Malware Analysis
Fall 2015
Lab 05 - Malware Behavior

Lab_05-1.malware

“””

Hey...it’s Shiela again. A few days ago I noticed that some emails that I had never read were being marked as read. I just figured my computer was being stupid and kicked it for punishment, that usually makes it work better...Anyway, I was doing some online shopping yesterday, and when I woke up today the bank called and said my credit cards were maxed out! I have no idea what’s going on, but Mr. Honcho wants you to make sure no-one else in the department is affected. Research is working on a way to make sure this sort of thing never happens again.

“””

1. (2 pts) What does the malware drop to disk?

2. (3 pts) How does the malware achieve persistence? Why does this make a great host-based signature?

3. (2 pts) How does the malware ensure more than one instance of itself isn’t running on the system at any given time?

4. (2 pts) Name 2 ways the malware tries to hide its presence from the user.

5. (2 pts) Name the 2 major WinAPI calls involved in enabling the key logging.

6. (3 pts) What are the names of the constants passed to each of these WinAPI calls?

7. (2 pts) What does the malware do with the collected data?

Lab_05-2.malware
“””

Unread Email (10/01/2015)

Dear HR Department,

It is with great honor that I present to you the results of our splendid Research Team’s valiant efforts at changing our small world. They have managed to devise a solution that will make it impossible for anymore keyloggers to steal our passwords or personal data! This ingenious creation of epic proportions shall surely lead the way to a future of success in our department.

Sincerely,
Mr. Honcho

Unread Email (10/02/2015)

Dear HR Department,

I have just fired out Research Team. I woke up this morning and found photoshopped pictures of my beautiful pug all over deviantart. You wouldn’t believe what they’re doing to poor Pugsy! These images were only on my personal myMist, so clearly their anti-keylogger scheme didn’t work! I’ve put IT up to making sure our computers are clear of this mess.

Regretfully,
Mr. Honcho
“””

1. (2 pts) Why does this sample use the internet? Where does it connect to?

2. (3 pts) How does the malware achieve persistence? Why does this make a great host-based signature?

3. (2 pts) Why is the second mutex necessary in this sample?

4. (1 pts) Briefly describe what SendMessage does.

5. (3 pts) What are the names and purposes of the 3 constants used (as the 2nd arg to SendMessage) by this sample?

6. (2 pts) How does this sample steal passwords? How does it differ from the last sample?

7. (2 pts) What does the malware do with the collected data?