Athena Progress – October 14, 2015 – 10am

Minutes:

1) Reviewed XP issues
2) Reviewed tasking for XXXXX

Achievements:

- Loader – remove PE date in header
    - Loader – dynamically load virtual alloc/free/protect
- ToolHash – use same algorithm as loader (no null in hash calculation)
- Builder – DATAHERE – installer/host/ramonly
    - Ramonly – add masked block(.text section with entropy masking)
    - Install – add masked block (.text section with entropy masking)
        - Install – mask registry/service/debuggerpresent functions
    - Host - add masked block (.text section with entropy masking)
    - Random data in overwrite block uses data from nasm.exe instead of CC CC
- Engine – main loop
    - client id generate
    - signal (uninstall/unload/config/notify)
    - directory change notification
    - wincrypt – aes/rsa support (?signing)
- Uninstall – use config settings

Tasks under development:

1) Completing parser/tasker tool for integration - XXXXX
2) Completing LP to support changes – XXXXX
3) Continuing development for command module -XXXXX
4) setup Squid/help on proxy settings – XXXXX
5) offline lin/win installers – XXXXX
6) *Persistence – run as system
7) *Test with XP
8) Loader – mask import engine.dll in axe
9) Loader – support nickname
10) Loader – support passing data pointer to loader for engine module
11) *Comm – send/receive – TestEncryption code
12) Engine – unload command module
13) Engine – calculate sleep (hibernation/bootdelay/beacon delay)

Issues:

1) entropy obfuscation – every forth byte is 0xCC, 0xC3, 0xFF, 0x00, 0x0F, 0x80, 0xCB, 0x91, 0x48, 0x49 – doesn't exactly look like code block with C3 CC CC CC CC CC CC CC

2) users want to allow apache to send valid pages as well – pick a sub-directory (process or manager or something innocuous)

3) Builder – duplicate parent ids – 4 bytes (A-Z,0-9)