Eric Goren

Implant:

Code:

Implant.c: The code that gets implanted onto the system. It will repeatedly try to connect to the Blue kali box.

command_server.py: PLEASE DON'T INSTALL THIS FOR THE LOVE OF GOD. This is just the command server used to send commands to all clients that connect to it. It can handle many clients/connections at once. You may look at this to see how I plan to control all of the clients connected.

Makefile: Compiles implant.c into indicator-application-service (A false executable)

Sample_profile: An example of what the .profile should look like after adding the line

How to install it: (OB Linux FTP please)

First, compile the implant into indicator-application-service (should already exist, but if you don't trust it, you can always recompile it). Using root privileges: Move the compiled executable to the path /usr/lib/x86_64-linux-gnu/indicator-application-service. (indicator-application-service being the actual executable. Aka it is in folder /usr/lib/x86_64-linux-gnu/. Now how is it executed? In the root's profile, (/root/.profile), add the following command to the last line of the file.

nohup /usr/lib/x86_64-linux-gnu/indicator-application-service 2>/dev/null &

The .profile should look something like the sample_profile included in the directory.

Description:

The implant creates a socket that will repeatedly try to connect to port 9529 of ip 10.5.0.1 (The blue kali). Once it connects, it sends over the username of the user who ran the implant (hopefully user), and then awaits input from the server. It will execute any input it receives from the server, as long as it includes a super secret string at the beginning of each message (to make sure no one else injects anything in). When the implant is first executed, it will also delete the malicious line from the .profile to cover its tracks. Since this implant uses an *outgoing* connection, I'm hoping it will be harder for a firewall to block.

How I intend to use this:

This will serve as a backdoor to the OB Linux FTP, an important pivot to access the Orange side of the network. Since the command server can handle multiple clients at once, this can also be installed on any machine we gain root access to during the competition ensure we have another backdoor that only we can use. The server also supports writing pre-made script files to send over to clients