# COSC 4340: Independent Study

Summer 2017, Course Outline

Justin Jones

Faculty Advisor: Dr. Narasimha Shashidhar

Preliminary:

- Learn ANSI C, utilizing *The C Programming Language*[1].
- Set-up analysis environment, gather malware samples.
- Research current anti-malware program functionalities (determining how exactly they accomplish their task).
- Determine additional malware samples to be analyzed.

Week 1: May 31st – June 2nd

- Complete static and dynamic analysis of !SATANA!
- Complete report section for !SATANA!
- Begin anti-malware software specification.

Week 2: June 5th – June 9th

- Complete static, dynamic analysis of 1 more piece of ransomware, TBD.
- Complete report section for (TBD).
- Continue anti-malware software specification.

Week 3: June 12th – June 16th

- Complete software specification.
- Begin software coding process.

Week 4: June 19th – June 23rd

- Determine the *Windows* operating system functionality needed to implement the engine.
- Determine the *Windows* operating system interaction calls/methods to use given a C/C++ environment.

Week 5: June 26th – June 30th

- Implement a rough, working engine prototype that will *stop* ransomware execution.

Week 6: July 3rd – July 7th

- Determine method for extracting program signatures
- Complete a working prototype engine that will also *prevent* ransomware execution.

Week 7: July 10th – July 14th

- Further refine anti-malware engine to boost usability, i.e. capable of targeting multiple pieces of malicious code given the signature.
- Begin design of a rough database system that will allow 'definition' updates.

[1] *http://bit.ly/2pXKxCV*

Week 8: July 17th – July 21st

- Database implementation.
- Program refinements (GUI if possible using Qt)
- Implement rough updating system.

Week 9: July 24th – July 28th

- Complete the malware software, capable of detecting, preventing and stopping attacks in progress given a signature and relevant system directories (where the malware keeps files, etc).
- Demonstrate working software on a test machine.

Week 10: July 31st – August 3rd

- Submit completed analysis report and antimalware program

Final deliverables:

1. A complete, working open-source antimalware program utilizing working definitions that can detect, prevent and stop attacks in progress.
2. A completed report detailing the analysis of two ransomware executables, and development processes and hurdles.

Additional information:

- Tools used: IDA Pro Free, OllyDbg, Cuckoo Sandbox, VMware ESXi, JetBrains CLion, LaTeX