Detecting Rootkits

(in Windows and Linux)

Hal Pomeranz
Deer Run Associates

Detection Options

Endpoint software

Memory Analysis

System anomalies

Endpoint Software

File integrity (Tripwire, OSSEC, …)

EDR (CarbonBlack, Falcon, …)

Event logs and Sysmon (SEIM, Splunk, Elastic, …)

Memory Analysis

Most effective method for seeing rootkits

Volatility™ supports Windows and Linux (and Mac!)

Issues

- Windows 10 support
- Linux profile creation

Useful Volatility™ Modules

Rootkit Type	Windows	Linux
User-mode	**malfind**, ldrmodules **apihooks**	
Kernel	modscan, **driverbl** **ssdt**, driverirp **psxview**	**linux_check_modules** **linux_hidden_modules** **linux_check_syscall** linux_lsmod linux_dmesg

Needle in a Needle Stack

```
$ vol.py -f APT.img modscan
Offset(P)          Name                 Base             Size File
------------------ -------------------- ---------- ---------- ----
0x0000000001f1c7d0 irykmmww.sys         0xf836f000     0x4000 \SystemRoot\system32\drivers\irykmmww.sys
0x0000000001fbd970 mrxdav.sys           0xf649b000    0x2d000 \SystemRoot\system32\DRIVERS\mrxdav.sys
0x0000000001fe34c8 ndiswan.sys          0xf82d2000    0x17000 \SystemRoot\system32\DRIVERS\ndiswan.sys
0x0000000001ff2568 watchdog.sys         0xf8a0a000     0x5000 \SystemRoot\System32\watchdog.sys
0x0000000001ff3338 dxg.sys              0xbf9c3000    0x12000 \SystemRoot\System32\drivers\dxg.sys
0x0000000001ff5630 dxgthk.sys           0xf8cba000     0x1000 \SystemRoot\System32\drivers\dxgthk.sys
0x0000000001ffb8c8 HTTP.sys             0xf6110000    0x41000 \SystemRoot\System32\Drivers\HTTP.sys
0x0000000002009670 mrxsmb.sys           0xf698e000    0x70000 \SystemRoot\system32\DRIVERS\mrxsmb.sys
…
$ vol.py -f APT.img modscan | wc -l
199
```

Baselines FTW!

```
$ vol.py driverbl -f APT.img -B baseline.img -U
Offset(P)  Service Key           Found Name  DName Module Size  IRPs  Path
---------- -------------------- ----- ----- ----- ------ ----- ----- ----
0x01f1c7d0 irykmmww.sys         False False False False  False False \??\C:\WINDOWS\system32\dri…
0x02163f60 vmdebug.sys          False False False False  False False \??\C:\WINDOWS\system32\Dri…
0x023665b8 vmmemctl.sys         False False False False  False False \??\C:\Program Files\VMware…
0x024e9c88 mktools.sys          False False False False  False False \??\C:\Program Files\Mandia…
0x128975b8 vmmemctl.sys         False False False False  False False \??\C:\Program Files\VMware…
```

Hook Shot

```
$ vol.py -f APT.img ssdt | egrep -v '(ntoskrnl|win32k)'
[x86] Gathering all referenced SSDTs from KTHREADs...
Finding appropriate address space for tables...
SSDT[0] at 80501b9c with 284 entries
  Entry 0x0042: 0xf836fe9c (NtDeviceIoControlFile) owned by irykmmww.sys
  Entry 0x0047: 0xf83706dc (NtEnumerateKey) owned by irykmmww.sys
  Entry 0x0049: 0xf837075e (NtEnumerateValueKey) owned by irykmmww.sys
  Entry 0x0077: 0xf837028f (NtOpenKey) owned by irykmmww.sys
  Entry 0x0091: 0xf8370a8c (NtQueryDirectoryFile) owned by irykmmww.sys
  Entry 0x00ad: 0xf836fe3e (NtQuerySystemInformation) owned by irykmmww.sys
  Entry 0x00b1: 0xf837091a (NtQueryValueKey) owned by irykmmww.sys
SSDT[1] at bf999d00 with 667 entries
```

Linux LKM Rootkits

```
$ vol.py -f rootkit.img --profile=LinuxCentOSx64 linux_check_modules
    Module Address       Core Address       Init Address Module Name
------------------ ------------------ ------------------ ------------------------
0xffffffffa0747000 0xffffffffa0745000                0x0 diamorphine

$ vol.py -f rootkit.img --profile=LinuxCentOSx64 linux_hidden_modules
Offset (V)         Name
------------------ ----
0xffffffffa0747000 diamorphine

$ vol.py -f rootkit.img --profile=LinuxCentOSx64 linux_check_syscall | grep HOOKED
64bit         62      0xffffffffa0745540 HOOKED: diamorphine/hacked_kill
64bit         78      0xffffffffa0745080 HOOKED: diamorphine/hacked_getdents
64bit        217      0xffffffffa0745230 HOOKED: diamorphine/hacked_getdents64
```

Find That Hidden Process!

```
root@siftworkstation:/memory# vol.py -f rootkit.img psxview -R

Offset(P)  Name                PID pslist psscan thrdproc pspcid csrss
---------- ----------------    --- ------ ------ -------- ------ -----
0x01ab1a20 services.exe        940 True   True   True     True   True
0x01a8db68 svchost.exe        1120 True   True   True     True   True
0x019bc590 alg.exe            1924 True   True   True     True   True
0x01666a70 winlogon.exe        896 True   True   True     True   True
0x0169bda0 svchost.exe        1188 True   True   True     True   True
0x01617600 explorer.exe       1288 True   True   True     True   True
0x015eb270 svchost.exe        1320 True   True   True     True   True
0x019887f0 spoolsv.exe        1824 True   True   True     True   True
0x019922c0 svchost.exe        1608 False  True   True     True   True
0x01838c88 csrss.exe           868 False  True   False    False  Okay
0x01a69a40 lsass.exe           952 True   True   True     True   True
0x01bcc830 System                4 True   True   True     True   Okay
0x01750020 csrss.exe           872 True   True   True     True   Okay
0x01a385a0 smss.exe            824 True   True   True     True   Okay
```

Linux CLKF FTW!

Hidden directories impact link counts

Hidden directories under /proc can be brute-forced

Thanks for Listening!

Hal Pomeranz
hal@sans.org
deer-run.com/~hal/
@hal_pomeranz