UC - 30

Malware Analysis Using Reverse Engineering

INTRO/ABSTRACT

One of the biggest threats faced by companies is the infection of malware. New forms of malware are created daily and ever evolving to evade detection methods. During this project we will be using reverse engineering methods to better understand the functionality of malware, as well as how it eludes detection. Using this knowledge, we will create a set of security standards to help companies to protect themselves from these infections.

METHODS

We used the tools IDA Pro and WinDbg for the reverse engineering. We used VirtualBox for the virtual machine. We took our information from how malware eludes detection to better help a set of security policies.

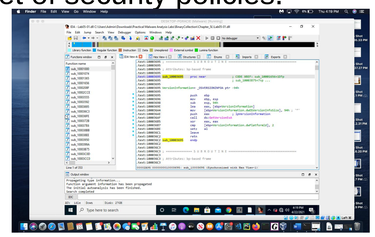

Fig.1 Is a function in the malware sample that is asking for the operating system of the host device.

RESULTS

Documentation on how malware eludes detection
Documentation on Analyzing Malware
Documentation on how to secure a Virtual Machine
A list of security policies for a business to implement

During this project we analyzed and documented the functionality of malware. Using this information, we created a set of security policies and documentation on how to secure a virtual machine.

SCAN ME

KENNESAW STATE UNIVERSITY
COLLEGE OF COMPUTING AND SOFTWARE ENGINEERING

Author(s): Will Pharr, Michael Lewis, Kelton Reid, Icyss Strong
Advisors(s): Hossain Shahriah