Slovak University of Technology in Bratislava
Faculty of Informatics and Information Technologies

FIIT-XXXXXX-82385

Tomáš Belluš

Bait network based monitoring of malicious actors

Master thesis

Supervisor: Ing. Tibor Csóka, PhD.

May 2020

Slovak University of Technology in Bratislava
Faculty of Informatics and Information Technologies

FIIT-XXXXXX-82385

Tomáš Belluš

Bait network based monitoring of malicious actors

Master thesis

Study program: Information Security

Field of study: 9.2.4 Computer Engineering

Training workplace: Institute of Computer Engineering and Applied Informatics

Supervisor: Ing. Tibor Csóka, PhD.

May 2020

Contents

Chapter 1

Analysis

This chapter introduces and characterizes malware analysis techniques (see section 1.1), differentiates the analysis techniques (see subsection 1.1.1), outlines and describes mechanisms and environments utilized by cyber security professionals and companies (see subsection 1.1.2), describes the virtualization technology KVM (see subsection 1.2.1) and the orchestration mechanism Kubernetes (see subsection 1.2.2).

1.1 Malware analysis

1.1.1 Dynamic and static

1.1.2 Mechanisms and environments

1.1.2.1 Honeypot and honeynet

Honeypot is a bait service, system or a even whole network (honeynet) usually hosted on public server. Its main purpose is to be scanned, attacked or compromised by the malicious actor. Every honeypot provides the desired functionality of the target resource, to mimic the production environment, leaving the malicious actor unaware of the honeypot [1].

Based on the ENISA honeypot study [1], honeypots are classified from the level of interaction view and based on the attacked resource type. The Low Interaction Honeypot (LIH) provides very low availability of the host OS. Most services and application are mocked and simulated in a static environment. Everything accessible is controlled by a decoy application with absolutely minimal in-depth features (e.g. shell, configuration files, other programs etc.). LIHs are more secure for the host, but far less capable or useful for malware/attack detection and inspection.

On the contrary, High Interaction Honeypot (HIH) is a fully responsive system with live applications and services with minimal to none emulated functionalities. It provides the attacker a wide attack surface ranking the HIH far less secure with the whole OS at the malicious actor's disposal. The idea is to make HIHs believable as possible and isolating it from production environment including virtualization [2].

Honeypots are differentiated by the type of attacked resource. The server-side honeypot is the well-known honeypot with running service(s) and monitoring the activity of the server-side connections. The attacked resources are the services listening on the dedicated ports. It's main purpose is to detect and identify botnets and forced authentication/authorization attempts.

The client-side honeypot is deployed as a user application, which utilizes the server's services. The monitored subject is the application (e.g web-browser, document editor). It's main purpose is to detect client-side attacks originating from the application (i.e. web-browser attacks via web pages and plugins).

1.1.2.2 Sandbox

1.2 Virtualization technology

1.2.1 Kernel Virtual Machine

1.2.2 Kubernetes

Literature

[1] Tomasz Grudziecki et al. “Proactive Detection of Security Incidents - Honeypots”. enisa study. Nov. 2012. URL: https://www.enisa.europa.eu/publications/proactive-detection-of-security-incidents-II-honeypots.

[2] Lenny Zeltser. “5 Steps to Building a Malware Analysis Toolkit Using Free Tools”. SANS Institute instructor. Mar. 2015. URL: https://zeltser.com/build-malware-analysis-toolkit/#allocate-virtual-systems.