Malware Analysis
Fall 2015
Lab 01 - Basic Analysis

Lab_01-1.malware

1. (1 pts) When was this file compiled?

2. (6 pts) List a few imports or sets of imports and describe how the malware might use them.
    a.

    b.

    c.

3. (6 pts) What are a few strings that stick out to you and why?
    a.

    b.

    c.

4. (2 pts) What happens when you run this malware? Is it what you expected and why?

5. (2 pts) Name a procmon filter and why you used it.

6. (4 pts) Are there any host-based signatures? (Files, registry keys, processes or services, etc). If so, what are they?

7. (4 pts) Are there any network based signatures? (URLs, packet contents. etc) If so, what are they?

8. (1 pts) Is there anything that impeded your analysis? How so? How might you overcome this?

9. (2 pts) What do you think is the purpose of this malware?

Lab_01-2.malware

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

2. (6 pts) List a few imports or sets of imports and describe how the malware might use them.

    a.

    b.

    c.

3. (6 pts) What are a few strings that stick out to you and why?

    a.

    b.

    c.

4. (2 pts) What happens when you run this malware? Is it what you expected and why?

5. (2 pts) Name a procmon filter and why you used it.

6. (4 pts) Are there any host-based signatures? (Files, registry keys, processes or services, etc). If so, what are they?

7. (4 pts) Are there any network based signatures? (URLs, packet contents. etc) If so, what are they?

8. (1 pts) Is there anything that impeded your analysis? How so? How might you overcome this?

9. (2 pts) What do you think is the purpose of this malware?

Lab_01-3.malware

1. (3 pts) Are there any indications that this malware is packed? What are they? What is it packed with?

2. (1 pts) Are you able to unpack it? Why or why not?

3. (3 pts) What are a few strings that stick out to you and why?
    a.
    b.
    c.

4. (2 pts) What happens when you run this malware? Is it what you expected and why?

5. (2 pts) Are there any host-based signatures? (Files, registry keys, processes or services, etc). If so, what are they?

6. (4 pts) Are there any network based signatures? (URLs, packet contents. etc) If so, what are they?

7. (3 pts) Is there anything that impeded your analysis? How so? How might you overcome this?

8. (2 pts) What do you think is the purpose of this malware?