Adding STIX Support to the Volatility Memory Forensics Framework

Abstract

Digital forensics techniques are commonly used in the investigation of cyber-attacks and malware and to support criminal and civil litigation. While most traditional forensics techniques focus on the recovery of evidence from the non-volatile storage devices in computer systems (hard drives, USB thumb drives, etc.), modern malware often leaves no traces on these storage devices, rendering traditional approaches ineffective for detection and analysis of advanced malware. Memory forensics has emerged as a solution to this problem, but using current generation memory forensics tools requires significant experience and deep knowledge of operating systems' internals and malware. The goal of this project is to integrate a commonly used threat intelligence language into the Volatility memory forensics framework, to facilitate sharing memory forensics knowledge and to make the framework easier to use.

Problem Statement

The current generation of memory forensic tools presents significant usability barriers. The Structured Threat Information Expression language (STIX), maintained by the MITRE Corporation, has become the standard for representing cyber threat intelligence information, but STIX is difficult for investigators to use.

Approach

This project integrates STIX into the open-source Volatility Framework, the most widely used

memory forensics toolset. Investigators will be able to import and export information about malicious computer activity into Volatility to document investigations and generate easy-to-digest reports on malicious activity. We will also create a repository of publicly available STIX documents that target malware infection, including detailed STIX documents corresponding to modern malware infections. Separately, we will map STIX document components, detailed descriptions of malware samples, groups of malware attributable to a single actor, network activity, and descriptions of related files to Volatility plugins. Our Volatility/STIX integration framework will ingest and parse STIX documents describing a potential attack or attacks in detail, perform analysis on each aspect of the attack using Volatility plugins, and correlate and present the results as a report. This report will include confirmation of whether the associated attacks have occurred or been attempted, as well as valuable supporting evidence, such as names of suspicious processes, related files, registry data, command and control addresses, etc.

Anticipated Impact for DHS

Our framework will make the current generation memory forensics tools like Volatility more accessible to a wider group of investigators. It will also support sharing of investigative processes and outcomes among researchers and practitioners. This research will primarily serve Homeland Security Investigations (HSI) and the Cybersecurity & Infrastructure Security Agency (CISA). CINA will present research progress and results to HSI's Cybercrime Division, CISA's Cybersecurity Division, and the Joint Cyber Defense Collaborative.