Practical Assignment 2

brbbot Malware Analysis

You are given a malware zip file on your Windows Desktop named `brbbot.zip` with zip password *malware*. You are also given a zipped file `brbconfig.tmp`. You have been told that this software was discovered in C:\WINDOWS\System32 on a machine that was displaying errant behavior.

You have until Monday 17 March at 11:55 PM to complete your assignment and turn in your report via Sakai.

I suggest you reserve three hour blocks for analysis of this malware and release your reservation (pressing the *I'm Done* button as soon as you are finished). Take screen shots, make good notes, record everything necessary for either your report or continued analysis in a later netlab session.

I strongly suggest you make a task list identifying all the steps you plan to take in your analysis in the order in which you take them.

Your report should take the following form:

1. Report Title Block

The report title block should include

a) Report title

b) Date of preparation

c) Your name

d) Your email address

e) Assignment and Class

2. Executive Summary

Briefly describe the purpose and behavior of this software providing a recap of all results noted below.

3. Basic Static Analysis

Check at least the following for the packed executable:

a) Report the MD5 hash of this executable?

b) Is the program packed? If so, what packer was used?

c) Identify the compilation date of the program.

d) Identify whether the program is a Windows GUI or Command-line program.

e) Identify any functions imported by the program.

f) Identify any relevant strings (ip addresses, urls, etc.).

g) Identify the program sections and their possible contents.

h) Use ResourceHacker to investigate resources (if any).

4. Basic Dynamic Analysis

Check at least the following:

a) To run this malware, install it in the C:\WINDOWS\System32 directory where it was found on the infected host. Document what programs you ran in what order to inspect its dynamic behavior. If you use RegShot, check the "scan dir1" check box so that you can identify any interesting file system activity as well as identifying registry changes.

b) Identify machines the malware attempts to contact. Using Wireshark, capture packets, find an http connection, and use the context menu to "Follow TCP Stream" so you can see what was transferred. Store the GET request parameters in a file on your REMnux host (using copy and paste) for later evaluation. You can edit this with either vi (really vim on REMnux) or Scite (more gui-ish). *All of you **must** know how to use vi. It is the mainstay of *unix systems*.

c) Identify any Registry Keys created/modified by the malware. What is the significance of any such changes?

d) Identify any files created/modified by the malware. What is their content?

5. Further Static and Dynamic Analysis

a) Unpack brbbot.exe. Feel free to use the unpacker (which is installed on your Windows host), but try to unpack it manually. (The tail jump for this packer happens just a little bit after a call to POPAD and before a sequence of 0 bytes.)

b) Identify any interesting strings and functions associated with the unpacked program. These include names of hosts on the internet and functions for file and registry operations as well as cryptography.

In particular, if the malware reads any files, identify which files it reads. (You can do this by setting a breakpoint at ReadFile and then selecting menu item View->Handles to find the hFile that is on the top of the stack just before the call to ReadFile.)

c) If the program decrypts any data using CryptDecrypt, step over the call to CryptDecrypt and look for the decrypted data in the stack. Record and report the decrypted data.

Data decrypted by the malware will identify a number of assignments to variables. Note these, especially any variables that might be associated with encodings and decodings. Try to determine what they mean.

d) Try to decrypt the string found in step 4b using xor decoding and the key identified in step 5c. You will need to turn the string into raw hexadecimal using the xxd program as follows:
`xxd -r -p source-file > destination-file`
And after that, you will need to use translate.py to perform xor decoding as follows:
`translate.py encoded decoded 'byte ^ 0xmn'`
where *mn* are the hexadecimal digits by which to xor each byte.

What is the significance of this string?

e) Assuming the decrypted file gives bindings of command names, specify what command might be issued back to the malware to execute notepad on the victim machine. If inetsym is not

running on your REMnux host, you can run the web server by issuing
httpd start
then you can store an ads.php file by echoing text into /var/www/ads.php.
Try to issue commands to the malware and report what occurs.
(You'll need to use the secret version of the commands identified in the string decrypted in step 5d.

f) Feel free to go beyond the scope of this assignment to identify more about the behavior of the program. Be specific about what you find.

6. Indicators

Identify both host-based indicators of infection and network behavior indicators that could be used by an IPS. Be specific. In particular explain how the file's md5 hash can be used as an indicator of either kind.