ABSTRACT

THESIS: Ransomware, A System-Centric Detection Approach

STUDENT: Brian R Cromis

DEGREE: Master of Science

COLLEGE: Sciences and Humanities

DATE: May 2017

PAGES: 59

There are three approaches taken to analyze defenses against ransomware: signature based patterns, similar to virus detection; observing execution behavior, such as deleting a large number of files and changing file types; and a data-centric method that watches for the changes to the contents of the victim's files. A fourth method currently being investigated focuses on the network connection used between the ransomware payload and its associated Command & Control server.

In order to fully understand ransomware's operation, researchers need to use dynamic analysis which has its own risks when dealing with known/unknown ransomware samples. Without the use of dynamic analysis, researchers are limited to static analysis of ransomware samples which can form the basis for some types of detection techniques. However, to test these techniques, these samples still require execution. Therefore, a fully dedicated system that would contain the sample's potential damage, a ransomware suite called SylverWare, was created to test ransomware samples.

With the SylverWare ransomware sample, the different detection approaches were studied. In each case, SylverWare was shown to be able to circumvent each detection method. It can be said that SylverWare is the Achilles' heel of ransomware detection.