Rootkits:
What they are and how to find them
Part 3

Xeno Kovah – 2010

xkovah at gmail

All materials is licensed under a Creative Commons “Share Alike” license.

- http://creativecommons.org/licenses/by-sa/3.0/

You are free:

to Share — to copy, distribute and transmit the work

to Remix — to adapt the work

Under the following conditions:

Attribution — You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).

Share Alike — If you alter, transform, or build upon this work, you may distribute the resulting work only under the same, similar or a compatible license.

Incident Response && Forensic Analysis

- Firewire memory capture if you can, otherwise…
- Plug in USB drive with win32dd on it
- Run win32dd from the USB drive, saving the results back to the USB drive
- Hard shutdown
- Physically remove HD, copy the HD with a hardware write blocker if available
- Turn a copy of the disk image into a virtual machine which can be run and examined using the tools described earlier
  - Being able to interact with and modify the system will be of critical importance if you're going to try and determine the causality behind an unknown change to system integrity
- Analyze the memory image with Volatility/WinDbg/ Memoryze/ResponderPro etc

win32dd

- http://www.moonsols.com/windows-memory-toolkit/
  - Download the "community edition"
- Pretending you had it running from and storing to the Z:\ drive:
  - win32dd /f Z:\machinename.dmp
  - win32dd /d /f Z:\machinename.dmp
    - /d is to put it in windbg crashdump form
- We were going to cheat and do it in the VM
- win32dd apparently doesn't run in vmware though. So we need to take the VM's .vmem file and run
  - bin2dmp.exe <path to .vmem> <name of .dmp>

Using Volatility for rootkit detection

- See Drew Hunt's class for more about memory analysis and Volatility
- The setup of Volatility is the standard 1.4 install (https://code.google.com/p/volatility/wiki/FullInstallation) with the following extra plugin in your Volatility-1.4_rc1\volatility\plugins folder
  - http://malwarecookbook.googlecode.com/svn/trunk/malware.py
- Good example usage of detecting various stuff here: http://code.google.com/p/volatility/wiki/CommandReference

SSDT hook detection

(also tells you when some threads possibly are being pointed to alternate, hooked, copies of the SSDT)

- python vol.py ssdt -f bla.dmp
- Built in (not from the malware plugin), unfortunately you need to sift it yourself

(Ctrl2Cap impersonator which hides files)
Entry 0x0091: 0xfa065592 (NtQueryDirectoryFile) owned by Ctr12Cap.sys
(Daemon Tools + SPTD)
Entry 0x00a0: 0xf97fd554 (NtQueryKey) owned by sptd.sys
(Trusteer Rapport normal hook)
Entry 0x00e0: 0xf9b4fa90 (NtSetInformationFile) owned by RapportCerberus_23645.sys
(Trusteer Rapport shadow SSDT hooks)
Entry 0x1124: 0xf0f27324 (NtGdiStretchBlt) owned by RapportPG.sys
<snip>
Entry 0x1299: 0xbf954c65 (NtGdiUMPDEngFreeUserMem) owned by win32k.sys
Entry 0x129a: 0xbf817637 (NtGdiDrawStream) owned by win32k.sys
SSDT[2] at e2187818 with 5 entries
Entry 0x2000: 0xefead620 (Unknown) owned by UNKNOWN
Entry 0x2001: 0xefead65e (Unknown) owned by UNKNOWN
Entry 0x2002: 0xefeadc1a (Unknown) owned by UNKNOWN
Entry 0x2003: 0xefeae15a (Unknown) owned by UNKNOWN
Entry 0x2004: 0xefead6a2 (Unknown) owned by UNKNOWN

He4Hook's user->kernel coms

SSDT hook detection 2

- python vol.py ssdt_by_threads -f bla.dmp
- Only shows things in main SSDT != nt, and shadow SSDT != win32k

```
Volatile Systems Volatility Framework 1.4_rc1
Pid      Tid      Name                 SSDT
  Entry 0x0013: 0xf0f20fa2 (NtAssignProcessToJobObject) owned by RapportPG.sys
  Entry 0x001f: 0xf0fd1534 (NtConnectPort) owned by vsdatant.sys
  Entry 0x0025: 0xf0f21a38 (NtCreateFile) owned by RapportPG.sys
<snip>
 4        8 System             0x80501030
     4       12 System             0x80501030
     4       16 System             0x80501030
     4       20 System             0x80501030
```

userspace inline/IAT hook detection

- python vol.py apihooks -f bla.dmp
- Looks for hooks in all the DLLs in the process memory space as well

```
Volatile Systems Volatility Framework 1.4_rc1
Name                            Type     Target                                  Value
smss.exe[612]                   syscall  ntdll.dll!NtAcceptConnectPort           0x7ffe0300 MOV
    EDX, 0x7ffe0300 (UNKNOWN)
smss.exe[612]                   syscall  ntdll.dll!NtAccessCheck                 0x7ffe0300 MOV
    EDX, 0x7ffe0300 (UNKNOWN)
<snip>
csrss.exe[688]@rpcrt4.dll       iat      KERNEL32.dll!SetCriticalSectionSpinCount 0x0 0x7c92a067
csrss.exe[688]                  inline   rpcrt4.dll!GlobalMutexClearExternal      0x77eb62b6 CALL
    [0x77e71358] =>> 0x7c9010e0
csrss.exe[688]                  inline   rpcrt4.dll!GlobalMutexRequestExternal   0x77eb62a5 CALL
    [0x77e7135c] =>> 0x7c901000
csrss.exe[688]                  inline   ntdll.dll!0x46                          0x7c9163c3 JMP
    0x7ffa4028 (UNKNOWN)
csrss.exe[688]                  inline   ntdll.dll!0x7b                          0x7c90d0ae JMP
    0x7ffa47d8 (UNKNOWN)
<snip>
csrss.exe[688]@advapi32.dll     iat      KERNEL32.dll!*invalid*                  0x0 0x7c90fe21
csrss.exe[688]@advapi32.dll     iat      KERNEL32.dll!*invalid*                  0x0 0x7c91137a
```

IRP hook detection

- python vol.py driverirp -f bla.dmp
- Can use -r to specify a regex if you only want to look at one driver

```
Volatile Systems Volatility Framework 1.4_rc1
DriverStart  Name             IRP                                IrpAddr      IrpOwner         HookAddr     HookOwner
0xefee5000   'msdirectx'      IRP_MJ_CREATE                      0xefee62d0   - (X: not named because hidden? but still the
     address is clearly close to the module space)-           -
0xefee5000   'msdirectx'      IRP_MJ_CREATE_NAMED_PIPE           0x804f355a   ntoskrnl.exe     -            -
0xf9a3c000   'i8042prt'       IRP_MJ_DEVICE_CONTROL              0xf9a42e4b   i8042prt.sys     -            -
0xf9a3c000   'i8042prt'       IRP_MJ_INTERNAL_DEVICE_CONTROL     0xf99f06b0   RapportKELL.sys  -            - (3rd party module
     hooking keyboard driver IRP)
0xf9a3c000   'i8042prt'       IRP_MJ_SHUTDOWN                    0x804f355a   ntoskrnl.exe     -            -
0xf9601000   'Ntfs'           IRP_MJ_CREATE                      0xefeb3bdc   -                -            -
0xf9601000   'Ntfs'           IRP_MJ_CREATE_NAMED_PIPE           0xefeb3bdc   -                -            -
0xf9601000   'Ntfs'           IRP_MJ_CLOSE                       0xefeb3bdc   -                -            -
0xf9601000   'Ntfs'           IRP_MJ_READ                        0xefeb3bdc   -                -            -
...
0xf9b8c000   'Cdfs'           IRP_MJ_CREATE                      0xefeb3bdc   -                -            -
0xf9d7c000   'Msfs'           IRP_MJ_CREATE                      0xefeb3bdc   -                -            -
0xf9d8c000   'Npfs'           IRP_MJ_CREATE                      0xefeb3bdc   -                -            -
...(something hooking everything in ntfs, cdfs, msfs, npfs, and others)
```

IDT hook detection

- python vol.py idt -f bla.dmp
- Shows hooks to the IDT itself, as well as any inline hooks immediately at the target of the IDT entry
- Can have semi-misleading results in that most all of the KiUnexpectedInterrupt# entries naturally have a jmp to a common function as their first instruction. Also doesn't know about KINTERRUPTs, therefore induces unnecessary suspicion on those entries, and doesn't find KINTERRUPT inline or ServiceRoutine hooks (but it will get improved with feedback)
- D 8 KiTrap0D 0x8053fd90 ntoskrnl.exe .text
- E 8 KiTrap0E 0xf9f5c816 mmpc.sys .text (shadowwalker)
- F 8 KiTrap0F 0x805407c8 ntoskrnl.exe .text
- 61 8 KiUnexpectedInterrupt49 0x8053cd5a ntoskrnl.exe .text => JMP 0x8053d357
- 62 8 KiUnexpectedInterrupt50 0x81784044
- 63 8 KiUnexpectedInterrupt51 0x8053cd6e ntoskrnl.exe .text => JMP 0x8053d357
- 82 8 KiUnexpectedInterrupt82 0x8186fdd4
- 83 8 KiUnexpectedInterrupt83 0x81acaa14
- (62, 82, 83 and others turn out to be KINTERRUPTs)

GDT modification detection

- python vol.py gdt -f bla.dmp
- Callgates are suspicious, GDT index 1 should be DPL 0 code, index 2 should be DPL 0 data, index 3: DPL 3 code, index 4: DPL 3 data
- All IDT entries except task gates should point at GDT index 1

```
Volatile Systems Volatility Framework 1.4_rc1
Sel     Base          Limit         Type            DPL     Gr      Pr
0x0     0x0           0x0           <Reserved>      0       By      Np
0x8     0x0           0xffffffff    Code RE Ac      0       Pg      P
0x10    0x0           0xffffffff    Data RW Ac      0       Pg      P
0x18    0x0           0xffffffff    Code RE Ac      3       Pg      P
0x20    0x0           0xffffffff    Data RW Ac      3       Pg      P
0x28    0x80042000    0x20ab        TSS32 Busy      0       By      P
0x30    0xffdff000    0x1fff        Data RW Ac      0       Pg      P
0x38    0x0           0xfff         Data RW Ac      3       By      P
0x40    0x400         0xffff        Data RW         3       By      P
0x48    0xfa0ad530    -             CallGate32      3       -       P
```

Listing callbacks

- python vol.py callbacks -f bla.dmp
- Prints kernel callbacks of the following types:
  - PsSetCreateProcessNotifyRoutine (process creation).
  - PsSetCreateThreadNotifyRoutine (thread creation).
  - PsSetImageLoadNotifyRoutine (DLL/image load).
  - IoRegisterFsRegistrationChange (file system registration).
  - KeRegisterBugCheck and KeRegisterBugCheckReasonCallback.
  - CmRegisterCallback (registry callbacks on XP).
  - CmRegisterCallbackEx (registry callbacks on Vista and 7).
  - IoRegisterShutdownNotification (shutdown callbacks).
  - DbgSetDebugPrintCallback (debug print callbacks on Vista and 7).
  - DbgkLkmdRegisterCallback (debug callbacks on 7).
- Currently seems to take forever

Detecting hidden processes

(process = ps, cross-view = xview)

- python vol.py psxview -f bla.dmp
- Shows which process enumeration plugins a given process occurs in (and therefore take a long time to run)

```
Volatile Systems Volatility Framework 1.4_rc1
Offset       Name                 Pid      pslist     psscan     thrdproc   pspcid     csr_hnds
     csr_list
0x81aea020L  lsass.exe            768      1          1          1          1          1          1
0x818f9388L  svchost.exe          1280     1          1          1          1          1          1
0x8170cbe0L  svchost.exe          1028     1          1          1          1          1          1
0x81bcc830L  System               0        0          1          1          0          0          0
hidden with FUTo
<snip>
0x81978310L  hxdef100.exe         3720     1          1          1          1          1          1
Maybe only hidden with userspace hooks, therefore everything else finds it fine
0x817f2b80L  csrss.exe            688      1          1          1          1          0          0
0x81769020L  smss.exe             612      1          1          1          1          0          0
dunno what's up with that
```

Listing Windows services

- python vol.py svcscan -f bla.dmp
- Lots of good stuff there at the end
- Still lots to sort through though, doesn't exclude default - this is where you need histograms!

```
0x38b268     0x108    1192     WZCSVC           Wireless Zero Configuration
SERVICE_WIN32_SHARE_PROCESS    SERVICE_RUNNING
 C:\WINDOWS\System32\svchost.exe -k netsvcs
0x38b2f8     0x109    -------- xmlprov          Network Provisioning Service
SERVICE_WIN32_SHARE_PROCESS    SERVICE_STOPPED
 --------
0x38b388     0x10a    -------- msdirectx        msdirectx                                SERVICE_KERNEL_DRIVER
SERVICE_RUNNING
 \Driver\msdirectx
0x38b418     0x10b    -------- mmpc             mmpc                                     SERVICE_KERNEL_DRIVER
SERVICE_RUNNING
 \Driver\mmpc
0x38b4a0     0x10c    -------- vanquish         Vanquish Autoloader v0.2.1
SERVICE_WIN32_OWN_PROCESS|SERVICE_INTERACTIVE_PROCE
SS SERVICE_STOPPED      --------
0x38b530     0x10d    3720     HackerDefender100 HXD Service 100
SERVICE_WIN32_OWN_PROCESS      SERVICE_RUNNING
  C:\hxdef100r\hxdef100.exe
0x38b5d0     0x10e    -------- Ctr12Cap         Ctr12Cap                                 SERVICE_KERNEL_DRIVER
SERVICE_RUNNING
 \Driver\Ctr12Cap
0x38b660     0x10f    -------- 000627CE         000627CE                                 SERVICE_KERNEL_DRIVER
SERVICE_STOPPED
```

Time-Permitting

KOH country for old men

- http://www.rootkit.com/newsread.php?newsid=501 (use wayback machine)
- Kernel Object Hooking (KOH) is technically a subset of DKOM
- Only thing about kernel objects that it's manipulating is function pointers
- Just like in IDT/SSDT/IAT cases, you are just replacing function pointers
- The thing is, as opposed to those big name tables, the locations to target for KOH require deeper knowledge of the data structures.
- But the idea is that the objects targeted for KOH are going to be potentially popping in and out of existence, or will just generally be in kernel heap memory, and therefore not at well-known locations that the defender can check.
- Further, in some case (such as Deferred Procedure Calls) it may be a generic mechanism which can have many different possible function pointers, making it harder to baseline expectations.

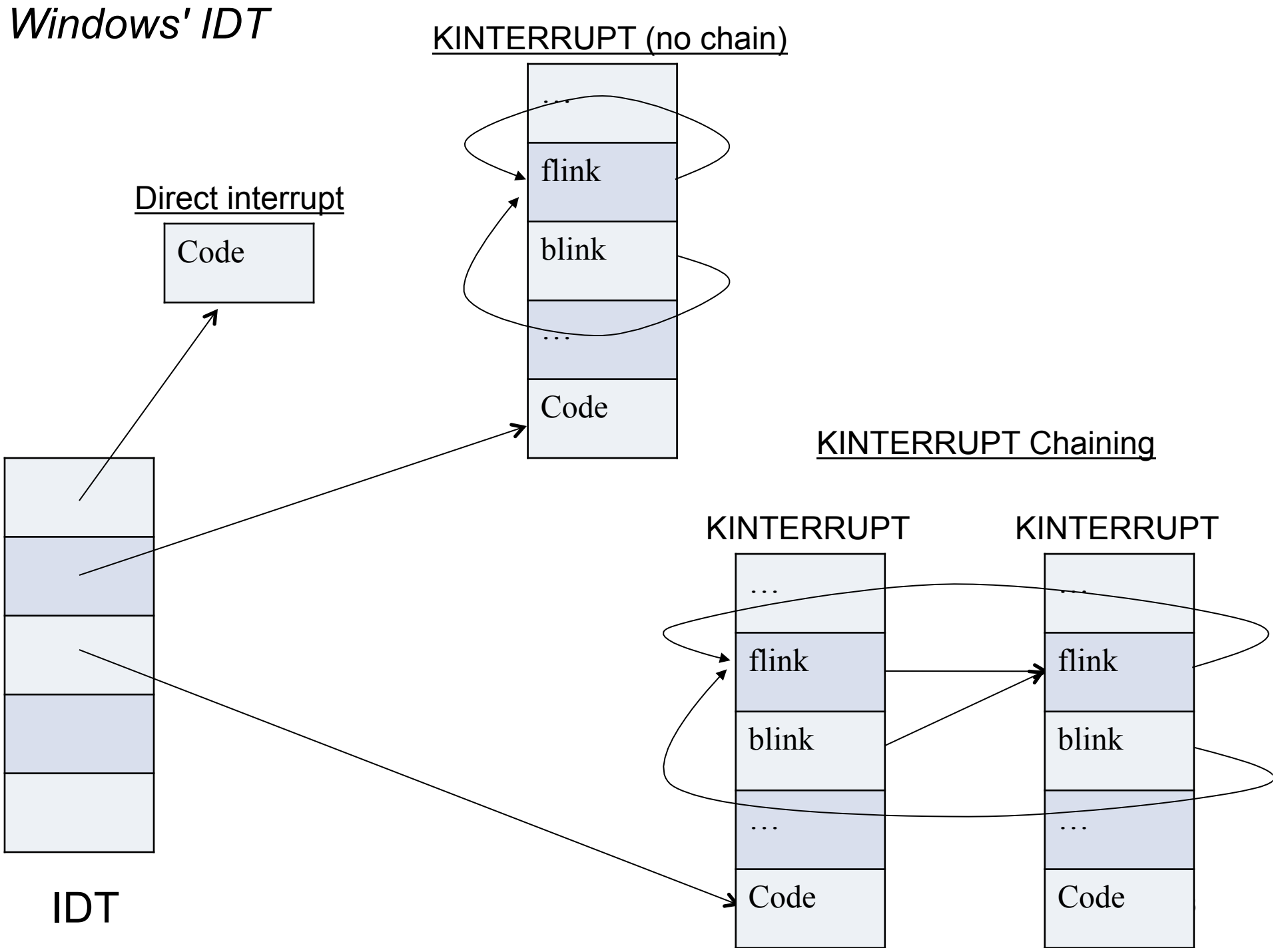
_KINTERRUPT KOH

- http://www.phrack.org/issues.html?issue=65&id=4

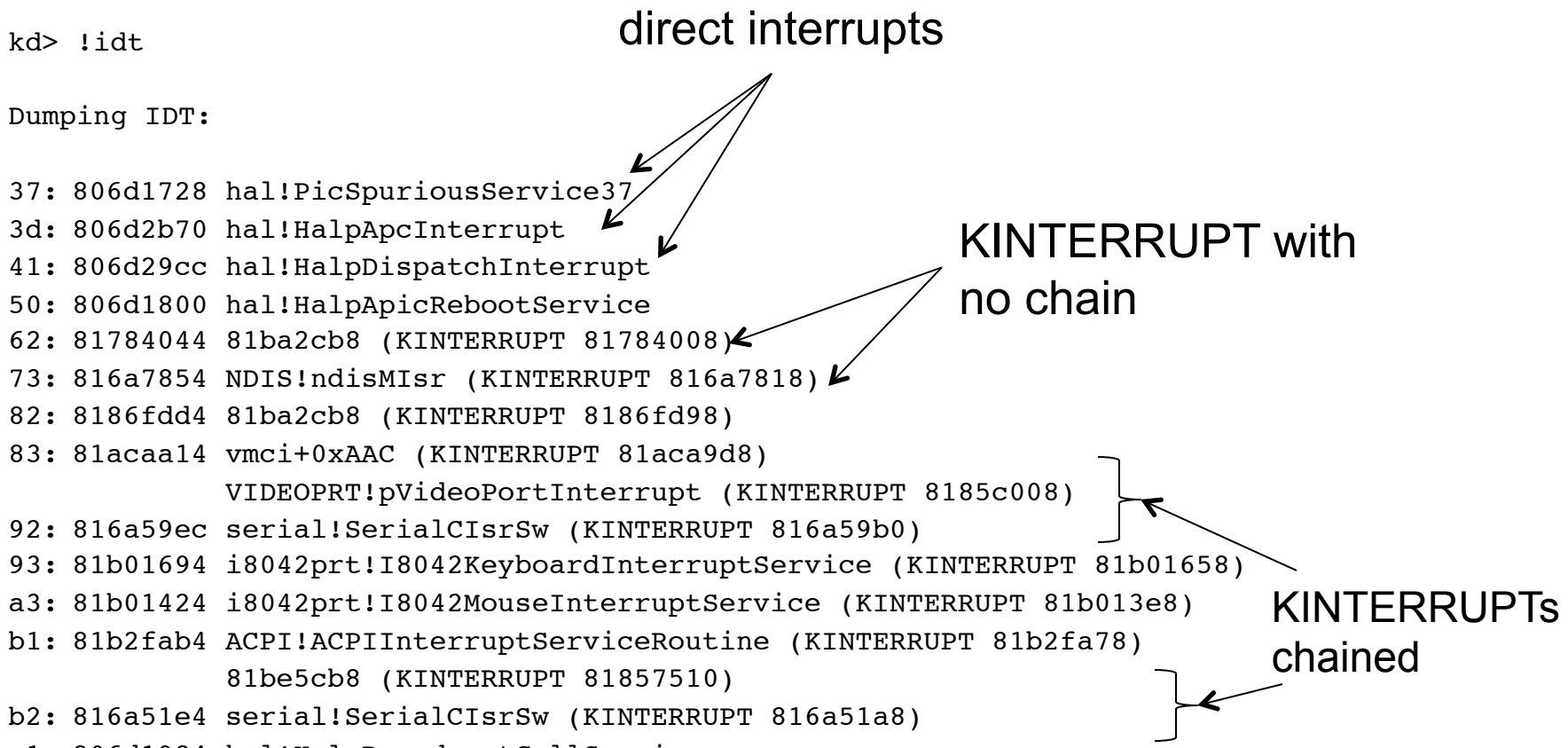
  - Is actually trying to avoid using KOH ("This article present a way of subverting the Windows kernel by modifying only data. No function pointers, no static hooking or others classical technique.")

  - But they're using inline hooking in the KINTERRUPT so…what is that? Kernel Object Inline-hooking! KOI! (nah I just made that up)
  - Just giving it as a reference since it talks about the structure of the KINTERRUPT a bit

Windows' IDT


KINTERRUPT (no chain)
…
flink
blink
…
Code
Direct interrupt
Code
KINTERRUPT Chaining
KINTERRUPT
KINTERRUPT
IDT

Viewing partial IDT in WinDbg




```
kd> !idt

Dumping IDT:

37: 806d1728 hal!PicSpuriousService37
3d: 806d2b70 hal!HalpApcInterrupt
41: 806d29cc hal!HalpDispatchInterrupt
50: 806d1800 hal!HalpApicRebootService
62: 81784044 81ba2cb8 (KINTERRUPT 81784008)
73: 816a7854 NDIS!ndisMIsr (KINTERRUPT 816a7818)
82: 8186fdd4 81ba2cb8 (KINTERRUPT 8186fd98)
83: 81acaa14 vmci+0xAAC (KINTERRUPT 81aca9d8)
             VIDEOPRT!pVideoPortInterrupt (KINTERRUPT 8185c008)
92: 816a59ec serial!SerialCIsrSw (KINTERRUPT 816a59b0)
93: 81b01694 i8042prt!I8042KeyboardInterruptService (KINTERRUPT 81b01658)
a3: 81b01424 i8042prt!I8042MouseInterruptService (KINTERRUPT 81b013e8)
b1: 81b2fab4 ACPI!ACPIInterruptServiceRoutine (KINTERRUPT 81b2fa78)
             81be5cb8 (KINTERRUPT 81857510)
b2: 816a51e4 serial!SerialCIsrSw (KINTERRUPT 816a51a8)
c1: 806d1984 hal!HalpBroadcastCallService
d1: 806d0d34 hal!HalpClockInterrupt
e1: 806d1f0c hal!HalpIpiHandler
e3: 806d1c70 hal!HalpLocalApicErrorService
fd: 806d2464 hal!HalpProfileInterrupt
fe: 806d2604 hal!HalpPerfInterrupt
```

<snip>

73:**816a7854** NDIS!ndisMIsr (KINTERRUPT *816a7818*)

<snip>

```
kd> u 816a7854
816a7854 54              push    esp
816a7855 55              push    ebp
816a7856 53              push    ebx
816a7857 56              push    esi
816a7858 57              push    edi
816a7859 83ec54          sub     esp,54h
<snip>
```

```
kd> dt _KINTERRUPT 816a7818
nt!_KINTERRUPT
   +0x000 Type             : 22
   +0x002 Size             : 484
   +0x004 InterruptListEntry : _LIST_ENTRY [ 0x816a781c - 0x816a781c ]
   +0x00c ServiceRoutine   : 0xf95ece10     unsigned char  NDIS!ndisMIsr+0
   +0x010 ServiceContext   : 0x819652bc
   +0x014 SpinLock         : 0
   +0x018 TickCount        : 0xffffffff
   +0x01c ActualLock       : 0x816a7a7c  -> 0
   +0x020 DispatchAddress  : 0x80541550     void  nt!KiInterruptDispatch+0
   +0x024 Vector           : 0x173
   +0x028 Irql             : 0x6 ''
   +0x029 SynchronizeIrql  : 0x6 ''
   +0x02a FloatingSave     : 0 ''
   +0x02b Connected        : 0x1 ''
   +0x02c Number           : 0 ''
   +0x02d ShareVector      : 0x1 ''
   +0x030 Mode             : 0 ( LevelSensitive )
   +0x034 ServiceCount     : 0
   +0x038 DispatchCount    : 0xffffffff
   +0x03c DispatchCode     : [106] 0x56535554
```

_NDIS_PROTOCOL_CHARACTERISTICS KOH

- NDIS = Network Driver Interface Specification. MS's network driver abstraction system
- Every NDIS driver has to register a bunch of callback functions for how it will handle various activities such as receiving packets, sending packets,
- It does this with NdisRegisterProtocol which takes a pointer to the NDIS_PROTOCOL_CHARACTERISTICS structure which has all those callbacks filled in.
  - http://msdn.microsoft.com/en-us/library/ff554653(v=vs.85).aspx
- The callbacks are a target for KOH
- http://www.f-secure.com/weblog/archives/00001393.html
  - KOHed by mebroot, rustock, srizbi

Book page 614

_NDIS_PROTOCOL_CHARACTERISTICS KOH

```
typedef struct _NDIS_PROTOCOL_CHARACTERISTICS {
    UCHAR MajorNdisVersion;
    UCHAR MinorNdisVersion;
    UINT Reserved;
    OPEN_ADAPTER_COMPLETE_HANDLER OpenAdapterCompleteHandler;
    CLOSE_ADAPTER_COMPLETE_HANDLER CloseAdapterCompleteHandler;
    SEND_COMPLETE_HANDLER SendCompleteHandler;
    TRANSFER_DATA_COMPLETE_HANDLER TransferDataCompleteHandler;
    RESET_COMPLETE_HANDLER ResetCompleteHandler;
    REQUEST_COMPLETE_HANDLER RequestCompleteHandler;
    RECEIVE_HANDLER ReceiveHandler;
    RECEIVE_COMPLETE_HANDLER ReceiveCompleteHandler;
    STATUS_HANDLER StatusHandler;
    STATUS_COMPLETE_HANDLER StatusCompleteHandler;
    NDIS_STRING Name;
//
// MajorNdisVersion must be set to 0x04 or 0x05
// with any of the following members.
//
    RECEIVE_PACKET_HANDLER ReceivePacketHandler;
    BIND_HANDLER BindAdapterHandler;
    UNBIND_HANDLER UnbindAdapterHandler;
    PNP_EVENT_HANDLER PnPEventHandler;
    UNLOAD_PROTOCOL_HANDLER UnloadHandler;
//
// MajorNdisVersion must be set to 0x05
// with any of the following members.
//
    CO_SEND_COMPLETE_HANDLER CoSendCompleteHandler;
    CO_STATUS_HANDLER CoStatusHandler;
    CO_RECEIVE_PACKET_HANDLER CoReceivePacketHandler;
    CO_AF_REGISTER_NOTIFY_HANDLER CoAfRegisterNotifyHandler;
} NDIS_PROTOCOL_CHARACTERISTICS, *PNDIS_PROTOCOL_CHARACTERISTICS;
```

_OBJECT_TYPE_INITIALIZER KOH

- Think of it like a structure which holds function pointer for constructors/descructors/ accessors for an object
- http://www.prevx.com/blog/120/MBR-rootkit-changes-itself-and-strikes-again.html
  - The mebroot people are apparently quite familiar with the concept of KOH

_OBJECT_TYPE_INITIALIZER

```
nt!_OBJECT_TYPE_INITIALIZER
   +0x000 Length          : Uint2B
   +0x002 UseDefaultObject : UChar
   +0x003 CaseInsensitive  : UChar
   +0x004 InvalidAttributes : Uint4B
   +0x008 GenericMapping   : _GENERIC_MAPPING
   +0x018 ValidAccessMask  : Uint4B
   +0x01c SecurityRequired : UChar
   +0x01d MaintainHandleCount : UChar
   +0x01e MaintainTypeList : UChar
   +0x020 PoolType         : _POOL_TYPE
   +0x024 DefaultPagedPoolCharge : Uint4B
   +0x028 DefaultNonPagedPoolCharge : Uint4B
   +0x02c DumpProcedure    : Ptr32     void
   +0x030 OpenProcedure    : Ptr32     long
   +0x034 CloseProcedure   : Ptr32     void
   +0x038 DeleteProcedure  : Ptr32     void
   +0x03c ParseProcedure   : Ptr32     long
   +0x040 SecurityProcedure : Ptr32     long
   +0x044 QueryNameProcedure : Ptr32     long
   +0x048 OkayToCloseProcedure : Ptr32     unsigned char
```

Some others

- A catalog of windows local kernel-mode backdoors
- http://www.uninformed.org/?v=8&a=2&t=sumry
- Very good document, highly recommended read
- And again, more structures are mentioned offhandedly in that original KOH article

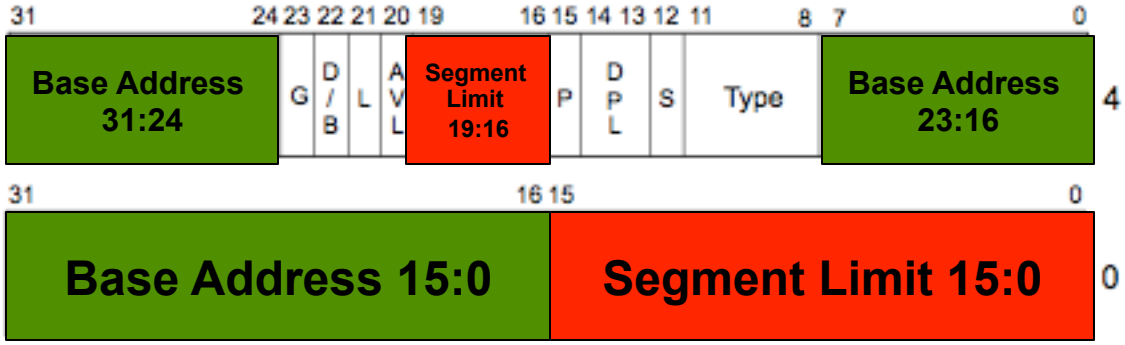
Segment Hooking

(Xeno's tiny contribution to the understanding of hooking)

- Recall that an interrupt descriptor is actually a far pointer. That means there's a 32 bit offset and a 16 bit segment selector.
- A normal hook on a direct interrupt changes the 32 bit offset
- Xeno found that we can change the segment selector to select a new segment where the base + existing 32 bit offset = attacker code.
- The crazy thing is that we can actually purposely overflow the 32 bit space in order to jump to code which is at a lower address than the existing 32 bit offset.
- Existing tools (WinDbg, GMER, Memoryze, etc) only look for a change to the 32 bit offset, so this is invisible for the moment (everyone has been informed)

Review: Segment Descriptors

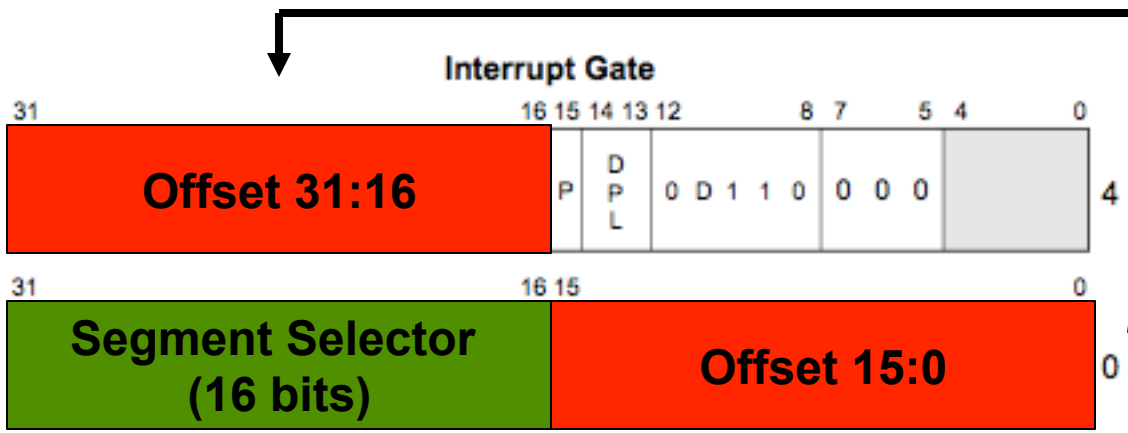
- "Each segment has a segment descriptor, which specifies the size of the segment, the access rights and privilege level for the, the segment type, and the location of the first byte of the segment in the linear address space (called the base address of the segment)."



L — 64-bit code segment (IA-32e mode only)
AVL — Available for use by system software
BASE — Segment base address
D/B — Default operation size (0 = 16-bit segment; 1 = 32-bit segment)
DPL — Descriptor privilege level
G — Granularity
LIMIT — Segment Limit
P — Segment present
S — Descriptor type (0 = system; 1 = code or data)
TYPE — Segment type

Figure 3-8. Segment Descriptor

Review: Interrupt Gate Descriptor



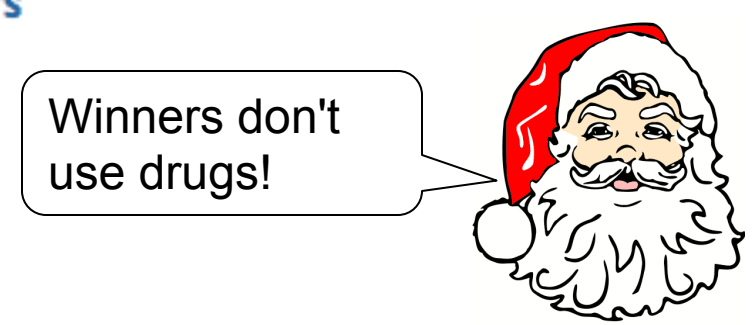
Note that the two halves of the offset form a 32 bit address.

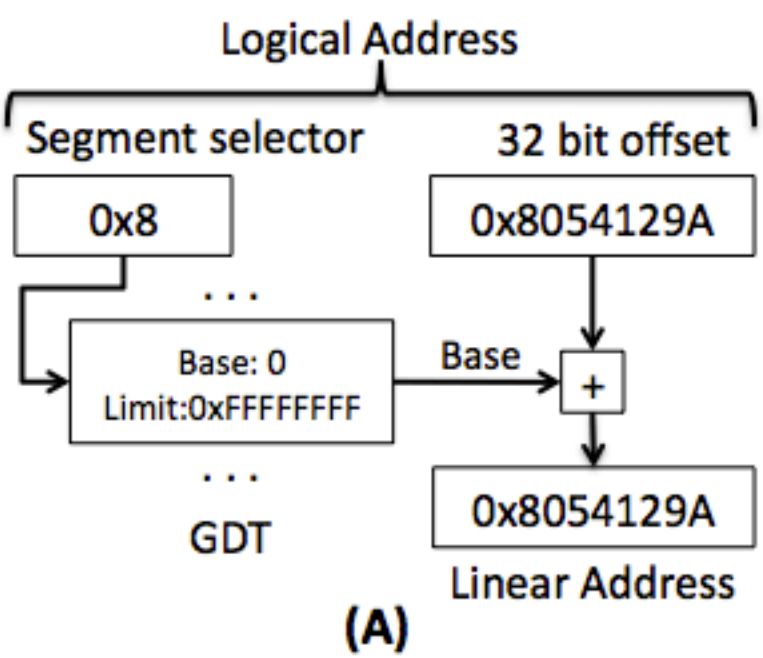
DPL	Descriptor Privilege Level
Offset	Offset to procedure entry point
P	Segment Present flag
Selector	Segment Selector for destination code segment
D	Size of gate: 1 = 32 bits; 0 = 16 bits

Reserved

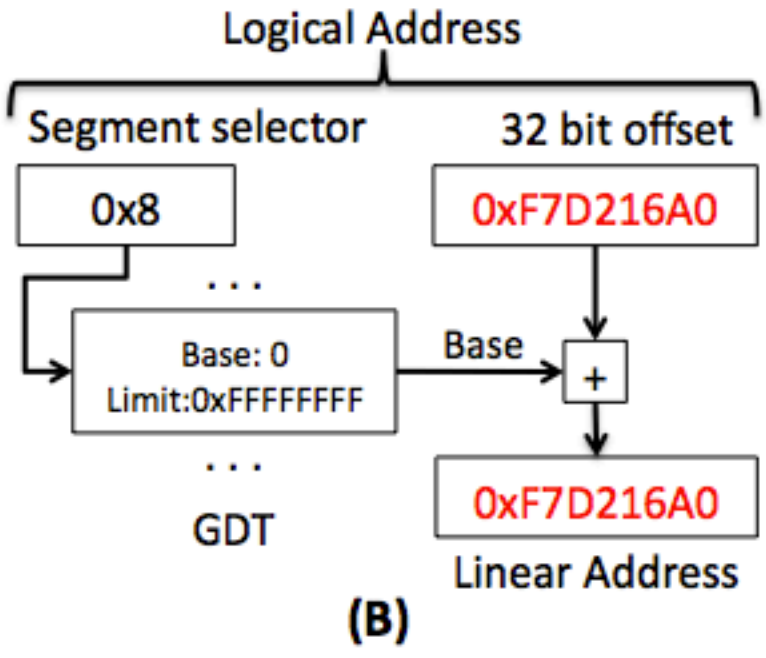
Descriptors not in use should have P = 0

Figure 5-2. IDT Gate Descriptors

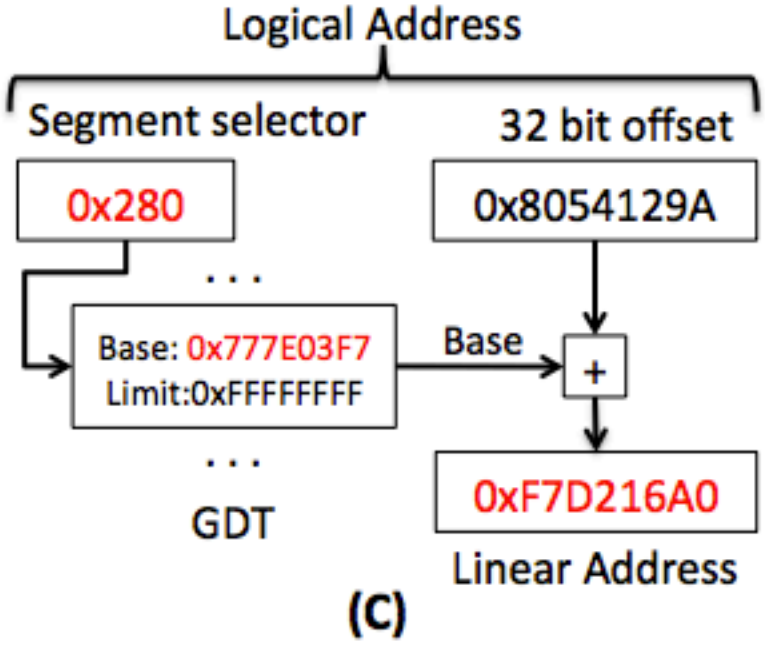



Logical Address
Segment selector
32 bit offset
0x8
0x8054129A
Base: 0
Limit:0xFFFFFFFF
Base
+
GDT
0x8054129A
Linear Address

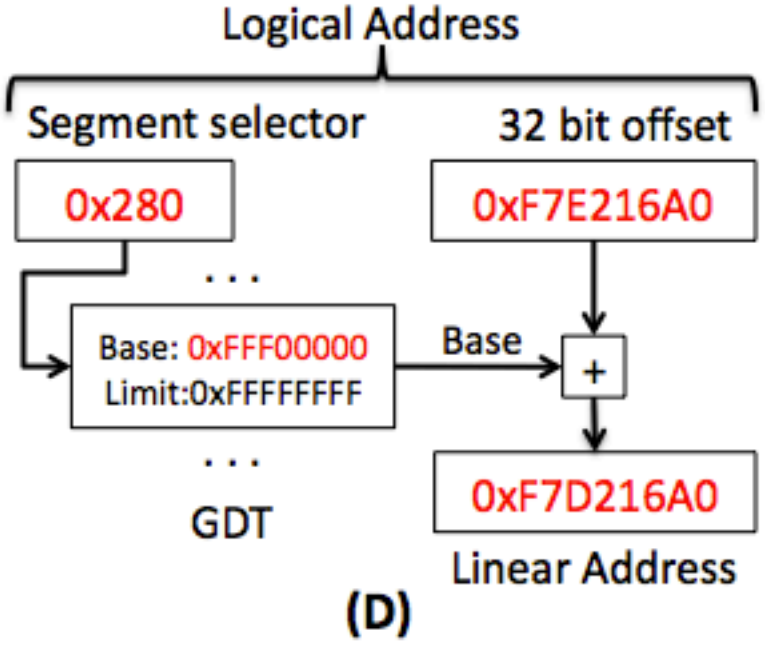
(A)


Logical Address
Segment selector
32 bit offset
0x8
0xF7D216A0
Base: 0
Limit:0xFFFFFFFF
Base
+
GDT
0xF7D216A0
Linear Address

(B)


Logical Address
Segment selector
32 bit offset
0x280
0x8054129A
Base: 0x777E03F7
Limit:0xFFFFFFFF
Base
+
GDT
0xF7D216A0
Linear Address

(C)


Logical Address
Segment selector
32 bit offset
0x280
0xF7E216A0
Base: 0xFFF00000
Limit:0xFFFFFFFF
Base
+
GDT
0xF7D216A0
Linear Address

(D)

Chaff

- As I'm sure you noticed, I threw in some 3rd party software as chaff - Ctrl2Cap, Daemon Tools, Zone Alarm, Trusteer Rapport
- I knew this software would make changes to things like the IDT, SSDT, Inline Hooks, IATs, IRP Major Function hooks, IRP device attachment
- 3rd party software's use of hooking techniques makes integrity verification that much harder

Ctrl2Cap by itself (device attachment)

Type	Name	Value
AttachedD...	\Driver\Kbdclass \Device\KeyboardClass0	Ctrl2cap.SYS (Windows NT Caps-lock Ctrl Swapper/Systems Internals)
AttachedD...	\Driver\Kbdclass \Device\KeyboardClass1	Ctrl2cap.SYS (Windows NT Caps-lock Ctrl Swapper/Systems Internals)

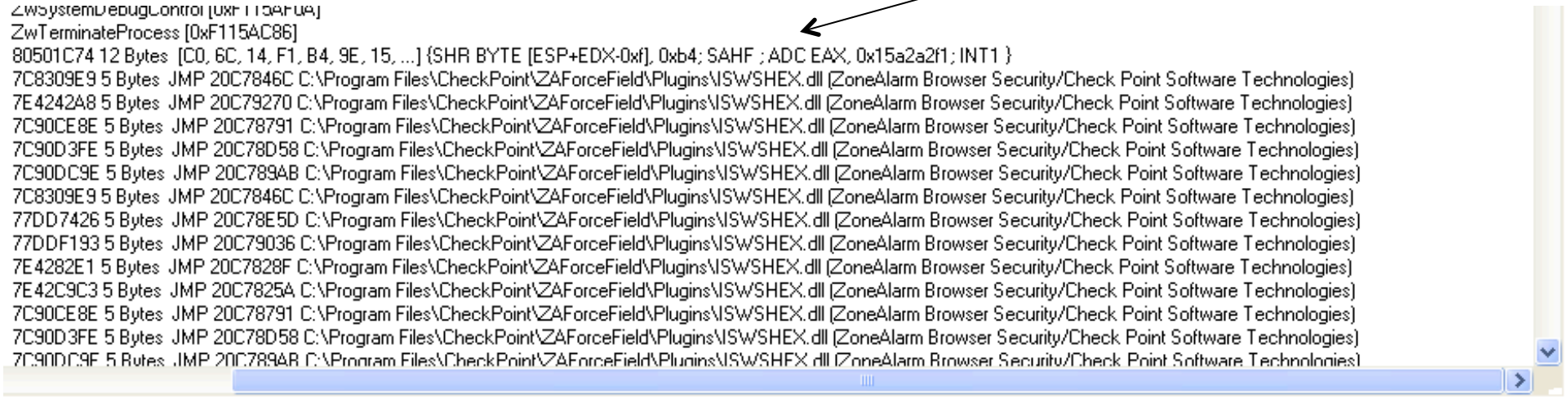
Rapport by itself (SSDT, inline kernel, inline userspace w/dll inject, IRP hook (not shown)

Type	Name	Value
SSDT	\??\C:\Program Files\Trusteer\Rapport\bin\RapportPG.sys (RapportPG/Trusteer Ltd.)	ZwAssignProcessToJobObject [0xF04B0FA2]
SSDT	\??\C:\Program Files\Trusteer\Rapport\bin\RapportPG.sys (RapportPG/Trusteer Ltd.)	ZwCreateFile [0xF04B1A38]
SSDT	\??\C:\Documents and Settings\All Users.WINDOWS\Application Data\Trusteer\Rapport\store\exts\RapportC...	ZwCreateThread [0xF0464890]
SSDT	\??\C:\Documents and Settings\All Users.WINDOWS\Application Data\Trusteer\Rapport\store\exts\RapportC...	ZwDeleteFile [0xF0463A1C]
SSDT	\??\C:\Program Files\Trusteer\Rapport\bin\RapportPG.sys (RapportPG/Trusteer Ltd.)	ZwDeleteKey [0xF04B51AC]
SSDT	\??\C:\Program Files\Trusteer\Rapport\bin\RapportPG.sys (RapportPG/Trusteer Ltd.)	ZwDeleteValueKey [0xF04B51DE]
SSDT	\??\C:\Program Files\Trusteer\Rapport\bin\RapportPG.sys (RapportPG/Trusteer Ltd.)	ZwLoadKey [0xF04B5340]
SSDT	\??\C:\Program Files\Trusteer\Rapport\bin\RapportPG.sys (RapportPG/Trusteer Ltd.)	ZwOpenFile [0xF04B1B0E]
SSDT	\??\C:\Program Files\Trusteer\Rapport\bin\RapportPG.sys (RapportPG/Trusteer Ltd.)	ZwOpenProcess [0xF04B10E6]
SSDT	\??\C:\Program Files\Trusteer\Rapport\bin\RapportPG.sys (RapportPG/Trusteer Ltd.)	ZwOpenThread [0xF04B12D8]
SSDT	\??\C:\Program Files\Trusteer\Rapport\bin\RapportPG.sys (RapportPG/Trusteer Ltd.)	ZwProtectVirtualMemory [0xF04B140A]
SSDT	\??\C:\Program Files\Trusteer\Rapport\bin\RapportPG.sys (RapportPG/Trusteer Ltd.)	ZwQueryValueKey [0xF04B52B6]
SSDT	\??\C:\Program Files\Trusteer\Rapport\bin\RapportPG.sys (RapportPG/Trusteer Ltd.)	ZwRenameKey [0xF04B5220]
SSDT	\??\C:\Program Files\Trusteer\Rapport\bin\RapportPG.sys (RapportPG/Trusteer Ltd.)	ZwReplaceKey [0xF04B5252]
SSDT	\??\C:\Program Files\Trusteer\Rapport\bin\RapportPG.sys (RapportPG/Trusteer Ltd.)	ZwRestoreKey [0xF04B5284]
SSDT	\??\C:\Program Files\Trusteer\Rapport\bin\RapportPG.sys (RapportPG/Trusteer Ltd.)	ZwSetContextThread [0xF04B0F48]
SSDT	\??\C:\Documents and Settings\All Users.WINDOWS\Application Data\Trusteer\Rapport\store\exts\RapportC...	ZwSetInformationFile [0xF0463A90]
SSDT	\??\C:\Documents and Settings\All Users.WINDOWS\Application Data\Trusteer\Rapport\store\exts\RapportC...	ZwSetValueKey [0xF046476C]
SSDT	\??\C:\Program Files\Trusteer\Rapport\bin\RapportPG.sys (RapportPG/Trusteer Ltd.)	ZwSuspendThread [0xF04B0EE4]
SSDT	\??\C:\Documents and Settings\All Users.WINDOWS\Application Data\Trusteer\Rapport\store\exts\RapportC...	ZwTerminateProcess [0xF04639A2]
SSDT	\??\C:\Program Files\Trusteer\Rapport\bin\RapportPG.sys (RapportPG/Trusteer Ltd.)	ZwTerminateThread [0xF04B0E80]
PAGE	ntkrnlpa.exe!ZwQueryValueKey + 349	806188B1 7 Bytes JMP F9FF7B40
.text	C:\Program Files\Trusteer\Rapport\bin\RapportMgmtService.exe[2424] ntdll.dll!KiUserApcDispatcher	7C90E450 5 Bytes JMP 00413D30 C:\Program Files\Trusteer\Rapport\bin\RapportMgmtService.ex...
.text	C:\Program Files\Trusteer\Rapport\bin\RapportMgmtService.exe[2424] kernel32.dll!LoadLibraryExW + C4	7C801BB9 4 Bytes CALL 71A70001
.text	C:\Program Files\Trusteer\Rapport\bin\RapportMgmtService.exe[2424] WS2_32.dll!getaddrinfo	71AB2A6F 5 Bytes JMP 71A10022
.text	C:\Program Files\Trusteer\Rapport\bin\RapportMgmtService.exe[2424] WS2_32.dll!gethostbyname	71AB5355 5 Bytes JMP 71AE0022
.text	C:\Program Files\Trusteer\Rapport\bin\RapportService.exe[2556] ntdll.dll!KiUserApcDispatcher	7C90E450 5 Bytes JMP 0043E9D0 C:\Program Files\Trusteer\Rapport\bin\RapportService.exe (Ra...
.text	C:\Program Files\Trusteer\Rapport\bin\RapportService.exe[2556] kernel32.dll!LoadLibraryExW + C4	7C801BB9 4 Bytes CALL 71A80001
.text	C:\Program Files\Trusteer\Rapport\bin\RapportService.exe[2556] USER32.dll!GetGUIThreadInfo + FB	7E428023 6 Bytes JMP 71AE001E
.text	C:\Program Files\Trusteer\Rapport\bin\RapportService.exe[2556] WS2_32.dll!getaddrinfo	71AB2A6F 5 Bytes JMP 719E0022
.text	C:\Program Files\Trusteer\Rapport\bin\RapportService.exe[2556] WS2_32.dll!gethostbyname	71AB5355 5 Bytes JMP 71A20022

Zone Alarm by itself (ssdt, inline kernel, inline userspace w/ dll injection)

Type	Name	Value
SSDT	\SystemRoot\System32\vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Software Technologies LTD)	ZwConnectPort [0xF1146534]
SSDT	\SystemRoot\System32\vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Software Technologies LTD)	ZwCreateFile [0xF1140782]
SSDT	\SystemRoot\System32\vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Software Technologies LTD)	ZwCreateKey [0xF115F6DC]
SSDT	\SystemRoot\System32\vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Software Technologies LTD)	ZwCreatePort [0xF1146CC0]
SSDT	\SystemRoot\System32\vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Software Technologies LTD)	ZwCreateProcess [0xF1159EB4]
SSDT	\SystemRoot\System32\vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Software Technologies LTD)	ZwCreateProcessEx [0xF115A2A2]
SSDT	\SystemRoot\System32\vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Software Technologies LTD)	ZwCreateSection [0xF1163916]
SSDT	\SystemRoot\System32\vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Software Technologies LTD)	ZwCreateWaitablePort [0xF1146DF6]
SSDT	\SystemRoot\System32\vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Software Technologies LTD)	ZwDeleteFile [0xF1141398]
SSDT	\SystemRoot\System32\vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Software Technologies LTD)	ZwDeleteKey [0xF1160FE4]
SSDT	\SystemRoot\System32\vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Software Technologies LTD)	ZwDeleteValueKey [0xF116093C]
SSDT	\SystemRoot\System32\vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Software Technologies LTD)	ZwDuplicateObject [0xF1158DF0]
SSDT	\SystemRoot\System32\vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Software Technologies LTD)	ZwLoadKey [0xF116193C]
SSDT	\SystemRoot\System32\vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Software Technologies LTD)	ZwLoadKey2 [0xF1161B44]
SSDT	\SystemRoot\System32\vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Software Technologies LTD)	ZwOpenFile [0xF1140FAA]
SSDT	\SystemRoot\System32\vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Software Technologies LTD)	ZwOpenProcess [0xF115C1CE]
SSDT	\SystemRoot\System32\vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Software Technologies LTD)	ZwOpenThread [0xF115BDF8]
SSDT	\SystemRoot\System32\vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Software Technologies LTD)	ZwRenameKey [0xF11628D2]
SSDT	\SystemRoot\System32\vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Software Technologies LTD)	ZwReplaceKey [0xF1162208]
SSDT	\SystemRoot\System32\vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Software Technologies LTD)	ZwRequestWaitReplyPort [0xF11460F4]
SSDT	\SystemRoot\System32\vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Software Technologies LTD)	ZwRestoreKey [0xF11632A4]
SSDT	\SystemRoot\System32\vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Software Technologies LTD)	ZwSecureConnectPort [0xF11467DC]
SSDT	\SystemRoot\System32\vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Software Technologies LTD)	ZwSetInformationFile [0xF114175C]
SSDT	\SystemRoot\System32\vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Software Technologies LTD)	ZwSetSecurityObject [0xF1162E12]
SSDT	\SystemRoot\System32\vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Software Technologies LTD)	ZwSetValueKey [0xF11600C4]
SSDT	\SystemRoot\System32\vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Software Technologies LTD)	ZwSystemDebugControl [0xF115AF0A]
SSDT	\SystemRoot\System32\vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Software Technologies LTD)	ZwTerminateProcess [0xF115AC86]
.text	ntkrnlpa.exe!ZwCallbackReturn + 243C	80501C74 12 Bytes [C0, 6C, 14, F1, B4, 9E, 15, ...] {SHR BYTE [ESP+EDX-0xf], 0xb4; SAHF ; AD(
.text	C:\Program Files\CheckPoint\ZAForceField\IswSvc.exe[192] kernel32.dll!OpenProcess	7C8309E9 5 Bytes JMP 20C7846C C:\Program Files\CheckPoint\ZAForceField\Plugins\ISWSHE>
.text	C:\Program Files\CheckPoint\ZAForceField\IswSvc.exe[192] USER32.dll!DefDlgProcW + 56E	7E4242A8 5 Bytes JMP 20C79270 C:\Program Files\CheckPoint\ZAForceField\Plugins\ISWSHE>
.text	C:\WINDOWS\system32\spoolsv.exe[264] ntdll.dll!NtAccessCheckByType	7C90CE8E 5 Bytes JMP 20C78791 C:\Program Files\CheckPoint\ZAForceField\Plugins\ISWSHE>
.text	C:\WINDOWS\system32\spoolsv.exe[264] ntdll.dll!NtImpersonateClientOfPort	7C90D3FE 5 Bytes JMP 20C78D58 C:\Program Files\CheckPoint\ZAForceField\Plugins\ISWSHE>
.text	C:\WINDOWS\system32\spoolsv.exe[264] ntdll.dll!NtSetInformationProcess	7C90DC9E 5 Bytes JMP 20C789AB C:\Program Files\CheckPoint\ZAForceField\Plugins\ISWSHE>
.text	C:\WINDOWS\system32\spoolsv.exe[264] kernel32.dll!OpenProcess	7C8309E9 5 Bytes JMP 20C7846C C:\Program Files\CheckPoint\ZAForceField\Plugins\ISWSHE>
.text	C:\WINDOWS\system32\spoolsv.exe[264] ADVAPI32.dll!ImpersonateNamedPipeClient	77DD7426 5 Bytes JMP 20C78E5D C:\Program Files\CheckPoint\ZAForceField\Plugins\ISWSHE>
.text	C:\WINDOWS\system32\spoolsv.exe[264] ADVAPI32.dll!SetThreadToken	77DDF193 5 Bytes JMP 20C79036 C:\Program Files\CheckPoint\ZAForceField\Plugins\ISWSHE>
.text	C:\WINDOWS\system32\spoolsv.exe[264] USER32.dll!FindWindowA	7E4282E1 5 Bytes JMP 20C7828F C:\Program Files\CheckPoint\ZAForceField\Plugins\ISWSHE>
.text	C:\WINDOWS\system32\spoolsv.exe[264] USER32.dll!FindWindowW	7E42C9C3 5 Bytes JMP 20C7825A C:\Program Files\CheckPoint\ZAForceField\Plugins\ISWSHE>
.text	C:\WINDOWS\system32\wuauclt.exe[368] ntdll.dll!NtAccessCheckByType	7C90CE8E 5 Bytes JMP 20C78791 C:\Program Files\CheckPoint\ZAForceField\Plugins\ISWSHE>
.text	C:\WINDOWS\system32\wuauclt.exe[368] ntdll.dll!NtImpersonateClientOfPort	7C90D3FE 5 Bytes JMP 20C78D58 C:\Program Files\CheckPoint\ZAForceField\Plugins\ISWSHE>
.text	C:\WINDOWS\system32\wuauclt.exe[368] ntdll.dll!NtSetInformationProcess	7C90DC9E 5 Bytes JMP 20C789AB C:\Program Files\CheckPoint\ZAForceField\Plugins\ISWSHE>

Zone Alarm by itself (showing the entire inline hook)



Zone Alarm by itself 2

Type	Name	Value
IAT	\SystemRoot\system32\DRIVERS\tcpip.sys[NDIS.SYS!NdisCloseAdapter]	[F114BCBA] \SystemRoot\System32\vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Softw
IAT	\SystemRoot\system32\DRIVERS\tcpip.sys[NDIS.SYS!NdisOpenAdapter]	[F114B4C8] \SystemRoot\System32\vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Softw
IAT	\SystemRoot\system32\DRIVERS\tcpip.sys[NDIS.SYS!NdisRegisterProtocol]	[F114B672] \SystemRoot\System32\vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Softw
IAT	\SystemRoot\system32\DRIVERS\wanarp.sys[NDIS.SYS!NdisDeregisterProtocol]	[F1149C2A] \SystemRoot\System32\vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Softw
IAT	\SystemRoot\system32\DRIVERS\wanarp.sys[NDIS.SYS!NdisRegisterProtocol]	[F114B672] \SystemRoot\System32\vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Softw
IAT	\SystemRoot\system32\DRIVERS\wanarp.sys[NDIS.SYS!NdisOpenAdapter]	[F114B4C8] \SystemRoot\System32\vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Softw
IAT	\SystemRoot\system32\DRIVERS\wanarp.sys[NDIS.SYS!NdisCloseAdapter]	[F114BCBA] \SystemRoot\System32\vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Softw
IAT	\SystemRoot\system32\DRIVERS\ndisuio.sys[NDIS.SYS!NdisRegisterProtocol]	[F114B672] \SystemRoot\System32\vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Softw
IAT	\SystemRoot\system32\DRIVERS\ndisuio.sys[NDIS.SYS!NdisDeregisterProtocol]	[F1149C2A] \SystemRoot\System32\vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Softw
IAT	\SystemRoot\system32\DRIVERS\ndisuio.sys[NDIS.SYS!NdisCloseAdapter]	[F114BCBA] \SystemRoot\System32\vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Softw
IAT	\SystemRoot\system32\DRIVERS\ndisuio.sys[NDIS.SYS!NdisOpenAdapter]	[F114B4C8] \SystemRoot\System32\vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Softw
IAT	C:\WINDOWS\system32\spoolsv.exe[264] @ C:\WINDOWS\system32\USER32.dll [KERNEL32.dll!LoadLibrar...	[20C7835C] C:\Program Files\CheckPoint\ZAForceField\Plugins\ISWSHEX.dll (ZoneAlarm Browser
IAT	C:\WINDOWS\system32\wuauclt.exe[368] @ C:\WINDOWS\system32\USER32.dll [KERNEL32.dll!LoadLibrar...	[20C7835C] C:\Program Files\CheckPoint\ZAForceField\Plugins\ISWSHEX.dll (ZoneAlarm Browser
IAT	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe[492] @ C:\WINDOWS\system32\USER32.dll [KERNEL...	[20C7835C] C:\Program Files\CheckPoint\ZAForceField\Plugins\ISWSHEX.dll (ZoneAlarm Browser
IAT	C:\WINDOWS\system32\winlogon.exe[700] @ C:\WINDOWS\system32\USER32.dll [KERNEL32.dll!LoadLibra...	[20C7835C] C:\Program Files\CheckPoint\ZAForceField\Plugins\ISWSHEX.dll (ZoneAlarm Browser
IAT	C:\WINDOWS\system32\services.exe[744] @ C:\WINDOWS\system32\USER32.dll [KERNEL32.dll!LoadLibrar...	[20C7835C] C:\Program Files\CheckPoint\ZAForceField\Plugins\ISWSHEX.dll (ZoneAlarm Browser
IAT	C:\WINDOWS\system32\lsass.exe[756] @ C:\WINDOWS\system32\USER32.dll [KERNEL32.dll!LoadLibraryE...	[20C7835C] C:\Program Files\CheckPoint\ZAForceField\Plugins\ISWSHEX.dll (ZoneAlarm Browser
IAT	C:\Program Files\VMware\VMware Tools\vmacthlp.exe[904] @ C:\WINDOWS\system32\USER32.dll [KERNE...	[20C7835C] C:\Program Files\CheckPoint\ZAForceField\Plugins\ISWSHEX.dll (ZoneAlarm Browser
IAT	C:\WINDOWS\system32\svchost.exe[928] @ C:\WINDOWS\system32\USER32.dll [KERNEL32.dll!LoadLibrar...	[20C7835C] C:\Program Files\CheckPoint\ZAForceField\Plugins\ISWSHEX.dll (ZoneAlarm Browser
IAT	C:\WINDOWS\system32\wbem\wmiprvse.exe[948] @ C:\WINDOWS\system32\USER32.dll [KERNEL32.dll!Lo...	[20C7835C] C:\Program Files\CheckPoint\ZAForceField\Plugins\ISWSHEX.dll (ZoneAlarm Browser
IAT	C:\WINDOWS\system32\svchost.exe[1008] @ C:\WINDOWS\system32\USER32.dll [KERNEL32.dll!LoadLibr...	[20C7835C] C:\Program Files\CheckPoint\ZAForceField\Plugins\ISWSHEX.dll (ZoneAlarm Browser
IAT	C:\Program Files\VMware\VMware Tools\VMwareTray.exe[1088] @ C:\WINDOWS\system32\USER32.dll [KE...	[20C7835C] C:\Program Files\CheckPoint\ZAForceField\Plugins\ISWSHEX.dll (ZoneAlarm Browser
IAT	C:\Program Files\VMware\VMware Tools\VMwareUser.exe[1096] @ C:\WINDOWS\system32\USER32.dll [KE...	[20C7835C] C:\Program Files\CheckPoint\ZAForceField\Plugins\ISWSHEX.dll (ZoneAlarm Browser
IAT	C:\WINDOWS\System32\svchost.exe[1120] @ C:\WINDOWS\system32\USER32.dll [KERNEL32.dll!LoadLibr...	[20C7835C] C:\Program Files\CheckPoint\ZAForceField\Plugins\ISWSHEX.dll (ZoneAlarm Browser
IAT	C:\WINDOWS\system32\svchost.exe[1200] @ C:\WINDOWS\system32\USER32.dll [KERNEL32.dll!LoadLibr...	[20C7835C] C:\Program Files\CheckPoint\ZAForceField\Plugins\ISWSHEX.dll (ZoneAlarm Browser
IAT	C:\WINDOWS\system32\ctfmon.exe[1232] @ C:\WINDOWS\system32\USER32.dll [KERNEL32.dll!LoadLibrar...	[20C7835C] C:\Program Files\CheckPoint\ZAForceField\Plugins\ISWSHEX.dll (ZoneAlarm Browser
IAT	C:\WINDOWS\system32\svchost.exe[1280] @ C:\WINDOWS\system32\USER32.dll [KERNEL32.dll!LoadLibr...	[20C7835C] C:\Program Files\CheckPoint\ZAForceField\Plugins\ISWSHEX.dll (ZoneAlarm Browser
IAT	C:\Program Files\VMware\VMware Tools\VMUpgradeHelper.exe[1336] @ C:\WINDOWS\system32\USER32.d...	[20C7835C] C:\Program Files\CheckPoint\ZAForceField\Plugins\ISWSHEX.dll (ZoneAlarm Browser
IAT	C:\WINDOWS\system32\svchost.exe[1732] @ C:\WINDOWS\system32\USER32.dll [KERNEL32.dll!LoadLibr...	[20C7835C] C:\Program Files\CheckPoint\ZAForceField\Plugins\ISWSHEX.dll (ZoneAlarm Browser
IAT	C:\Program Files\MySQL\MySQL Server 5.1\bin\mysqld.exe[1816] @ C:\WINDOWS\system32\USER32.dll [K...	[20C7835C] C:\Program Files\CheckPoint\ZAForceField\Plugins\ISWSHEX.dll (ZoneAlarm Browser
IAT	C:\WINDOWS\Explorer.EXE[1916] @ C:\WINDOWS\system32\USER32.dll [KERNEL32.dll!LoadLibraryExW]	[20C7835C] C:\Program Files\CheckPoint\ZAForceField\Plugins\ISWSHEX.dll (ZoneAlarm Browser
IAT	C:\WINDOWS\System32\alg.exe[2312] @ C:\WINDOWS\system32\USER32.dll [KERNEL32.dll!LoadLibraryEx...	[20C7835C] C:\Program Files\CheckPoint\ZAForceField\Plugins\ISWSHEX.dll (ZoneAlarm Browser
IAT	C:\WINDOWS\system32\wscntfy.exe[2364] @ C:\WINDOWS\system32\USER32.dll [KERNEL32.dll!LoadLibra...	[20C7835C] C:\Program Files\CheckPoint\ZAForceField\Plugins\ISWSHEX.dll (ZoneAlarm Browser
IAT	C:\Documents and Settings\user\Desktop\20t0r147.exe[4040] @ C:\WINDOWS\system32\USER32.dll [KERN...	[20C7835C] C:\Program Files\CheckPoint\ZAForceField\Plugins\ISWSHEX.dll (ZoneAlarm Browser
Device	\Driver\Tcpip \Device\Ip	vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Software Technologies LTD)
Device	\Driver\Tcpip \Device\Tcp	vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Software Technologies LTD)
Device	\Driver\Tcpip \Device\Udp	vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Software Technologies LTD)
Device	\Driver\Tcpip \Device\RawIp	vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Software Technologies LTD)
Device	\Driver\Tcpip \Device\IPMULTICAST	vsdatant.sys (ZoneAlarm Firewalling Driver/Check Point Software Technologies LTD)
AttachedD...	\FileSystem\Fastfat \Fat	fltMgr.sys (Microsoft Filesystem Filter Manager/Microsoft Corporation)

Daemon Tools Lite w/ SPTD

(SPTD is responsible for most hooks)

(SSDT, IDT, inline kernel, missing (possibly hidden) files, IAT, IRP MJ table hooks)

Type	Name	Value
SSDT	sptd.sys	ZwCreateKey [0xF97C89E0]
SSDT	sptd.sys	ZwEnumerateKey [0xF97FD0EE]
SSDT	sptd.sys	ZwEnumerateValueKey [0xF97FD47C]
SSDT	sptd.sys	ZwOpenKey [0xF97C89C0]
SSDT	sptd.sys	ZwQueryKey [0xF97FD554]
SSDT	sptd.sys	ZwQueryValueKey [0xF97FD3D4]
SSDT	sptd.sys	ZwSetValueKey [0xF97FD5E6]
INT 0x62	?	819DBCB8
INT 0x82	?	819DBCB8
.text	sptd.sys	F978C000 32 Bytes [98, 22, 6D, 80, 20, 27, 6D, ...]
.text	sptd.sys	F978C024 4 Bytes [74, EF, 77, F9] {JZ 0xfffffffffffffff1; JA 0xfffffffffffffffd}
.text	sptd.sys	F978C02C 116 Bytes [5E, 36, 5A, 80, 9C, AD, 52, ...]
.text	sptd.sys	F978C0A1 67 Bytes [5C, 53, 80, E4, 51, 50, 80, ...]
.text	sptd.sys	F978C0E5 239 Bytes [4F, 54, 80, 50, 6C, 53, 80, ...]
.text	...	
.sptd2	C:\WINDOWS\system32\drivers\sptd.sys	entry point in ".sptd2" section [0xF98660AD]
?	C:\WINDOWS\system32\drivers\sptd.sys	The process cannot access the file because it is being used by another process.
?	System32\Drivers\ae3rgovd.SYS	The system cannot find the path specified. !
IAT	\WINDOWS\system32\DRIVERS\PCIIDEX.SYS[HAL.dll!WRITE_PORT_ULONG]	[F978E22E] sptd.sys
IAT	\WINDOWS\system32\DRIVERS\PCIIDEX.SYS[HAL.dll!READ_PORT_UCHAR]	[F978D71C] sptd.sys
IAT	\WINDOWS\system32\DRIVERS\PCIIDEX.SYS[HAL.dll!WRITE_PORT_UCHAR]	[F978DF0E] sptd.sys
IAT	atapi.sys[HAL.dll!READ_PORT_UCHAR]	[F978D71C] sptd.sys
IAT	atapi.sys[HAL.dll!READ_PORT_BUFFER_USHORT]	[F978D910] sptd.sys
IAT	atapi.sys[HAL.dll!READ_PORT_USHORT]	[F978D852] sptd.sys
IAT	atapi.sys[HAL.dll!WRITE_PORT_BUFFER_USHORT]	[F978E0EC] sptd.sys
IAT	atapi.sys[HAL.dll!WRITE_PORT_UCHAR]	[F978DF0E] sptd.sys
IAT	\SystemRoot\System32\DRIVERS\i8042prt.sys[HAL.dll!READ_PORT_UCHAR]	[F97A1CE8] sptd.sys
Device	\FileSystem\Ntfs \Ntfs	819A81E8
Device	\Driver\NetBT \Device\NetBT_Tcpip_{19AF6820-E1BC-4DD4-AB6E-BDE3E1F9DE...	817AB1E8
Device	\Driver\Cdrom \Device\CdRom0	819A91E8
Device	\Driver\atapi \Device\Ide\IdeDeviceP0T0L0-3	[F96E0B40] atapi.sys[unknown section] {MOV EDX, [ESP+0x8]; LEA ECX, [ESP+0x4]; PUSH EAX; MOV EAX, ESP; PUSH EA
Device	\Driver\atapi \Device\Ide\IdePort0	[F96E0B40] atapi.sys[unknown section] {MOV EDX, [ESP+0x8]; LEA ECX, [ESP+0x4]; PUSH EAX; MOV EAX, ESP; PUSH EA
Device	\Driver\atapi \Device\Ide\IdePort1	[F96E0B40] atapi.sys[unknown section] {MOV EDX, [ESP+0x8]; LEA ECX, [ESP+0x4]; PUSH EAX; MOV EAX, ESP; PUSH EA
Device	\Driver\atapi \Device\Ide\IdeDeviceP1T0L0-e	[F96E0B40] atapi.sys[unknown section] {MOV EDX, [ESP+0x8]; LEA ECX, [ESP+0x4]; PUSH EAX; MOV EAX, ESP; PUSH EA
Device	\Driver\Cdrom \Device\CdRom3	819A91E8
Device	\Driver\NetBT \Device\NetBt_Wins_Export	817AB1E8
Device	\Driver\NetBT \Device\NetbiosSmb	817AB1E8
Device	\Driver\PCI_PNP6892 \Device\0000007a	sptd.sys
Device	\Driver\PCI_PNP6892 \Device\0000007a	sptd.sys
Device	\FileSystem\MRxSmb \Device\LanmanDatagramReceiver	815251E8
Device	\FileSystem\MRxSmb \Device\LanmanRedirector	815251E8

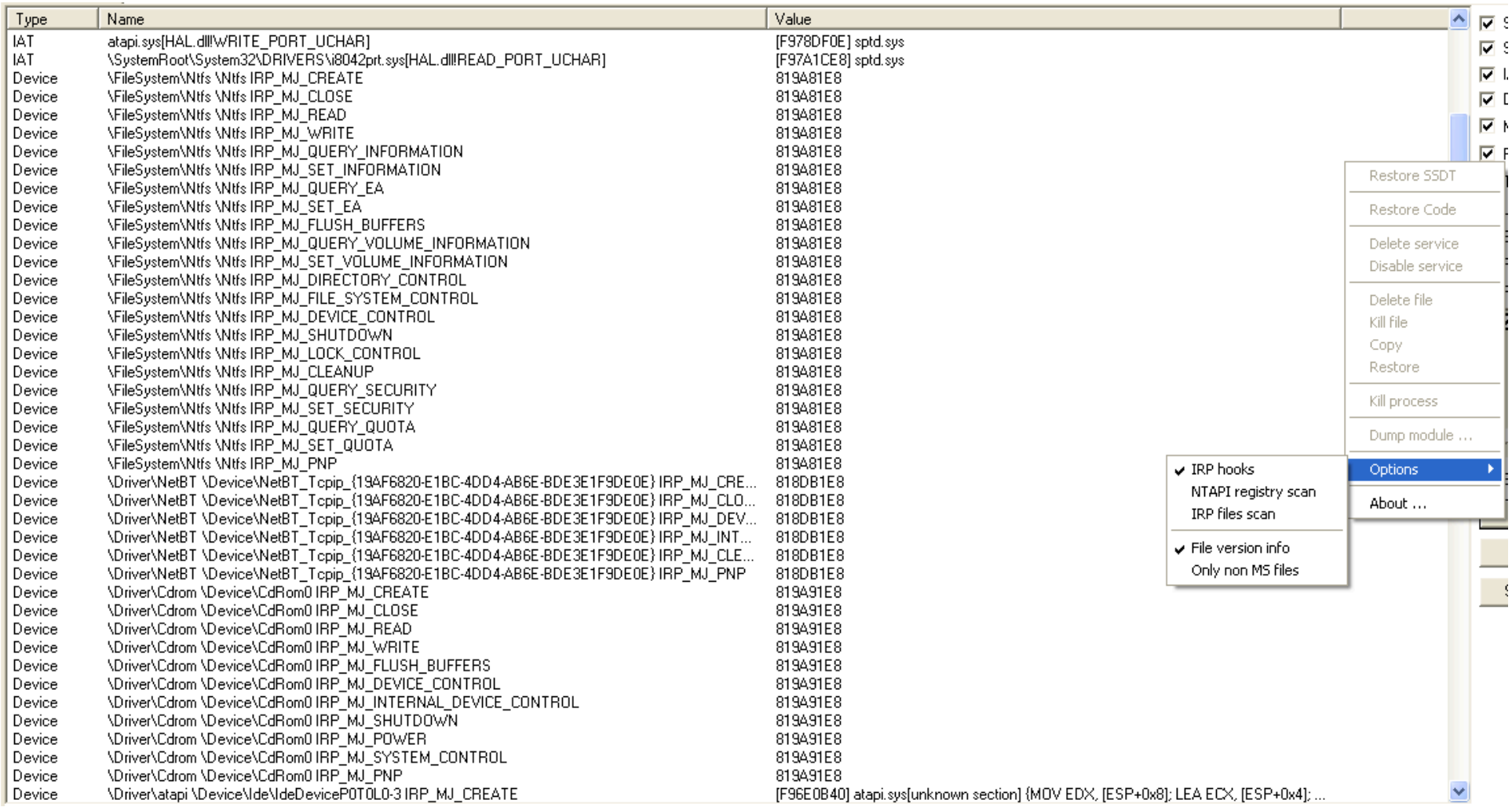
Daemon Tools Lite w/ SPTD

(SPTD is responsible for most hooks) (hidden registry entries)

Device	\Driver\atapi \Device\Ide\IdeDeviceP0T0L0-3	[F96E0B40] atapi.sys[unknown section] {MOV EDX, [ESP+0x8]; LEA ECX, [ESP+0x4]; PUSH EAX; MOV EAX, ESP; PUSH E
Device	\Driver\atapi \Device\Ide\IdePort0	[F96E0B40] atapi.sys[unknown section] {MOV EDX, [ESP+0x8]; LEA ECX, [ESP+0x4]; PUSH EAX; MOV EAX, ESP; PUSH E
Device	\Driver\atapi \Device\Ide\IdePort1	[F96E0B40] atapi.sys[unknown section] {MOV EDX, [ESP+0x8]; LEA ECX, [ESP+0x4]; PUSH EAX; MOV EAX, ESP; PUSH E
Device	\Driver\atapi \Device\Ide\IdeDeviceP1T0L0-e	[F96E0B40] atapi.sys[unknown section] {MOV EDX, [ESP+0x8]; LEA ECX, [ESP+0x4]; PUSH EAX; MOV EAX, ESP; PUSH E
Device	\Driver\Cdrom \Device\CdRom3	819A91E8
Device	\Driver\NetBT \Device\NetBt_Wins_Export	817AB1E8
Device	\Driver\NetBT \Device\NetbiosSmb	817AB1E8
Device	\Driver\PCI_PNP6892 \Device\0000007a	sptd.sys
Device	\Driver\PCI_PNP6892 \Device\0000007a	sptd.sys
Device	\FileSystem\MRxSmb \Device\LanmanDatagramReceiver	815251E8
Device	\FileSystem\MRxSmb \Device\LanmanRedirector	815251E8
Device	\Driver\ae3rgovd \Device\Scsi\ae3rgovd1Port2Path0Target0Lun0	818EE1E8
Device	\Driver\ae3rgovd \Device\Scsi\ae3rgovd1	818EE1E8
Device	\FileSystem\Cdfs \Cdfs	818C01E8
Reg	HKLM\SYSTEM\CurrentControlSet\Services\sptd\Cfg@s1	771343423
Reg	HKLM\SYSTEM\CurrentControlSet\Services\sptd\Cfg@s2	285507792
Reg	HKLM\SYSTEM\CurrentControlSet\Services\sptd\Cfg@h0	1
Reg	HKLM\SYSTEM\CurrentControlSet\Services\sptd\Cfg\14919EA49A8F3B4AA3CF105...	
Reg	HKLM\SYSTEM\CurrentControlSet\Services\sptd\Cfg\14919EA49A8F3B4AA3CF105...	C:\Program Files\DAEMON Tools Lite\
Reg	HKLM\SYSTEM\CurrentControlSet\Services\sptd\Cfg\14919EA49A8F3B4AA3CF105...	0x00 0x00 0x00 0x00 ...
Reg	HKLM\SYSTEM\CurrentControlSet\Services\sptd\Cfg\14919EA49A8F3B4AA3CF105...	0
Reg	HKLM\SYSTEM\CurrentControlSet\Services\sptd\Cfg\14919EA49A8F3B4AA3CF105...	0xAB 0x04 0x25 0x35 ...
Reg	HKLM\SYSTEM\CurrentControlSet\Services\sptd\Cfg\14919EA49A8F3B4AA3CF105...	
Reg	HKLM\SYSTEM\CurrentControlSet\Services\sptd\Cfg\14919EA49A8F3B4AA3CF105...	0xA0 0x02 0x00 0x00 ...
Reg	HKLM\SYSTEM\CurrentControlSet\Services\sptd\Cfg\14919EA49A8F3B4AA3CF105...	0x27 0x19 0x4D 0xE8 ...
Reg	HKLM\SYSTEM\CurrentControlSet\Services\sptd\Cfg\14919EA49A8F3B4AA3CF105...	
Reg	HKLM\SYSTEM\CurrentControlSet\Services\sptd\Cfg\14919EA49A8F3B4AA3CF105...	0x6F 0x26 0x1E 0x60 ...
Reg	HKLM\SYSTEM\ControlSet002\Services\sptd\Cfg\14919EA49A8F3B4AA3CF1058D...	
Reg	HKLM\SYSTEM\ControlSet002\Services\sptd\Cfg\14919EA49A8F3B4AA3CF1058D...	C:\Program Files\DAEMON Tools Lite\
Reg	HKLM\SYSTEM\ControlSet002\Services\sptd\Cfg\14919EA49A8F3B4AA3CF1058D...	0x00 0x00 0x00 0x00 ...

Daemon Tools Lite w/ SPTD

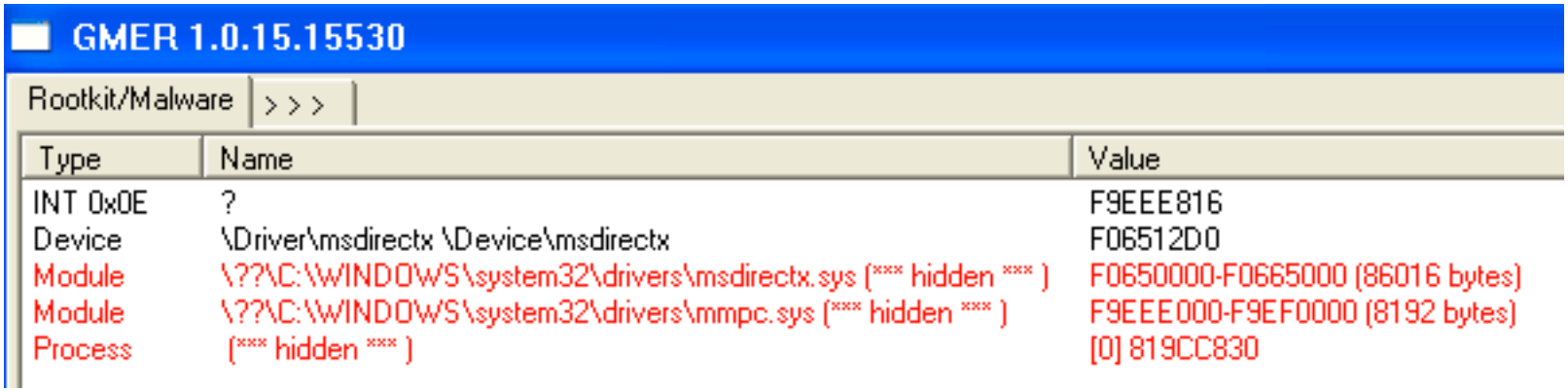
(SPTD is responsible for most hooks) (IAT, IRP MJ table hooks)



Type	Name	Value
IAT	atapi.sys[HAL.dll!WRITE_PORT_UCHAR]	[F978DF0E] sptd.sys
IAT	\SystemRoot\System32\DRIVERS\i8042prt.sys[HAL.dll!READ_PORT_UCHAR]	[F97A1CE8] sptd.sys
Device	\FileSystem\Ntfs \Ntfs IRP_MJ_CREATE	819A81E8
Device	\FileSystem\Ntfs \Ntfs IRP_MJ_CLOSE	819A81E8
Device	\FileSystem\Ntfs \Ntfs IRP_MJ_READ	819A81E8
Device	\FileSystem\Ntfs \Ntfs IRP_MJ_WRITE	819A81E8
Device	\FileSystem\Ntfs \Ntfs IRP_MJ_QUERY_INFORMATION	819A81E8
Device	\FileSystem\Ntfs \Ntfs IRP_MJ_SET_INFORMATION	819A81E8
Device	\FileSystem\Ntfs \Ntfs IRP_MJ_QUERY_EA	819A81E8
Device	\FileSystem\Ntfs \Ntfs IRP_MJ_SET_EA	819A81E8
Device	\FileSystem\Ntfs \Ntfs IRP_MJ_FLUSH_BUFFERS	819A81E8
Device	\FileSystem\Ntfs \Ntfs IRP_MJ_QUERY_VOLUME_INFORMATION	819A81E8
Device	\FileSystem\Ntfs \Ntfs IRP_MJ_SET_VOLUME_INFORMATION	819A81E8
Device	\FileSystem\Ntfs \Ntfs IRP_MJ_DIRECTORY_CONTROL	819A81E8
Device	\FileSystem\Ntfs \Ntfs IRP_MJ_FILE_SYSTEM_CONTROL	819A81E8
Device	\FileSystem\Ntfs \Ntfs IRP_MJ_DEVICE_CONTROL	819A81E8
Device	\FileSystem\Ntfs \Ntfs IRP_MJ_SHUTDOWN	819A81E8
Device	\FileSystem\Ntfs \Ntfs IRP_MJ_LOCK_CONTROL	819A81E8
Device	\FileSystem\Ntfs \Ntfs IRP_MJ_CLEANUP	819A81E8
Device	\FileSystem\Ntfs \Ntfs IRP_MJ_QUERY_SECURITY	819A81E8
Device	\FileSystem\Ntfs \Ntfs IRP_MJ_SET_SECURITY	819A81E8
Device	\FileSystem\Ntfs \Ntfs IRP_MJ_QUERY_QUOTA	819A81E8
Device	\FileSystem\Ntfs \Ntfs IRP_MJ_SET_QUOTA	819A81E8
Device	\FileSystem\Ntfs \Ntfs IRP_MJ_PNP	819A81E8
Device	\Driver\NetBT \Device\NetBT_Tcpip_{19AF6820-E1BC-4DD4-AB6E-BDE3E1F9DE0E} IRP_MJ_CRE...	818DB1E8
Device	\Driver\NetBT \Device\NetBT_Tcpip_{19AF6820-E1BC-4DD4-AB6E-BDE3E1F9DE0E} IRP_MJ_CLO...	818DB1E8
Device	\Driver\NetBT \Device\NetBT_Tcpip_{19AF6820-E1BC-4DD4-AB6E-BDE3E1F9DE0E} IRP_MJ_DEV...	818DB1E8
Device	\Driver\NetBT \Device\NetBT_Tcpip_{19AF6820-E1BC-4DD4-AB6E-BDE3E1F9DE0E} IRP_MJ_INT...	818DB1E8
Device	\Driver\NetBT \Device\NetBT_Tcpip_{19AF6820-E1BC-4DD4-AB6E-BDE3E1F9DE0E} IRP_MJ_CLE...	818DB1E8
Device	\Driver\NetBT \Device\NetBT_Tcpip_{19AF6820-E1BC-4DD4-AB6E-BDE3E1F9DE0E} IRP_MJ_PNP	818DB1E8
Device	\Driver\Cdrom \Device\CdRom0 IRP_MJ_CREATE	819A91E8
Device	\Driver\Cdrom \Device\CdRom0 IRP_MJ_CLOSE	819A91E8
Device	\Driver\Cdrom \Device\CdRom0 IRP_MJ_READ	819A91E8
Device	\Driver\Cdrom \Device\CdRom0 IRP_MJ_WRITE	819A91E8
Device	\Driver\Cdrom \Device\CdRom0 IRP_MJ_FLUSH_BUFFERS	819A91E8
Device	\Driver\Cdrom \Device\CdRom0 IRP_MJ_DEVICE_CONTROL	819A91E8
Device	\Driver\Cdrom \Device\CdRom0 IRP_MJ_INTERNAL_DEVICE_CONTROL	819A91E8
Device	\Driver\Cdrom \Device\CdRom0 IRP_MJ_SHUTDOWN	819A91E8
Device	\Driver\Cdrom \Device\CdRom0 IRP_MJ_POWER	819A91E8
Device	\Driver\Cdrom \Device\CdRom0 IRP_MJ_SYSTEM_CONTROL	819A91E8
Device	\Driver\Cdrom \Device\CdRom0 IRP_MJ_PNP	819A91E8
Device	\Driver\atapi \Device\Ide\IdeDeviceP0T0L0-3 IRP_MJ_CREATE	[F96E0B40] atapi.sys[unknown section] {MOV EDX, [ESP+0x8]; LEA ECX, [ESP+0x4]; ...

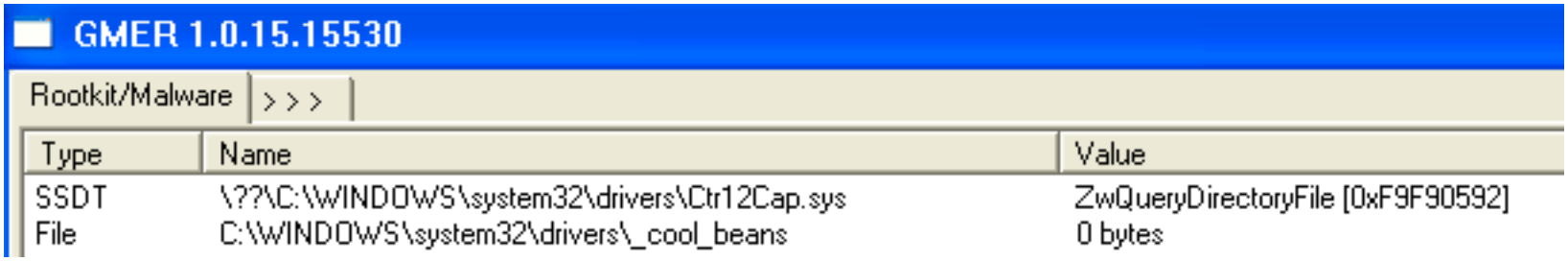
Shadow Walker + FUTo

(shadow walker not relevant without fu/futo because it's hardcoded to search for msdirectx.sys
FUTo set to hide msdirectx.sys, mmpc.sys, and pid 4 (System))



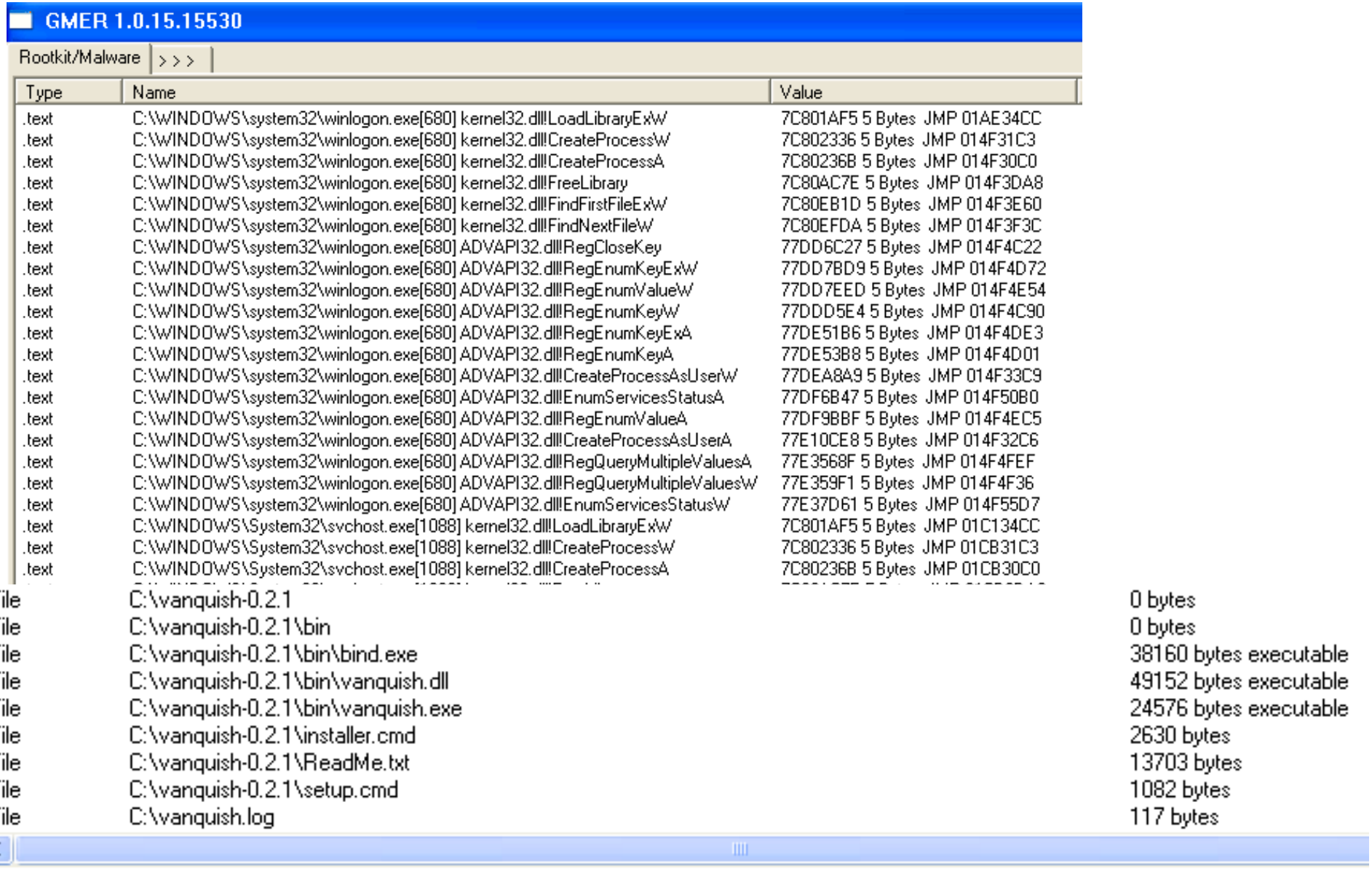
Basic Hook Hide File only

(SSDT hook, had to make a file with _cool_ in the name to hide)



Vanquish only 1

(inline hooks, hidden DLLs, hidden service, hidden registry keys, hidden files)



Vanquish only 2

(inline hooks, hidden DLLs, hidden service, hidden registry keys, hidden files)

GMER 1.0.15.15530

Rootkit/Malware > > >

Type	Name	Value
.text	C:\WINDOWS\Explorer.EXE[1836] ADVAPI32.dll!RegQueryMultipleValuesW	77E359F1 5 Bytes JMP 01844F36
.text	C:\WINDOWS\Explorer.EXE[1836] ADVAPI32.dll!EnumServicesStatusW	77E37D61 5 Bytes JMP 018455D7
Library	(*** hidden ***) @ C:\Program Files\VMware\VMware Tools\VMwareTray.exe [380]	0x01AE0000
Library	(*** hidden ***) @ C:\Program Files\VMware\VMware Tools\VMwareTray.exe [380]	0x00C70000
Library	(*** hidden ***) @ C:\Program Files\VMware\VMware Tools\VMwareTray.exe [380]	0x00CA0000
Library	(*** hidden ***) @ C:\Program Files\VMware\VMware Tools\VMwareUser.exe [388]	0x01AE0000
Library	(*** hidden ***) @ C:\Program Files\VMware\VMware Tools\VMwareUser.exe [388]	0x003F0000
Library	(*** hidden ***) @ C:\Program Files\VMware\VMware Tools\VMwareUser.exe [388]	0x00B20000
Library	(*** hidden ***) @ C:\WINDOWS\system32\ctfmon.exe [404]	0x01AE0000
Library	(*** hidden ***) @ C:\WINDOWS\system32\ctfmon.exe [404]	0x003A0000
Library	(*** hidden ***) @ C:\WINDOWS\system32\ctfmon.exe [404]	0x003F0000
Library	(*** hidden ***) @ C:\WINDOWS\system32\winlogon.exe [680]	0x01520000
Library	(*** hidden ***) @ C:\WINDOWS\system32\winlogon.exe [680]	0x01550000
Library	(*** hidden ***) @ C:\WINDOWS\system32\winlogon.exe [680]	0x00BF0000
Library	(*** hidden ***) @ C:\WINDOWS\system32\svchost.exe [908]	0x01AE0000
Library	(*** hidden ***) @ C:\WINDOWS\system32\svchost.exe [908]	0x00A90000
Library	(*** hidden ***) @ C:\WINDOWS\system32\svchost.exe [908]	0x00AC0000
Library	(*** hidden ***) @ C:\Documents and Settings\user\Desktop\20t0r147.exe [1092]	0x01AE0000
Library	(*** hidden ***) @ C:\Documents and Settings\user\Desktop\20t0r147.exe [1092]	0x00380000
Library	(*** hidden ***) @ C:\Documents and Settings\user\Desktop\20t0r147.exe [1092]	0x003B0000
Library	(*** hidden ***) @ C:\WINDOWS\system32\cmd.exe [1228]	0x01AE0000
Library	(*** hidden ***) @ C:\WINDOWS\system32\cmd.exe [1228]	0x00910000
Library	(*** hidden ***) @ C:\WINDOWS\system32\cmd.exe [1228]	0x00940000
Library	(*** hidden ***) @ C:\WINDOWS\Explorer.EXE [1836]	0x01AE0000
Library	(*** hidden ***) @ C:\WINDOWS\Explorer.EXE [1836]	0x01810000
Library	(*** hidden ***) @ C:\WINDOWS\Explorer.EXE [1836]	0x01840000
Service	C:\WINDOWS\vanquish.exe (*** hidden ***)	[AUTO] vanquish
Reg	HKLM\SYSTEM\CurrentControlSet\Services\vanquish	
Reg	HKLM\SYSTEM\CurrentControlSet\Services\vanquish@Type	272
Reg	HKLM\SYSTEM\CurrentControlSet\Services\vanquish@Start	2
Reg	HKLM\SYSTEM\CurrentControlSet\Services\vanquish@ErrorControl	1
Reg	HKLM\SYSTEM\CurrentControlSet\Services\vanquish@ImagePath	"C:\WINDOWS\vanquish.exe"
Reg	HKLM\SYSTEM\CurrentControlSet\Services\vanquish@DisplayName	Vanquish Autoloader v0.2.1
Reg	HKLM\SYSTEM\CurrentControlSet\Services\vanquish@ObjectName	LocalSystem

Hacker Defender only 1

(inline hooks, hidden files, process, services, network port 4500 (not shown))

Rootkit/Malware | >>>

Type	Name	Value
?	C:\hxdef100r\hxdefdrv.sys	The system cannot find the file specifi...
.text	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe[192] ntdll.dll!NtCreateFile	7C90D0AE 1 Byte [E9]
.text	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe[192] ntdll.dll!NtCreateFile	7C90D0AE 5 Bytes JMP 7FFA47D8
.text	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe[192] ntdll.dll!NtDeviceIoControlFile	7C90D27E 5 Bytes JMP 7FFA444E
.text	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe[192] ntdll.dll!NtEnumerateKey	7C90D2CE 5 Bytes JMP 7FFA3CCC
.text	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe[192] ntdll.dll!NtEnumerateValueKey	7C90D2EE 5 Bytes JMP 7FFA3DC1
.text	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe[192] ntdll.dll!NtOpenFile	7C90D59E 5 Bytes JMP 7FFA4861
.text	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe[192] ntdll.dll!NtOpenProcess	7C90D5FE 5 Bytes JMP 7FFA476D
.text	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe[192] ntdll.dll!NtQueryDirectoryFile	7C90D76E 5 Bytes JMP 7FFA3BA0
.text	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe[192] ntdll.dll!NtQuerySystemInformation	7C90D92E 5 Bytes JMP 7FFA3A0E
.text	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe[192] ntdll.dll!NtQueryVolumeInformationFile	7C90D98E 5 Bytes JMP 7FFA437E
.text	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe[192] ntdll.dll!NtReadVirtualMemory	7C90D9FE 5 Bytes JMP 7FFA3E28
.text	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe[192] ntdll.dll!NtResumeThread	7C90DB3E 5 Bytes JMP 7FFA3C71
.text	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe[192] ntdll.dll!NtVdmControl	7C90DF1E 5 Bytes JMP 7FFA3C02
.text	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe[192] ntdll.dll!LdrLoadDll	7C9163C3 5 Bytes JMP 7FFA4028
.text	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe[192] kernel32.dll!ReadFile	7C801812 5 Bytes JMP 7FFA3924
.text	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe[192] ADVAPI32.dll!EnumServicesStatusA	77DF6B47 5 Bytes JMP 7FFA4206
.text	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe[192] ADVAPI32.dll!EnumServicesStatusExW	77E369B8 5 Bytes JMP 7FFA426C
.text	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe[192] ADVAPI32.dll!EnumServiceGroupW	77E36A89 5 Bytes JMP 7FFA419D
.text	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe[192] ADVAPI32.dll!EnumServicesStatusExA	77E36C2F 5 Bytes JMP 7FFA42D8
.text	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe[192] WS2_32.dll!WSARecv	71AB4CB5 5 Bytes JMP 7FFA40CA
.text	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe[192] WS2_32.dll!recv	71AB676F 5 Bytes JMP 7FFA406A
.text	C:\WINDOWS\System32\alg.exe[260] ntdll.dll!NtCreateFile	7C90D0AE 1 Byte [E9]
.text	C:\WINDOWS\System32\alg.exe[260] ntdll.dll!NtCreateFile	7C90D0AE 5 Bytes JMP 7FFA47D8
.text	C:\WINDOWS\System32\alg.exe[260] ntdll.dll!NtDeviceIoControlFile	7C90D27E 5 Bytes JMP 7FFA444E
.text	C:\WINDOWS\System32\alg.exe[260] ntdll.dll!NtEnumerateKey	7C90D2CE 5 Bytes JMP 7FFA3CCC
.text	C:\WINDOWS\System32\alg.exe[260] ntdll.dll!NtEnumerateValueKey	7C90D2EE 5 Bytes JMP 7FFA3DC1
.text	C:\WINDOWS\System32\alg.exe[260] ntdll.dll!NtOpenFile	7C90D59E 5 Bytes JMP 7FFA4861
.text	C:\WINDOWS\System32\alg.exe[260] ntdll.dll!NtOpenProcess	7C90D5FE 5 Bytes JMP 7FFA476D
.text	C:\WINDOWS\System32\alg.exe[260] ntdll.dll!NtQueryDirectoryFile	7C90D76E 5 Bytes JMP 7FFA3BA0
.text	C:\WINDOWS\System32\alg.exe[260] ntdll.dll!NtQuerySystemInformation	7C90D92E 5 Bytes JMP 7FFA3A0E
.text	C:\WINDOWS\System32\alg.exe[260] ntdll.dll!NtQueryVolumeInformationFile	7C90D98E 5 Bytes JMP 7FFA437E
.text	C:\WINDOWS\System32\alg.exe[260] ntdll.dll!NtReadVirtualMemory	7C90D9FE 5 Bytes JMP 7FFA3E28
.text	C:\WINDOWS\System32\alg.exe[260] ntdll.dll!NtResumeThread	7C90DB3E 5 Bytes JMP 7FFA3C71
.text	C:\WINDOWS\System32\alg.exe[260] ntdll.dll!NtVdmControl	7C90DF1E 5 Bytes JMP 7FFA3C02

Hacker Defender only 2

(inline hooks, hidden files, process, services, network port 4500 (not shown))

.text	C:\Documents and Settings\user\Desktop\20t0r147.exe[2292] ADVAPI32.dll!EnumServicesStatusExA	77E36C2F 5 Bytes JMP 7FFA42D8
Process	C:\hxdef100r\hxdef100.exe (*** hidden ***)	1644
Library	C:\hxdef100r\hxdef100.exe (*** hidden ***) @ C:\hxdef100r\hxdef100.exe [1644]	0x00400000
Service	C:\hxdef100r\hxdef100.exe (*** hidden ***)	[AUTO] HackerDefender100
Service	C:\hxdef100r\hxdefdrv.sys (*** hidden ***)	[MANUAL] HackerDefenderDrv100
Reg	HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\HackerDefender100	
Reg	HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\HackerDefender100@	Service
Reg	HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\HackerDefender100	
Reg	HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\HackerDefender100@	Service
Reg	HKLM\SYSTEM\CurrentControlSet\Services\HackerDefender100	
Reg	HKLM\SYSTEM\CurrentControlSet\Services\HackerDefender100@Type	16
Reg	HKLM\SYSTEM\CurrentControlSet\Services\HackerDefender100@Start	2
Reg	HKLM\SYSTEM\CurrentControlSet\Services\HackerDefender100@ErrorControl	0
Reg	HKLM\SYSTEM\CurrentControlSet\Services\HackerDefender100@ImagePath	C:\hxdef100r\hxdef100.exe
Reg	HKLM\SYSTEM\CurrentControlSet\Services\HackerDefender100@DisplayName	HXD Service 100
Reg	HKLM\SYSTEM\CurrentControlSet\Services\HackerDefender100@ObjectName	LocalSystem
Reg	HKLM\SYSTEM\CurrentControlSet\Services\HackerDefender100@Description	powerful NT rootkit
Reg	HKLM\SYSTEM\CurrentControlSet\Services\HackerDefender100\Security	
Reg	HKLM\SYSTEM\CurrentControlSet\Services\HackerDefender100\Security@Security	0x01 0x00 0x14 0x80 ...
Reg	HKLM\SYSTEM\CurrentControlSet\Services\HackerDefenderDrv100	
Reg	HKLM\SYSTEM\CurrentControlSet\Services\HackerDefenderDrv100@ErrorControl	0
Reg	HKLM\SYSTEM\CurrentControlSet\Services\HackerDefenderDrv100@ImagePath	\??\C:\hxdef100r\hxdefdrv.sys
Reg	HKLM\SYSTEM\CurrentControlSet\Services\HackerDefenderDrv100@Start	3
Reg	HKLM\SYSTEM\CurrentControlSet\Services\HackerDefenderDrv100@Type	1
Reg	HKLM\SYSTEM\ControlSet002\Control\SafeBoot\Minimal\HackerDefender100 (not active ControlSet)	
Reg	HKLM\SYSTEM\ControlSet002\Control\SafeBoot\Minimal\HackerDefender100@	Service
Reg	HKLM\SYSTEM\ControlSet002\Control\SafeBoot\Network\HackerDefender100 (not active Control...	
Reg	HKLM\SYSTEM\ControlSet002\Control\SafeBoot\Network\HackerDefender100@	Service
Reg	HKLM\SYSTEM\ControlSet002\Services\HackerDefender100 (not active ControlSet)	
Reg	HKLM\SYSTEM\ControlSet002\Services\HackerDefender100@Type	16
Reg	HKLM\SYSTEM\ControlSet002\Services\HackerDefender100@Start	2
Reg	HKLM\SYSTEM\ControlSet002\Services\HackerDefender100@ErrorControl	0
Reg	HKLM\SYSTEM\ControlSet002\Services\HackerDefender100@ImagePath	C:\hxdef100r\hxdef100.exe
Reg	HKLM\SYSTEM\ControlSet002\Services\HackerDefender100@DisplayName	HXD Service 100
Reg	HKLM\SYSTEM\ControlSet002\Services\HackerDefender100@ObjectName	LocalSystem

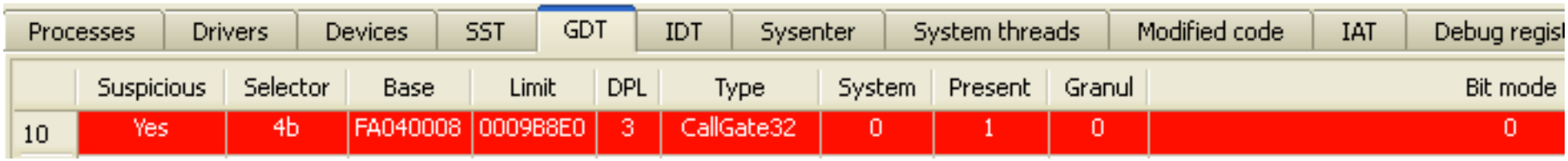
Hacker Defender only 3

(inline hooks, hidden files, process, services, network port 4500 (not shown))

Reg	HKLM\SYSTEM\ControlSet002\Services\HackerDefenderDrv100@ImagePath	\??\C:\hxdef100r\hxdefdrv.sys
Reg	HKLM\SYSTEM\ControlSet002\Services\HackerDefenderDrv100@Start	3
Reg	HKLM\SYSTEM\ControlSet002\Services\HackerDefenderDrv100@Type	1
File	C:\Documents and Settings\user\Local Settings\Temporary Internet Files\Content.IE5\4YK3P5WP\h...	58598 bytes
File	C:\hxdef100r	0 bytes
File	C:\hxdef100r\bdcli100.exe	26624 bytes
File	C:\hxdef100r\hxdef-OFdis.exe	70656 bytes
File	C:\hxdef100r\hxdef100.exe	70656 bytes
File	C:\hxdef100r\hxdef100.ini	3940 bytes
File	C:\hxdef100r\hxdefdrv.sys	3342 bytes executable
File	C:\hxdef100r\rdrbs100.exe	49152 bytes
File	C:\hxdef100r\readmecz.txt	37407 bytes
File	C:\hxdef100r\readmeen.txt	37905 bytes
File	C:\hxdef100r\src	0 bytes
File	C:\hxdef100r\src\bdcli100.dpr	10361 bytes
File	C:\hxdef100r\src\driver	0 bytes
File	C:\hxdef100r\src\driver\driver.c	8995 bytes
File	C:\hxdef100r\src\driver\driver.h	756 bytes
File	C:\hxdef100r\src\driver\driver.sys	3342 bytes executable
File	C:\hxdef100r\src\driver\makefile	36 bytes
File	C:\hxdef100r\src\driver\sources	140 bytes
File	C:\hxdef100r\src\driver.res	3408 bytes
File	C:\hxdef100r\src\hxdef100.dpr	353366 bytes
File	C:\hxdef100r\src\rdrbs100.dpr	57931 bytes
File	C:\hxdef100r\src\rdrbs100.res	1220 bytes
File	C:\hxdef100r\src\units	0 bytes
File	C:\hxdef100r\src\units\UJQCompress.pas	5268 bytes
File	C:\hxdef100r\src\units\UList.pas	7496 bytes
File	C:\hxdef100r\src\units\UProcAPI.pas	12835 bytes
File	C:\hxdef100r\src\units\USockets.pas	3692 bytes
File	C:\hxdef100r\src\units\USysUtils-Case.inc	1607 bytes
File	C:\hxdef100r\src\units\USysUtils-NumStrConv.inc	1608 bytes
File	C:\hxdef100r\src\units\USysUtils.pas	9272 bytes
File	C:\hxdef100r\src\units\UTcp.pas	10279 bytes
File	C:\hxdef100r\src.zip	93679 bytes

Basic Callgate only

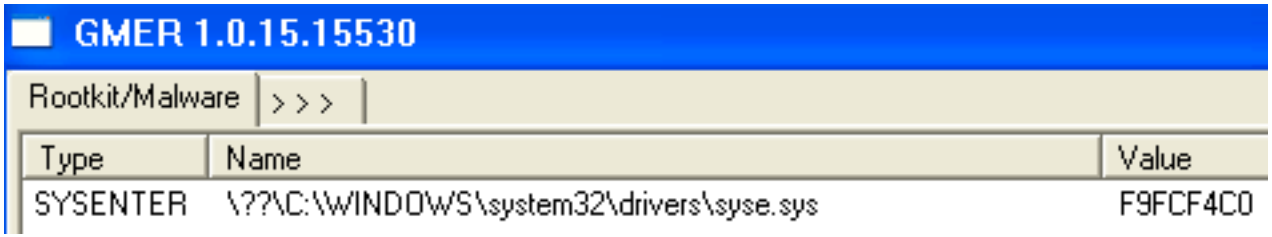
(does nothing but install a simple call gate)



	Suspicious	Selector	Base	Limit	DPL	Type	System	Present	Granul	Bit mode
10	Yes	4b	FA040008	0009B8E0	3	CallGate32	0	1	0	0

Sysenter Hook only

(does nothing but passthrough hook the IA32_SYSENTER_EIP MSR
may be named sysenter.sys in your VM)



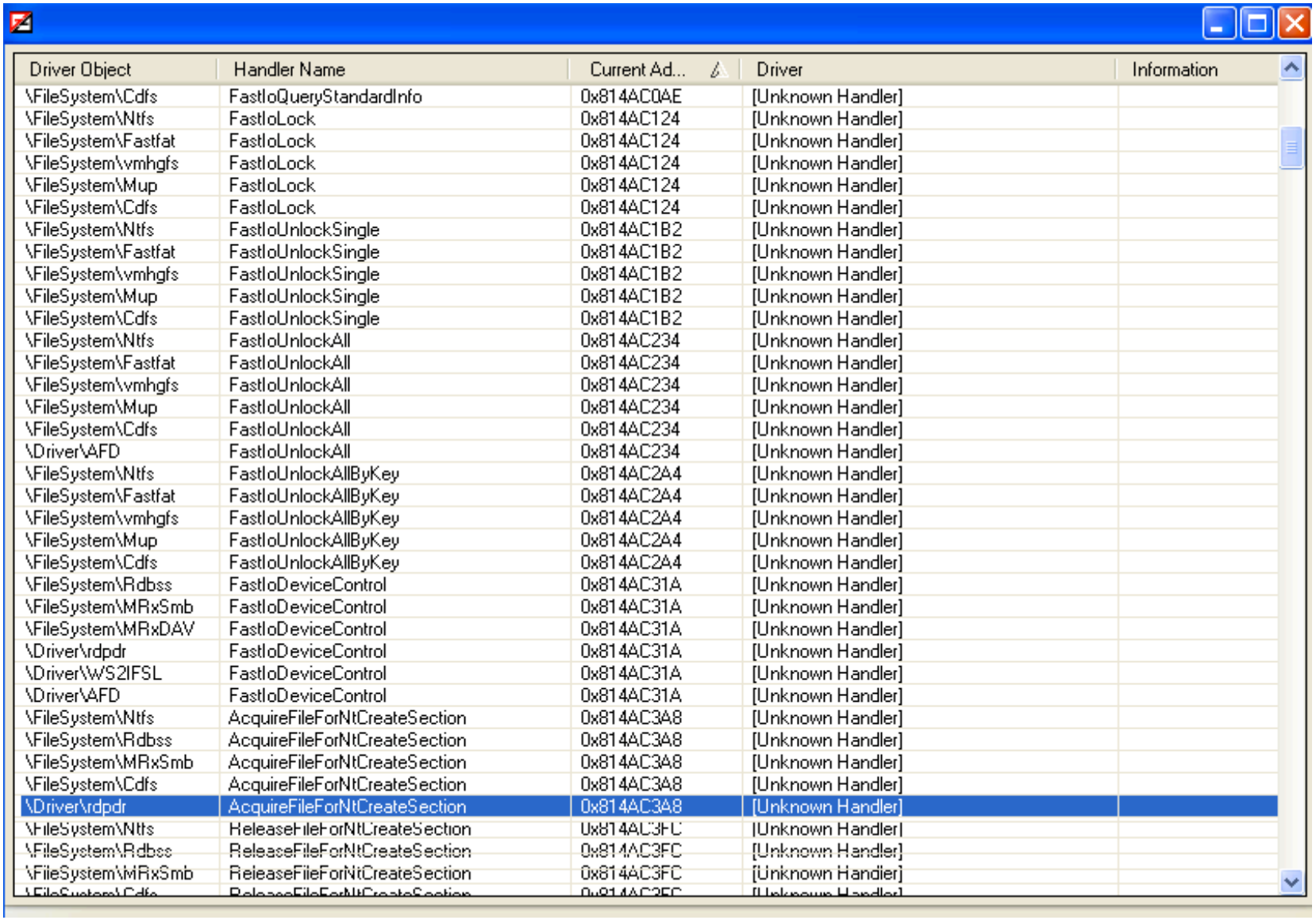
He4Hook only 1

(hiding only file C:\WINDOWS\system32\drivers\fu.exe, IRP major function hooks, copies self to dynamically allocated memory, process and thread callback routine, orphan thread, adds extra SSDT entry)

Type	Address	Driver	Addition	Information
LoadImage	0x81508900	Vba32 AntiRootKit Handler		VBA32
CreateThread	0x8159A000	[Unknown Handler]		
CreateProcess	0x8159A008	[Unknown Handler]		
Shutdown	0x814ACBDC	[Unknown Handler]	DeviceObject = 0x819E9BF0	
Shutdown	0x814ACBDC	[Unknown Handler]	DeviceObject = 0x8180ACA0	
Shutdown	0x814ACBDC	[Unknown Handler]	DeviceObject = 0x8192ECC0	
Shutdown	0x814ACBDC	[Unknown Handler]	DeviceObject = 0x8192EB98	
Shutdown	0x814ACBDC	[Unknown Handler]	DeviceObject = 0x8192EA70	
Shutdown	0x814ACBDC	[Unknown Handler]	DeviceObject = 0x8192E780	
Shutdown	0x814ACBDC	[Unknown Handler]	DeviceObject = 0x8192E658	
Shutdown	0x814ACBDC	[Unknown Handler]	DeviceObject = 0x81900030	
Shutdown	0x814ACBDC	[Unknown Handler]	DeviceObject = 0x8193B838	

He4Hook only 3

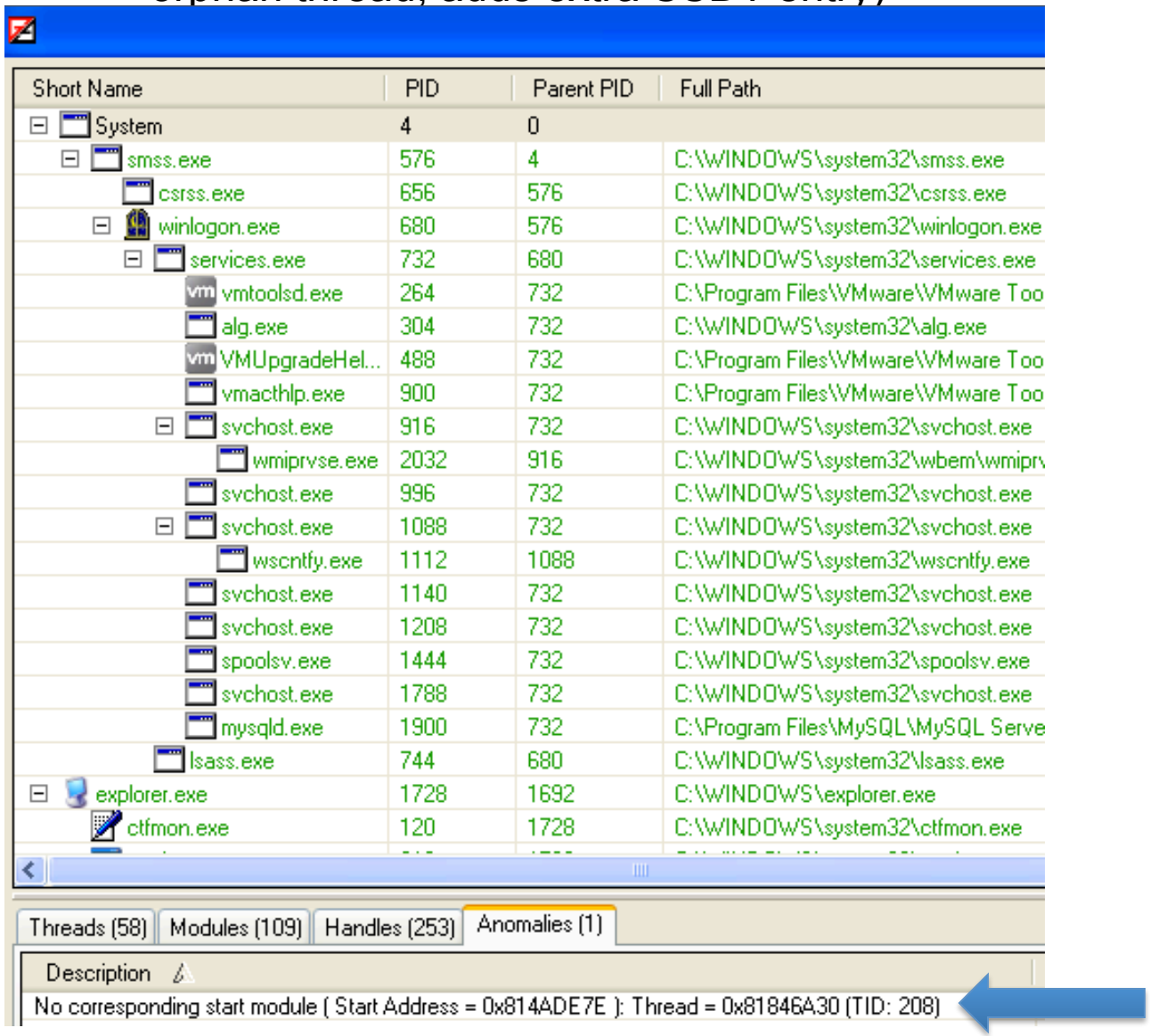
(hiding only file C:\WINDOWS\system32\drivers\fu.exe, IRP major function hooks, copies self to dynamically allocated memory, process and thread callback routine, orphan thread, adds extra SSDT entry)



Driver Object	Handler Name	Current Ad...	Driver	Information
\FileSystem\Cdfs	FastIoQueryStandardInfo	0x814AC0AE	[Unknown Handler]	
\FileSystem\Ntfs	FastIoLock	0x814AC124	[Unknown Handler]	
\FileSystem\Fastfat	FastIoLock	0x814AC124	[Unknown Handler]	
\FileSystem\vmhgfs	FastIoLock	0x814AC124	[Unknown Handler]	
\FileSystem\Mup	FastIoLock	0x814AC124	[Unknown Handler]	
\FileSystem\Cdfs	FastIoLock	0x814AC124	[Unknown Handler]	
\FileSystem\Ntfs	FastIoUnlockSingle	0x814AC1B2	[Unknown Handler]	
\FileSystem\Fastfat	FastIoUnlockSingle	0x814AC1B2	[Unknown Handler]	
\FileSystem\vmhgfs	FastIoUnlockSingle	0x814AC1B2	[Unknown Handler]	
\FileSystem\Mup	FastIoUnlockSingle	0x814AC1B2	[Unknown Handler]	
\FileSystem\Cdfs	FastIoUnlockSingle	0x814AC1B2	[Unknown Handler]	
\FileSystem\Ntfs	FastIoUnlockAll	0x814AC234	[Unknown Handler]	
\FileSystem\Fastfat	FastIoUnlockAll	0x814AC234	[Unknown Handler]	
\FileSystem\vmhgfs	FastIoUnlockAll	0x814AC234	[Unknown Handler]	
\FileSystem\Mup	FastIoUnlockAll	0x814AC234	[Unknown Handler]	
\FileSystem\Cdfs	FastIoUnlockAll	0x814AC234	[Unknown Handler]	
\Driver\AFD	FastIoUnlockAll	0x814AC234	[Unknown Handler]	
\FileSystem\Ntfs	FastIoUnlockAllByKey	0x814AC2A4	[Unknown Handler]	
\FileSystem\Fastfat	FastIoUnlockAllByKey	0x814AC2A4	[Unknown Handler]	
\FileSystem\vmhgfs	FastIoUnlockAllByKey	0x814AC2A4	[Unknown Handler]	
\FileSystem\Mup	FastIoUnlockAllByKey	0x814AC2A4	[Unknown Handler]	
\FileSystem\Cdfs	FastIoUnlockAllByKey	0x814AC2A4	[Unknown Handler]	
\FileSystem\Rdbss	FastIoDeviceControl	0x814AC31A	[Unknown Handler]	
\FileSystem\MRxSmb	FastIoDeviceControl	0x814AC31A	[Unknown Handler]	
\FileSystem\MRxDAV	FastIoDeviceControl	0x814AC31A	[Unknown Handler]	
\Driver\rdpdr	FastIoDeviceControl	0x814AC31A	[Unknown Handler]	
\Driver\WS2IFSL	FastIoDeviceControl	0x814AC31A	[Unknown Handler]	
\Driver\AFD	FastIoDeviceControl	0x814AC31A	[Unknown Handler]	
\FileSystem\Ntfs	AcquireFileForNtCreateSection	0x814AC3A8	[Unknown Handler]	
\FileSystem\Rdbss	AcquireFileForNtCreateSection	0x814AC3A8	[Unknown Handler]	
\FileSystem\MRxSmb	AcquireFileForNtCreateSection	0x814AC3A8	[Unknown Handler]	
\FileSystem\Cdfs	AcquireFileForNtCreateSection	0x814AC3A8	[Unknown Handler]	
\Driver\rdpdr	AcquireFileForNtCreateSection	0x814AC3A8	[Unknown Handler]	
\FileSystem\Ntfs	ReleaseFileForNtCreateSection	0x814AC3FC	[Unknown Handler]	
\FileSystem\Rdbss	ReleaseFileForNtCreateSection	0x814AC3FC	[Unknown Handler]	
\FileSystem\MRxSmb	ReleaseFileForNtCreateSection	0x814AC3FC	[Unknown Handler]	

He4Hook only 3

(hiding only file C:\WINDOWS\system32\drivers\fu.exe, IRP major function hooks, copies self to dynamically allocated memory, process and thread callback routine, orphan thread, adds extra SSDT entry)



He4Hook only 4

(hiding only file C:\WINDOWS\system32\drivers\fu.exe, IRP major function hooks, copies self to dynamically allocated memory, process and thread callback routine, orphan thread, adds extra SSDT entry)

- python vol.py ssdt -f bla.dmp
- Built in (not from the malware plugin), unfortunately you need to sift it yourself

(Ctrl2Cap impersonator which hides files)
Entry 0x0091: 0xfa065592 (NtQueryDirectoryFile) owned by Ctr12Cap.sys
(Daemon Tools + SPTD)
Entry 0x00a0: 0xf97fd554 (NtQueryKey) owned by sptd.sys
(Trusteer Rapport normal hook)
Entry 0x00e0: 0xf9b4fa90 (NtSetInformationFile) owned by RapportCerberus_23645.sys
(Trusteer Rapport shadow SSDT hooks)
Entry 0x1124: 0xf0f27324 (NtGdiStretchBlt) owned by RapportPG.sys
<snip>
Entry 0x1299: 0xbf954c65 (NtGdiUMPDEngFreeUserMem) owned by win32k.sys
Entry 0x129a: 0xbf817637 (NtGdiDrawStream) owned by win32k.sys
SSDT[2] at e2187818 with 5 entries
Entry 0x2000: 0xefead620 (Unknown) owned by UNKNOWN
Entry 0x2001: 0xefead65e (Unknown) owned by UNKNOWN
Entry 0x2002: 0xefeadc1a (Unknown) owned by UNKNOWN
Entry 0x2003: 0xefeae15a (Unknown) owned by UNKNOWN
Entry 0x2004: 0xefead6a2 (Unknown) owned by UNKNOWN

He4Hook's user->kernel coms

WinDbg Rootkit Searching Cheat-Sheet

- List all processes
  - !process 0 0
  - will be fooled by DKOM process unlinking!
- Change into a process contest
  - .process <pid> or .process <EPROCESS address>
- List all kernel drivers
  - lmf
    - "list loaded modules with file information"
  - will be fooled by DKOM driver unlinking!

WinDbg Rootkit Searching Cheat-Sheet 2

- Search for inline hooks in a exe/dll/sys file
  - !chkimg -d <*module name*>
  - !for_each_module !chkimg -d @#ModuleName
- Examine each thread's ServiceTable to see which SystemServiceDescriptorTable struct it's pointing at (there should only be two results and they should correspond to the addresses of KeServiceDescriptorTable or KeServiceDescriptorTableShadow
  - !for_each_thread ".echo Thread: @#Thread; dt nt!_kthread ServiceTable @#Thread"

WinDbg Rootkit Searching Cheat-Sheet 3

- Examine the SSDT function pointers
  - dd KeServiceDescriptorTable L 10
    - says to print 0x10 dword values starting at KeServiceDescriptorTable

```
8055c700  80504480 00000000 0000011c 805048f4
8055c710  00000000 00000000 00000000 00000000
8055c720  00000000 00000000 00000000 00000000
8055c730  00000000 00000000 00000000 00000000
```

  - The 0x80504480 is ServiceTableBase (start of the array of function pointers) and 0x11C is the total number of function pointers
  - dds 0x80504480 L 112
    - Says to print the symbol names for the 0x112 dwords which are going to be printed out

```
80504480  805a4630 nt!NtAcceptConnectPort
80504484  805f140e nt!NtAccessCheck
80504488  805f4c44 nt!NtAccessCheckAndAuditAlarm
8050448c  805f1440 nt!NtAccessCheckByType
80504490  805f4c7e nt!NtAccessCheckByTypeAndAuditAlarm
…
```

WinDbg Rootkit Searching Cheat-Sheet 3

- Check the sysenter MSRs
  - rdmsr 0x176 (for IA32_SYSENTER_EIP)
  - rdmsr 0x174 (for IA32_SYSENTER_CS)
- Examine the IDT and GDT by using the !protmode plugin from Intermediate x86 class
- Examine the IDT
  - !idt –a (shows all entries)
  - !idt (shows only some entries which don't point at nt or hal)
- Break on each module load during boot
  - sxe -c ".lastevent" ld
- Just list each module loading
  - sxn -c ".lastevent" ld
- Turn off breaks/notifications
  - sxi -c "" ld

Listing registered callbacks in WinDbg

- ~~http://analyze-v.com/?p=746 - process/memory image load (**PsSetCreateProcessNotifyRoutine[Ex]/PsSetImageLoadNotifyRoutine)**~~
- ~~http://analyze-v.com/?p=756 - registry callbacks(**CmRegisterCallback[Ex])**~~
- **Here comes a new challenger! Hadoken!**
- http://www.moonsols.com/2011/02/17/global-windows-callbacks-and-windbg/

kd> $$>a<c:\pscallbacks.wbs

****

* This command brought to you by Analyze-v.com *

****

****

* Printing image load callbacks... *

****

****

* Printing process notification callbacks... *

****

814ec008 ff2508605c81 jmp dword ptr ds:[815C6008h]

WinDbg (display device driver stack)

```
kd> !object \device\keyboardclass0
Object: 814e7d28  Type: (819b8ca0) Device
    ObjectHeader: 814e7d10 (old version)
    HandleCount: 0  PointerCount: 3
    Directory Object: e1006948  Name: KeyboardClass0
kd> !devstack 814e7d28
  !DevObj   !DrvObj            !DevExt   ObjectName
> 814e7d28  \Driver\Kbdclass   814e7de0  KeyboardClass0
  814e7020  \Driver\i8042prt   814e70d8
  8167c030  \Driver\ACPI       819a32e8  00000070
!DevNode 818f7348 :
  DeviceInst is "ACPI\PNP0303\4&5289e18&0"
  ServiceName is "i8042prt"
```

WinDbg 2 (display driver object)

```
kd> !devobj 814e7d28
Device object (814e7d28) is for:
 KeyboardClass0 \Driver\Kbdclass DriverObject 814ea0b8
Current Irp 00000000 RefCount 0 Type 0000000b Flags 00002044
Dacl e13cf7cc DevExt 814e7de0 DevObjExt 814e7ec0
ExtensionFlags (0000000000)
AttachedTo (Lower) 814e7020 \Driver\i8042prt
Device queue is not busy.
kd> dt nt!_DRIVER_OBJECT 814ea0b8
   +0x000 Type           : 4
   +0x002 Size           : 168
   +0x004 DeviceObject   : 0x81872030 _DEVICE_OBJECT
   +0x008 Flags          : 0x12
   +0x00c DriverStart    : 0xf9c4c000
   +0x010 DriverSize     : 0x6000
   +0x014 DriverSection  : 0x819b7aa8
   +0x018 DriverExtension  : 0x814ea160 _DRIVER_EXTENSION
   +0x01c DriverName     : _UNICODE_STRING "\Driver\Kbdclass"
   +0x024 HardwareDatabase : 0x80670de0 _UNICODE_STRING "\REGISTRY\MACHINE\HARDWARE
      \DESCRIPTION\SYSTEM"
   +0x028 FastIoDispatch   : (null)
   +0x02c DriverInit     : 0xf9c50610     long  kbdclass!GsDriverEntry+0
   +0x030 DriverStartIo  : (null)
   +0x034 DriverUnload   : (null)
   +0x038 MajorFunction  : [28] 0xf9c4cdd0     long  kbdclass!KeyboardClassCreate+0
```

WinDbg 3 (display next driver object)

```
kd> !devobj 814e7020
Device object (814e7020) is for:
  \Driver\i8042prt DriverObject 814ea410
Current Irp 00000000 RefCount 0 Type 00000027 Flags 00002004
DevExt 814e70d8 DevObjExt 814e7368
ExtensionFlags (0000000000)
AttachedDevice (Upper) 814e7d28 \Driver\Kbdclass
AttachedTo (Lower) 8167c030 \Driver\ACPI
Device queue is not busy.
kd> dt nt!_DRIVER_OBJECT 814ea410
   +0x000 Type           : 4
   +0x002 Size           : 168
   +0x004 DeviceObject   : 0x817dda40 _DEVICE_OBJECT
   +0x008 Flags          : 0x12
   +0x00c DriverStart    : 0xf9a2c000
   +0x010 DriverSize     : 0xcd00
   +0x014 DriverSection  : 0x81973070
   +0x018 DriverExtension  : 0x814ea4b8 _DRIVER_EXTENSION
   +0x01c DriverName     : _UNICODE_STRING "\Driver\i8042prt"
   +0x024 HardwareDatabase : 0x80670de0 _UNICODE_STRING "\REGISTRY\MACHINE\HARDWARE
      \DESCRIPTION\SYSTEM"
   +0x028 FastIoDispatch   : (null)
   +0x02c DriverInit     : 0xf9a35285     long  i8042prt!GsDriverEntry+0
   +0x030 DriverStartIo  : 0xf9a2c910     void  i8042prt!I8xStartIo+0
   +0x034 DriverUnload   : 0xf9a32eb6     void  i8042prt!I8xUnload+0
   +0x038 MajorFunction  : [28] 0xf9a2faa6     long  i8042prt!I8xCreate+0
```

WinDbg 4 (print IRP table)

```
kd> dps 814ea410+0x38 L1C
814ea448  f9a2faa6 i8042prt!I8xCreate
814ea44c  804f355a nt!IopInvalidDeviceRequest
814ea450  f9a32e18 i8042prt!I8xClose
814ea454  804f355a nt!IopInvalidDeviceRequest
814ea458  804f355a nt!IopInvalidDeviceRequest
814ea45c  804f355a nt!IopInvalidDeviceRequest
814ea460  804f355a nt!IopInvalidDeviceRequest
814ea464  804f355a nt!IopInvalidDeviceRequest
814ea468  804f355a nt!IopInvalidDeviceRequest
814ea46c  f9a2e1f9 i8042prt!I8xFlush
814ea470  804f355a nt!IopInvalidDeviceRequest
814ea474  804f355a nt!IopInvalidDeviceRequest
814ea478  804f355a nt!IopInvalidDeviceRequest
814ea47c  804f355a nt!IopInvalidDeviceRequest
814ea480  f9a32e4b i8042prt!I8xDeviceControl
814ea484  f9a2c836 i8042prt!I8xInternalDeviceControl
814ea488  804f355a nt!IopInvalidDeviceRequest
814ea48c  804f355a nt!IopInvalidDeviceRequest
814ea490  804f355a nt!IopInvalidDeviceRequest
814ea494  804f355a nt!IopInvalidDeviceRequest
814ea498  804f355a nt!IopInvalidDeviceRequest
814ea49c  804f355a nt!IopInvalidDeviceRequest
814ea4a0  f9a337ea i8042prt!I8xPower
814ea4a4  f9a2fa59 i8042prt!I8xSystemControl
814ea4a8  804f355a nt!IopInvalidDeviceRequest
814ea4ac  804f355a nt!IopInvalidDeviceRequest
814ea4b0  804f355a nt!IopInvalidDeviceRequest
814ea4b4  f9a2f990 i8042prt!I8xPnP
```

dps = **d**isplay **p**rocessor-sized pointer (meaning it decides whether it should be 16-64 bits), as a pointer to a **s**ymbol

dds = **d**isplay **d**word as a pointer to a **s**ymbol

Level up!

- +120 WinDbg EXP
- +1 Skill Point, +1 r0x0r Point
- You gained new tool "Laboskopia WinDbg scripts"!
  - http://www.laboskopia.com/download/SysecLabs-Windbg-Script.zip
- Now use em!
  - http://www.reconstructer.org/papers/Hunting%20rootkits%20with%20Windbg.pdf

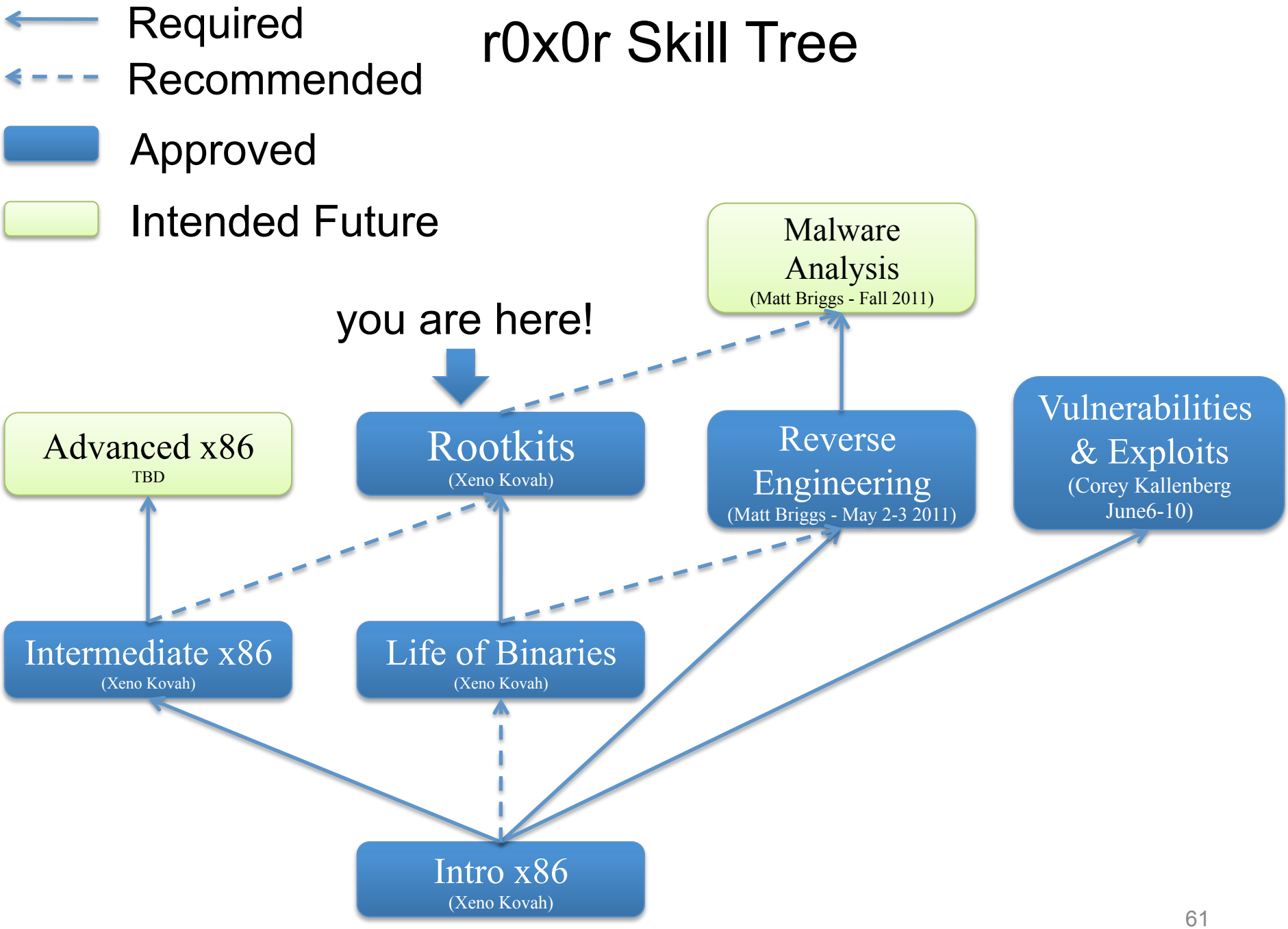
Teardown close out

- What did we learn?
  - Using GMER, Tuluka, Virus Blok Ada Anti-Rookit for in-system rootkit detection
  - Using WinDbg for live debugging
  - Using Volatility for offline memory analysis
  - IDT, IAT, inline, SSDT, SYSENTER, IRP hooking
  - GDT call gates, DKOM, KOH, kernel callbacks, bootkits

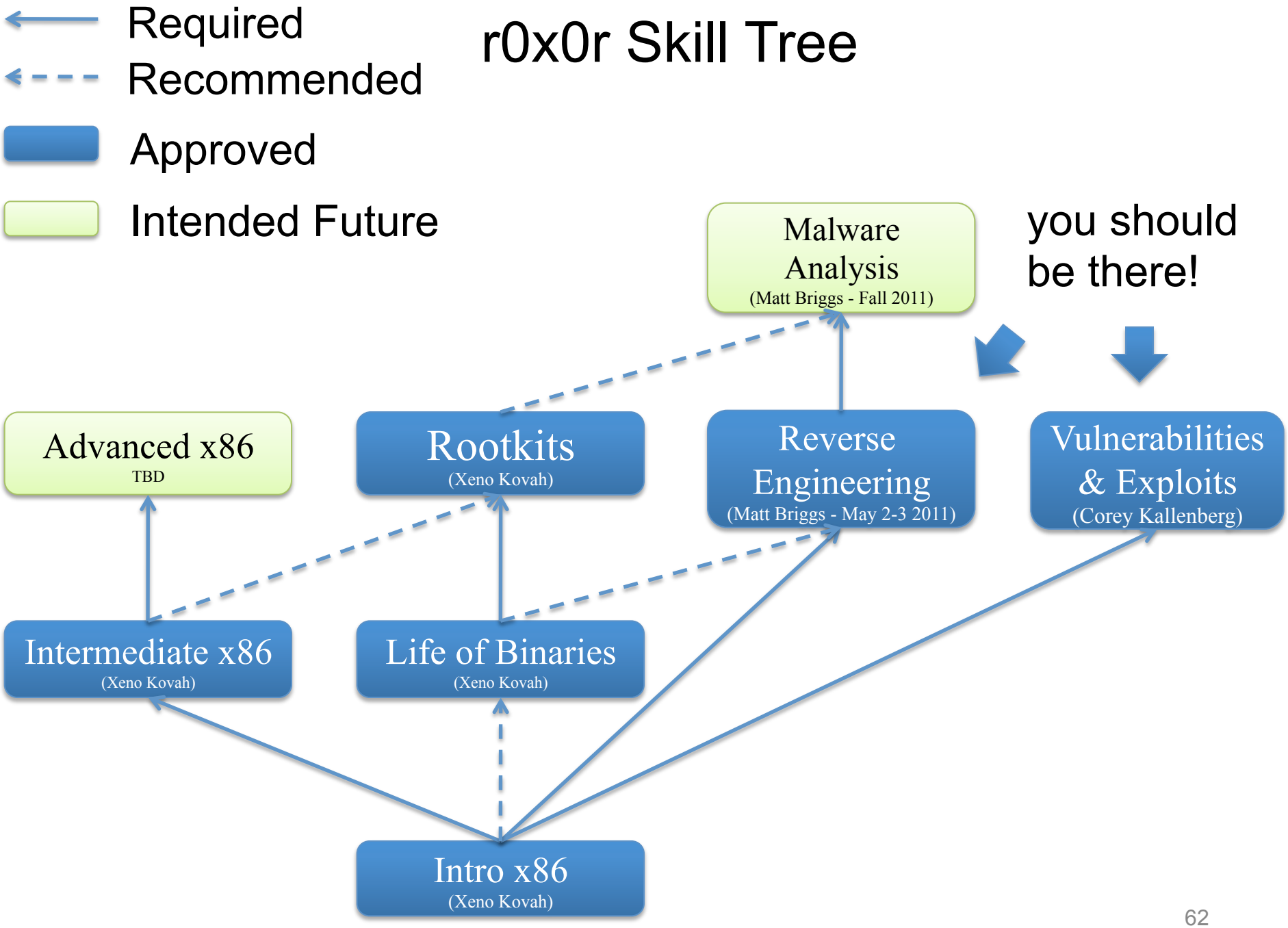
Materials for you

- These slides
- The anonymized writeups from people who submitted their homework
- Spreadsheet showing what tools detect
- TiddlyWiki with example of running to ground a false positive (due to Symantec), and the true positive (shadowwalker).
- Collection of rootkits installed on the VM + the .bat file used to install them. (Don't download to any system with on-access AV scanning, since some of them will be flagged.)
- Go analyze the existing VM again with different tools to get more familiarity with them. I will distribute a VM in the future which will have a couple things installed which will be more difficult to detect, but which will still be within the materials covered in this class.

r0x0r Skill Tree



r0x0r Skill Tree



Rootkits: