3
177 +       CertificateType: CA
```

```
178 +       IsCodeSigning: true
179 +       IsCA: true
180 +       TBS:
181 +         MD5: b30c31a572b0409383ed3fbe17e56e81
182 +         SHA1: 4843a82ed3b1f2bfbee9671960e1940c942f688d
183 +         SHA256:
    03cda47a6e654ed85d932714fc09ce4874600eda29ec6628cfbaeb155cab78c9
184 +         SHA384:
    bbda8407c4f9fc4e54d772f1c7fb9d30bc97e1f97ecd51c443063d1fa0644e266328781776cd5c4
    4896c457c75f4d7da
185 +     Signer:
186 +     - SerialNumber: 2badad20ccbc170164bdec8fbca06924
187 +       Issuer: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=Terms of
    use at
188 +         https://www.verisign.com/rpa (c)10, CN=VeriSign Class 3 Code Signing
    2010
189 +         CA
190 +       Version: 1
```

## Comments 0

Please sign in to comment.