COMP 4970/7720/7726
Software Re-Engineering
Summer 2018

Assignment:	Team Project
Objective:	To demonstrate reverse engineering skills acquired over the semester
Guidance	The attached file contains an actual malware sample collected off the Internet. Please analyze the sample and write a report addressing the following areas: • What is the general functionality of the sample? • What are the indicators that this sample is malicious? • How does this sample interact with the local system (e.g., system DLLs, files, etc.)? • What files and registry keys does this sample create, modify and access? • What is the network behavior (including hosts, domains and IP addresses accessed)? • What are the time and local system dependent features? • What is method and means by which this sample communicates to the external environment? • What is the original infection vector and propagation methodology? • What use does this sample make of encryption for storage, communication? • What self modifying or encrypted code does this sample employ? • What ancillary information is available concerning the development of this sample (compiler type, country of origin, author names/handles, etc.) Areas that are not applicable should be indicated as such on your report. The analysis and report should be accomplished in teams, which have been set up in Canvas. The executable for this assignment came from an educational reverse engineering malware site. While you can use Internet references to assist you in your reversing efforts, you are on your honor not to look up solutions to this specific executable.
Deliverables:	Please submit a report in .doc, .docx, .rtf, or .pdf format addressing the points above.

Rubric

Your project will be assessed based on the following guidelines:

SCORE LEVELS 90-100
Accurate, thorough, complete. Address all requisite areas. Supported by illustrated code/data excerpts of the binary. Demonstrates superior reverse engineering facility.

SCORE LEVELS 80-89
Accurate, complete. Lacks specificity in insubstantial areas. Reliant on narrative with relatively few illustrated excepts. Demonstrates competence.

SCORE LEVELS 70-79
Accurate. Lacks full analysis and/or specificity in substantial areas. Heavily reliant on narrative with few illustrated excepts. Demonstrates adequacy.

SCORE LEVELS 60-69
Exhibits inaccuracies in substantial areas. Analysis appears to be a veneer. Demonstrates acquaintance with reverse engineering.

SCORE LEVELS 1-59

Displays serious inaccuracies or is incomplete.

SCORE LEVEL 0

Portions of content are not original.