Malware Analysis Report 1
CSCI 4976 - Fall 2015
Malware Analysis

Overview

You have been given a sample of malware by the head-honcho over at the Cyber Incident Response Operations Center over at Corporate HQ. His team wasn't able to determine anything from the sample using their Networking Fu, and he needs your help. Mr. Honcho heard that you were successful in a similar situation not long ago, and he has high hopes (and possibly a promotion) waiting for you if you do what he needs.

The sample was found on most of the computers over in the HR department. CIROC is unsure of where the sample originated from but they are guessing it was some chain email that Marketing thought was cute. The infection wasn't contained very well (if at all) and it made its way to some upper-level management over at HR. After hearing about the Target, Home Depot, and OPM Mr. Honcho is very concerned for the welfare of his company.

You must analyze the sample and create a detailed, professional report for Mr. Honcho and the rest of CIROC. Mr. Honcho isn't technical, so be sure to include an executive summary at the top. You must document your analysis process, your findings along the way, any stumbling blocks, and your conclusions. If a tool doesn't report anything interesting, you should still include it in your report. Mr. Honcho doesn't want any stones left unturned, and if you say he's safe he'd like to know why!

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-technically 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.
85	**Total**	