black hat USA 2019

AUGUST 3-8, 2019

MANDALAY BAY / LAS VEGAS

KSBox: A Fine-Grained macOS Malware Sandbox

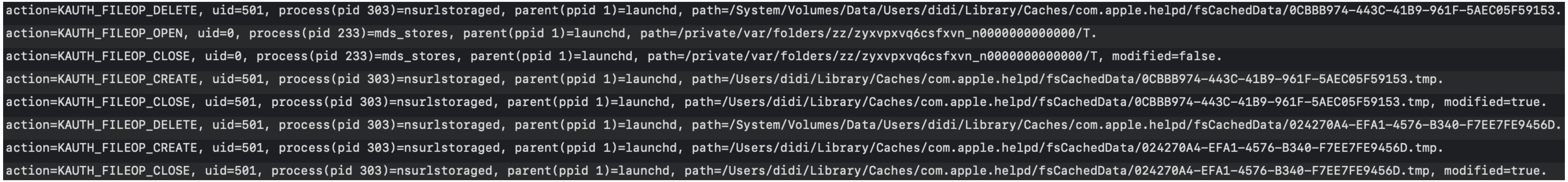
wang yu

Black Hat US’19 Arsenal

KEXT Source Code

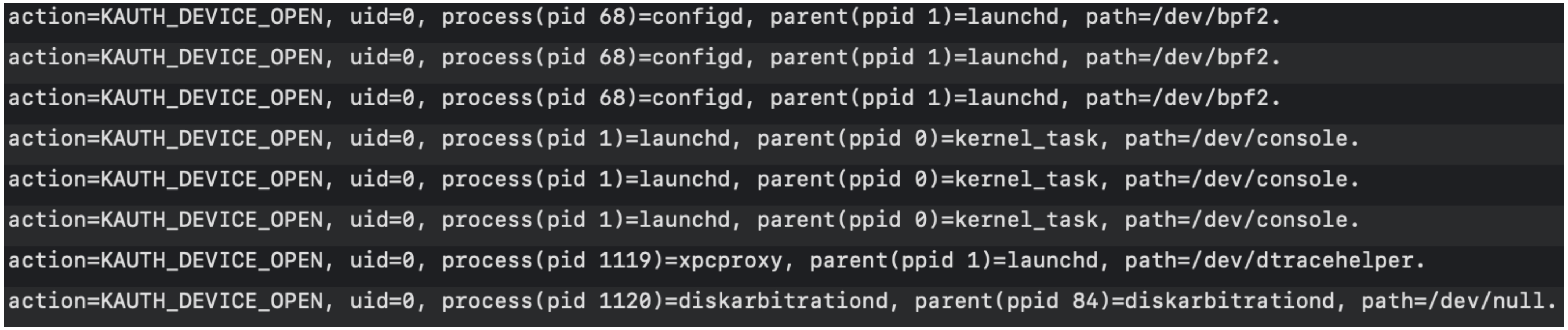
https://github.com/didi/kemon

File Operation Monitoring



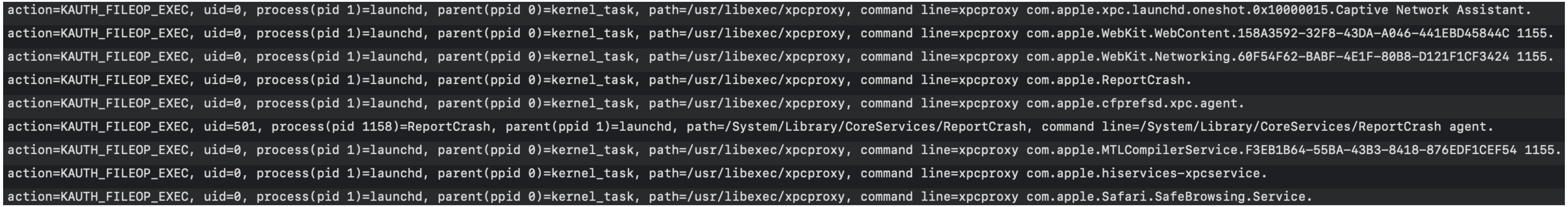
```
action=KAUTH_FILEOP_DELETE, uid=501, process(pid 303)=nsurlstoraged, parent(ppid 1)=launchd, path=/System/Volumes/Data/Users/didi/Library/Caches/com.apple.helpd/fsCachedData/0CBBB974-443C-41B9-961F-5AEC05F59153.
action=KAUTH_FILEOP_OPEN, uid=0, process(pid 233)=mds_stores, parent(ppid 1)=launchd, path=/private/var/folders/zz/zyxvpxvq6csfxvn_n0000000000000/T.
action=KAUTH_FILEOP_CLOSE, uid=0, process(pid 233)=mds_stores, parent(ppid 1)=launchd, path=/private/var/folders/zz/zyxvpxvq6csfxvn_n0000000000000/T, modified=false.
action=KAUTH_FILEOP_CREATE, uid=501, process(pid 303)=nsurlstoraged, parent(ppid 1)=launchd, path=/Users/didi/Library/Caches/com.apple.helpd/fsCachedData/0CBBB974-443C-41B9-961F-5AEC05F59153.tmp.
action=KAUTH_FILEOP_CLOSE, uid=501, process(pid 303)=nsurlstoraged, parent(ppid 1)=launchd, path=/Users/didi/Library/Caches/com.apple.helpd/fsCachedData/0CBBB974-443C-41B9-961F-5AEC05F59153.tmp, modified=true.
action=KAUTH_FILEOP_DELETE, uid=501, process(pid 303)=nsurlstoraged, parent(ppid 1)=launchd, path=/System/Volumes/Data/Users/didi/Library/Caches/com.apple.helpd/fsCachedData/024270A4-EFA1-4576-B340-F7EE7FE9456D.
action=KAUTH_FILEOP_CREATE, uid=501, process(pid 303)=nsurlstoraged, parent(ppid 1)=launchd, path=/Users/didi/Library/Caches/com.apple.helpd/fsCachedData/024270A4-EFA1-4576-B340-F7EE7FE9456D.tmp.
action=KAUTH_FILEOP_CLOSE, uid=501, process(pid 303)=nsurlstoraged, parent(ppid 1)=launchd, path=/Users/didi/Library/Caches/com.apple.helpd/fsCachedData/024270A4-EFA1-4576-B340-F7EE7FE9456D.tmp, modified=true.
```

File Operation Monitoring (cont)



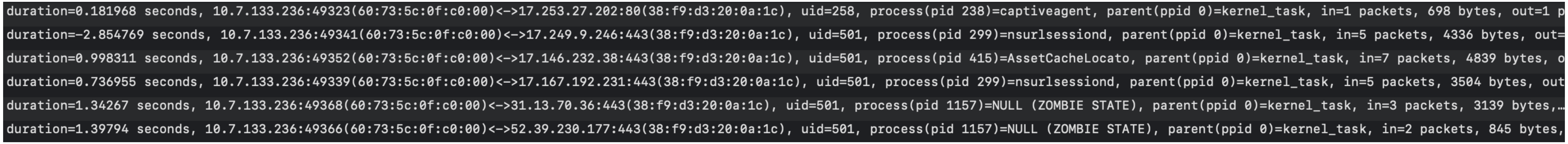
```
action=KAUTH_DEVICE_OPEN, uid=0, process(pid 68)=configd, parent(ppid 1)=launchd, path=/dev/bpf2.
action=KAUTH_DEVICE_OPEN, uid=0, process(pid 68)=configd, parent(ppid 1)=launchd, path=/dev/bpf2.
action=KAUTH_DEVICE_OPEN, uid=0, process(pid 68)=configd, parent(ppid 1)=launchd, path=/dev/bpf2.
action=KAUTH_DEVICE_OPEN, uid=0, process(pid 1)=launchd, parent(ppid 0)=kernel_task, path=/dev/console.
action=KAUTH_DEVICE_OPEN, uid=0, process(pid 1)=launchd, parent(ppid 0)=kernel_task, path=/dev/console.
action=KAUTH_DEVICE_OPEN, uid=0, process(pid 1)=launchd, parent(ppid 0)=kernel_task, path=/dev/console.
action=KAUTH_DEVICE_OPEN, uid=0, process(pid 1119)=xpcproxy, parent(ppid 1)=launchd, path=/dev/dtracehelper.
action=KAUTH_DEVICE_OPEN, uid=0, process(pid 1120)=diskarbitrationd, parent(ppid 84)=diskarbitrationd, path=/dev/null.
```

Process Monitoring

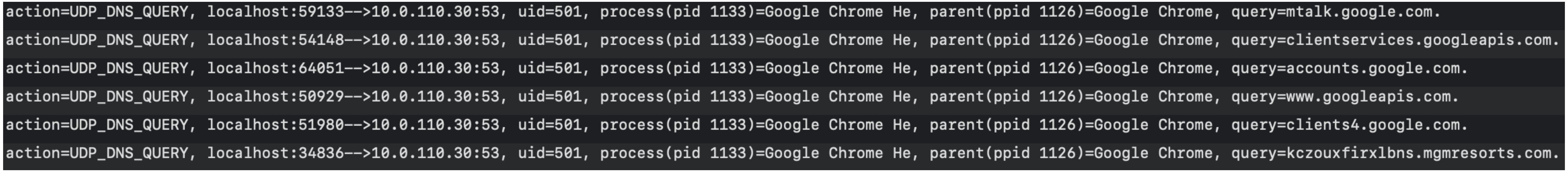


```
action=KAUTH_FILEOP_EXEC, uid=0, process(pid 1)=launchd, parent(ppid 0)=kernel_task, path=/usr/libexec/xpcproxy, command line=xpcproxy com.apple.xpc.launchd.oneshot.0x10000015.Captive Network Assistant.
action=KAUTH_FILEOP_EXEC, uid=0, process(pid 1)=launchd, parent(ppid 0)=kernel_task, path=/usr/libexec/xpcproxy, command line=xpcproxy com.apple.WebKit.WebContent.158A3592-32F8-43DA-A046-441EBD45844C 1155.
action=KAUTH_FILEOP_EXEC, uid=0, process(pid 1)=launchd, parent(ppid 0)=kernel_task, path=/usr/libexec/xpcproxy, command line=xpcproxy com.apple.WebKit.Networking.60F54F62-BABF-4E1F-80B8-D121F1CF3424 1155.
action=KAUTH_FILEOP_EXEC, uid=0, process(pid 1)=launchd, parent(ppid 0)=kernel_task, path=/usr/libexec/xpcproxy, command line=xpcproxy com.apple.ReportCrash.
action=KAUTH_FILEOP_EXEC, uid=0, process(pid 1)=launchd, parent(ppid 0)=kernel_task, path=/usr/libexec/xpcproxy, command line=xpcproxy com.apple.cfprefsd.xpc.agent.
action=KAUTH_FILEOP_EXEC, uid=501, process(pid 1158)=ReportCrash, parent(ppid 1)=launchd, path=/System/Library/CoreServices/ReportCrash, command line=/System/Library/CoreServices/ReportCrash agent.
action=KAUTH_FILEOP_EXEC, uid=0, process(pid 1)=launchd, parent(ppid 0)=kernel_task, path=/usr/libexec/xpcproxy, command line=xpcproxy com.apple.MTLCompilerService.F3EB1B64-55BA-43B3-8418-876EDF1CEF54 1155.
action=KAUTH_FILEOP_EXEC, uid=0, process(pid 1)=launchd, parent(ppid 0)=kernel_task, path=/usr/libexec/xpcproxy, command line=xpcproxy com.apple.hiservices-xpcservice.
action=KAUTH_FILEOP_EXEC, uid=0, process(pid 1)=launchd, parent(ppid 0)=kernel_task, path=/usr/libexec/xpcproxy, command line=xpcproxy com.apple.Safari.SafeBrowsing.Service.
```

Network Traffic Monitoring

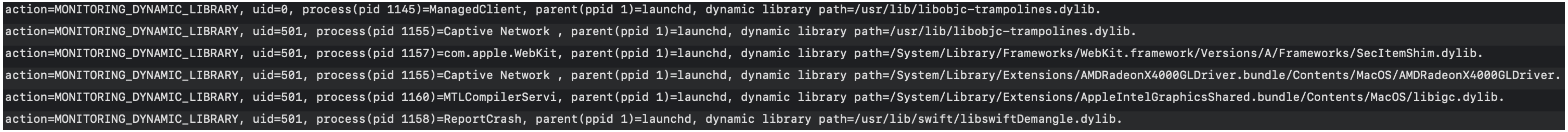


```
duration=0.181968 seconds, 10.7.133.236:49323(60:73:5c:0f:c0:00)<->17.253.27.202:80(38:f9:d3:20:0a:1c), uid=258, process(pid 238)=captiveagent, parent(ppid 0)=kernel_task, in=1 packets, 698 bytes, out=1 p
duration=-2.854769 seconds, 10.7.133.236:49341(60:73:5c:0f:c0:00)<->17.249.9.246:443(38:f9:d3:20:0a:1c), uid=501, process(pid 299)=nsurlsessiond, parent(ppid 0)=kernel_task, in=5 packets, 4336 bytes, out=
duration=0.998311 seconds, 10.7.133.236:49352(60:73:5c:0f:c0:00)<->17.146.232.38:443(38:f9:d3:20:0a:1c), uid=501, process(pid 415)=AssetCacheLocato, parent(ppid 0)=kernel_task, in=7 packets, 4839 bytes, o
duration=0.736955 seconds, 10.7.133.236:49339(60:73:5c:0f:c0:00)<->17.167.192.231:443(38:f9:d3:20:0a:1c), uid=501, process(pid 299)=nsurlsessiond, parent(ppid 0)=kernel_task, in=5 packets, 3504 bytes, out
duration=1.34267 seconds, 10.7.133.236:49368(60:73:5c:0f:c0:00)<->31.13.70.36:443(38:f9:d3:20:0a:1c), uid=501, process(pid 1157)=NULL (ZOMBIE STATE), parent(ppid 0)=kernel_task, in=3 packets, 3139 bytes,…
duration=1.39794 seconds, 10.7.133.236:49366(60:73:5c:0f:c0:00)<->52.39.230.177:443(38:f9:d3:20:0a:1c), uid=501, process(pid 1157)=NULL (ZOMBIE STATE), parent(ppid 0)=kernel_task, in=2 packets, 845 bytes,
```

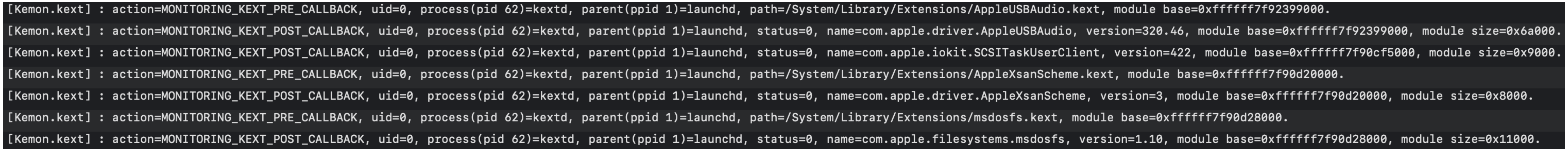


```
action=UDP_DNS_QUERY, localhost:59133-->10.0.110.30:53, uid=501, process(pid 1133)=Google Chrome He, parent(ppid 1126)=Google Chrome, query=mtalk.google.com.
action=UDP_DNS_QUERY, localhost:54148-->10.0.110.30:53, uid=501, process(pid 1133)=Google Chrome He, parent(ppid 1126)=Google Chrome, query=clientservices.googleapis.com.
action=UDP_DNS_QUERY, localhost:64051-->10.0.110.30:53, uid=501, process(pid 1133)=Google Chrome He, parent(ppid 1126)=Google Chrome, query=accounts.google.com.
action=UDP_DNS_QUERY, localhost:50929-->10.0.110.30:53, uid=501, process(pid 1133)=Google Chrome He, parent(ppid 1126)=Google Chrome, query=www.googleapis.com.
action=UDP_DNS_QUERY, localhost:51980-->10.0.110.30:53, uid=501, process(pid 1133)=Google Chrome He, parent(ppid 1126)=Google Chrome, query=clients4.google.com.
action=UDP_DNS_QUERY, localhost:34836-->10.0.110.30:53, uid=501, process(pid 1133)=Google Chrome He, parent(ppid 1126)=Google Chrome, query=kczouxfirxlbns.mgmresorts.com.
```

Dynamic Library and Kernel Extension Monitoring

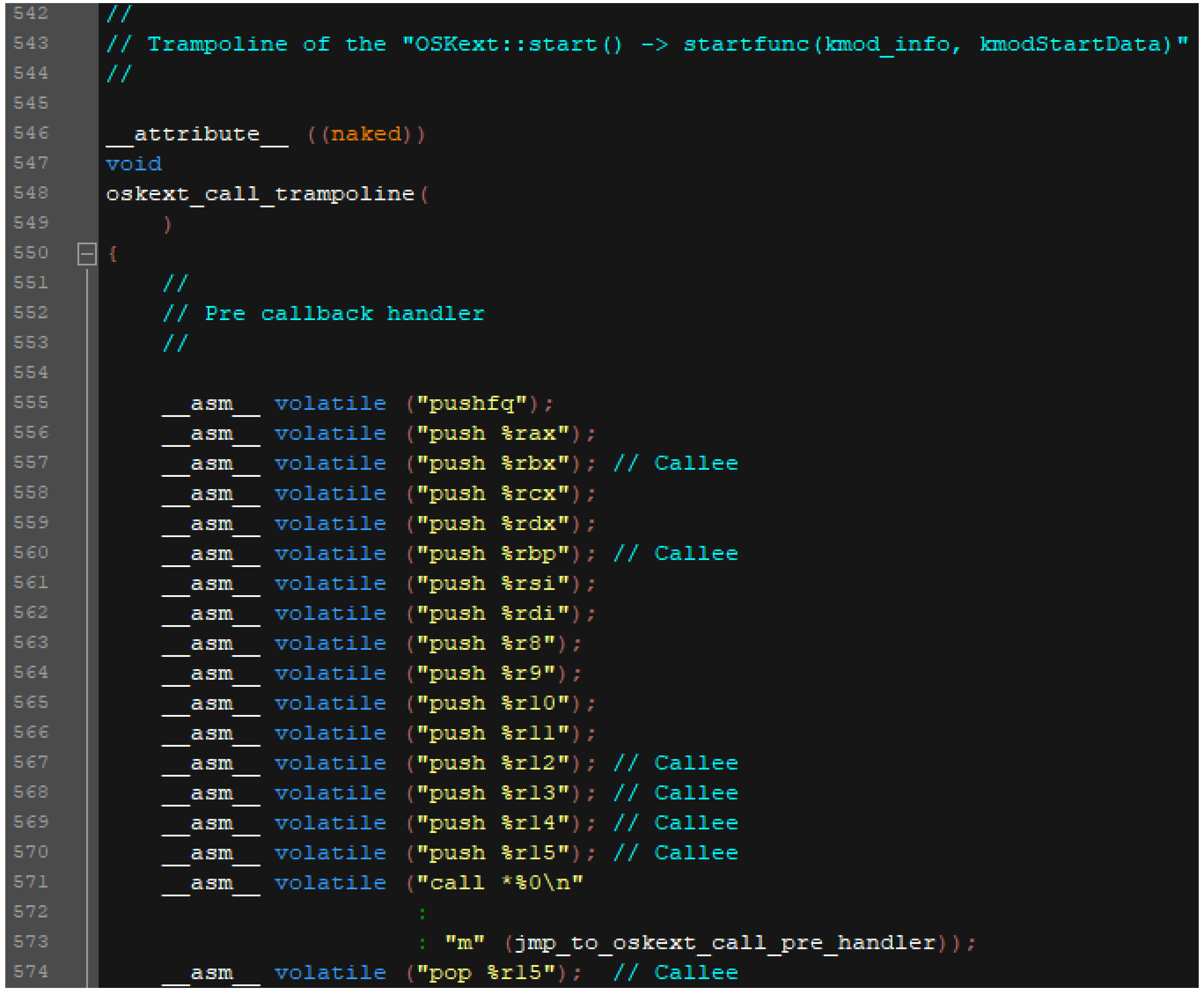


```
action=MONITORING_DYNAMIC_LIBRARY, uid=0, process(pid 1145)=ManagedClient, parent(ppid 1)=launchd, dynamic library path=/usr/lib/libobjc-trampolines.dylib.
action=MONITORING_DYNAMIC_LIBRARY, uid=501, process(pid 1155)=Captive Network , parent(ppid 1)=launchd, dynamic library path=/usr/lib/libobjc-trampolines.dylib.
action=MONITORING_DYNAMIC_LIBRARY, uid=501, process(pid 1157)=com.apple.WebKit, parent(ppid 1)=launchd, dynamic library path=/System/Library/Frameworks/WebKit.framework/Versions/A/Frameworks/SecItemShim.dylib.
action=MONITORING_DYNAMIC_LIBRARY, uid=501, process(pid 1155)=Captive Network , parent(ppid 1)=launchd, dynamic library path=/System/Library/Extensions/AMDRadeonX4000GLDriver.bundle/Contents/MacOS/AMDRadeonX4000GLDriver.
action=MONITORING_DYNAMIC_LIBRARY, uid=501, process(pid 1160)=MTLCompilerServi, parent(ppid 1)=launchd, dynamic library path=/System/Library/Extensions/AppleIntelGraphicsShared.bundle/Contents/MacOS/libigc.dylib.
action=MONITORING_DYNAMIC_LIBRARY, uid=501, process(pid 1158)=ReportCrash, parent(ppid 1)=launchd, dynamic library path=/usr/lib/swift/libswiftDemangle.dylib.
```



```
[Kemon.kext] : action=MONITORING_KEXT_PRE_CALLBACK, uid=0, process(pid 62)=kextd, parent(ppid 1)=launchd, path=/System/Library/Extensions/AppleUSBAudio.kext, module base=0xffffff7f92399000.
[Kemon.kext] : action=MONITORING_KEXT_POST_CALLBACK, uid=0, process(pid 62)=kextd, parent(ppid 1)=launchd, status=0, name=com.apple.driver.AppleUSBAudio, version=320.46, module base=0xffffff7f92399000, module size=0x6a000.
[Kemon.kext] : action=MONITORING_KEXT_POST_CALLBACK, uid=0, process(pid 62)=kextd, parent(ppid 1)=launchd, status=0, name=com.apple.iokit.SCSITaskUserClient, version=422, module base=0xffffff7f90cf5000, module size=0x9000.
[Kemon.kext] : action=MONITORING_KEXT_PRE_CALLBACK, uid=0, process(pid 62)=kextd, parent(ppid 1)=launchd, path=/System/Library/Extensions/AppleXsanScheme.kext, module base=0xffffff7f90d20000.
[Kemon.kext] : action=MONITORING_KEXT_POST_CALLBACK, uid=0, process(pid 62)=kextd, parent(ppid 1)=launchd, status=0, name=com.apple.driver.AppleXsanScheme, version=3, module base=0xffffff7f90d20000, module size=0x8000.
[Kemon.kext] : action=MONITORING_KEXT_PRE_CALLBACK, uid=0, process(pid 62)=kextd, parent(ppid 1)=launchd, path=/System/Library/Extensions/msdosfs.kext, module base=0xffffff7f90d28000.
[Kemon.kext] : action=MONITORING_KEXT_POST_CALLBACK, uid=0, process(pid 62)=kextd, parent(ppid 1)=launchd, status=0, name=com.apple.filesystems.msdosfs, version=1.10, module base=0xffffff7f90d28000, module size=0x11000.
```

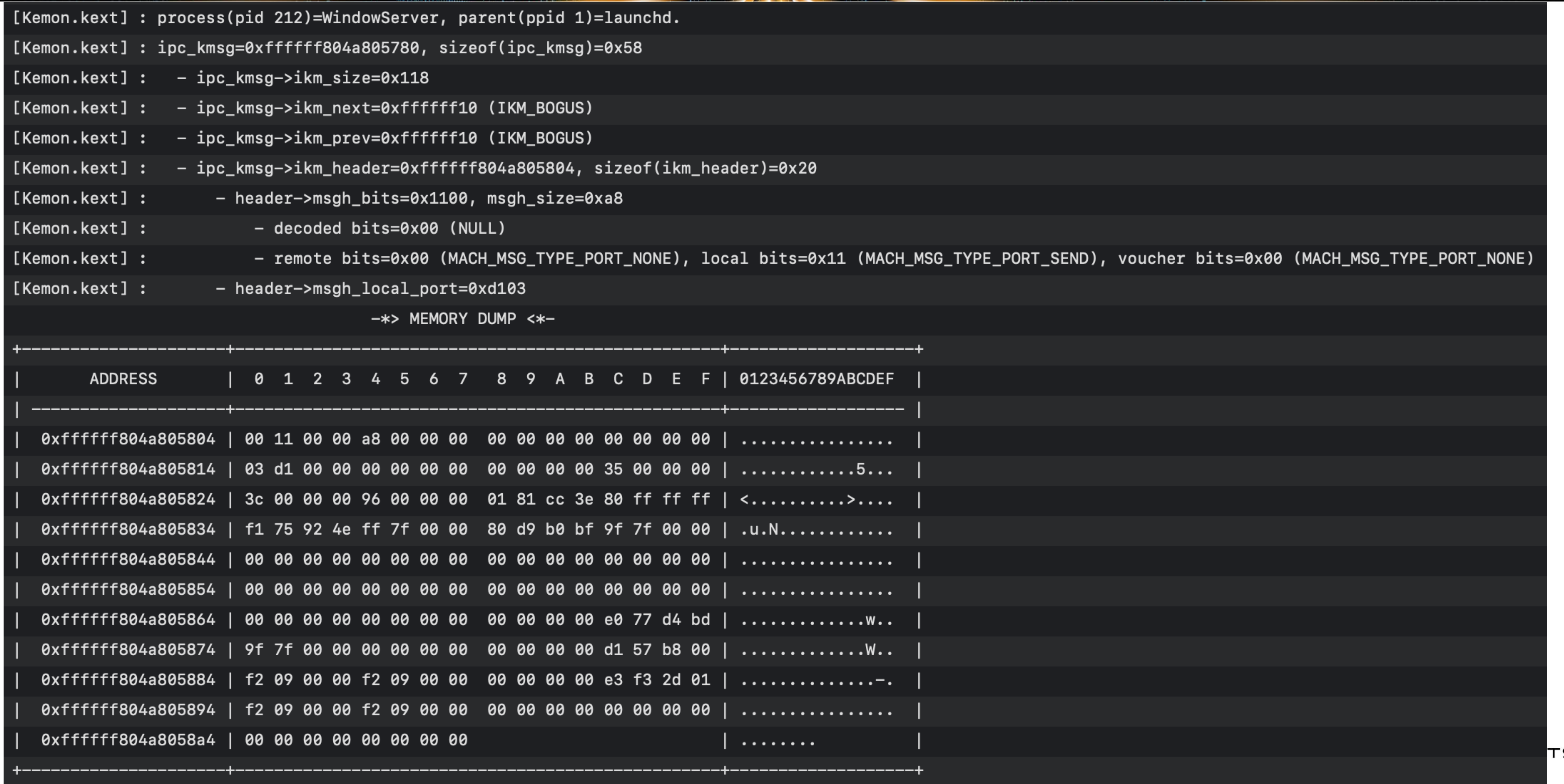
Kernel Inline Hook Engine



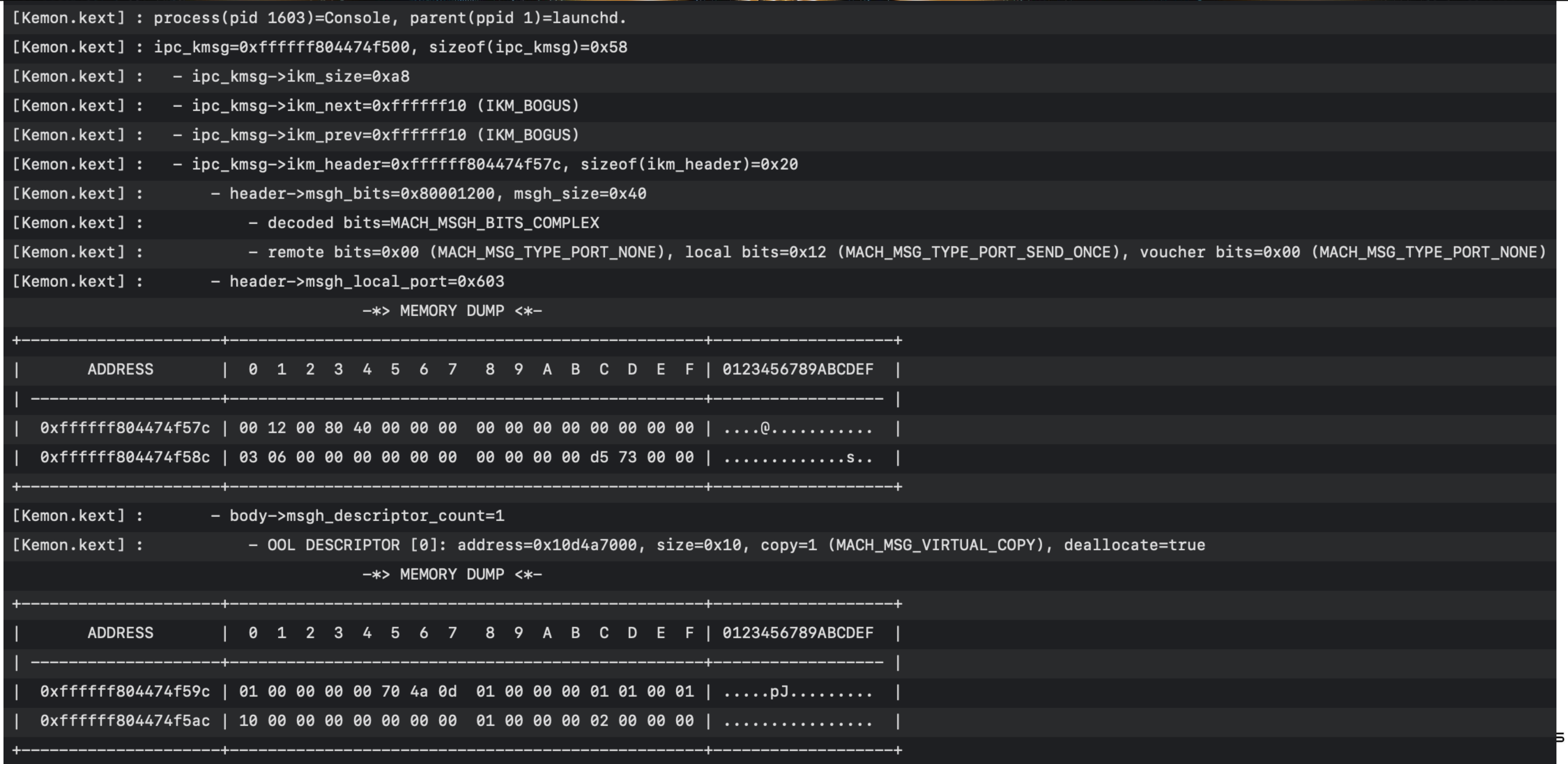
```
//
// Trampoline of the "OSKext::start() -> startfunc(kmod_info, kmodStartData)"
//

__attribute__ ((naked))
void
oskext_call_trampoline(
    )
{
    //
    // Pre callback handler
    //

    __asm__ volatile ("pushfq");
    __asm__ volatile ("push %rax");
    __asm__ volatile ("push %rbx"); // Callee
    __asm__ volatile ("push %rcx");
    __asm__ volatile ("push %rdx");
    __asm__ volatile ("push %rbp"); // Callee
    __asm__ volatile ("push %rsi");
    __asm__ volatile ("push %rdi");
    __asm__ volatile ("push %r8");
    __asm__ volatile ("push %r9");
    __asm__ volatile ("push %r10");
    __asm__ volatile ("push %r11");
    __asm__ volatile ("push %r12"); // Callee
    __asm__ volatile ("push %r13"); // Callee
    __asm__ volatile ("push %r14"); // Callee
    __asm__ volatile ("push %r15"); // Callee
    __asm__ volatile ("call *%0\n"
                      :
                      : "m" (jmp_to_oskext_call_pre_handler));
    __asm__ volatile ("pop %r15");  // Callee
```

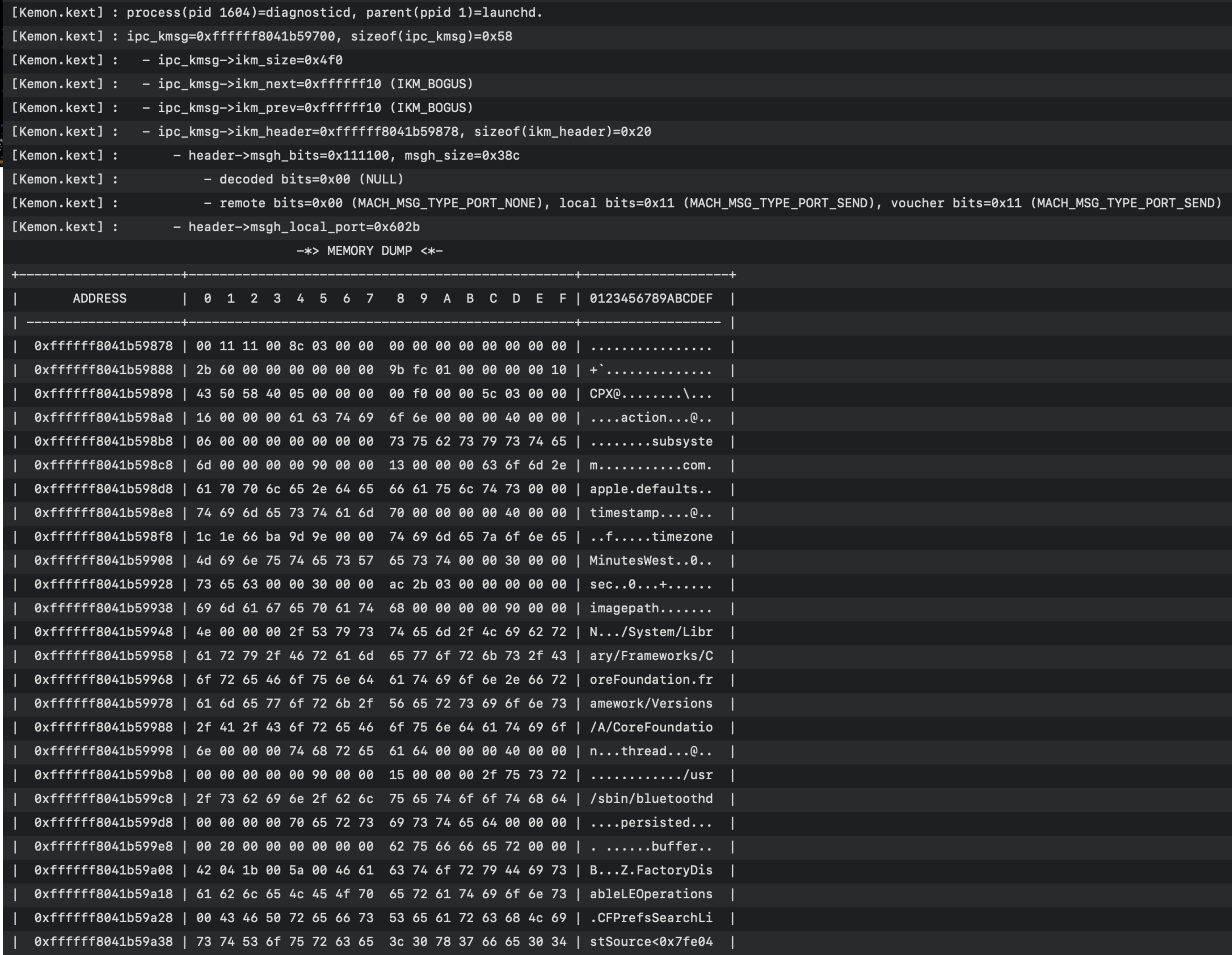


```
[Kemon.kext] : process(pid 212)=WindowServer, parent(ppid 1)=launchd.
[Kemon.kext] : ipc_kmsg=0xffffff804a805780, sizeof(ipc_kmsg)=0x58
[Kemon.kext] :   - ipc_kmsg->ikm_size=0x118
[Kemon.kext] :   - ipc_kmsg->ikm_next=0xffffff10 (IKM_BOGUS)
[Kemon.kext] :   - ipc_kmsg->ikm_prev=0xffffff10 (IKM_BOGUS)
[Kemon.kext] :   - ipc_kmsg->ikm_header=0xffffff804a805804, sizeof(ikm_header)=0x20
[Kemon.kext] :       - header->msgh_bits=0x1100, msgh_size=0xa8
[Kemon.kext] :           - decoded bits=0x00 (NULL)
[Kemon.kext] :           - remote bits=0x00 (MACH_MSG_TYPE_PORT_NONE), local bits=0x11 (MACH_MSG_TYPE_PORT_SEND), voucher bits=0x00 (MACH_MSG_TYPE_PORT_NONE)
[Kemon.kext] :       - header->msgh_local_port=0xd103
                                     -*> MEMORY DUMP <*-
+---------------------+--------------------------------------------------+-------------------+
|       ADDRESS       |  0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F | 0123456789ABCDEF  |
| --------------------+--------------------------------------------------+------------------ |
|  0xffffff804a805804 | 00 11 00 00 a8 00 00 00  00 00 00 00 00 00 00 00 | ................  |
|  0xffffff804a805814 | 03 d1 00 00 00 00 00 00  00 00 00 00 35 00 00 00 | ............5...  |
|  0xffffff804a805824 | 3c 00 00 00 96 00 00 00  01 81 cc 3e 80 ff ff ff | <..........>....  |
|  0xffffff804a805834 | f1 75 92 4e ff 7f 00 00  80 d9 b0 bf 9f 7f 00 00 | .u.N............  |
|  0xffffff804a805844 | 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 | ................  |
|  0xffffff804a805854 | 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 | ................  |
|  0xffffff804a805864 | 00 00 00 00 00 00 00 00  00 00 00 00 e0 77 d4 bd | .............w..  |
|  0xffffff804a805874 | 9f 7f 00 00 00 00 00 00  00 00 00 00 d1 57 b8 00 | .............W..  |
|  0xffffff804a805884 | f2 09 00 00 f2 09 00 00  00 00 00 00 e3 f3 2d 01 | ..............-.  |
|  0xffffff804a805894 | f2 09 00 00 f2 09 00 00  00 00 00 00 00 00 00 00 | ................  |
|  0xffffff804a8058a4 | 00 00 00 00 00 00 00 00                          | ........          |
+---------------------+--------------------------------------------------+-------------------+
```



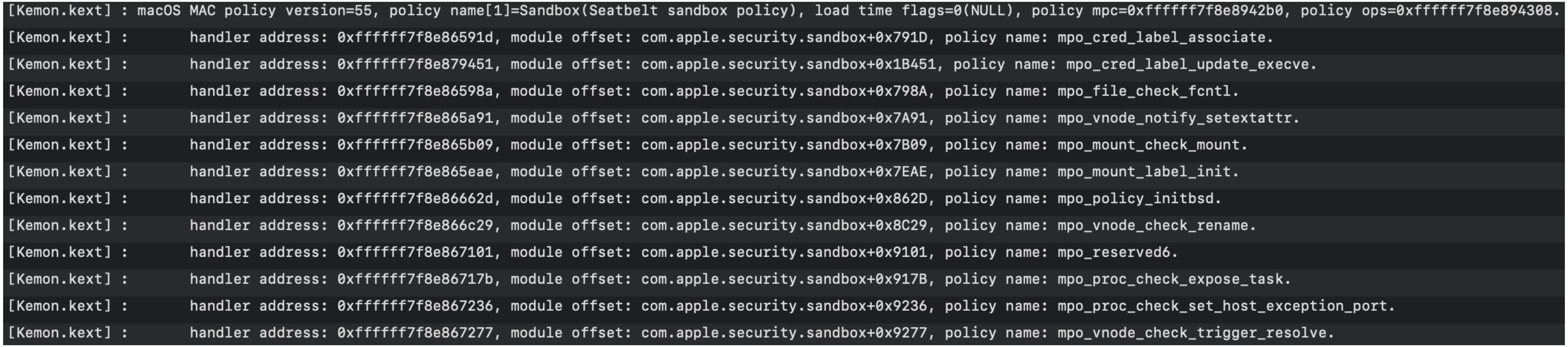
```
[Kemon.kext] : process(pid 1603)=Console, parent(ppid 1)=launchd.
[Kemon.kext] : ipc_kmsg=0xffffff804474f500, sizeof(ipc_kmsg)=0x58
[Kemon.kext] :   - ipc_kmsg->ikm_size=0xa8
[Kemon.kext] :   - ipc_kmsg->ikm_next=0xffffff10 (IKM_BOGUS)
[Kemon.kext] :   - ipc_kmsg->ikm_prev=0xffffff10 (IKM_BOGUS)
[Kemon.kext] :   - ipc_kmsg->ikm_header=0xffffff804474f57c, sizeof(ikm_header)=0x20
[Kemon.kext] :       - header->msgh_bits=0x80001200, msgh_size=0x40
[Kemon.kext] :           - decoded bits=MACH_MSGH_BITS_COMPLEX
[Kemon.kext] :           - remote bits=0x00 (MACH_MSG_TYPE_PORT_NONE), local bits=0x12 (MACH_MSG_TYPE_PORT_SEND_ONCE), voucher bits=0x00 (MACH_MSG_TYPE_PORT_NONE)
[Kemon.kext] :       - header->msgh_local_port=0x603
                                     -*> MEMORY DUMP <*-
+---------------------+--------------------------------------------------+-------------------+
|       ADDRESS       |  0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F | 0123456789ABCDEF  |
| --------------------+--------------------------------------------------+------------------ |
|  0xffffff804474f57c | 00 12 00 80 40 00 00 00  00 00 00 00 00 00 00 00 | ....@...........  |
|  0xffffff804474f58c | 03 06 00 00 00 00 00 00  00 00 00 00 d5 73 00 00 | .............s..  |
+---------------------+--------------------------------------------------+-------------------+
[Kemon.kext] :       - body->msgh_descriptor_count=1
[Kemon.kext] :           - OOL DESCRIPTOR [0]: address=0x10d4a7000, size=0x10, copy=1 (MACH_MSG_VIRTUAL_COPY), deallocate=true
                                     -*> MEMORY DUMP <*-
+---------------------+--------------------------------------------------+-------------------+
|       ADDRESS       |  0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F | 0123456789ABCDEF  |
| --------------------+--------------------------------------------------+------------------ |
|  0xffffff804474f59c | 01 00 00 00 00 70 4a 0d  01 00 00 00 01 01 00 01 | .....pJ.........  |
|  0xffffff804474f5ac | 10 00 00 00 00 00 00 00  01 00 00 00 02 00 00 00 | ................  |
+---------------------+--------------------------------------------------+-------------------+
```

Mach XPC/IPC Communication Sniffing



```
[Kemon.kext] : process(pid 1604)=diagnosticd, parent(ppid 1)=launchd.
[Kemon.kext] : ipc_kmsg=0xffffff8041b59700, sizeof(ipc_kmsg)=0x58
[Kemon.kext] :   - ipc_kmsg->ikm_size=0x4f0
[Kemon.kext] :   - ipc_kmsg->ikm_next=0xffffff10 (IKM_BOGUS)
[Kemon.kext] :   - ipc_kmsg->ikm_prev=0xffffff10 (IKM_BOGUS)
[Kemon.kext] :   - ipc_kmsg->ikm_header=0xffffff8041b59878, sizeof(ikm_header)=0x20
[Kemon.kext] :       - header->msgh_bits=0x111100, msgh_size=0x38c
[Kemon.kext] :           - decoded bits=0x00 (NULL)
[Kemon.kext] :           - remote bits=0x00 (MACH_MSG_TYPE_PORT_NONE), local bits=0x11 (MACH_MSG_TYPE_PORT_SEND), voucher bits=0x11 (MACH_MSG_TYPE_PORT_SEND)
[Kemon.kext] :       - header->msgh_local_port=0x602b
                             -*> MEMORY DUMP <*-
+---------------------+--------------------------------------------------+-------------------+
|       ADDRESS       |  0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F  | 0123456789ABCDEF  |
| --------------------+--------------------------------------------------+------------------ |
|  0xffffff8041b59878 | 00 11 11 00 8c 03 00 00  00 00 00 00 00 00 00 00 | ................  |
|  0xffffff8041b59888 | 2b 60 00 00 00 00 00 00  9b fc 01 00 00 00 00 10 | +`..............  |
|  0xffffff8041b59898 | 43 50 58 40 05 00 00 00  00 f0 00 00 5c 03 00 00 | CPX@........\...  |
|  0xffffff8041b598a8 | 16 00 00 00 61 63 74 69  6f 6e 00 00 00 40 00 00 | ....action...@..  |
|  0xffffff8041b598b8 | 06 00 00 00 00 00 00 00  73 75 62 73 79 73 74 65 | ........subsyste  |
|  0xffffff8041b598c8 | 6d 00 00 00 00 90 00 00  13 00 00 00 63 6f 6d 2e | m...........com.  |
|  0xffffff8041b598d8 | 61 70 70 6c 65 2e 64 65  66 61 75 6c 74 73 00 00 | apple.defaults..  |
|  0xffffff8041b598e8 | 74 69 6d 65 73 74 61 6d  70 00 00 00 00 40 00 00 | timestamp....@..  |
|  0xffffff8041b598f8 | 1c 1e 66 ba 9d 9e 00 00  74 69 6d 65 7a 6f 6e 65 | ..f.....timezone  |
|  0xffffff8041b59908 | 4d 69 6e 75 74 65 73 57  65 73 74 00 00 30 00 00 | MinutesWest..0..  |
|  0xffffff8041b59928 | 73 65 63 00 00 30 00 00  ac 2b 03 00 00 00 00 00 | sec..0...+......  |
|  0xffffff8041b59938 | 69 6d 61 67 65 70 61 74  68 00 00 00 00 90 00 00 | imagepath.......  |
|  0xffffff8041b59948 | 4e 00 00 00 2f 53 79 73  74 65 6d 2f 4c 69 62 72 | N.../System/Libr  |
|  0xffffff8041b59958 | 61 72 79 2f 46 72 61 6d  65 77 6f 72 6b 73 2f 43 | ary/Frameworks/C  |
|  0xffffff8041b59968 | 6f 72 65 46 6f 75 6e 64  61 74 69 6f 6e 2e 66 72 | oreFoundation.fr  |
|  0xffffff8041b59978 | 61 6d 65 77 6f 72 6b 2f  56 65 72 73 69 6f 6e 73 | amework/Versions  |
|  0xffffff8041b59988 | 2f 41 2f 43 6f 72 65 46  6f 75 6e 64 61 74 69 6f | /A/CoreFoundatio  |
|  0xffffff8041b59998 | 6e 00 00 00 74 68 72 65  61 64 00 00 00 40 00 00 | n...thread...@..  |
|  0xffffff8041b599b8 | 00 00 00 00 00 90 00 00  15 00 00 00 2f 75 73 72 | ............/usr  |
|  0xffffff8041b599c8 | 2f 73 62 69 6e 2f 62 6c  75 65 74 6f 6f 74 68 64 | /sbin/bluetoothd  |
|  0xffffff8041b599d8 | 00 00 00 00 70 65 72 73  69 73 74 65 64 00 00 00 | ....persisted...  |
|  0xffffff8041b599e8 | 00 20 00 00 00 00 00 00  62 75 66 66 65 72 00 00 | . ......buffer..  |
|  0xffffff8041b59a08 | 42 04 1b 00 5a 00 46 61  63 74 6f 72 79 44 69 73 | B...Z.FactoryDis  |
|  0xffffff8041b59a18 | 61 62 6c 65 4c 45 4f 70  65 72 61 74 69 6f 6e 73 | ableLEOperations  |
|  0xffffff8041b59a28 | 00 43 46 50 72 65 66 73  53 65 61 72 63 68 4c 69 | .CFPrefsSearchLi  |
|  0xffffff8041b59a38 | 73 74 53 6f 75 72 63 65  3c 30 78 37 66 65 30 34 | stSource<0x7fe04  |
```

Mandatory Access Control (MAC) Policy Monitoring



```
[Kemon.kext] : macOS MAC policy version=55, policy name[1]=Sandbox(Seatbelt sandbox policy), load time flags=0(NULL), policy mpc=0xffffff7f8e8942b0, policy ops=0xffffff7f8e894308.
[Kemon.kext] :        handler address: 0xffffff7f8e86591d, module offset: com.apple.security.sandbox+0x791D, policy name: mpo_cred_label_associate.
[Kemon.kext] :        handler address: 0xffffff7f8e879451, module offset: com.apple.security.sandbox+0x1B451, policy name: mpo_cred_label_update_execve.
[Kemon.kext] :        handler address: 0xffffff7f8e86598a, module offset: com.apple.security.sandbox+0x798A, policy name: mpo_file_check_fcntl.
[Kemon.kext] :        handler address: 0xffffff7f8e865a91, module offset: com.apple.security.sandbox+0x7A91, policy name: mpo_vnode_notify_setextattr.
[Kemon.kext] :        handler address: 0xffffff7f8e865b09, module offset: com.apple.security.sandbox+0x7B09, policy name: mpo_mount_check_mount.
[Kemon.kext] :        handler address: 0xffffff7f8e865eae, module offset: com.apple.security.sandbox+0x7EAE, policy name: mpo_mount_label_init.
[Kemon.kext] :        handler address: 0xffffff7f8e86662d, module offset: com.apple.security.sandbox+0x862D, policy name: mpo_policy_initbsd.
[Kemon.kext] :        handler address: 0xffffff7f8e866c29, module offset: com.apple.security.sandbox+0x8C29, policy name: mpo_vnode_check_rename.
[Kemon.kext] :        handler address: 0xffffff7f8e867101, module offset: com.apple.security.sandbox+0x9101, policy name: mpo_reserved6.
[Kemon.kext] :        handler address: 0xffffff7f8e86717b, module offset: com.apple.security.sandbox+0x917B, policy name: mpo_proc_check_expose_task.
[Kemon.kext] :        handler address: 0xffffff7f8e867236, module offset: com.apple.security.sandbox+0x9236, policy name: mpo_proc_check_set_host_exception_port.
[Kemon.kext] :        handler address: 0xffffff7f8e867277, module offset: com.apple.security.sandbox+0x9277, policy name: mpo_vnode_check_trigger_resolve.
```

macOS Kernel Vulnerability Hunting

- CVE-2017-7155
- CVE-2017-7163
- CVE-2017-13883
- CVE-2018-4350
- CVE-2018-4396
- CVE-2018-4418
- etc.
- Apple Product-Security Follow-up: 717716778 (08/02/19)

Try it Now!

https://github.com/didi/kemon

macOS Catalina 10.15 Beta (19A526h) is supported!

Q&A

wang yu

Didi Research America