Adding STIX Support to the Volatility Memory Forensics Framework

PI/s: Dr. Golden G. Richard III

PhD Student: Lauren Pace

Department: Division of Electrical and Computer Engineering, Center for Computation and Technology

Institution: Louisiana State University

Date: 3/21/2024

Criminal Investigations and Network Analysis
A DHS CENTER OF EXCELLENCE

GEORGE MASON UNIVERSITY

Agenda

1. Research Challenge
2. Project Introduction
3. Technical Approach
4. Application and Stakeholder Engagement
5. Transfer of Tech and Results
6. Questions

Research Challenge

Challenge - Make memory forensics techniques more accessible and facilitate sharing of investigative processes to strengthen memory forensics research and practices.

Research Question/s –

- How can STIX be used to document memory forensics investigations?
- How can STIX be integrated in Volatility?
- Is the existing STIX format robust enough to support this integration?
- Can a Volatility based investigation be driven by a STIX document?

Project Introduction

- Memory forensics allows for evidence to be acquired that would be lost in traditional “pull-the-plug” procedures
- Memory-only and file-less malware
- Time and experience is imperative in investigations
- Goal is to integrate STIX into Volatility to allow investigators to feed Volatility STIX documents and Volatility will run the plugins needed
- The output show the analysis steps our framework took
  - This has the potential to be used in training
- Report generated showing evidence supporting compromise on system

Technical Approach

- Create STIX documents that target malware infection
- Map STIX document components to Volatility plugins
- We have an extensive collection of memory images of infected and clean machines
- Team expertise

Application and Stakeholder Engagement

- Our STIX/Volatility integration can be used for investigations and training
- Automatically perform memory forensics investigations to reveal malware infection from STIX document
- Stakeholders – anyone local, state, or federal who are performing investigations that require memory forensics
- Our work will allow for more investigators to become trained in memory forensics

Transfer of Tech and Results

- STIX integration into Volatility will be open-source
- Sample STIX documents will be made public
- All documentation and code will be made public
- Publications to document and call attention to research

Questions

- Seeking recommendations for non-sensitive, accessible sources of STIX documents from investigators.
  - Few publicly available
  - Protected from public disclosure like YARA rules

- Open input from the DHS community
  - Interested in additional use cases
  - welcoming suggestions and guidance from the DHS audience.

Questions?

Dr. Golden G. Richard III, Professor of Computer Science: golden@cct.lsu.edu

Lauren Pace, PhD Student: lpace9@lsu.edu

Dr. Brook Hefright, CINA Director: bhefrigh@gmu.edu

Jamie Lee, CINA Project Manager: jlee397@gmu.edu

Criminal Investigations and Network Analysis
A DHS CENTER OF EXCELLENCE

GEORGE MASON UNIVERSITY

BACKUP SLIDES

Criminal Investigations and Network Analysis
A DHS CENTER OF EXCELLENCE

GEORGE MASON UNIVERSITY

Project Alignment to the DHS Strategic Plan

Goal 3: **Secure Cyberspace and Critical Infrastructure**

- **Objectives:** 3.2 & 3.4:

Sub-Objectives:

- **3.2.1** – Identify gaps and prioritize solutions for current national risk management efforts
- **3.2.3** – Collect and share threat indicators and other cybersecurity intelligence and information
- **3.4.1** – Investigate cybercrimes targeting individuals, private organizations, and publish interests consistent with DHS authorities and core homeland security investigative responsibilities
- **3.4.2** – Engage in joint or collaborative investigation and provide voluntary cyber investigative assistance to law enforcement partners nationwide and globally as appropriate
- **3.4.3** –Share information and best practices with stakeholders to prevent and disrupt criminal schemes involving cyberspace

CINA Research Areas

Criminal Network Analysis and Predictive Modeling

- Illicit Gold from Peru and Colombia: Understanding the Trade, Routes, and U.S. Linkages
- Exploring Graph Neural Networks for Attributed Multilayer Criminal Network Analysis
- Graph Analytics and Visualization for Criminal Network Identification
- Location Data Analytics and Visualization for Criminal Network Identification
- Cross-platforms Cybercrime Detection on Inter-connected Heterogeneous Networks
- *Detecting Criminal Disruption of Supply Chains Study*

Analysis of Dynamic Patterns of Criminal Activity

- Innovative Spatiotemporal Pattern Detection: Examining Changes in Crime Hot Spots Across 6 U.S. Cities
- Understanding the Economy and Social Organization of the Underground Market for Cybercrime as a Service
- Effects of Natural Disasters on Spatio-Temporal Patterns of Crime Types in the United States
- The Emergence and Diffusion of Illicit Virtual Goods across the International Cybercrime Ecosystem

Traditional and Digital Forensics

- Identity Sciences Interdisciplinary Research
- Digital Holographic Acquisition, Storage, Retrieval and Analysis of Three-Dimensional Fingermarks Developed with the Nanoscale Columnar-Thin-Film Technique
- A machine learning-based approach to analyzing and triaging encrypted data containers in law enforcement applications
- Digital Forensic Investigations involving Cryptocurrency Wallets Installed on Mobile Devices
- Data Science-integrated Experiential Digital Forensics Training based on Real-world Case Studies of Cybercrime Artifacts
- Digital Forensic Tools & Techniques for Investigating Control Logic Attacks in Industrial Control Systems
- Agent-Based Learning to Utilize Local Surveillance Data for Activity Recognition

Improving Criminal Investigative Processes

- Overcoming Reluctance and Increasing Intelligence Gathering from Victims of Trafficking
- Training on Intelligence and Evidence Gathering in Darknet Environments
- Is There Money Laundering in Cryptocurrency Markets?
- Time Series Analysis of Anonymized Communication Channels
- Detection of Illicit Massage Businesses through Spatial and Socio-Demographic Data Enrichment
- The Next Battlefield: Illicit Markets Hosted on Encrypted Communication Platforms
- An Architectural Model for Web-Based Technologies to Enhance Text-Image Capabilities in Detecting Sex Trafficking Cases
- *Evaluate Current NCFI Course Offerings and Develop Recommendations for Prerequisites and Post Curriculum Evaluations*
- *NCFI Curriculum Development*

Criminal Investigations and Network Analysis
A DHS CENTER OF EXCELLENCE

GEORGE MASON UNIVERSITY