Malware Analysis Report 4
CSCI 4976 - Fall 2015
Malware Analysis

Overview

Your Advanced Cyber Intrusion Specialist Defense Team has just discovered a new APT presence on your network. You currently have no idea how for this infection has spread, and you need to find out fast. Eight different samples were identified on the network, and they may or may not be from a single APT. The team has been split into smaller groups that will each work on a single sample. Work with your group to analyze the sample, create a report, and give a presentation to bring the rest of the team up to speed on this new threat.

Be sure to identify the sample's key functionality, what it placed on or took from the network, how it persists on the network, and anything else you find. This information will be key in removing the APT from the network and determining and containing the damage.

Rubric

Below is the point breakdown for each of the major section we expect your report to include. You will be graded not only on the accuracy and quality of the technical content, but also on its presentation. Make the report pleasing to the eye, easy to follow, professional, and include screenshots (lots of them). The main idea is to document your analysis and then to make it presentable.

Pts	Title	Description
5	Executive Summary	Summary of the results of the analysis for upper-management. They can't read the rest of the document, so use this to make them understand what happened, if/why they should be worried, and non-technical specific course of action.
15	Basic Static Analysis	Document the results of each tool as you go through your analysis. Start making hypotheses about the functionality of the malware, and justify them with your findings.
15	Basic Dynamic Analysis	
20	Advanced Static Analysis	Make note of important subroutines and chunks of code, and their purpose. Which ones confirm or disprove any hypotheses you made during basic analysis?
20	Advanced Dynamic Analysis	Describe what you used the debugger for, any hurdles you faced, and walk through how you overcame them.
10	Summary / Conclusion	Draw conclusions from the results of your analysis and summarize them here.
15	Presentation	You will have <10 minutes to present your findings to the class. This should be a technical presentation. Do not just read your report; create slides and a prepare a demo, as if you were presenting at a conference.