From: "Greg Hoglund" <greg@hbgary.com>
To: <Stuart_McClure@mcafee.com>
Sent: Friday, July 30, 2010 12:06 AM
Attach: stuxnet_rawdata.rar
Subject: our raw data

Stu,

Attached is the raw data and notes for stuxnet. We didn't have time to format this into a report, and as I said before, Martin still has most of it in his head right now. There is a great deal of data in a Responder project file as well, but I didn't include that since I'm not sure your guys would know how to use that. We also made a REcon trace of it executing, but I didn't include that either. Those resources can both be made available if you think you can use them, but as I said you would need Responder PRO to make use of it, and even then it would be equivalent to taking another RE's IDA-Pro project and trying to understand it (that was a joke). In the raw notes I think you will find the timeline interesting. The encryption routines might be new information but I'm not sure. Martin told me that one of the rootkits had a project-name of 'guava' if I remember correctly, he didn't write that down in the notes. Some other things I learned that aren't written in the notes - the thing has robust RPC wrapping for all the functions - we reversed about 3/4ths of the Command/Control functions, these are called via RPC and spawned as a separate process before being called. The things has very robust exception handling around everything (overkill, you might say). We have found that it trojans one of the DLL's included in the step-7 controller package - it wraps this and redirects a bunch of calls that are made through this DLL. I have this in a Responder project as well, but not written up in a report. As for attribution, everything looks like it was developed on an English version of the dev studio platform.

I hope this helps, I regret we can't do more at this time, and I look forward to tackling a different and more interesting malware that we can work together on in the future.

-Greg