Anti-Forensics AF

@dualcoremusic
mov eax, 0x6b; int 0x80

• Rapper
• Some other stuff idk
Overview

• Memory Forensics vs SMC*
  – Windows
  – Linux
• Android (Anti-)Forensics
• Fun with SD cards
Disclaimers

• !Professional
• TROLOLOLOL
• !Expert / YMMV
• DO ILLEGAL THINGS
Memory Forensics

- Focus on software protection (malware)
- Persist, thwart detection
- Inhibit acquisition and analysis
Memory Forensics

• All the cool stuff happens in memory
• Loading from disk
• Why can’t I hold all these sections?
Memory Forensics

- No longer referenced, no longer needed
- Analysis tools madbro
- Lots of fun to be had
Memory Forensics

• Demo
  – thekeysarelikerightnexttoeachother.exe
  • Rekall (winpmem)

<tatclass> YOU ALL SUCK DICK
<tatclass> er.
<tatclass> hi.
<andy\code> A common typo.
<tatclass> the keys are like right next to each other.
Memory Forensics

- PE header not needed after loading
- Zero the header (RtlZeroMemory)
- Process continues to run
- Analysis tools fail
- Win: XP → 10
Memory Forensics

• Completeness:

winpmem-2.1.post4.exe -o lol.aff4

"C:\Program Files\Rekall\rekal.exe" -f lol.aff4

> procdump proc_regex="thekeys",
dump_dir="C:/Users/int0x80/Desktop/"
Memory Forensics

• Demo
  – thekeysarelikerightnexttoeachother-linux
    • LiME
    • Volatility
Memory Forensics

- ELF header not needed after loading
- Zero the header (memset)
- Process continues to run
- Analysis tools fail
Memory Forensics

• Completeness:

git clone https://github.com/504ensicsLabs/LiME

cd LiME/src/

make

sudo insmod ./lime-$\$(uname -r).ko \ "path=/tmp/lol.lime format=lime"
Memory Forensics

• Completeness:

git clone https://github.com/volatilityfoundation/volatility

cd volatility/

sudo python setup.py install
Memory Forensics

• Completeness:

    cd tools/linux/

    make

    head module.dwarf

    .debug_info

    ...
Memory Forensics

• Completeness:

```bash
sudo zip \
volutility/plugins/overlays/linux/Ubuntu1604.zip \
tools/linux/module.dwarf \ 
/boot/System.map-$($uname -r)$
```

```python
python vol.py --info | grep ^Linux
```

Volatility Foundation Volatility Framework 2.5
LinuxUbuntu1604x64 - A Profile for Linux Ubuntu1604 x64
Memory Forensics

• Completeness:

```python
python vol.py -f /tmp/lol.lime \
   --profile=LinuxUbuntu1604x64 linux_pslist

python vol.py -f /tmp/lol.lime \
   --profile=LinuxUbuntu1604x64 linux_procdump \
   -D /tmp -p <PID>
```
Android (Anti-)Forensics

- Use Encryption
Android (Anti-)Forensics

- Use Encryption
- Also "Use Tor, Use Signal"
Android (Anti-)Forensics

- Use Encryption
- Also "Use Tor, Use Signal"

---

@thegrugg

Q: I’m planning thanksgiving din
A: use Tor, use Signal
%
Q: my wife left me & took my dog
A: use Tor, use Signal

- privacy activist advice
• Use Encryption
• Also "Use Tor, Use Signal"

- privacy activist advice
Android (Anti-)Forensics

• Use Encryption
• Also "Use Tor, Use Signal"
Android (Anti-)Forensics

- Use Tor. Use Signal.
- I fucking give up. Parody has nothing on reality.

Xerio @Nf1C0
Selling SSN's for BTC please contact me on my XMPP and will discuss further
Android (Anti-)Forensics

- Use Encryption
- But first, a word about Android forensics
Android Forensics

• Not the easiest
• Acquisition/Imaging is a pain
  – Numerous caveats
  – CONFIG_MODULES=y
  – Cross-compile nc
  – Different interfaces
Android Forensics

• Acquisition/Imaging caveats:
  – Power
  – Decrypted
  – Unlocked
  – Rooted
  – USB Debugging
Android Forensics

• Memory acquisition/imaging caveats:
  – Power
  – Decrypted
  – Unlocked
  – Rooted
  – USB Debugging
  – CONFIG_MODULES=y
• NAND acquisition done with nc

adb devices
adb push ./nc /sdcard/nc
adb forward tcp:4444 tcp:4444
adb shell
su
cp /sdcard/nc /dev/nc
chmod 777 /dev/nc
Android Forensics

• NAND acquisition done with nc

    dd if=/dev/block/mmcblk0 bs=65535 | \
        /dev/nc -nvlp 4444
    nc -nv 127.0.0.1 4444 > image.nand
    sha256sum image.nand
    cp -a image.nand image.nand.copy
    sha256sum image.nand*

Android Forensics

- NAND exposed via different interfaces
- Check /proc/partitions
  - /dev/block/mmcblk*
  - /dev/mtd/mtd*
  - /dev/mtdblock*
  - /dev/emmc*
  - /*//*/*/* no, comment
• Logical acquisition is easier
  – `adb pull / ./dump`
  – `adb shell dumpsys &> ./dumpsys.log`
  – `adb backup -apk -obb -shared -all -system`

  `java -jar abe.jar unpack <backup.ab> <backup.tar> [pin]`
Android Forensics

• Logical acquisition is easier
  – adb shell dumpstate \\n  &> ./dumpstate.log
  – adb bugreport &> ./bugreport.log
  – aflogical-ose
Android Forensics

• Complete forensic acquisition/analysis sucks
• Likely violate traditional methodology
• Easy to disrupt :)
Android Anti-Forensics

• Use Encryption
• Example scenarios:
  – Raided by LE
  – Deploying hardware implant
  – ฯIRECTION HEAD ฯ
Android Anti-Forensics

• Use Encryption
• Easiest solution:
  – Power down device
  – Everything encrypted
  – Lawyer up
Android Anti-Forensics

- Power down if tampering detected
- Leverage device sensors
  - Bluetooth
  - Cellular
  - GPS
  - Motion
  - Power
  - WiFi
Android Anti-Forensics

• Android app: Duck The Police
• Device assertions:
  – Encrypted
  – Rooted
  – Magnets
  – Sensors
• DEMO
Android Anti-Forensics

• Use Encryption

• Example scenarios:
  – Raided by LE
  – Deploying hardware implant
  – ˘(ツ)_/˘

• WIN
SD Cards

- CTF Time!
SD Cards

- [SPOILER PREVENTION INTENSIFIES]
SD Cards

- sdtool
- Lock/Unlock device
- Physical lock disengaged
- Writes happen in memory
- Nothing written to device
- NO LOGS, NO CRIME
SD Cards

• sdtool caveats:
  – Direct access to MMC device required
  – Some USB hubs only expose mass storage
    • WON'T WORK
SD Cards

• Example scenarios:
  – Hardware implant
  – PORTAL of Pi (@thegruugq)
    • https://github.com/int0x80/notes/wiki/Linux:-PORTAL-of-Pi
  – Attack VM
SD Cards

- Edit Makefile to use clang instead of gcc

```
sudo ./sdtool /dev/mmcblk0 status
sudo ./sdtool /dev/mmcblk0 lock
sudo ./sdtool /dev/mmcblk0 unlock
```
Questions?

@dualcoremusic
dualcoremusic@gmail.com