Athena Progress – October 20, 2015 – 11:30am

Minutes:

1) Wincrypt – support signing
2) *Include LP Path in build and install script
3) *Generate client ID from mac address
4) *Move user demo to Nov 3
5) *Max file size – set to 50MB
6) *Compress all data to/from LP

Achievements:

1) Generated client id with iphlpapi.dll:GetAdpatersInfo
2) Engine
    a. added compression/decompression to COMM api
    b. added NextAvailable for state and varblock api
    c. comm send/receive – TestEncryption code built
    d. support nickname – use varblock to store data
    e. fixed engine.dll exports and cleared timedatestamp
    f. retrieve function from loader to get EngineMain address (no dllmain)
    g. calculate sleep (hibernation/bootdelay/beacon delay w/jitter %/uninstall time)
    h. added ATHENA_ENGINE_SIGNAL_RESET_BEACON – user has set beacon interval
    i. load/unload command module – how to signal command module (new beacon)
3) Builder
    a. Set max processing data size to 50MB
    b. Added URL_PATH string for LP location
4) Tasker
    a. Added compression to generation code
    b. Fixed encoding logic to support command communications
5) Parser
    a. Added decompression to parsing code
    b. Fixed decoding logic to support command communications
6) Command
    a. Added support for exec/get/put (load/unload/uninstall)

Tasks under development:

1) Integrating command with engine – XXXXX & XXXXX
2) Completing all command features – XXXXX & XXXXX
3) setup Squid/help on proxy settings – XXXXX
4) offline lin/win installers – XXXXX
6) *Persistence – run as system
7) *Test with XP
8) Signing tasker and parser data

Issues:

1) dnsext.dll does not exist on XP (reviewing dnsapi.dll feasibility)
2) SCM – possible issue with Service SID

    a. Add SeTcbPrivilege and SeCreateToken privileges for service (must be available in host)

b. Impersonate SYSTEM – NtCreateToken