CIS2376 PRACTICAL

Week 16

Analysis

This week you are expected to use the *Reverse Engineering Toolkit* virtual machine to perform a behavioral analysis of some unknown malware sample.

1. First ensure that the *Handler Data* section of the *Malware Handling Checklist* has been correctly filled in. This checklist form needs to be handed in to your laboratory supervisor at the **end** of this week's practical session.

2. Add `sample1.zip` to your analysis machine. Remember that, without any exceptions, **all handling of malware** should occur via the **command line prompt**.

3. Unpack `sample1.zip` and fill in the *Malware Sample* section of the *Malware Handling Checklist.*

4. Open up a new DOS prompt and navigate to `C:\Program Files\Capture`. At this point, create a new snapshot of your virtual machine. We will regularly rollback to this snapshot as your analysis progresses. Prior to snapshotting your virtual machine, ensure your analysis machine's NIC is setup as follows:

   - its IP address is manually assigned to be `192.168.127.254/24` (don't worry about the gateway address)
   - the DNS server is set to be at `127.0.0.1`

5. Now, fill in one of the tables in the *Handling Checklist* section of the *Malware Handling Checklist.* Having filled the table in, execute:

   ```
   captureBAT -n -c >C:\output.txt
   ```

   This will capture OS changes and log them to `C:\output.txt`. In addition, any network data will be caught and dumped into a PCAP file in the logs subdirectory of the Capture folder.

   Now that your analysis environment is fully setup, execute your malware sample and interact with it a little (eg. enter your email address and password, then press signup).

   Once you've finished interacting with your malware sample, stop captureBAT and then analyze:

   - output.txt to see: what processes were created; registry entries interacted with; files that were created or referenced
   - the saved PCAP file to see what network interactions the malware sample was attempting to make

Once you've made a note of the information you've gathered on this analysis run, rollback your analysis machine to your previously saved snapshot.

6. Repeat the setup and documentation activities in 5. However, this time copy the specimen configuration data file to `C:\WINDOWS`. Ensure that you create a new snapshot of your analysis machine (on the following analysis runs, you will be reverting to this snapshot!). Run your malware sample again and see if you discover any new behavior.

   Again, once you've made a note of any information that you've gathered on this analysis run, rollback your analysis machine to your saved snapshot.

7. Repeat the setup and documentation activities in 5. However, this time use iDefences fake DNS to setup a DNS server that resolves all domain names to localhost (ie. `127.0.0.1`). Run your malware sample again and see if you discover any new behavior now that a DNS server is operational.

   Again, once you've made a note of any information that you've gathered on this analysis run, rollback your analysis machine to your saved snapshot.

8. Repeat the setup and documentation activities in 5. However, this time use iDefences fake DNS server and (should you think it necessary) its fake SMTP server (ie. Mailpot). Run your malware sample again and see if you discover any new behavior now that both a fake DNS and SMTP server are in place.

   Again, once you've made a note of any information that you've gathered on this analysis run, rollback your analysis machine to your saved snapshot.

Important Note: At the end of your practical session, ensure that your practical supervisor verifies that your analysis machine has been correctly cleansed of **all** software contaminants!

Questions

Use the data from your analysis to answer the following questions:

1. What network connections does your malware sample engage in?

2. Why did the CWSandbox report miss some of the samples network interactions?

3. How does the malware sample communicate information back to its control node?

4. Does the malware sample listen on any host machine ports for connections?

5. Beyond the presence of the malware sample within the filesystem, does the malware sample have any means to persist across host restarts?