ODDJOB 3.4.0.0 Testing

**The new functionality included in ODDJOB 3.4.0.0 version was only manually tested on Windows Server 2003 and Windows Server 2008. The below methods were used for testing the main functionality of ODDJOB in earlier versions, however the below tests were not carried out on 3.4.0.0.**

PSP:

PSP testing was done in the same manner as the functionality testing. The only difference was that the target virtual machines had PSPs installed, and were running the latest MS patches available.

Functionality:

A Win2k8R2 LP was set up to deliver the payloads to the targets. On the LP, a script was used to watch the log, and then create payloads upon seeing a callback. Once a new callback was seen, 4 payloads were created, a change time payload, a long running DLL, a short running DLL, and a process list command. The script would also watch the uploads directory on the LP. When a process list was uploaded, the script would then create a final .exe payload for the implant. This methodology on the LP allowed for every type of payload to be tested, as well the oddjob upload functionality (used by the process list function).

On the target, another python script was running which create and test each of the compatible combinations of payload type and architecture for the target (DLL/EXE, x86/x64) one after another. The script would then check the results of each payload to ensure that all payloads were running properly. First it would check if the change time payload worked, by checking the RETRY DELAY key in the bitsadmin output. Next, it would look for certain files placed in the temp directory by the dlls. The testing DLLs were also watching for these files to appear in the right order, so ODDJOB's re-registration functionality could be tested. Once the process listing had succeeded, as verified by the LP script, a final exe payload would touch another file in the temp directory. Once the time had been changed on the bits job, and all of the requisite files were present in the temp directory, the script would log a successful test case. The script would then reset the environment, and test the next payload type/architecture combination.

Manual testing:

Manual testing was carried out to ensure that the issue with Win2k3 was properly fixed. Manual PSP testing was also carried out against Avira and Norton.