WRITING MULTI-PLATFORM SPYWARE
*DISCLAIMER* this talk is about techniques, not actions. You and ONLY you are responsible for what you do.
MISSION:

the job of spy ware, is to spy, the goal of the spy ware operator is to spy on humans...
the goal is simple, acquire as much data as possible, while remaining as hidden as possible.
memory corruption
- disk writes
- "event" triggers
- network "volume"
- CPU load
visible changes to the UX
reverse engineering is an ever-present risk.
TL;DR, ONCE YOUR TARGET SUSPECTS YOUR EXISTENCE, YOU LOSE.
INTELLIGENCE GATHERING
MEMORY PERSISTANCE

SHARED OBJECT INJECTION

PROCESS

ENTER
PTRACE SNAPSHOT
OVERRIDE PT EXCEPTION
SETUP NULL CALL
REPLACE REGISTERS
RESUME
MEMORY PERSISTANCE

"THEY’RE IN THE KERNEL!"
MEMORY PERSISTANCE

DLL INJECTION

CreateRemoteThread()
MEMORY PERSISTANCE

HOOKING ON WINDOWS

SetWindowsHookEx()
SetThreadContext()
DLL redirection
MEMORY PERSISTANCE

LDPRELOAD ON /
DYLD_INSERT_LIBRARIES

PROCESS MIGRATION
MEMORY PERSISTANCE

then kill the original process (and restart it if required)
ROOT@LOCALHOST:~# BACKDOOR-FACTORY

AUTHOR: JOSHUA PITTS
EMAIL: THE.MIDNITE.RUNR[A T]GMAIL<D O T>COM
TWITTER: @MIDNITE_RUNR
MEMORY PERSISTANCE

INSTALL A WINDOWS SERVICE

CRON

LAUNCHD

DLL REDIRECTION
MEMORY PERSISTANCE

- C:\Users\<user name>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\
- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\
- .bashrc ...
- init.d modification
- USB / CDROM autorun
- network connection auto run (Little Snitch, Microsoft)

Not sure if serious...
MEMORY PERSISTANCE
DATA MINING
DATA MINING
DATA MINING
DATA MINING
DATA MINING

- SSH, VPN, SSL, VNC, RDP, DOMAIN, etc, keys / certs
- key logger data
- password databases
- packet captures
- GPG, in-memory key tokens
  - what's app
  - signal
  - tor
  - SMIME
  - bio-metric scanners
  - etc...
DATA PROCESSING
DATA PROCESSING

#slack
DATA PROCESSING
DATA PROCESSING
DATA PROCESSING

ELASTICSEARCH
DATA PROCESSING

STRINGS, SED, AWK, GREP, CUT, HEXDUMP, FILE, ETC...
CONCLUSION

• YOUR TARGETS ARE HUMANS, SO STUDY HUMANS
• DON’T RE INVENT THE WHEEL
• PRACTICE PRACTICE PRACTICE PRACTICE
• MULTIPLAYER IS ALWAYS BETTER