Windows Forensics & Overview of Exploit Kits

Term Paper - Proposal

Presented By: Betrant Titus (AM.EN.P2CSN18006)

Introduction

Windows has been the most widely used operating system which makes it a popular attack vector and a platform for cyber-criminals to conduct malicious activities. Its widespread usage has also given it unnecessary attention in the manner of a smorgasbord of exploits against the core operating system and third-party applications that are intended for use with the said operating system. Thus, in this paper we try and run through a standardized triage procedure to recover digital evidence from a Windows 10 machine image, and in the process build a comprehensive database of locations of sensitive locations inside the operating system. We also discuss the possibility of utilizing custom-built filelists used for system maintenance for discovery of sensitive data, which aims to enhance the standardized approach with additional sensitive data gathered from third-party applications.

Exploit Kits are a curated collection of exploits which are integrated within a relatively user-friendly GUI which also includes payload delivery and execution, testing, exploit customization and weaponization in the same, making it easy for users without much technical knowledge to utilize these exploits to attack their intended targets. We attempt to gain an understanding of what these are, how they work and how we use one to launch an attack by running through an interactive session that weaponizes an exploit and launches an attack using a well-known exploit kit.

Aim

This term paper aims to do the following:

1. **Windows Forensics:** This paper attempts to provide an insight into how a typical forensics operation is carried out in a suspect/victim machine running Windows, and aims to generate maximal volume of digital evidence from a machine image of Windows 10.

2. **Exploit Kits:** This paper attempts to provide an overview of the basics of an exploit kit, and provide some exposure into the most relevant EKs present today, and also try to provide the practical knowledge of how an EK is used by demonstrating exploit creation and deployment using any of the well-known EKs such as ExploitPack, Angular, RIG etc.

Topics Covered

This term paper attempts to cover the following topics:

1. **Typical OS forensics procedure on Windows machines:** The standardized procedure that is used to perform post-mortem analysis of acquired Windows 10 images is glanced over and a database of locations from which sensitive data can be captured is built.

2. **Introduction to Windows Registry:** The Windows Registry is a hierarchical database that stores low-level settings for the Microsoft Windows operating system and for applications that opt to use the registry, and as such is a cornerstone of forensics operations on the Windows platform. We take a look at how registry forensics operations are handled and build a database for extraction of sensitive data from the Windows Registry too.

   a. **Overview of Windows Registry structure:** The hive structure and the components of each hive are discussed in an attempt to understand the Windows Registry from the perspective of digital evidence collection.

   b. **Extraction of sensitive Windows Registry keys:** We list and extract sensitive Windows Registry keys, building a database of such key locations in the process.

3. **Exploit Kits:** An exploit kit or exploit pack is a type of toolkit cybercriminals use to attack vulnerabilities in systems so they can distribute malware or perform other malicious activities. We try to understand EKs by doing the following:

   a. **Overview of Exploit Kits:** We take a quick overview of how a EK is structured alongside its mode of usage, and the common EKs available today, and compare the effectiveness of each in a comparative manner.

   b. **Demonstration of exploitation using Exploit Kit:** We visualize a live attack session using a popular exploit kit, which includes targeting a specific vulnerability, weaponizing and customizing the exploit code for the target, binding a payload and finally delivery and execution.

Research Plan

The term paper aims to bring a new method of discovery and extraction of sensitive data on a Windows machine by repurposing custom-built filelists which are primarily intended for system maintenance, which will be further discussed in the presentation.

- **Assumptions Made:** We assume that we are running recent copies of Windows 10 in the triage environment, and that a number of the applications mentioned in the lists we use are installed in the machines.
- **Related Work:** There are some attempts to use databases that pinpoint the location of data but all of them use sources that are built for evidence triage purposes only. We differ in the method that we are repurposing source-lists that are primarily intended for system maintenance in order to triage
- **Software required:** Forensic images for recent builds of Windows 10, preferably with a good number of third party applications installed and used.