CS 491/591 Spring 2016 Lab 2

Due 11:59pm on Friday, 6 May 2016 – extensions will not be possible because I'm not supposed to have major assignments due during finals week as a matter of University policy.

Please send your submission for lab 1 as a single PDF attachment to an email to "crandall@cs.unm.edu". The subject of the email should contain both the strings "lab2" and "reclass". Do not submit your lab writeup to any other address, attach any files that are not the one single PDF, or put any part of your lab submission in the text body of the email. Include your name in the body of the email in case it's not obvious from your email address.

Your writeup should be in PDF format (no other formats will be accepted, especially not Microsoft Word).

In the reclass directory on the Dept. NFS mount, you'll find lab2.zip. The password to decrypt it is "cs591". **This is a real malware sample, not a toy example, so be extremely careful!**

You are expected to do your own work. From reverse engineering to modifications to writing the writeup, for all phases of this project you should do your own work. Any instance of not doing your own work will be considered cheating. For your writeup, if you copy even a single sentence from an existing source without clearly attributing it to the correct authors, that will be considered cheating. If you're not sure whether something will be considered cheating or not, ask me before you do it. You are encouraged to discuss the assignment with your classmates at a very high level only, *e.g.*, general strategies for reverse engineering that are not specific to this lab. Exchanging tools, source code that existed before the assignment was assigned, and thoughts about approaches to general problems is okay. **(Note that the wording is different than for Lab 1---In Lab 2 you're expected to work individually and only talk to each other in general ways that are not specific to the lab!)** As a reminder of the course policy, if you cheat on any assignment in this class including this assignment (cheating includes, but is not limited to, representing somebody else's work as your own or fabricating files to make it look like you completed the assignment) you will receive an F in the class. Using Google as much as possible is encouraged, but you need to confirm anything you learn *via* Google in your report by reverse engineering and verifying that any reported information you find is correct.

Your report should start with a summary paragraph, and then answer the following questions:

- What host-based indicators (HBIs) were you able to identify?
- What network-based indicators (NBIs) were you able to identify?
- How does the malware configure itself?
- What data encodings does it use?
- How does it communicate to the Command and Control (C2) server?
- How does it process the C2 commands?
- What different capabilities does it have?