Attacking the macOS Kernel Graphics Driver

wang yu

Didi Research America

- About me

- Background

9 Years, 3 Billion Miles: The Journey of New Horizons

Pluto Flyby: The Story of a Lifetime, NASA, 2016

New Horizons Team Reacts to Latest Image of Pluto, NASA, 2015

- Weapon X rootkit
- Rubilyn rootkit
- OS X/Crisis DAVINCI rootkit (Hacking Team)

  https://github.com/hackedteam/driver-macos
- Inficere rootkit

  https://github.com/enzolovesbacon/inficere
- Uninformed volume 4 - Abusing Mach on Mac OS X
- Phrack magazine #64 - Mac OS X wars - a XNU Hope
- Phrack magazine #66 - Developing Mac OS X Kernel Rootkits
- Phrack magazine #69 - Revisiting Mac OS X Kernel Rootkits

- Process/Dynamic library
- File/Configuration
- Kernel kext module
- Network traffic
- User mode/Kernel mode communication mechanism

- Doubly-linked list manipulation
- DKOM(Direct Kernel Object Manipulation)/Hot Patch
- Dispatch table hook/Inline hook
- Mach-O format parser/Kernel symbol
- Kernel exploitation

Windows/Android Linux/macOS Malware

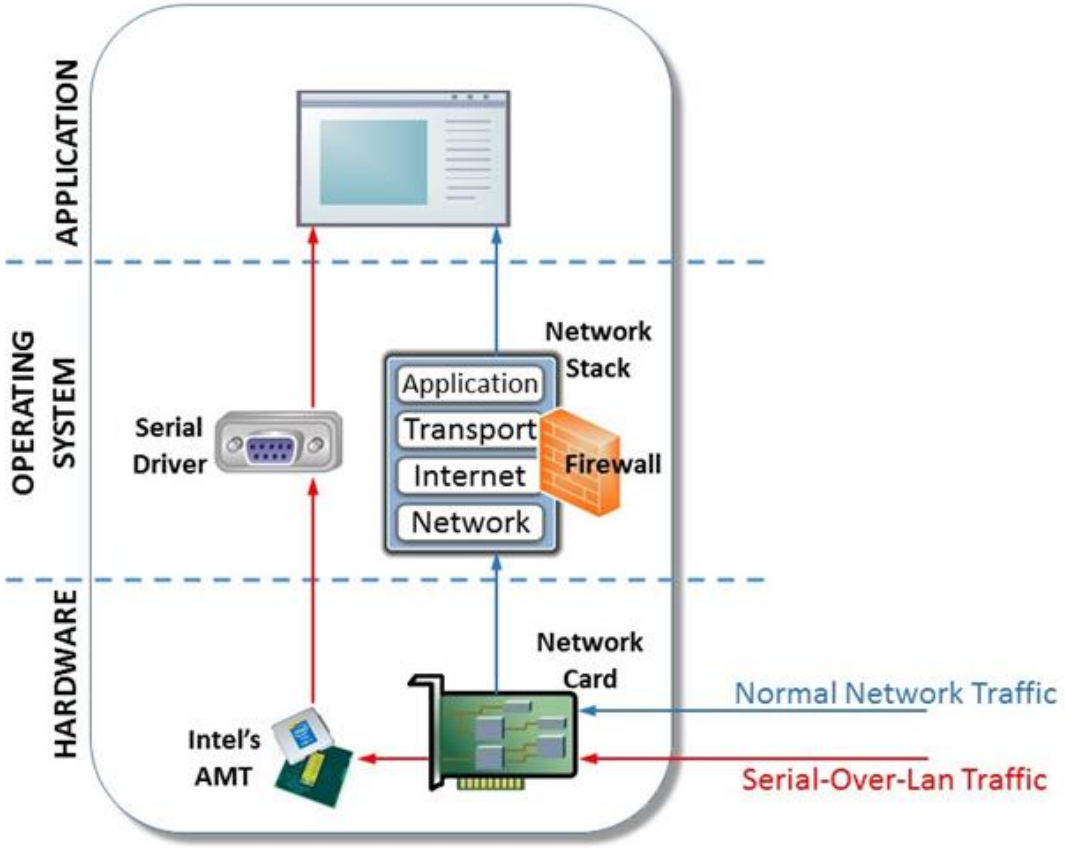
Man in the Binder - He who Controls IPC, Controls the Droid, Black Hat Europe 2014

1. Anti-debugging (object hook sys_ptrace)
   https://github.com/enzolovesbacon/inficere/blob/master/kext/inficere/anti.c#L312
2. Hide process (object hook sys_sysctl)
   https://github.com/enzolovesbacon/inficere/blob/master/kext/inficere/anti.c#L335
3. Hide file (object hook sys_getdirentries/sys_getdirentries64/sys_getdirentriesattr)
   https://github.com/enzolovesbacon/inficere/blob/master/kext/inficere/anti.c#L471
   https://github.com/enzolovesbacon/inficere/blob/master/kext/inficere/anti.c#L542
   https://github.com/enzolovesbacon/inficere/blob/master/kext/inficere/anti.c#L547
4. Hide user (object hook sys_open_nocancel/sys_read_nocancel)
   https://github.com/enzolovesbacon/inficere/blob/master/kext/inficere/anti.c#L615
   https://github.com/enzolovesbacon/inficere/blob/master/kext/inficere/anti.c#L635
5. Self-protection (object hook sys_kill)
   https://github.com/enzolovesbacon/inficere/blob/master/kext/inficere/anti.c#L448
6. Patch machine_thread_set_state
   https://github.com/enzolovesbacon/inficere/blob/master/kext/inficere/kpatch.c#L50
7. Patch kauth_authorize_process
   https://github.com/enzolovesbacon/inficere/blob/master/kext/inficere/kpatch.c#L142
8. Patch task_for_pid
   https://github.com/enzolovesbacon/inficere/blob/master/kext/inficere/kpatch.c#L95
9. EOP (sys_seteuid)
   https://github.com/enzolovesbacon/inficere/blob/master/kext/inficere/backdoor.c#L80
10. File system monitoring (Kernel Authorization)
    https://github.com/enzolovesbacon/inficere/blob/master/kext/inficere/file_monitor.c#L350
11. Network traffic monitoring (ipf_addv4, not implemented yet)
    https://github.com/enzolovesbacon/inficere/blob/master/kext/inficere/backdoor.c#L176

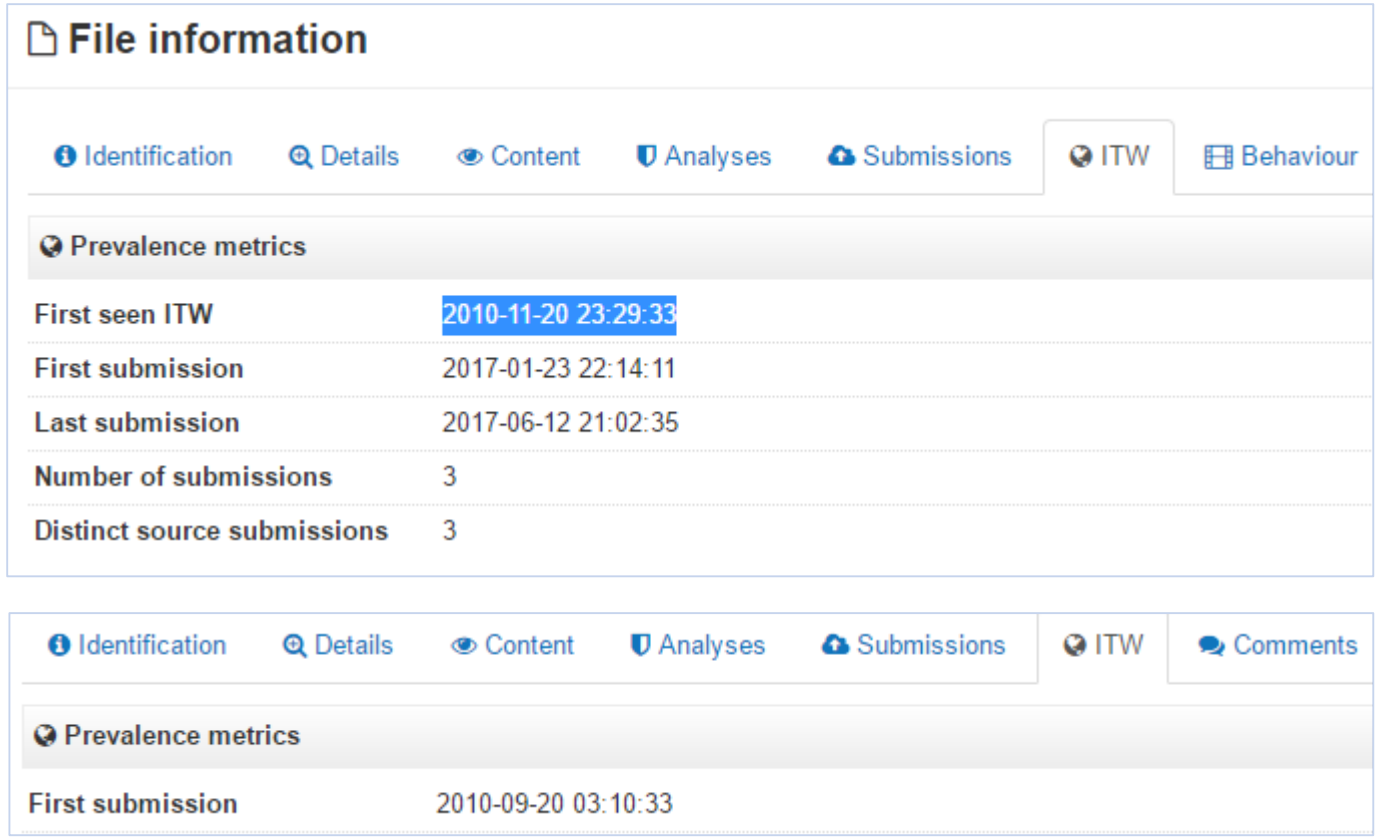
1. Use-After-Free vulnerability
   https://github.com/enzolovesbacon/inficere/blob/master/kext/inficere/inficere.c#L87
   https://github.com/apple/darwin-xnu/blob/master/bsd/kern/uipc_socket.c#L1757
2. Hardcode (syscall table)
   https://github.com/enzolovesbacon/inficere/blob/master/kext/inficere/syscall.h
3. Hardcode (object offset)
   https://github.com/enzolovesbacon/inficere/blob/master/kext/inficere/kinfo.c#L115
   https://github.com/enzolovesbacon/inficere/blob/master/kext/inficere/kinfo.c#L123
   https://github.com/enzolovesbacon/inficere/blob/master/kext/inficere/kinfo.c#L131
   https://github.com/enzolovesbacon/inficere/blob/master/kext/inficere/kinfo.c#L139
4. Lack of examination (MALLOC)
   https://github.com/enzolovesbacon/inficere/blob/master/kext/inficere/kctl.c#L170
5. Memory leak
   https://github.com/enzolovesbacon/inficere/blob/master/kext/inficere/kctl.c#L176
6. Kernel panic issue
   https://github.com/enzolovesbacon/inficere/blob/master/kext/inficere/cpu_protections.c#L66
7. Should use the “Inter-locked-xchg”
   https://github.com/enzolovesbacon/inficere/blob/master/kext/inficere/anti.c#L149

PLATINUM Continues to Evolve, Find Ways to Maintain Invisibility

https://blogs.technet.microsoft.com/mmpc/2017/06/07/platinum-continues-to-evolve-find-ways-to-maintain-invisibility/



"... Until this incident, no malware had been discovered misusing the AMT SOL feature for communication."



macOS Anti-Rootkit Technology

Kernel Module List Enumeration

```
[Agent.kext] : name=com.didi.agent, version=1.0.3, module base=0xffffff7f8e83f000, module size=0x21000.
[Agent.kext] : name=com.vmware.kext.vmhgfs, version=0505.56.93, module base=0xffffff7f8e835000, module size=0xa000.
[Agent.kext] : name=com.apple.driver.AudioAUUC, version=1.70, module base=0xffffff7f8e078000, module size=0x5000.
[Agent.kext] : name=com.apple.driver.AppleTyMCEDriver, version=1.0.2d2, module base=0xffffff7f8e130000, module size=0x9000.
[Agent.kext] : name=com.apple.filesystems.autofs, version=3.0, module base=0xffffff7f8dfb8000, module size=0x9000.
[Agent.kext] : name=com.apple.kext.triggers, version=1.0, module base=0xffffff7f8dfb3000, module size=0x5000.
[Agent.kext] : name=com.apple.driver.AppleOSXWatchdog, version=1, module base=0xffffff7f8e342000, module size=0x4000.
[Agent.kext] : name=com.apple.driver.AppleHDAHardwareConfigDriver, version=274.12, module base=0xffffff7f8e4e5000, module size=0x2000.
[Agent.kext] : name=com.apple.driver.AppleHDA, version=274.12, module base=0xffffff7f8e655000, module size=0xb3000.
[Agent.kext] : name=com.apple.driver.DspFuncLib, version=274.12, module base=0xffffff7f8e51a000, module size=0x131000.
[Agent.kext] : name=com.apple.kext.OSvKernDSPLib, version=525, module base=0xffffff7f8e507000, module size=0x13000.
[Agent.kext] : name=com.apple.driver.AppleHDAController, version=274.12, module base=0xffffff7f8e4e9000, module size=0x1e000.
[Agent.kext] : name=com.apple.iokit.IOHDAFamily, version=274.12, module base=0xffffff7f8e4d6000, module size=0xc000.
[Agent.kext] : name=com.apple.iokit.IOAudioFamily, version=204.4, module base=0xffffff7f8e03f000, module size=0x31000.
[Agent.kext] : name=com.apple.vecLib.kext, version=1.2.0, module base=0xffffff7f8dfc3000, module size=0x7c000.
[Agent.kext] : name=com.apple.driver.AppleFIVRDriver, version=4.1.0, module base=0xffffff7f8e766000, module size=0x3000.
[Agent.kext] : name=com.apple.iokit.IOBluetoothHostControllerUSBTransport, version=4.4.6f1, module base=0xffffff7f8dd9f000, module size=0x2c000.
[Agent.kext] : name=com.apple.driver.ACPI_SMC_PlatformPlugin, version=1.0.0, module base=0xffffff7f8dbb3000, module size=0x11000.
[Agent.kext] : name=com.apple.driver.IOPlatformPluginLegacy, version=1.0.0, module base=0xffffff7f8db84000, module size=0x12000.
[Agent.kext] : name=com.apple.driver.IOPlatformPluginFamily, version=6.0.0d7, module base=0xffffff7f8db7a000, module size=0xa000.
[Agent.kext] : name=com.apple.driver.AppleUpstreamUserClient, version=3.6.1, module base=0xffffff7f8e127000, module size=0x5000.
[Agent.kext] : name=com.apple.driver.AppleMCCSControl, version=1.2.13, module base=0xffffff7f8e360000, module size=0xe000.
[Agent.kext] : name=com.apple.driver.AppleSMBusController, version=1.0.14d1, module base=0xffffff7f8e34f000, module size=0xe000.
[Agent.kext] : name=com.apple.iokit.IOSMBusFamily, version=1.1, module base=0xffffff7f8daff000, module size=0x4000.
[Agent.kext] : name=com.apple.driver.pmtelemetry, version=1, module base=0xffffff7f8d4f6000, module size=0xb000.
[Agent.kext] : name=com.apple.iokit.IOUserEthernet, version=1.0.1, module base=0xffffff7f8d626000, module size=0x6000.
[Agent.kext] : name=com.apple.iokit.IOSurface, version=108.2.3, module base=0xffffff7f8daea000, module size=0x13000.
[Agent.kext] : name=com.apple.iokit.IOBluetoothSerialManager, version=4.4.6f1, module base=0xffffff7f8dcb9000, module size=0xa000.
[Agent.kext] : name=com.apple.iokit.IOSerialFamily, version=11, module base=0xffffff7f8db0e000, module size=0xe000.
[Agent.kext] : name=com.apple.iokit.IOBluetoothFamily, version=4.4.6f1, module base=0xffffff7f8dcc9000, module size=0xc3000.
[Agent.kext] : name=com.apple.Dont_Steal_Mac_OS_X, version=7.0.0, module base=0xffffff7f8de75000, module size=0x5000.
[Agent.kext] : name=com.apple.driver.AppleSMC, version=3.1.9, module base=0xffffff7f8db98000, module size=0x19000.
```

Network Traffic Monitoring

```
[Agent.kext] : duration=128.  2709 seconds, 192.168.87.128:49222(mac 00:50:56:e2:df:7e)<->203.208.41.56:443(mac 00:0c:29:2e:2a:94), process(pid
0)=kernel_task, in=4 packets,4413 bytes, out=2 packets,467 bytes.
[Agent.kext] : Dump first IN packet.
-*> MEMORY DUMP <*-
+--------------------+-------------------------------------------------+------------------+
|       ADDRESS      |  0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F | 0123456789ABCDEF |
| -------------------+-------------------------------------------------+----------------- |
|  0xffffff8014e2ca70 | 00 0c 29 2e 2a 94 00 50  56 e2 df 7e 08 00 45 00 | ..).*..PV..~..E. |
|  0xffffff8014e2ca80 | bc 05 12 ce 00 00 80 06  15 29 cb d0 29 38 c0 a8 | .........)..)8.. |
|  0xffffff8014e2ca90 | 57 80 01 bb c0 46 a2 f1  0c f5 49 83 fb 81 50 18 | W....F....I...P. |
|  0xffffff8014e2caa0 | f0 fa 00 00 00 00 16 03  03 01 44 02 00 01 40 03 | ..........D...@. |
|  0xffffff8014e2cab0 | 03 59 3f 7f 92 13 a8 d5  35 61 e9 ff 03 bf 11 f1 | .Y?.....5a...... |
|  0xffffff8014e2cac0 | 91 f9 81 ad 16 10 43 7b  ba 25 bb e6 da dc d4 8b | ......C{.%...... |
|  0xffffff8014e2cad0 | e5 00 c0 2b 00 01 18 ff  01 00 01 00 00 17 00 00 | ...+............ |
|  0xffffff8014e2cae0 | 00 23 00 00 00 12 00 f4  00 f2 00 77 00 ee 4b bd | .#.........w..K. |
|  0xffffff8014e2caf0 | b7 75 ce 60 ba e1 42 69  1f ab e1 9e 66 a3 0f 7e | .u.`..Bi....f..~ |
|  0xffffff8014e2cb00 | 5f b0 72 d8 83 00 c4 7b  89 7a a8 fd cb 00 00 01 | _.r....{.z...... |
|  0xffffff8014e2cb10 | 5c 5f b9 cf d5 00 00 04  03 00 48 30 46 02 21 00 | \_........H0F.!. |
|  0xffffff8014e2cb20 | f4 ae fc 46 6d fe a0 9f  45 0f 84 54 ce c5 8e 2e | ...Fm...E..T.... |
|  0xffffff8014e2cb30 | a3 68 96 ec bc 4a 7b b3  ad 4b 09 91 e3 80 74 d5 | .h...J{..K....t. |
|  0xffffff8014e2cb40 | 02 21 00 f9 9c e2 68 6b  c5 49 94 b6 f9 36 54 b6 | .!....hk.I...6T. |
|  0xffffff8014e2cb50 | 90 fb 3a eb 59 4e 15 7c  b7 bb 3c 15 fb 9f eb cf | ..:.YN.|..<..... |
|  0xffffff8014e2cb60 | f3 14 08 00 77 00 dd eb  1d 2b 7a 0d 4f a6 20 8b | ....w....+z.O. . |
|  0xffffff8014e2cb70 | 81 ad 81 68 70 7e 2e 8e  9d 01 d5 5c 88 8d 3d 11 | ...hp~.....\..=. |
|  0xffffff8014e2cb80 | c4 cd b6 ec be cc 00 00  01 5c 5f b9 ce 44 00 00 | .........\_..D.. |
|  0xffffff8014e2cb90 | 04 03 00 48 30 46 02 21  00 e3 1b 6c 4d ec 61 1c | ...H0F.!...lM.a. |
|  0xffffff8014e2cba0 | 10 68 49 26 95 01 f7 aa  63 07 60 39 81 08 73 82 | .hI&....c.`9..s. |
|  0xffffff8014e2cbb0 | 11 a0 35 13 67 45 8d 02  27 02 21 00 92 30 46 10 | ..5.gE..'.!..0F. |
|  0xffffff8014e2cbc0 | 5f d7 bf 25 84 5b ac 59  f0 80 8f e8 57 22 cd 17 | _..%.[.Y....W".. |
|  0xffffff8014e2cbd0 | 37 85 cc 49 91 68 66 f5  9d 37 e3 ac 00 10 00 05 | 7..I.hf..7...... |
|  0xffffff8014e2cbe0 | 00 03 02 68 32 75 50 00  00 00 0b 00 02 01 00 16 | ...h2uP......... |
   ..................
```

Process Creation Monitoring

```
   ..................
|  0xffffff80674533d0 | 33 35 35 33 3b 32 2c 31  30 2c 33 35 35 33 3b 32 | 3553;2,10,3553;2  |
|  0xffffff80674533e0 | 2c 31 31 2c 33 35 35 33  3b 32 2c 31 32 2c 33 34 | ,11,3553;2,12,34  |
|  0xffffff80674533f0 | 30 33 37 3b 32 2c 31 33  2c 33 35 35 33 3b 32 2c | 037;2,13,3553;2,  |
|  0xffffff8067453400 | 31 34 2c 33 34 30 33 37  3b 32 2c 31 35 2c 33 34 | 14,34037;2,15,34  |
|  0xffffff8067453410 | 30 33 37 3b 33 2c 30 2c  33 35 35 33 3b 33 2c 31 | 037;3,0,3553;3,1  |
|  0xffffff8067453420 | 2c 33 35 35 33 3b 33 2c  32 2c 33 35 35 33 3b 33 | ,3553;3,2,3553;3  |
|  0xffffff8067453430 | 2c 33 2c 33 35 35 33 3b  33 2c 34 2c 33 35 35 33 | ,3,3553;3,4,3553  |
|  0xffffff8067453440 | 3b 33 2c 35 2c 33 34 30  33 37 3b 33 2c 36 2c 33 | ;3,5,34037;3,6,3  |
|  0xffffff8067453450 | 35 35 33 3b 33 2c 37 2c  33 35 35 33 3b 33 2c 38 | 553;3,7,3553;3,8  |
|  0xffffff8067453460 | 2c 33 35 35 33 3b 33 2c  39 2c 33 35 35 33 3b 33 | ,3553;3,9,3553;3  |
|  0xffffff8067453470 | 2c 31 30 2c 33 35 35 33  3b 33 2c 31 31 2c 33 35 | ,10,3553;3,11,35  |
|  0xffffff8067453480 | 35 33 3b 33 2c 31 32 2c  33 34 30 33 37 3b 33 2c | 53;3,12,34037;3,  |
|  0xffffff8067453490 | 31 33 2c 33 35 35 33 3b  33 2c 31 34 2c 33 34 30 | 13,3553;3,14,340  |
|  0xffffff80674534a0 | 33 37 3b 33 2c 31 35 2c  33 34 30 33 37 00 2d 2d | 37;3,15,34037.--  |
|  0xffffff80674534b0 | 73 65 72 76 69 63 65 2d  72 65 71 75 65 73 74 2d | service-request-  |
|  0xffffff80674534c0 | 63 68 61 6e 6e 65 6c 2d  74 6f 6b 65 6e 3d 37 31 | channel-token=71  |
|  0xffffff80674534d0 | 38 31 37 42 46 31 36 30  45 34 45 30 38 44 45 44 | 817BF160E4E08DED  |
|  0xffffff80674534e0 | 36 38 39 32 33 43 41 43  37 37 46 36 30 37 00 2d | 68923CAC77F607.-  |
|  0xffffff80674534f0 | 2d 72 65 6e 64 65 72 65  72 2d 63 6c 69 65 6e 74 | -renderer-client  |
|  0xffffff8067453500 | 2d 69 64 3d 39                                   | -id=9             |
+---------------------+--------------------------------------------------+-------------------+
[Agent.kext] : action=KAUTH_FILEOP_EXEC, uid=501, process(pid 538)=Google Chrome, parent(ppid 1)=launchd, path=/Applications/Google
Chrome.app/Contents/Versions/57.0.2987.98/Google Chrome Helper.app/Contents/MacOS/Google Chrome Helper, command line=/Applications/Google
Chrome.app/Contents/Versions/57.0.2987.98/Google Chrome Helper.app/Contents/MacOS/Google Chrome Helper --type=renderer --field-trial-handle=1 --
primordial-pipe-token=71817BF160E4E08DED68923CAC77F607 --lang=en-US --enable-offline-auto-reload --enable-offline-auto-reload-visible-only --
enable-pinch --num-raster-threads=1 --enable-zero-copy --enable-gpu-memory-buffer-compositor-resources --content-image-texture-
target=0,0,3553;0,1,3553;0,2,3553;0,3,3553;0,4,3553;0,5,3553;0,6,3553;0,7,3553;0,8,3553;0,9,3553;0,10,34037;0,11,34037;0,12,34037;0,13,3553;0,14
,3553;0,15,3553;1,0,3553;1,1,3553;1,2,3553;1,3,3553;1,4,3553;1,5,3553;1,6,3553;1,7,3553;1,8,3553;1,9,3553;1,10,34037;1,11,34037;1,12,34037;1,13,
3553;1,14,3553;1,15,3553;2,0,3553;2,1,3553;2,2,3553;2,3,3553;2,4,3553;2,5,34037;2,6,3553;2,7,3553;2,8,3553;2,9,3553;2,10,3553;2,11,3553;2,12,340
37;2,13,3553;2,14,34037;2,15,34037;3,0,3553;3,1,3553;3,2,3553;3,3,3553;3,4,3553;3,5,34037;3,6,3553;3,7,3553;3,8,3553;3,9,3553;3,10,3553;3,11,355
3;3,12,34037;3,13,3553;3,14,34037;3,15,34037 --service-request-channel-token=71817BF160E4E08DED68923CAC77F607 --renderer-client-id=9.
```

DEMO : macOS Kernel Agent

Kernel Authorization

Technical Note TN2127

https://developer.apple.com/library/content/technotes/tn2127/_index.html

https://v2dev.sartle.com/sites/default/files/images/blog/tumblr_inline_nhtxaveT4p1sthg2o.jpg

Kernel Call Stack/Disassembler Library

```
-*> MEMORY DUMP <*-
+--------------------+-------------------------------------+------------------+
|       ADDRESS      |  7 6 5 4  3 2 1 0   F E D C  B A 9 8 | 0123456789ABCDEF |
| -------------------+-------------------------------------+----------------- |
|  0xffffff806c17bba0 | fffffff80`6c17bc00  ffffff80`0cd45f23 | ...l....#_...... |
|  0xffffff806c17bbb0 | 00000000`00000000  ffffff80`12e11000 | ................ |
|  0xffffff806c17bbc0 | ffffff80`1329c710  ffffff80`12e11000 | ..)............. |
|  0xffffff806c17bbd0 | 00000016`d51f0016  ffffff80`0d0832d0 | .........2...... |
|  0xffffff806c17bbe0 | ffffff80`135e2a08  00000000`00000000 | .*^............. |
|  0xffffff806c17bbf0 | ffffff80`1c290878  ffffff80`1c290808 | x.).......)..... |
|  0xffffff806c17bc00 | fffffff80`6c17bcb0  ffffff80`0cd6536d | ...l....mS...... |
|  0xffffff806c17bc10 | ffffff80`00000008  ffffff80`1329c710 | ..........)..... |
|  0xffffff806c17bc20 | ffffff80`6c17bc68  ffffff80`15c7ba78 | h..l....x....... |
|  0xffffff806c17bc30 | ffffff80`15c7bad0  ffffff80`15c7ba78 | ........x....... |
|  0xffffff806c17bc40 | 00000000`00000000  ffffff80`135e2a00 | .........*^..... |
|  0xffffff806c17bc50 | 00000000`00000001  ffffff80`15c7ba78 | ........x....... |
|  0xffffff806c17bc60 | ffffff80`67453010  00000000`00000000 | .0Eg............ |
|  0xffffff806c17bc70 | ffffff80`67453010  ffffff80`0cd54aa6 | .0Eg.....J...... |
|  0xffffff806c17bc80 | 3ec19f54`d51f0016  ffffff80`1c290800 | ....T..>..)..... |
|  0xffffff806c17bc90 | 00000000`00000000  00000000`00000000 | ................ |
|  0xffffff806c17bca0 | ffffff80`1c290808  ffffff80`15c7ba78 | ..).....x....... |
|  0xffffff806c17bcb0 | fffffff80`6c17bf50  ffffff80`0cd638de | P..l.....8...... |
|  0xffffff806c17bcc0 | ffffff80`6c17bf18  ffffff80`16f82058 | ...l....X ...... |
|  0xffffff806c17bcd0 | ffffff80`6c17bd70  ffffff80`15029000 | p..l............ |
|  0xffffff806c17bce0 | 00000000`0000400c  00000001`6c17bce8 | .@.........l.... |
|  0xffffff806c17bcf0 | ffffff80`1c290800  00000000`00000001 | ..)............. |
|  0xffffff806c17bd00 | 00007f8e`2a193338  ffffff80`15029040 | 83.*....@....... |
|  0xffffff806c17bd10 | 00000000`00000000  ffffff80`1c290808 | ..........)..... |
|  0xffffff806c17bd20 | ffffff80`15c7ba78  00000000`00000001 | x............... |
|  0xffffff806c17bd30 | ffffff80`15c7ba78  00000000`00000800 | x............... |
|  0xffffff806c17bd40 | ffffff80`6c17be70  00000000`000000f6 | p..l............ |
+--------------------+-------------------------------------+------------------+
```

```
[Agent.kext] : Disassemble the exec_activate_image().
(01) 55 PUSH RBP
(03) 4889e5 MOV RBP, RSP
(02) 4157 PUSH R15
(02) 4156 PUSH R14
(02) 4155 PUSH R13
(02) 4154 PUSH R12
(01) 53 PUSH RBX
(04) 4883ec78 SUB RSP, 0x78
(03) 4989ff MOV R15, RDI
....
```

Mandiant Monitor.app/osxAgent

Documented data structure image_params:

https://developer.apple.com/reference/kernel/image_params

```
47  if ( (unsigned int)vnode_isreg(a2) )
48  {
49    if ( *(_DWORD *)version_major == 0xE )      // OS X Yosemite
50    {
51      v17 = a7 - 0x2D8;
52      if ( a7 < 0x2D8 )
53      {
54        v18 = "osx.agent.error";
55        v19 = "%s(%d): int underflow, err=%d\n\n";
56        v20 = "procCbYosemite";
57        v21 = 228LL;
58LABEL_15:
59        v22 = 18LL;
60        goto LABEL_16;
61      }
62      v23 = *(_DWORD *)(v17 + 0x60);
63      v24 = *(const char **)(v17 + 0x58);
64      v25 = v23 < (unsigned int)v24;
65      v26 = v23 - (_DWORD)v24;
66      if ( v25 )
67      {
68        v18 = "osx.agent.error";
69        v19 = "%s(%d): int underflow, err=%d\n\n";
70        v20 = "procCbYosemite";
71        v21 = 237LL;
72        goto LABEL_15;
73      }
74    }
75    else
76    {
77      v17 = a7 - 0x2D0;
78      if ( a7 < 0x2D0 )
79      {
80        v18 = "osx.agent.error";
```

https://www.fireeye.com/services/freeware/monitor.html

Mandatory Access Control Framework

Technical Q&A QA1574

https://developer.apple.com/library/content/qa/qa1574/_index.html

https://github.com/apple/darwin-xnu/blob/xnu-4570.1.46/security/mac_policy.h#L84

https://github.com/apple/darwin-xnu/blob/xnu-4570.1.46/security/mac_base.c#L778
https://github.com/apple/darwin-xnu/blob/xnu-4570.1.46/security/mac_base.c#L782

https://v2dev.sartle.com/sites/default/files/images/blog/tumblr_inline_nhtxaveT4p1sthg2o.jpg

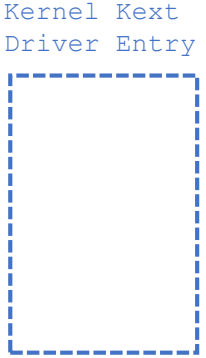
```
[Agent.kext] : macOS MAC policy[0]=TMSafetyNet(Safety net for Time Machine), loadtime flags=2(MPC_LOADTIME_FLAG_UNLOADOK), policy mpc=0xffffff7f8d413010, policy ops=0xffffff7f8d413068.
[Agent.kext] :           policy handler - 0xffffff7f8d412491 (mpo_cred_check_label_update)
[Agent.kext] :           policy handler - 0xffffff7f8d412499 (mpo_cred_label_associate_fork)
[Agent.kext] :           policy handler - 0xffffff7f8d4124ae (mpo_cred_label_associate)
[Agent.kext] :           policy handler - 0xffffff7f8d4124cd (mpo_cred_label_associate_user)
[Agent.kext] :           policy handler - 0xffffff7f8d4124e4 (mpo_cred_label_externalize)
[Agent.kext] :           policy handler - 0xffffff7f8d412539 (mpo_cred_label_internalize)
[Agent.kext] :           policy handler - 0xffffff7f8d4125a9 (mpo_cred_label_update)
[Agent.kext] :           policy handler - 0xffffff7f8d4125ca (mpo_policy_init)
[Agent.kext] :           policy handler - 0xffffff7f8d4125c4 (mpo_policy_destroy)
[Agent.kext] :           policy handler - 0xffffff7f8d4125d0 (mpo_system_check_swapon)
[Agent.kext] :           policy handler - 0xffffff7f8d412636 (mpo_vnode_check_access)
[Agent.kext] :           policy handler - 0xffffff7f8d4126c1 (mpo_vnode_check_create)
[Agent.kext] :           policy handler - 0xffffff7f8d412727 (mpo_vnode_check_deleteextattr)
[Agent.kext] :           policy handler - 0xffffff7f8d41278d (mpo_vnode_check_exchangedata)
[Agent.kext] :           policy handler - 0xffffff7f8d412813 (mpo_vnode_check_link)
[Agent.kext] :           policy handler - 0xffffff7f8d412879 (mpo_vnode_check_open)
[Agent.kext] :           policy handler - 0xffffff7f8d412904 (mpo_vnode_check_rename_from)
[Agent.kext] :           policy handler - 0xffffff7f8d41296a (mpo_vnode_check_rename_to)
[Agent.kext] :           policy handler - 0xffffff7f8d4129f5 (mpo_vnode_check_setattrlist)
[Agent.kext] :           policy handler - 0xffffff7f8d412a5b (mpo_vnode_check_setextattr)
[Agent.kext] :           policy handler - 0xffffff7f8d412ac1 (mpo_vnode_check_setflags)
[Agent.kext] :           policy handler - 0xffffff7f8d412b27 (mpo_vnode_check_setmode)
[Agent.kext] :           policy handler - 0xffffff7f8d412b8d (mpo_vnode_check_setowner)
[Agent.kext] :           policy handler - 0xffffff7f8d412bf3 (mpo_vnode_check_setutimes)
[Agent.kext] :           policy handler - 0xffffff7f8d412c59 (mpo_vnode_check_truncate)
[Agent.kext] :           policy handler - 0xffffff7f8d412cbf (mpo_vnode_check_unlink)
[Agent.kext] : macOS MAC policy[1]=AMFI(Apple Mobile File Integrity), loadtime flags=0(NULL), policy mpc=0xffffff7f8d4b3448, policy ops=0xffffff7f8d4b29d0.
[Agent.kext] :           policy handler - 0xffffff7f8d4ae73f (mpo_cred_check_label_update_execve)
[Agent.kext] :           policy handler - 0xffffff7f8d4ae74a (mpo_cred_label_associate)
[Agent.kext] :           policy handler - 0xffffff7f8d4ae797 (mpo_cred_label_destroy)
[Agent.kext] :           policy handler - 0xffffff7f8d4ae827 (mpo_cred_label_init)
[Agent.kext] :           policy handler - 0xffffff7f8d4ad539 (mpo_cred_label_update_execve)
[Agent.kext] :           policy handler - 0xffffff7f8d4ad01c (mpo_file_check_mmap)
[Agent.kext] :           policy handler - 0xffffff7f8d4af291 (mpo_policy_initbsd)
[Agent.kext] :           policy handler - 0xffffff7f8d4ae85e (mpo_proc_check_inherit_ipc_ports)
[Agent.kext] :           policy handler - 0xffffff7f8d4aebe4 (mpo_vnode_check_signature)
[Agent.kext] : macOS MAC policy[2]=Sandbox(Seatbelt sandbox policy), loadtime flags=0(NULL), policy mpc=0xffffff7f8d4d80e0, policy ops=0xffffff7f8d4d8130.
[Agent.kext] :           policy handler - 0xffffff7f8d4cfe53 (mpo_cred_check_label_update_execve)
[Agent.kext] :           policy handler - 0xffffff7f8d4c2e58 (mpo_cred_check_label_update)
[Agent.kext] :           policy handler - 0xffffff7f8d4c2e80 (mpo_cred_label_associate)
[Agent.kext] :           policy handler - 0xffffff7f8d4c2ea4 (mpo_cred_label_destroy)
[Agent.kext] :           policy handler - 0xffffff7f8d4cfe79 (mpo_cred_label_update_execve)
```

Mandiant Monitor.app/osxAgent

```
[Agent.kext] : macOS MAC policy[4]=procmon_m(procmon_m), loadtime flags=2(MPC_LOADTIME_FLAG_UNLOADOK), policy mpc=0xffffff7f8e852198, policy ops=0xffffff7f8e852238.
[Agent.kext] :           policy handler - 0xffffff7f8e847f57 (mpo_cred_label_update_execve)
[Agent.kext] : macOS MAC policy[5]=dylibmon_m(dylibmon_m), loadtime flags=2(MPC_LOADTIME_FLAG_UNLOADOK), policy mpc=0xffffff7f8e8516d0, policy ops=0xffffff7f8e851720.
[Agent.kext] :           policy handler - 0xffffff7f8e844b81 (mpo_file_check_mmap)
[Agent.kext] : macOS MAC policy[6]=ttymon_grant_m(ttymon_grant_m), loadtime flags=2(MPC_LOADTIME_FLAG_UNLOADOK), policy mpc=0xffffff7f8e8500b0, policy ops=0xffffff7f8e850150.
[Agent.kext] :           policy handler - 0xffffff7f8e84256d (mpo_pty_notify_grant)
[Agent.kext] : macOS MAC policy[7]=ttymon_close_m(ttymon_close_m), loadtime flags=2(MPC_LOADTIME_FLAG_UNLOADOK), policy mpc=0xffffff7f8e850100, policy ops=0xffffff7f8e850bc8.
[Agent.kext] :           policy handler - 0xffffff7f8e842b9a (mpo_pty_notify_close)
[Agent.kext] : macOS MAC policy[8]=monitor_kextmon_m(monitor_kextmon_h), loadtime flags=2(MPC_LOADTIME_FLAG_UNLOADOK), policy mpc=0xffffff7f8e853728, policy ops=0xffffff7f8e853778.
[Agent.kext] :           policy handler - 0xffffff7f8e84a79c (mpo_kext_check_load)
```

Kernel Inline Hook (the OSKext::start)

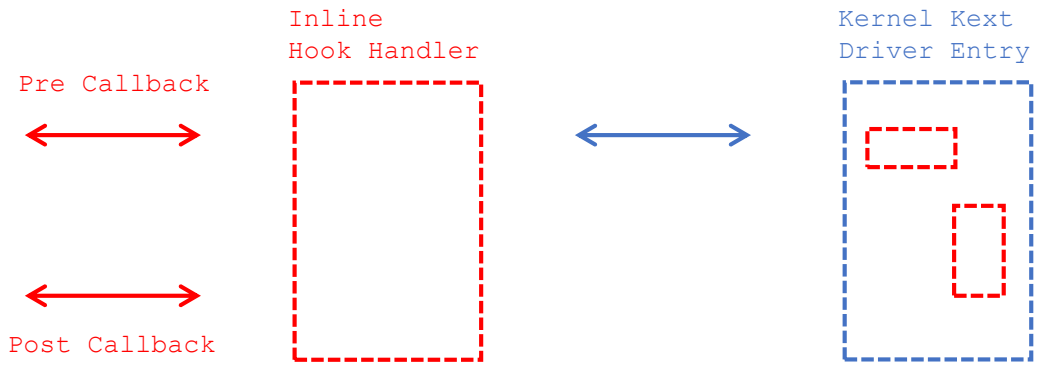
```
(lldb) di -b -n OSKext::start
kernel.development`OSKext::start:
    0xffffff800ce1aa00 <+0>:    55              pushq  %rbp
    0xffffff800ce1aa01 <+1>:    48 89 e5        movq   %rsp, %rbp
    0xffffff800ce1aa04 <+4>:    41 57           pushq  %r15
    0xffffff800ce1aa06 <+6>:    41 56           pushq  %r14
    0xffffff800ce1aa08 <+8>:    41 55           pushq  %r13
    0xffffff800ce1aa0a <+10>:   41 54           pushq  %r12
    0xffffff800ce1aa0c <+12>:   53              pushq  %rbx
    0xffffff800ce1aa0d <+13>:   48 83 ec 28     subq   $0x28, %rsp
    0xffffff800ce1aa11 <+17>:   41 89 f6        movl   %esi, %r14d
    0xffffff800ce1aa14 <+20>:   49 89 ff        movq   %rdi, %r15
    0xffffff800ce1aa17 <+23>:   49 8b 07        movq   (%r15), %rax
    ...................
    0xffffff800ce1adfd <+1021>: 4c 8b 65 c0     movq   -0x40(%rbp), %r12
    0xffffff800ce1ae01 <+1025>: 49 8b 7f 48     movq   0x48(%r15), %rdi
    0xffffff800ce1ae05 <+1029>: 4c 89 e6        movq   %r12, %rsi
    0xffffff800ce1ae08 <+1032>: ff 55 b0        callq  *-0x50(%rbp)
    ...................
    0xffffff800ce1ae60 <+1120>: 5b              popq   %rbx
    0xffffff800ce1ae61 <+1121>: 41 5c           popq   %r12
    0xffffff800ce1ae63 <+1123>: 41 5d           popq   %r13
    0xffffff800ce1ae65 <+1125>: 41 5e           popq   %r14
    0xffffff800ce1ae67 <+1127>: 41 5f           popq   %r15
    0xffffff800ce1ae69 <+1129>: 5d              popq   %rbp
    0xffffff800ce1ae6a <+1130>: c3              retq
```



http://simpsons.wikia.com/wiki/File:Woo_hool_poster.jpg

Pre and Post Callback Handler

```
(lldb) di -b -n OSKext::start
kernel.development`OSKext::start:
    0xffffff800ce1aa00 <+0>:    55              pushq  %rbp
    0xffffff800ce1aa01 <+1>:    48 89 e5        movq   %rsp, %rbp
    0xffffff800ce1aa04 <+4>:    41 57           pushq  %r15
    0xffffff800ce1aa06 <+6>:    41 56           pushq  %r14
    0xffffff800ce1aa08 <+8>:    41 55           pushq  %r13
    0xffffff800ce1aa0a <+10>:   41 54           pushq  %r12
    0xffffff800ce1aa0c <+12>:   53              pushq  %rbx
    0xffffff800ce1aa0d <+13>:   48 83 ec 28     subq   $0x28, %rsp
    0xffffff800ce1aa11 <+17>:   41 89 f6        movl   %esi, %r14d
    0xffffff800ce1aa14 <+20>:   49 89 ff        movq   %rdi, %r15
    0xffffff800ce1aa17 <+23>:   49 8b 07        movq   (%r15), %rax
    ...................
    0xffffff800ce1adfd <+1021>: 4c 8b 65 c0     movq   -0x40(%rbp), %r12
    0xffffff800ce1ae01 <+1025>: 49 8b 7f 48     movq   0x48(%r15), %rdi
    0xffffff800ce1ae05 <+1029>: 4c 89 e6        movq   %r12, %rsi
    0xffffff800ce1ae08 <+1032>: ff 55 b0        callq  *-0x50(%rbp)
    ...................
    0xffffff800ce1ae60 <+1120>: 5b              popq   %rbx
    0xffffff800ce1ae61 <+1121>: 41 5c           popq   %r12
    0xffffff800ce1ae63 <+1123>: 41 5d           popq   %r13
    0xffffff800ce1ae65 <+1125>: 41 5e           popq   %r14
    0xffffff800ce1ae67 <+1127>: 41 5f           popq   %r15
    0xffffff800ce1ae69 <+1129>: 5d              popq   %rbp
    0xffffff800ce1ae6a <+1130>: c3              retq
```



DEMO : Pre and Post Kernel Inline Hook

macOS Kernel Debugging

keen — lldb — 159×54

```
       fop = 0x0000
        ip = 0x00000000
        cs = 0x0000
        dp = 0x00000000
        ds = 0x0000
     mxcsr = 0x00000000
  mxcsrmask = 0x00000000
     stmm0 = {0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00}
     stmm1 = {0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00}
     stmm2 = {0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00}
     stmm3 = {0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00}
     stmm4 = {0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00}
     stmm5 = {0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00}
     stmm6 = {0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00}
     stmm7 = {0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00}
      xmm0 = {0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00}
      xmm1 = {0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00}
      xmm2 = {0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00}
      xmm3 = {0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00}
      xmm4 = {0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00}
      xmm5 = {0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00}
      xmm6 = {0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00}
      xmm7 = {0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00}
      xmm8 = {0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00}
      xmm9 = {0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00}
     xmm10 = {0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00}
     xmm11 = {0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00}
     xmm12 = {0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00}
     xmm13 = {0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00}
     xmm14 = {0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00}
     xmm15 = {0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00}

Exception State Registers:
3 registers were unavailable.

(lldb) bt
* thread #1, stop reason = signal SIGSTOP
  * frame #0: 0xffffff800c84d8e8 kernel.development`kdp_register_send_receive(send=<unavailab
    frame #1: 0xffffff7f8d5f6a43 IONetworkingFamily`IOKernelDebugger::registerHandler(target=
MetaClass), rxHandler=(IONetworkingFamily`IONetworkController::debugRxHandler(IOService*, voi
 linkStatusHandler=0xffffff80134ace00, setModeHandler=(IONetworkingFamily`IONetworkController
:1615))(IOService*, void*, unsigned int), void (*)(IOService*, void*, unsigned int*, unsigned
t IOKernelDebugger.cpp:659 [opt]
    frame #2: 0xffffff7f8d5f6b74 IONetworkingFamily`IOKernelDebugger::handleOpen(this=0xffffff
arg=<unavailable>) at IOKernelDebugger.cpp:768 [opt]
    frame #3: 0xffffff800ce622a4 kernel.development`IOService::open(this=0xffffff80134f0000,
t IOService.cpp:2753 [opt]
    frame #4: 0xffffff7f8d5f608c IONetworkingFamily`IOKDP::start(this=0xffffff8013567040, provider=0xffffff80134f0000) at IOKernelDebugger.cpp:228 [opt]
    frame #5: 0xffffff800ce6383d kernel.development`IOService::startCandidate(this=0xffffff80134f0000, service=0xffffff8013567040) at IOService.cpp:3311 [opt]
    frame #6: 0xffffff800ce630b6 kernel.development`IOService::probeCandidates(this=0xffffff80134f0000, matches=<unavailable>) at IOService.cpp:3230 [opt]
    frame #7: 0xffffff800ce5de98 kernel.development`IOService::doServiceMatch(this=0xffffff80134f0000, options=<unavailable>) at IOService.cpp:3524 [opt]
    frame #8: 0xffffff800ce63fdc kernel.development`_IOConfigThread::main(arg=0xffffff80134af300, result=<unavailable>) at IOService.cpp:3834 [opt]
    frame #9: 0xffffff800c98cc57 kernel.development`call_continuation + 23
(lldb)
```

OS X 10.11

```
000000.857416 S1F00@1000000: AppleUSBXHCI::createPorts: created port 1
000000.858600 S1F00@1000000: AppleUSBXHCI::createPorts: created port 2
000000.859319 S1F00@1000000: AppleUSBXHCI::createPorts: created port 3
000000.859968 S1F00@1000000: AppleUSBXHCI::createPorts: created port 4
000000.860717 S1F00@1000000: AppleUSBXHCI::createPorts: created port 5
000000.861592 S1F00@1000000: AppleUSBXHCI::createPorts: created port 6
000000.862368 S1F00@1000000: AppleUSBXHCI::createPorts: created port 7
000000.863022 S1F00@1000000: AppleUSBXHCI::createPorts: created port 8
000000.863616 AppleUSBHostResources@: AppleUSBHostResources::allocateDownstreamBusCurrentGated: assuming successful wakeU
0 sleepUnits 0
000000.864716 AppleUSBHostResources@: AppleUSBHostResources::allocateDownstreamBusCurrentGated: assuming successful wakeU
0 sleepUnits 0
000000.865826 AppleUSBHostResources@: AppleUSBHostResources::allocateDownstreamBusCurrentGated: assuming successful wakeU
0 sleepUnits 0
Intel82574L::start - Built Jan  9 2017 23:50:29 -- running on device at b3 d0 f0
000000.867903 AppleUSBHostResources@: AppleUSBHostResources::allocateDownstreamBusCurrentGated: assuming successful wakeU
0 sleepUnits 0
000000.869643 AppleUSBHostResources@: AppleUSBHostResources::allocateDownstreamBusCurrentGated: assuming successful wakeU
0 sleepUnits 0
000000.870898 AppleUSBHostResources@: AppleUSBHostResources::allocateDownstreamBusCurrentGated: assuming successful wakeU
0 sleepUnits 0
000000.872178 AppleUSBHostResources@: AppleUSBHostResources::allocateDownstreamBusCurrentGated: assuming successful wakeU
0 sleepUnits 0
000000.873470 AppleUSBHostResources@: AppleUSBHostResources::allocateDownstreamBusCurrentGated: assuming successful wakeU
0 sleepUnits 0
Got boot device = IOService:/AppleACPIPlatformExpert/PCI0@0/AppleACPIPCI/P2P0@11/IOPP/S5F0@4/AppleAHCI/PRT0@0/IOAHCIDevic
leAHCIDiskDriver/IOAHCIBlockStorageDevice/IOBlockStorageDriver/VMware Virtual SATA Hard Drive Media/IOGU
BSD root: disk0s2, major 1, minor 2
hfs: mounted Macintosh HD on device root_device
No POST boot-arg set.
VM Swap Subsystem is ON
0x1face000, 0x00000000  Intel82574L::setLinkStatus - not active
Darwin Bootstrapper Version 3.4.0: Sat Apr  2 20:54:16 PDT 2016; root:TempContent/launchd/RELEASE_X86_64
boot-args = debug=0x1 kext-dev-mode=1 pmuflags=1 kcsuffix=development -v
** /dev/rdisk0s2 (NO WRITE)
** Root file system
   Executing fsck_hfs (version hfs-305.10.1).
BootCacheControl: Unable to open /var/db/BootCaches/PreheatedUser/Merged.playlist: 2 No such file or directory
kextcache -Boot -U /
Warning: couldn't block sleep during cache update
Warning: proceeding w/o DiskArb
IOKernelDebugger: registering debugger
ethernet MAC address: 00:0c:29:2e:2a:94
ip address: 192.168.87.128

Waiting for remote debugger connection.
Connected to remote debugger.
```

```
| LLDB (F1) | Target (F2) | Process (F3) | Thread (F4) | View (F5) | Help (F6) |
```

<Sources>

```
IONetworkingFamily`IOKDP::start(IOService*)
0xffffff7f8d5f6040 | pushq    %rbp
0xffffff7f8d5f6041 | movq     %rsp, %rbp
0xffffff7f8d5f6044 | pushq    %r14
0xffffff7f8d5f6046 | pushq    %rbx
0xffffff7f8d5f6047 | movq     %rsi, %rbx
0xffffff7f8d5f604a | movq     %rdi, %r14
0xffffff7f8d5f604d | movq     0x1003c(%rip), %rax
0xffffff7f8d5f6054 | callq    *0x5d0(%rax)
0xffffff7f8d5f605a | testb    %al, %al
0xffffff7f8d5f605c | je       0xffffff7f8d5f60c1        ; <+129> at IOKernelDebugger.cpp:236
0xffffff7f8d5f605e | movq     0x1831b(%rip), %rdi       ; gIOKDPLock
0xffffff7f8d5f6065 | testq    %rdi, %rdi
0xffffff7f8d5f6068 | je       0xffffff7f8d5f60c1        ; <+129> at IOKernelDebugger.cpp:236
0xffffff7f8d5f606a | callq    0xffffff800c984e00        ; lck_mtx_lock
0xffffff7f8d5f606f | cmpq     $0x0, 0x18319(%rip)       ; gDebugBootArg + 7
0xffffff7f8d5f6077 | jne      0xffffff7f8d5f60b5        ; <+117> at IOKernelDebugger.cpp:236
0xffffff7f8d5f6079 | movq     (%rbx), %rax
0xffffff7f8d5f607c | xorl     %edx, %edx
0xffffff7f8d5f607e | xorl     %ecx, %ecx
0xffffff7f8d5f6080 | movq     %rbx, %rdi
0xffffff7f8d5f6083 | movq     %r14, %rsi
0xffffff7f8d5f6086 | callq    *0x5d0(%rax)
0xffffff7f8d5f608c | testb    %al, %al
0xffffff7f8d5f608e | je       0xffffff7f8d5f60b5        ; <+117> at IOKernelDebugger.cpp:236
0xffffff7f8d5f6090 | movq     %r14, 0x182f9(%rip)       ; gIOKDP
0xffffff7f8d5f6097 | movq     0x182e2(%rip), %rdi       ; gIOKDPLock
0xffffff7f8d5f609e | callq    0xffffff800c985400        ; lck_mtx_unlock
0xffffff7f8d5f60a3 | movq     (%r14), %rax
0xffffff7f8d5f60a6 | xorl     %esi, %esi
0xffffff7f8d5f60a8 | movq     %r14, %rdi
0xffffff7f8d5f60ab | callq    *0x5b0(%rax)
0xffffff7f8d5f60b1 | movb     $0x1, %al
0xffffff7f8d5f60b3 | jmp      0xffffff7f8d5f60c3        ; <+131> at IOKernelDebugger.cpp:241
0xffffff7f8d5f60b5 | movq     0x182c4(%rip), %rdi       ; gIOKDPLock
0xffffff7f8d5f60bc | callq    0xffffff800c985400        ; lck_mtx_unlock
0xffffff7f8d5f60c1 | xorl     %eax, %eax
0xffffff7f8d5f60c3 | popq     %rbx
0xffffff7f8d5f60c4 | popq     %r14
0xffffff7f8d5f60c6 | popq     %rbp
```

<Threads>

```
◆─process 1
└─◆─thread #1: tid = 0x0001, stop reas
  ├─frame #0: kdp_register_send_receiv
  ├─frame #1: IOKernelDebugger::regist
  ├─frame #2: IOKernelDebugger::handle
  ├─frame #3: IOService::open(IOServic
  ├─frame #4: IOKDP::start(IOService*)
  ├─frame #5: IOService::startCandidat
  ├─frame #6: IOService::probeCandidat
  ├─frame #7: IOService::doServiceMatc
  ├─frame #8: _IOConfigThread::main(vo
  └─frame #9: call_continuation + 23
```

<Variables>

```
◆─(IOKDP *) this = 0xffffff8013567040
◆─(IOKernelDebugger *) provider = 0xffffff80134f0000
├─◆─(IOService) IOService
├─◆─(IOService *) _target
├─◆─(IODebuggerTxHandler) _txHandler = 0xffffff7f8d5fa2ec (IONetworkingFamily`I
ON├─◆─(IODebuggerRxHandler) _rxHandler = 0xffffff7f8d5fa2fe (IONetworkingFamily`I
ON├─◆─(IOService *) _clientHandler(IOService*, void*, unsigned int*, unsigned int
) ├─(bool) _pmDisabled = false574)
└─◆─(IOKernelDebugger::ExpansionData *) _reserved = 0xffffff80135693a0
(bool) ret = false
◆─(MetaClass) IOKernelDebugger::gMetaClass
(UInt32) ::gIODebuggerTxBytes = 134933
◆─(IOKDP *) gIOKDP = 0x0000000000000000
◆─(IODebuggerSetModeHandler) ::gIODebuggerSetModeHandler = 0xffffff7f8d5fa31e (
IO◆─(const OSMetaClass *const) IOKDP::metaClass = 0xffffff7f8d60e068e*, bool) at
IO◆─(const OSMetaClass *const) IOKernelDebugger::metaClass = 0xffffff7f8d60e090
◆─(IOLock *) gIOKDPLock = 0xffffff8013371640
```

<Registers>

```
◆─General Purpose Registers
├─(unsigned long) rax
├─(unsigned long) rbx = 0xffffff80134f0000
├─(unsigned long) rcx
├─(unsigned long) rdx
├─(unsigned long) rdi
├─(unsigned long) rsi
├─(unsigned long) rbp = 0xffffff886cffbe70
├─(unsigned long) rsp = 0xffffff886cffbe60
├─(unsigned long) r8
├─(unsigned long) r9
├─(unsigned long) r10
├─(unsigned long) r11
├─(unsigned long) r12 = 0xffffff800d1553e0
├─(unsigned long) r13 = 0xffffff8013567040
├─(unsigned long) r14 = 0xffffff8013567040
├─(unsigned long) r15 = 0xffffff8013567040
```

```
Process:     1     stopped             Thread: 0x0001      Frame:    4   PC = 0xffffff7f8d5f608c
```

Kernel 'com:pipe,port=\\.\pipe\com_1,baud=115200,reconnect' - WinDbg:6.3.9600.16384 AMD64

File Edit View Debug Window Help

Disassembly

Offset: @$scopeip Previous Next

```
fffff803`4f09aaeb b8890100c0      mov     eax,0C0000189h
fffff803`4f09aaf0 e96affffff      jmp     nt!CmOpenKey+0x33f (fffff803`4f09aa5f)
fffff803`4f09aaf5 cc              int     3
fffff803`4f09aaf6 cc              int     3
fffff803`4f09aaf7 cc              int     3
fffff803`4f09aaf8 cc              int     3
fffff803`4f09aaf9 cc              int     3
fffff803`4f09aafa cc              int     3
fffff803`4f09aafb cc              int     3
fffff803`4f09aafc cc              int     3
fffff803`4f09aafd cc              int     3
fffff803`4f09aafe cc              int     3
fffff803`4f09aaff cc              int     3
nt!ObOpenObjectByNameEx:
fffff803`4f09ab00 4c8bdc          mov     r11,rsp
fffff803`4f09ab03 49897320        mov     qword ptr [r11+20h],rsi
fffff803`4f09ab07 55              push    rbp
fffff803`4f09ab08 57              push    rdi
fffff803`4f09ab09 4154            push    r12
fffff803`4f09ab0b 4155            push    r13
fffff803`4f09ab0d 4156            push    r14
fffff803`4f09ab0f 498d6bc8        lea     rbp,[r11-38h]
fffff803`4f09ab13 4881ec10010000  sub     rsp,110h
fffff803`4f09ab1a 488b4578        mov     rax,qword ptr [rbp+78h]
fffff803`4f09ab1e 4c8bf1          mov     r14,rcx
fffff803`4f09ab21 33c9            xor     ecx,ecx
```

Memory

Virtual: @$scopeip Next Previous

Display format: Quad Hex

```
fffff803`4f09ab00 5520738949dc8b4c 4956415541544157
fffff803`4f09ab10 0110ec8148c86b8d 8b4c78458b480000
fffff803`4f09ab20 8948f18b49c933f1 8b4ce0b60f45804d
fffff803`4f09ab30 0ff6854d088948ea d285480000066784
fffff803`4f09ab40 89490000065e840f 4c65187b894d105b
fffff803`4f09ab50 4900000020253c8b 8b4800000800bf8b
fffff803`4f09ab60 cca6d7e81447ffcf 0fc08548d88b48ff
fffff803`4f09ab70 478b41000004ed84 4c0389904d8d4c24
fffff803`4f09ab80 01b8000000a0bb8d 4489c68b4d000000
fffff803`4f09ab90 0f41d4b60f412824 8920247c894cccb6
fffff803`4f09aba0 8b00000659e84045 143e5d880fc085f8
fffff803`4f09abb0 00a1850ff6854800 8825048b48650000
fffff803`4f09abc0 8b4865d233000001 8b4c00000188253c
fffff803`4f09abd0 878b49000000b8b8 d0458948000002e8
fffff803`4f09abe0 0005b2840fff8548 a8000006c0878b00
fffff803`4f09abf0 440000034f850f08 8d49b875894cf28b
fffff803`4f09ac00 2df6e8000003588f c08548f08b4cffbe
fffff803`4f09ac10 3d8300000598840f 75894c00002c13ef
fffff803`4f09ac20 4400143e49850fc8 4c4c458d49604d8b
fffff803`4f09ac30 8948000000e0838d 8d48d38b48202444
fffff803`4f09ac40 8bffbe2eb9e8b84d 0002e4880fc085f8
fffff803`4f09ac50 a0bb8d4cf38b4800 00c0838b48000000
fffff803`4f09ac60 6c850fc085480000 48407e8b48000004
fffff803`4f09ac70 00000468850fff85 7824448d48078b45
```

Registers

Customize...

Reg	Value
rax	0
rcx	1d84d7f280
rdx	ffff870e2434ef20
rbx	ffff870e2567c0a8
rsp	ffffac0142f45958
rbp	ffffac0142f45b80
rsi	28
rdi	ffff870e2567c010
r8	1
r9	0
r10	0
r11	36
r12	0
r13	1
r14	c0140000
r15	1d84d7f280
rip	fffff8034f09ab00
efl	246
cs	10
ds	2b
es	2b
fs	53
gs	2b
ss	18
dr0	0
dr1	0
dr2	0
dr3	0
dr6	ffff0ff0
dr7	400
fpcw	ebf0
fpsw	275b
fptw	e
st0	0.000000000000000e
st1	1.#INF0000000000e
st2	-1.#INF0000000000e
st3	-1.#INF0000000000e
st4	-1.#INF0000000000e
st5	0.000000000000000e
st6	0.000000000000000e

Command - Kernel 'com:pipe,port=\\.\pipe\com_1,baud=115200,reconnect' - WinDbg:6.3.9600.16384 AMD64

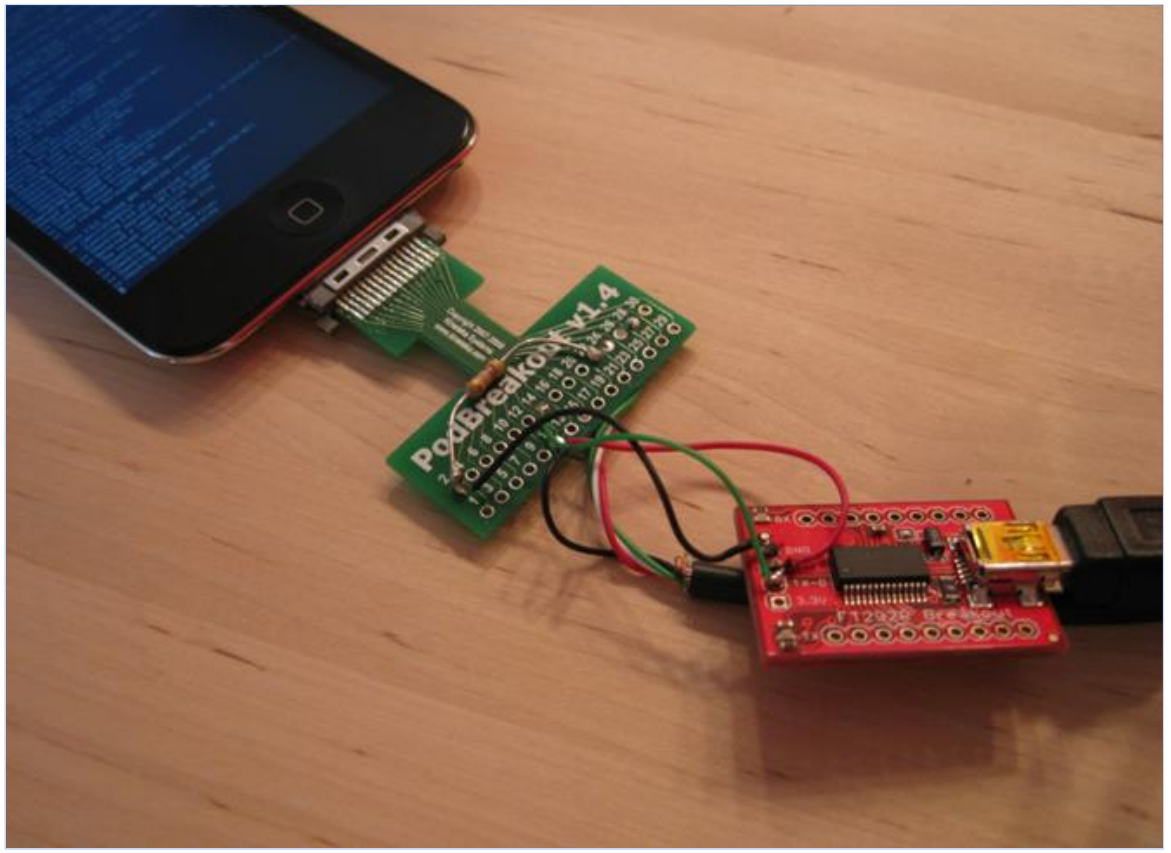
```
0000001d`84d7f2c0  00 00 00 00 00 0f 1e 00-41 66 64 4f 70 65 6e 50  ........AfdOpenP
0000001d`84d7f2d0  61 63 6b 65 74 58 58 00-11 00 00 00 00 00 00 00  acketXX.........
0000001d`84d7f2e0  17 00 00 00 02 00 00 00-11 00 00 00 00 00 00 00  ................
0000001d`84d7f2f0  01 00 00 00 00 00 00 00-60 00 00 00 00 00 00 00  ........`.......
1: kd> kb
RetAddr           : Args to Child                                                     : Call Site
fffff803`4f07dae9 : 00000000`dc9d0205 00000000`00000039 ffff870e`61456f49 00000000`00000001 : nt!ObOpenObjectByNameEx
fffff803`4f07d6f9 : 0000001d`84d7f238 00000000`00000000 0000001d`84d7f280 0000001d`84d7f270 : nt!IopCreateFile+0x3d9
fffff803`4ed6a393 : 00000000`00000102 00000000`00000001 00000000`00000000 0000001d`00000001 : nt!NtCreateFile+0x79
00007ffc`b5096b74 : 00007ffc`b0d266fa 00000000`000000e0 00000000`00000004 0000001d`00001e40 : nt!KiSystemServiceCopyEnd+0x13
00007ffc`b0d266fa : 00000000`000000e0 00000000`00000004 0000001d`00001e40 00000000`00000000 : 0x00007ffc`b5096b74
00000000`000000e0 : 00000000`00000004 0000001d`00001e40 00000000`00000000 00000000`00000000 : 0x00007ffc`b0d266fa
00000000`00000004 : 0000001d`00001e40 00000000`00000000 00000000`00000000 00000000`00000000 : 0xe0
0000001d`00001e40 : 00000000`00000000 00000000`00000000 00000000`00000000 0000001d`00000003 : 0x4
00000000`00000000 : 00000000`00000000 00000000`00000000 0000001d`00000003 0000001d`00000003 : 0x0000001d`00001e40
1: kd> dt _OBJECT_ATTRIBUTES 1d84d7f280
nt!_OBJECT_ATTRIBUTES
   +0x000 Length           : 0x30
   +0x008 RootDirectory    : (null)
   +0x010 ObjectName       : 0x0000001d`84d7f2b0 _UNICODE_STRING "\Device\Afd\Endpoint"
   +0x018 Attributes       : 0x42
   +0x020 SecurityDescriptor : (null)
   +0x028 SecurityQualityOfService : (null)
```

1: kd>

Kernel Debugging is an Interesting Topic

A Smooth Sea Never Made A Skilled Sailor

iOS Kernel Debugging



A Smooth Sea Never Made A Skilled Sailor

https://github.com/kashifmin/KashKernel_4.2/blob/master/mediatek/platform/mt6589/kernel/drivers/mmc-host/mt_sd_misc.c#L990

Android/Linux Kernel Debugging

```
shell@hwH30-U10:/ $ id
uid=2000(shell) gid=2000(shell) groups=1003(graphics),1004(input),1007(log),1009(mount),1011(adb),1015(sdcar
),3006(net_bw_stats)
shell@hwH30-U10:/ $ /data/local/tmp/mmc_erase_partition
---[ 00 ]---
Huawei, H30-U10, 3.4.5, #1 SMP PREEMPT Thu Jul 3 02:40:39 CST 2014
Huawei, H30-U10, 3.4.5, #1 SMP PREEMPT Thu Jul 3 02:40:39 CST 2014
shellcode at 0x111a000, temp stack at 0x111e000
                              -*> MEMORY DUMP <*-
+------------+-------------------------------------------------+------------------+
|    ADDRESS  |  0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F |                  |
| ------------+-------------------------------------------------+----------------- |
|  0x0111a000 | c0 01 0c f1 30 d0 9f e5  00 d0 9d e5 01 da 8d e2 | ....0........... |
|  0x0111a010 | 30 00 9f e5 00 00 90 e5  20 40 9f e5 34 ff 2f e1 | 0....... @..4./. |
|  0x0111a020 | 00 d0 a0 e1 c0 01 08 f1  18 00 9f e5 00 00 90 e5 | ................ |
|  0x0111a030 | 0c 40 9f e5 34 ff 2f e1  f0 ab 9d e8 ac c5 00 00 | .@..4./......... |
|  0x0111a040 | 18 8d 00 00 10 88 00 00  d0 c4 00 00             | ............     |
+------------+-------------------------------------------------+------------------+
                              -*> MEMORY DUMP <*-
+------------+-------------------------------------------------+------------------+
|    ADDRESS  |  0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F |                  |
| ------------+-------------------------------------------------+----------------- |
|  0xbed9d820 | cc cc cc cc cc cc cc cc  cc cc cc cc cc cc cc cc | ................ |
|  0xbed9d830 | cc cc cc cc cc cc cc cc  cc cc cc cc cc cc cc cc | ................ |
|  0xbed9d840 | cc cc cc cc cc cc cc cc  cc cc cc cc cc cc cc cc | ................ |
|  0xbed9d850 | cc cc cc cc cc cc cc cc  cc 00 a0 11 01          | .............    |
+------------+-------------------------------------------------+------------------+
[+] got root!
shell@hwH30-U10:/ # id
uid=0(root) gid=0(root)
shell@hwH30-U10:/ #
```

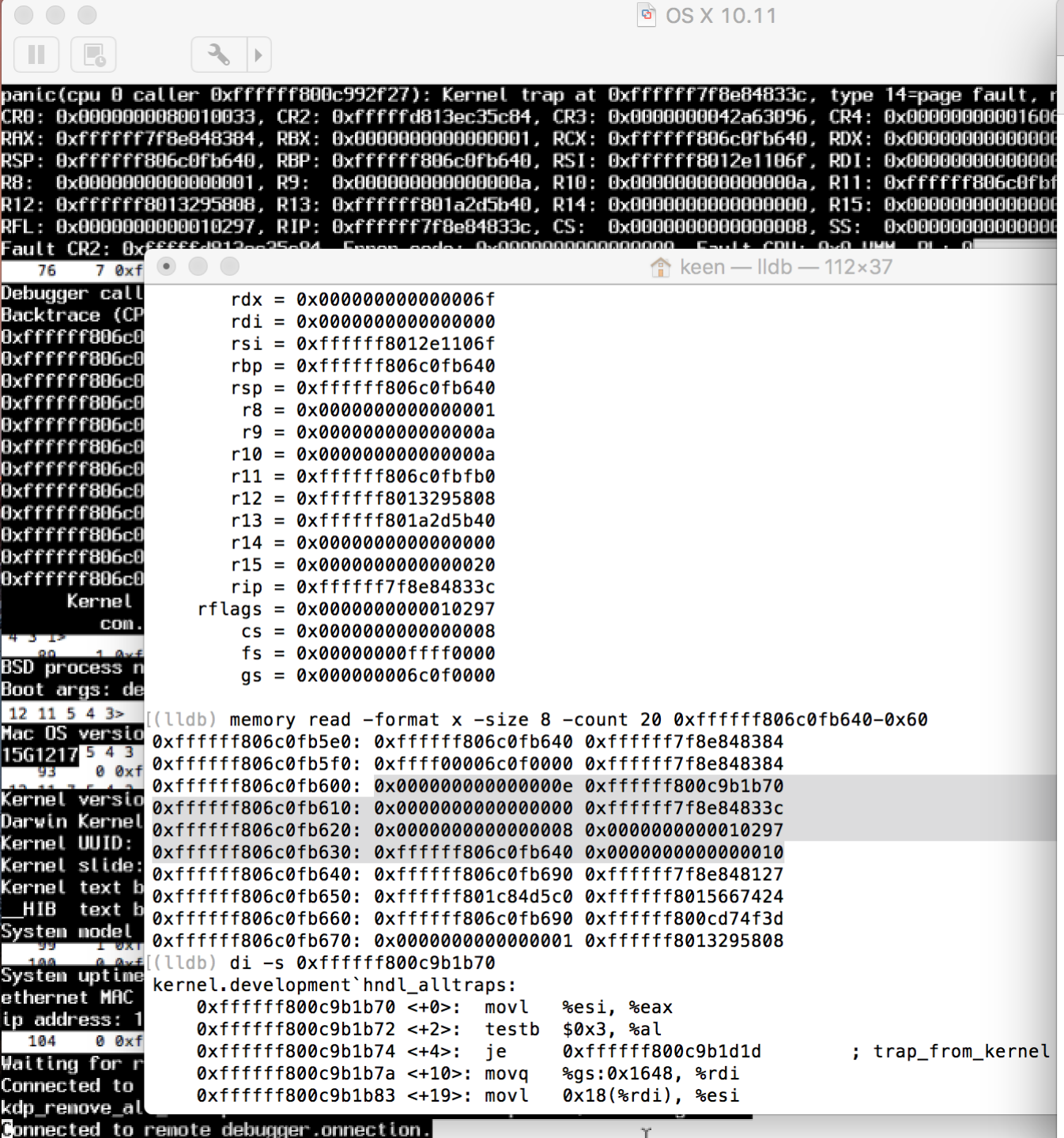
comma.ai/George Hotz

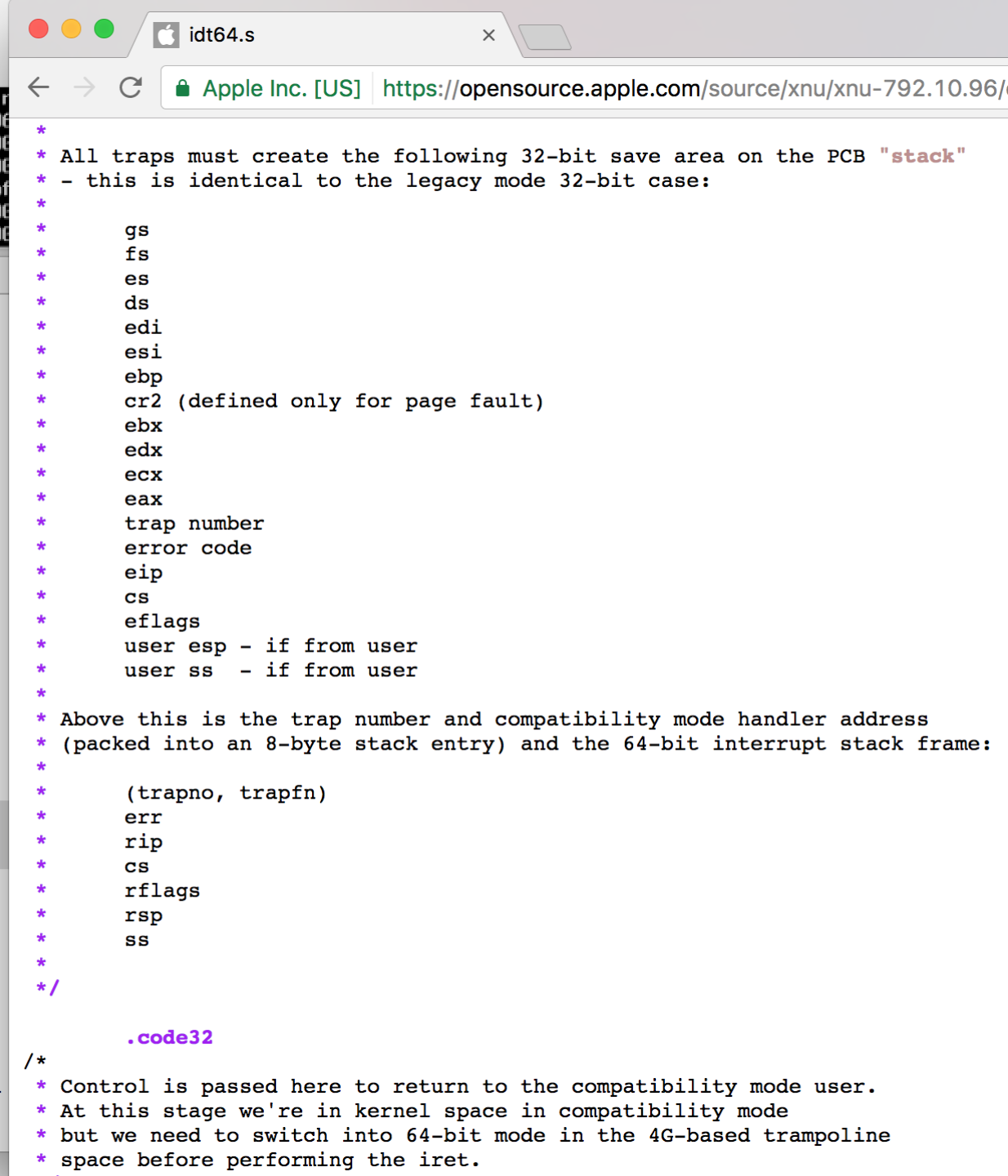
From Panics to Kernel Zero-day Vulnerabilities

well, well, well... kernel panics

```
[(lldb) register read
General Purpose Registers:
       rax = 0xffffff7f8e84eb40
       rbx = 0x0000000000000000
       rcx = 0xffffff800ce1ae0b  kernel.development`OSKext::start(bool)
       rdx = 0x0000000000000001
       rdi = 0xffffff7f8e84ff18
       rsi = 0x0000000000000000
       rbp = 0xffffff806c3f3880
       rsp = 0xffffff806c3f2e40
        r8 = 0xffffff80134d6800
        r9 = 0x0000000000000000
       r10 = 0x0000000000000000
       r11 = 0xfffffffffffffffb
       r12 = 0xffffff8013295808
       r13 = 0xffffff80140503c0
       r14 = 0xffffff80134d6800
       r15 = 0xffffff80140503c0
       rip = 0xffffff7f8e842a5b
    rflags = 0x0000000000010202
        cs = 0x0000000000000008
        fs = 0x00000000ffff0000
        gs = 0x000000000ce10000

[(lldb) memory read 0xffffff7f8e84eb40 -count 0x37
0xffffff7f8e84eb40: 44 44 43 54 46 2d 36 63 31 63 62 34 39 37 63 61  DDCTF-6c1cb497ca
0xffffff7f8e84eb50: 35 37 34 65 34 39 62 64 30 64 63 64 31 65 65 30  574e49bd0dcd1ee0
0xffffff7f8e84eb60: 36 33 33 65 65 34 40 64 69 64 69 63 68 75 78 69  633ee4@didichuxi
0xffffff7f8e84eb70: 6e 67 2e 63 6f 6d 00                             ng.com.
(lldb)
```


OS X 10.11
panic(cpu 0 caller 0xffffff800c992f27): Kernel trap at 0xffffff7f8e84833c, type 14=page fault,
CR0: 0x0000000080010033, CR2: 0xffffd813ec35c84, CR3: 0x0000000042a63096, CR4:
RAX: 0xffffff7f8e848384, RBX: 0x0000000000000001, RCX: 0xffffff806c0fb640, RDX:
RSP: 0xffffff806c0fb640, RBP: 0xffffff806c0fb640, RSI: 0xffffff8012e1106f, RDI:
R8: 0x0000000000000001, R9: 0x000000000000000a, R10: 0x000000000000000a, R11:
R12: 0xffffff8013295808, R13: 0xffffff801a2d5b40, R14: 0x0000000000000000, R15:
RFL: 0x0000000000010297, RIP: 0xffffff7f8e84833c, CS: 0x0000000000000008, SS:
Fault CR2:
keen — lldb — 112×37
rdx = 0x000000000000006f
rdi = 0x0000000000000000
rsi = 0xffffff8012e1106f
rbp = 0xffffff806c0fb640
rsp = 0xffffff806c0fb640
r8 = 0x0000000000000001
r9 = 0x000000000000000a
r10 = 0x000000000000000a
r11 = 0xffffff806c0fbfb0
r12 = 0xffffff8013295808
r13 = 0xffffff801a2d5b40
r14 = 0x0000000000000000
r15 = 0x0000000000000020
rip = 0xffffff7f8e84833c
rflags = 0x0000000000010297
cs = 0x0000000000000008
fs = 0x000000000000ffff0000
gs = 0x000000006c0f0000
(lldb) memory read -format x -size 8 -count 20 0xffffff806c0fb640-0x60
0xffffff806c0fb5e0: 0xffffff806c0fb640 0xffffff7f8e848384
0xffffff806c0fb5f0: 0xffff00006c0f0000 0xffffff7f8e848384
0xffffff806c0fb600: 0x000000000000000e 0xffffff800c9b1b70
0xffffff806c0fb610: 0x0000000000000000 0xffffff7f8e84833c
0xffffff806c0fb620: 0x0000000000000008 0x0000000000010297
0xffffff806c0fb630: 0xffffff806c0fb640 0x0000000000000010
0xffffff806c0fb640: 0xffffff806c0fb690 0xffffff7f8e848127
0xffffff806c0fb650: 0xffffff801c84d5c0 0xffffff8015667424
0xffffff806c0fb660: 0xffffff806c0fb690 0xffffff800cd74f3d
0xffffff806c0fb670: 0x0000000000000001 0xffffff8013295808
(lldb) di -s 0xffffff800c9b1b70
kernel.development`hndl_alltraps:
0xffffff800c9b1b70 <+0>: movl %esi, %eax
0xffffff800c9b1b72 <+2>: testb $0x3, %al
0xffffff800c9b1b74 <+4>: je 0xffffff800c9b1d1d ; trap_from_kernel
0xffffff800c9b1b7a <+10>: movq %gs:0x1648, %rdi
0xffffff800c9b1b83 <+19>: movl 0x18(%rdi), %esi
Connected to remote debugger.onnection.


idt64.s
Apple Inc. [US] https://opensource.apple.com/source/xnu/xnu-792.10.96/
* All traps must create the following 32-bit save area on the PCB "stack"
* - this is identical to the legacy mode 32-bit case:
* gs
* fs
* es
* ds
* edi
* esi
* ebp
* cr2 (defined only for page fault)
* ebx
* edx
* ecx
* eax
* trap number
* error code
* eip
* cs
* eflags
* user esp - if from user
* user ss - if from user
* Above this is the trap number and compatibility mode handler address
* (packed into an 8-byte stack entry) and the 64-bit interrupt stack frame:
* (trapno, trapfn)
* err
* rip
* cs
* rflags
* rsp
* ss
*/
.code32
/*
* Control is passed here to return to the compatibility mode user.
* At this stage we're in kernel space in compatibility mode
* but we need to switch into 64-bit mode in the 4G-based trampoline
* space before performing the iret.

Real War is Not a Game

```
                public _str_hex_b
_str_hex_b      proc near               ; CODE XREF: _dist
                                        ; _distorm_formatd

var_C           = dword ptr -0Ch
var_8           = qword ptr -8

                push    rbp
                mov     rbp, rsp
                lea     rax, _str_hex_b_TextBTable ; "00"
                mov     [rbp+var_8], rdi
                mov     [rbp+var_C], esi
                mov     rdi, [rbp+var_8]
                mov     esi, [rdi]
                mov     edi, esi
                mov     rcx, [rbp+var_8]
                mov     esi, [rbp+var_C]
                and     esi, 0FFh
                mov     esi, esi
                mov     edx, esi
                imul    rdx, 3
                add     rax, rdx
                mov     r8w, [rax]
                mov     [rcx+rdi+4], r8w
                mov     r9b, [rax+2]
                mov     [rcx+rdi+6], r9b
                mov     rax, [rbp+var_8]
                mov     esi, [rax]
                add     esi, 2
                mov     [rax], esi
                pop     rbp
                retn
_str_hex_b      endp
```

llvm clang compiler

```
                public _str_hex_b
_str_hex_b      proc near               ; CODE XREF: _dist
                                        ; _distorm_formatd

var_18          = qword ptr -18h
var_C           = dword ptr -0Ch
var_8           = qword ptr -8

                push    rbp
                mov     rbp, rsp
                sub     rsp, 20h
                mov     eax, 3
                mov     edx, eax        ; size_t
                lea     rcx, _str_hex_b_TextBTable
                mov     [rbp+var_8], rdi
                mov     [rbp+var_C], esi
                mov     rdi, [rbp+var_8]
                mov     eax, [rdi]
                mov     edi, eax
                mov     r8, [rbp+var_8]
                add     r8, 4
                add     r8, rdi
```

GCC compiler (with the "-kext" and "-lkmod" arguments)

DEMO : Arbitrary Kernel Memory Read/Write Zero-day Vulnerabilities

```
Process 1 stopped
* thread #1, stop reason = EXC_BREAKPOINT (code=3, subcode=0x0)
    frame #0: 0xffffff801817c8ea kernel.development`panic_trap_to_debugger [inlined] current_cpu_datap at cpu_data.h:400 [opt]
Target 0: (kernel.development) stopped.
(lldb) bt
* thread #1, stop reason = EXC_BREAKPOINT (code=3, subcode=0x0)
  * frame #0: 0xffffff801817c8ea kernel.development`panic_trap_to_debugger [inlined] current_cpu_datap at cpu_data.h:400 [opt]
    frame #1: 0xffffff801817c8ea kernel.development`panic_trap_to_debugger [inlined] current_processor at cpu.c:220 [opt]
    frame #2: 0xffffff801817c8ea kernel.development`panic_trap_to_debugger [inlined] DebuggerTrapWithState(db_op=DBOP_PANIC, db_message=<unavailable>, db_panic_str="\"a freed zone element has been modified in zone %s: expected %p but found %p, bits changed %p, at offset %d of %d in element %p, cookies %p %p\"@/BuildRoot/Library/Caches/com.apple.xbs/Sources/xnu/xnu-4570.61.1/osfmk/kern/zalloc.c:1122", db_panic_args=0xffffff9208c4bae0, db_panic_options=0, db_proceed_on_sync_failure=1, db_panic_caller=18446743524358321159) at debug.c:463 [opt]
    frame #3: 0xffffff801817c8ba kernel.development`panic_trap_to_debugger(panic_format_str="\"a freed zone element has been modified in zone %s: expected %p but found %p, bits changed %p, at offset %d of %d in element %p, cookies %p %p\"@/BuildRoot/Library/Caches/com.apple.xbs/Sources/xnu/xnu-4570.61.1/osfmk/kern/zalloc.c:1122", panic_args=0xffffff9208c4bae0, reason=0, ctx=0x0000000000000000, panic_options_mask=0, panic_caller=18446743524358321159) at debug.c:724 [opt]
    frame #4: 0xffffff801817c6bc kernel.development`panic(str=<unavailable>) at debug.c:611 [opt]
    frame #5: 0xffffff80181d7407 kernel.development`backup_ptr_mismatch_panic [inlined] zone_element_was_modified_panic(zone=<unavailable>, element=<unavailable>, found=<unavailable>, expected=<unavailable>, offset=0) at zalloc.c:1113 [opt]
    frame #6: 0xffffff80181d73bb kernel.development`backup_ptr_mismatch_panic(zone=<unavailable>, element=18446743525104646144, primary=0, backup=<unavailable>) at zalloc.c:1163 [opt]
    frame #7: 0xffffff80181d6b75 kernel.development`try_alloc_from_zone(zone=0xffffff8018ac1f70, tag=<unavailable>, check_poison=<unavailable>) at zalloc.c:1308 [opt]
    frame #8: 0xffffff80181d4d91 kernel.development`zalloc_internal(zone=0xffffff8018ac1f70, canblock=1, nopagewait=0, reqsize=5856, tag=<unavailable>) at zalloc.c:3084 [opt]
    frame #9: 0xffffff801818972c kernel.development`kalloc_canblock [inlined] zalloc_canblock_tag(zone=<unavailable>, canblock=1, reqsize=<unavailable>, tag=<unavailable>) at zalloc.c:3370 [opt]
    frame #10: 0xffffff8018189718 kernel.development`kalloc_canblock(psize=<unavailable>, canblock=1, site=0xffffff8018a06f60) at kalloc.c:693 [opt]
    frame #11: 0xffffff801815473f kernel.development`ipc_kmsg_alloc(msg_and_trailer_size=4352) at ipc_kmsg.c:934 [opt]
    frame #12: 0xffffff8018182c0d kernel.development`ipc_kobject_server(request=0xffffff80403e9c80, option=3) at ipc_kobject.c:298 [opt]
    frame #13: 0xffffff8018155cad kernel.development`ipc_kmsg_send(kmsg=0xffffff80403e9c80, option=3, send_timeout=0) at ipc_kmsg.c:1867 [opt]
    frame #14: 0xffffff8018170a9b kernel.development`mach_msg_overwrite_trap(args=<unavailable>) at mach_msg.c:570 [opt]
    frame #15: 0xffffff80182bf08a kernel.development`mach_call_munger64(state=0xffffff803bc4e140) at bsd_i386.c:573 [opt]
    frame #16: 0xffffff80181219f6 kernel.development`hndl_mach_scall64 + 22
```

```
Process 1 stopped
* thread #1, stop reason = EXC_BAD_ACCESS (code=1, address=0x20)
    frame #0: 0xffffff7f9d7919a4 IOAcceleratorFamily2`IOAccelMemoryMap::getLRUSeed() const + 4
IOAcceleratorFamily2`IOAccelMemoryMap::getLRUSeed:
->  0xffffff7f9d7919a4 <+4>:  movl   0x20(%rdi), %eax
    0xffffff7f9d7919a7 <+7>:  movq   0xa8(%rdi), %rcx
    0xffffff7f9d7919ae <+14>: testq  %rcx, %rcx
    0xffffff7f9d7919b1 <+17>: je     0xffffff7f9d7919d0        ; <+48>
Target 0: (kernel.development) stopped.
(lldb) bt
* thread #1, stop reason = EXC_BAD_ACCESS (code=1, address=0x20)
  * frame #0: 0xffffff7f9d7919a4 IOAcceleratorFamily2`IOAccelMemoryMap::getLRUSeed() const + 4
    frame #1: 0xffffff7f9d751ee0 IOAcceleratorFamily2`IOAccelMemory::getLRUSeed() const + 44
    frame #2: 0xffffff7f9d7816a4 IOAcceleratorFamily2`IOGraphicsAccelerator2::collectGartWirings() + 230
    frame #3: 0xffffff7f9d77d888 IOAcceleratorFamily2`IOGraphicsAccelerator2::gart_collector(IOInterruptEventSource*, int) + 384
    frame #4: 0xffffff801cc3d575 kernel.development`IOInterruptEventSource::checkForWork(this=0xffffff920d0f3ebc) at IOInterruptEventSource.cpp:325 [opt]
    frame #5: 0xffffff801cc3bde2 kernel.development`IOWorkLoop::runEventSources(this=0xffffff803dd554b0) at IOWorkLoop.cpp:368 [opt]
    frame #6: 0xffffff801cc3b55c kernel.development`IOWorkLoop::threadMain(this=0xffffff803dd554b0) at IOWorkLoop.cpp:396 [opt]
    frame #7: 0xffffff801c520567 kernel.development`call_continuation + 23
(lldb) re r rdi
     rdi = 0x0000000000000000
(lldb)
```

DEMO : Arbitrary Kernel Memory Read/Write Zero-day Vulnerabilities

DEMO : Arbitrary Kernel Memory Read/Write Zero-day Vulnerabilities

```
(lldb) bt
* thread #1, stop reason = EXC_BREAKPOINT (code=3, subcode=0x0)
  * frame #0: 0xffffff800057c8ea kernel.development`panic_trap_to_debugger [inlined] current_cpu_datap at cpu_data.h:400 [opt]
    frame #1: 0xffffff800057c8ea kernel.development`panic_trap_to_debugger [inlined] current_processor at cpu.c:220 [opt]
    frame #2: 0xffffff800057c8ea kernel.development`panic_trap_to_debugger [inlined] DebuggerTrapWithState(db_op=DBOP_PANIC, db_message=<unavailable>, db_panic_str="\"__memcpy_chk object size check failed: dst %p, src %p, (%zu < %zu)\"@/BuildRoot/Library/Caches/com.apple.xbs/Sources/xnu/xnu-4570.61.1/osfmk/device/subrs.c:665", db_panic_args=0xffffff81ebc7b610, db_panic_options=0, db_proceed_on_sync_failure=1, db_panic_caller=18446743523960612807) at debug.c:463 [opt]
    frame #3: 0xffffff800057c8ba kernel.development`panic_trap_to_debugger(panic_format_str="\"__memcpy_chk object size check failed: dst %p, src %p, (%zu < %zu)\"@/BuildRoot/Library/Caches/com.apple.xbs/Sources/xnu/xnu-4570.61.1/osfmk/device/subrs.c:665", panic_args=0xffffff81ebc7b610, reason=0, ctx=0x0000000000000000, panic_options_mask=0, panic_caller=18446743523960612807) at debug.c:724 [opt]
    frame #4: 0xffffff800057c6bc kernel.development`panic(str=<unavailable>) at debug.c:611 [opt]
    frame #5: 0xffffff800068e7c7 kernel.development`__memcpy_chk(dst=0xffffff81ebc7b6b4, src=0xffffff81ebc7b71c, s=204, chk_size=<unavailable>) at subrs.c:665 [opt]
    frame #6: 0xffffff7f8180bd75 AppleIntelFramebufferAzul`AppleIntelAzulController::WriteAUX(AppleIntelFramebuffer*, unsigned int, unsigned short, void*, DISPLAYPATH*) + 239
    frame #7: 0xffffff7f818548ec AppleIntelFramebufferAzul`CamelliaTcon::WriteCamelliaReg(unsigned int, unsigned char, unsigned int) + 156
    frame #8: 0xffffff7f81859ec7 AppleIntelFramebufferAzul`CamelliaTcon::processCmd(kFBControllerCommand_t, unsigned long*, unsigned long, unsigned long*, unsigned long*) + 2277
    frame #9: 0xffffff7f8185e158 AppleIntelFramebufferAzul`IntelFBClientControl::doAttribute(unsigned int, unsigned long*, unsigned long, unsigned long*, unsigned long*, IOExternalMethodArguments*) + 1792
    frame #10: 0xffffff7f8185e5d2 AppleIntelFramebufferAzul`IntelFBClientControl::actionWrapper(void*, void*, void*, void*) + 48
    frame #11: 0xffffff8000c3bbfe kernel.development`IOWorkLoop::runAction(this=0xffffff8022f09980, inAction=(AppleIntelFramebufferAzul`IntelFBClientControl::actionWrapper(void*, void*, void*, void*)), target=<unavailable>, arg0=<unavailable>, arg1=<unavailable>, arg2=<unavailable>, arg3=0x0000000000000000)(OSObject*, void*, void*, void*, void*), OSObject*, void*, void*, void*, void*) at IOWorkLoop.cpp:505 [opt]
    frame #12: 0xffffff7f8185e654 AppleIntelFramebufferAzul`IntelFBClientControl::vendor_doDeviceAttribute(unsigned int, unsigned long*, unsigned long, unsigned long*, unsigned long*, IOExternalMethodArguments*) + 124
    frame #13: 0xffffff7f818017e0 AppleGraphicsDeviceControl`AppleGraphicsDeviceControl::vendor_doDeviceAttribute(unsigned int, unsigned long*, unsigned long, unsigned long*, unsigned long*, AGDCClientState_t*) + 48
    frame #14: 0xffffff7f818013d0 AppleGraphicsDeviceControl`AppleGraphicsDeviceControl::filtered_doDeviceAttribute(AppleGraphicsDeviceControl::agdc_filtered_api_t, unsigned int, unsigned long*, unsigned long, unsigned long*, unsigned long*, AGDCClientState_t*) + 3604
    frame #15: 0xffffff7f81801955 AppleGraphicsDeviceControl`AppleGraphicsDeviceControl::UserKernelTransfer(unsigned int, AGDCClientState_t*) + 367
    frame #16: 0xffffff7f817ff72f AppleGraphicsDeviceControl`AppleGraphicsDeviceControlClient::externalMethod(unsigned int, IOExternalMethodArguments*, IOExternalMethodDispatch*, OSObject*, void*) + 205
    frame #17: 0xffffff8000c6e5c7 kernel.development`::is_io_connect_method(connection=0xffffff8029d535c0, selector=4278192209, scalar_input=<unavailable>, scalar_inputCnt=<unavailable>, inband_input=<unavailable>, inband_inputCnt=0, ool_input=<unavailable>, ool_input_size=<unavailable>, inband_output=<unavailable>, inband_outputCnt=<unavailable>, scalar_output=<unavailable>, scalar_outputCnt=<unavailable>, ool_output=<unavailable>, ool_output_size=<unavailable>) at IOUserClient.cpp:3971 [opt]
    frame #18: 0xffffff800068b224 kernel.development`_Xio_connect_method(InHeadP=<unavailable>, OutHeadP=0xffffff802a1b2de0) at device_server.c:8379 [opt]
    frame #19: 0xffffff8000582ca7 kernel.development`ipc_kobject_server(request=0xffffff8028d96800, option=<unavailable>) at ipc_kobject.c:351 [opt]
    frame #20: 0xffffff8000555cad kernel.development`ipc_kmsg_send(kmsg=0xffffff8028d96800, option=3, send_timeout=0) at ipc_kmsg.c:1867 [opt]
    frame #21: 0xffffff8000570a9b kernel.development`mach_msg_overwrite_trap(args=<unavailable>) at mach_msg.c:570 [opt]
    frame #22: 0xffffff80006bf08a kernel.development`mach_call_munger64(state=0xffffff80299207a0) at bsd_i386.c:573 [opt]
    frame #23: 0xffffff80005219f6 kernel.development`hndl_mach_scall64 + 22
```

The End

Think Deeply

Q&A

wang yu

Didi Research America