HW #6
COMP5370/6370
A. Skjellum, Instructor; A. Ravipati, TA
Assigned October 28, 2015
Due November 9, 2015 – 11:59pm

From the attached papers, give a write up of the following questions.

1. At the lowest levels of data gathering, what information did the investigators collect and what tool(s) did they use for that purpose?

2. How did they identify the malware (the Trojans) present in the infected computers?

3. How did the investigators discover the identities (meaning the IP addresses and the geographic locations) of the computers used as the command and control centers? Also, what role was played by the computers used as control centers and what role by the computers used as command centers?

4. What was the capability of the specific Trojan that played a large role in stealing information from the infected computers? How did this Trojan allow the humans to control the infected machines in real time?

5. Look up articles that explain the Trojan's components and capabilities and report on what you learn

6 (Grad required, Ugrad extra credit). Download the Trojan into a linux machine (where it will do no harm) and see what you can infer about its capabilities. Report on what you find out and compare with what you learned in problem #5.