Malware Analysis
Fall 2015
Lab 03 - Analyzing Windows Programs

Lab_03-1.malware
Shiela from marketing has been complaining about random popups. She claims she didn't do anything but we think she clicked on another "link" in her email again. Can you find out if we need to be worried?

1. (1 pts) Did you find any interesting resources? If so, how did you extract it?

2. (3 pts) List at least 3 imports or sets of imports. What is their purpose (from msdn), and how might the malware use them?

3. (3 pts) List at least 3 strings that stick out to you and describe how they might relate to malicious activity.

4. (3 pts) What persistence mechanism is used by this malware? What host-based signatures can you gather from this?

5. (2 pts) What is the CLSID served by this malware?

6. (2 pts) What is the name of the COM interface that this malware makes use of?

7. (2 pts) What two COM functions does this malware call from the above COM interface, and what are they used for? (hint: check the PMA book)

Lab_03-2.malware
The networking guys noticed a bunch of weird activity coming from a box on your network and had IT do an in-depth scan. This was the only file of interest, what can you tell us?

Basic Analysis
1. (1 pts) What is the md5sum? What of interest does VirusTotal Report?

2. (3 pts) List at least 3 imports or sets of imports you haven't seen before, what is their purpose (from msdn), and how might the malware use them.

3. (3 pts) List at least 3 strings that stick out to you and describe how they might relate to malicious activity.

4. (3 pts) What persistence mechanism is used by this malware? What host-based signatures can you gather from this?

Advanced Analysis
The networking guys gave you some more information about the traffic that tipped them off. They were able to extrapolate from the traffic and identify some functionality they want you to look into. Answer the following questions (5-8) for each of the functions identified by the networking team.

Identified functionality

- List processes, interactive remote shell, upload file (from infected machine)

5. (1 pts) What is the address of the subroutine that handles this functionality?

6. (1 pts) What is the command ID? It will help the networking guys group the traffic.

7. (1pts) Does the subroutine return anything to the attacker, if so, what?

8. (3 pts) Name 3 Windows API calls used and how they contribute to the functionality.
(send/recv don't count!)

9. (3 pts) Did the networking guys miss anything? Briefly name/describe 3 more functionalities offered by the malware. Provide the command IDs.