**SI110 Introduction to Cyber Security AY12S**
**Technical Foundations**

**Name:** _____

**Alpha:** _____

Hand in a stapled, printed copy with your answers.

**Homework: /SI110/Cyber Operations/Malware**

1. The categories of virus, worm, and trojan horse have to do with how malware gets onto a host. They don't tell us anything about what bad things the malware does once it's there. One thing a virus/worm/trojan horse might do is install a *key logger*. Briefly describe what a key logger is, and how it could endanger information like credit card numbers and passwords.

2. Refer to the Duqu case study in the lecture notes:

a. Is it true that just reading email was enough to get the malware installed on your machine? Explain your answer!

b. Would Duqu be more accurately described as a *worm* or a *trojan horse*?

3. In the context of malware, what is a *Command and Control Server*?

4. Watch Mikko Hypponen's TED Talk (link below). Check the box to indicate you did so.

http://www.youtube.com/watch?v=cf3zxHuSM2Y

☐ By checking this, I verify that I watched the video in its entirety.

What claim to fame did the two Pakistani men that Mikko went to visit have?

Mikko decrypted an image file that contained an exploit which downloads a backdoor. In addition to discovering the actual website URL, Mikko found the string 0600K078RUS. What was the importance of this seemingly random string?