I. Project Objectives:

(1) Understand ransomwares as a network programs
(2) Learn essential software analysis tools (VirusTotal and CyberChef)
(3) Practice document/report preparing for summarizing your intellectual work

II. Project Narrative:

Ransomwares are a type of malwares currently on a rampage. In the recent years, a significant increase in the accrual cases of ransomwares has been reported. Most of the existing ransomwares are implemented as computer viruses for them to infect target hosts. As virtually all of the existing computer viruses are sophisticated network programs for performing initial infections, ransomwares also perform their reconnaissance activities, spreading themselves to other near-by hosts, and disable data assets of the victim users while minimizing their counter detections by fully utilizing networking resources on their targets.

In this project, we will analyze an actual script-based ransomware to learn their designs as a network program, as well as the typical ransomware program structure as a network program. By analyzing an actual ransomware, we will learn the essential networking concepts many ransomwares these days utilize using two analysis tools (VirusTotal [1] and CyberChef [2]) many security administrators and law-enforcement officers use for collecting evidences from cyber-threats from ransomwares.

III. Project Requirements:

(a) Conduct a preliminary research to understand what activities most of the existing ransomwares perform using search engines in the Internet.

(b) Using the knowledge you learned in the previous step (i.e., (a)), analyze a given script-based ransomware (in java script) using the two tools (VirusTotal and CyberChef). For example, the technical details you are expected to find are (but not limited to):

* Which network applications does the given ransomware target for infection?
* Why do you think the given ransomware targets the network applications (can you find any technical articles that explain the reason(s))?
* Which application-layer protocol(s) the given ransomware uses (and why that protocol)?
* Is there any particular transport-layer port the given ransomware uses (and why that transport-layer port)?
* Do you see any fixed parameter(s) the given ransomware use? Why does the given ransomware use the fixed parameter(s) – why can’t the given ransomware use variable parameter(s)?
* Does the given ransomware use any technique for evading “early detection”? If yes, what is it? How will it make hard to detect the given ransomware?
Does the given ransomware use any technique for minimizing the risk of the ransomware attacker(s) to be nailed down? If yes, what is it? How will it make hard to detect the given ransomware?

(c) Develop a report that:

1. Summarizes what you learned during (b) above.
2. Describes every single step performed by the given ransomware.
3. Understand what each activity is for what purpose(s).
4. Most of the existing ransomwares use some network communication schemes (i.e., what kind of network communication structure(s) they use to minimize the risk of the ransomware attackers to be caught by law-enforcement officials?).
5. Do you see anything unique in the given ransomware for this project, compared with those you learned in your preliminary study (those you learned during (a) above)? What is (are) they? Is (are) it a serious concern for the defender side? If yes, why? If not, why not?

IV. Grading:

For (a) in Section III (30 points):

- Show the references you think most useful for conducting (a) (create a list of the references).
- For each of the references above, write a half-page summary (12-point, single-line, Times font, the US-standard letter format)

For (c) in Section III (70 points):

- Section (1): 25 points (20 to 25 points for an excellent work (those exceeds the expectations, 10 to 19 points for a decent work, 1 to 9 points for lacking work)
- Section (2): 35 points (30 to 35 points for an excellent work (those exceeds the expectations, 20 to 29 points for a decent work, 1 to 19 points for lacking work)
- Section (3): 20 points (15 to 20 points for an excellent work (those exceeds the expectations, 10 to 15 points for a decent work, 1 to 9 points for lacking work)
- Section (4): 20 points (15 to 20 points for an excellent work (those exceeds the expectations, 10 to 15 points for a decent work, 1 to 9 points for lacking work)

References: