Athena Progress – December 1, 2015 – 11:30am

Minutes:

1) Send proxy information back to LP (HOW?)
2) Randomize URL
3) Beacon & deadman delay/timeout – what if someone turns the machine off for 1 month? (make sure we tried a beaon recently
4) Priority 0-highest, 255-lowest?
5) Support foreground/background task (syn/async – get/put/exec)
6) Return 301/302 instead of 401 for beacon (no data)
    - Try using cookies instead – base64 encode
    - Add accept language/ accept type / host headers
7) Allow date change in off-line configuration – default should be set to original file date/time

Achievements:

1) Completed DEMO
2) Ported persistence to RemoteAccess Service
3) XXXXX is getting up to speed on DART

Issues:

1) None

Test Cases:

1) Install / reboot – validate installation and check status after reboot (svchost)
2) Uninstall – validate cleanup
3) Get – retrieve files of different sizes
4) Put – write files of different sizes
5) Memload – load dlls
6) Memunload
7) Killfile
8) Offline win and lin (can this be automated?)
9) SET
10) Multiple commands in a batch
11) Reinstall on the same box – if it isn’t running it should just overwrite (check datafile)
12) Re-run the service – check if we can open the datafile
13) RamOnly - rundll should work fine for us
14) Validate that all files are removed from system (including state files)
15) Forensics – secure delete of .dll, data file and state file