Evasive Behaviour for Malware in Linux

CS5231 System Security Project Proposal

Lee Kai Wen, Aloysius (A0154597N), Neo Ken Hong, Kelvin (A0154598M),  
Tay Zheng Yao, Schuyler (A0154604L), Tan Jia Le (A0159052H)

# Overview

There is a common misconception that malware does not exists for Linux machines. However, Linux malware have been on the rise in recent years due to the widespread adoption of Linux servers, Android smartphones and IoT devices. Many of these Linux malwares, such as keyloggers and cryptocurrency miners, adopt techniques to evade various forms detection. Such evasive actions include hiding network traffic, process creation and file existence.

This project aims to investigate the detection evasion techniques of a malware sample by analysing its execution and behaviour patterns.

# Goal

Understand techniques for evading detection of:

* Network traffic
* Process creation
* File existence
* Resource usage of
  + CPU
  + RAM
  + Disk

# Methodology

Analyse malware sample through reverse engineering and process monitoring.

Possibly develop a proof-of-concept of a stripped-down version of the evasion mechanic (KIV).

# Environment

## Test Machine

* x86\_64 Ubuntu Linux virtual machine

## Tools

* Binary Disassembly
  + Ghidra
  + Cutter
* Process monitoring and Function hooking
  + ProcMon
  + ftrace
* Network monitoring
  + Wireshark