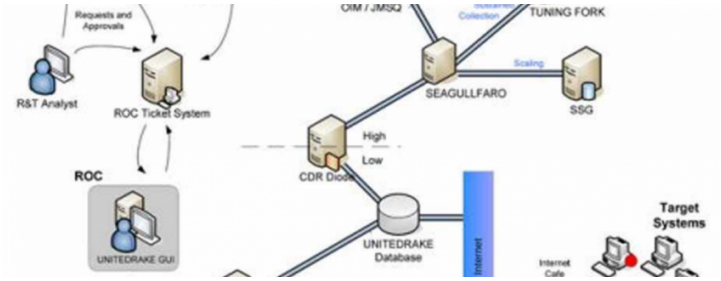
UNITEDRAKE AND HACKING UNDER FISA ORDERS



As I noted yesterday, along with the encrypted files you have to pay for, on September 6, Shadow Brokers released the manual for an NSA tool called UNITEDRAKE.

As Bruce Schneier points out, the tool has shown up in released documents on multiple occasions — in the catalog of TAO tools leaked by a second source (not Snowden) and released by Jacob Appelbaum, and in three other Snowden documents (one, two, three) talking about how the US hacks other computers, all of which first appeared in Der Spiegel's reporting (one, two, three). [Update: See ElectroSpaces comments about this Spiegel reporting and its source.]

The copy, as released, is a mess — it appears to have been altered by an open source graphics program and then re-saved as a PDF. Along with classification marks, the margins and the address for the company behind it appears to have been altered.

> © Contact Software, Inc.
> 12345 Main Street • Suite 100
> Phone 123.456.7890 • Fax 123.456.7890
> info@contactsw.com

The NSA is surely doing a comparison with the real manual (presumably as it existed at the time it may have been stolen) in an effort to understand how and why it got manipulated.

I suspect Shadow Brokers released it as a

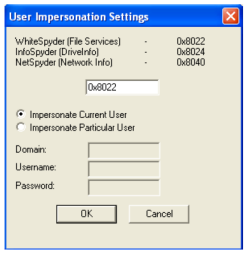
message to those pursuing him as much as to entice more Warez sales, for the observations I lay out below.

The tool permits NSA hackers to track and control implants, doing things like prioritizing collection, controlling when an implant calls back and how much data is collected at a given time, and destroying an implant and the associated UNITEDRAKE code (PDF 47 and following includes descriptions of these functions).

It includes doing things like impersonating the user of an implanted computer.

5.1.4. User Impersonation Field

This set of buttons allows the tasker to enable or disable UR's impersonation of a user on the client. This command is available in Client versions 4.3.6.21* and above. When you click the **Impersonation On** button, the following dialog appears:



User Impersonation is enabled / disabled on a per-plugin basis. The tasker must know the PluginID of the plugin he wishes to enable / disable. The dialog contains the pluginID of a few plugins likely to be used most often. If **Impersonate Current User** is selected, the specified plugin will attempt to use the token of the first user it finds logged on to perform all following commands. If **Impersonate Particular User** is selected, the tasker can specify the domain/username/password of a particular user. The plugin will see if the specified user is logged in, and if so, will use his token for all following commands. If the user is not logged in and the tasker specifies a password, the plugin will attempt to log on the user and use his credentials for all following commands. Impersonation for a particular plugin lasts

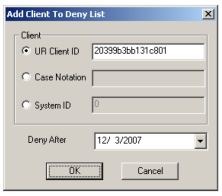
Depending on how dated this manual is, it may demonstrate that Shadow Brokers knows what ports the NSA will generally use to hack a target, and what code might be associated with an implant.

It also makes clear, at a time when the US is targeting Russia's use of botnets, that the NSA carries out its own sophisticated bot-facilitated collection.

Finally of particular interest to me, the manual shows that UNITEDRAKE can be used to hack targets of FISA orders.

When the **Set Client As Denied** command is activated, a dialog box is displayed allowing for selection based on the **UR Client ID** (unique identifier in hexadecimal format no leading "0x" required), **Case Notation**, or **System ID**. Selecting a client from the Target pane will automatically fill in these values. The **Deny After** date specifies when the server will start refusing connections from the client.

Figure 13: Add Client To Deny List dialog



The **Manage Collection Status** command is grayed out until the client is added to the Deny list. Selecting this command allows the operator to remove the client from the denied list or adjust the FISA expiration date.

To use it to target people under a FISA order, the NSA hacker would have to enter both the FISA order number and the date the FISA order expires. After that point, UNITEDRAKE will simply stop collecting off that implant.

Note, I believe that — at least in this deployment — these FISA orders would be strictly for use overseas. One of the previous references to UNITEDRAKE describes doing a USSID-18 check on location.

> SEPI analysts validate the target's identity and location (USSID-18 check), then provide a deployment list to Olympus operators to load a more sophisticated Trojan implant (currently OLYMPUS, future UNITEDRAKE).

That suggests this would be exclusively EO 12333 collection — or collection under FISA 704/705(b) orders.

But the way in which UNITEDRAKE is used with FISA is problematic. Note that it doesn't include a start date. So the NSA could collect data from before the period when the court permitted the government to spy on them. If an American were targeted only under Title I (permitting collection of data in motion, therefore prospective data), they'd automatically qualify for 705(b) targeting with Attorney General approval if they traveled overseas. Using UNITEDRAKE on — say, the laptop they brought with them — would allow the NSA to

exfiltrate historic data, effectively collecting on a person from a time when they weren't targeted under FISA. I believe this kind of temporal problem explains a lot of the recent problems NSA has had complying with 704/705(b) collection.

In any case, Shadow Brokers may or may not have UNITEDRAKE among the files he is selling. But what he has done by publishing this manual is tell the world a lot of details about how NSA uses implants to collect intelligence.

And very significantly for anyone who might be targeted by NSA hacking tools under FISA (including, presumably, him), he has also made it clear that with the click of a button, the NSA can pretend to be the person operating the computer. This *should* create real problems for using data hacked by NSA in criminal prosecutions.

Except, of course, especially given the provenance problems with this document, no defendant will ever be able to use it to challenge such hacking.