Cyber Operations, Defence and Forensics

William Bradley Glisson
Louisiana Tech University
glisson@latech.edu

George Grispos
University of Nebraska at Omaha
ggrispos@unomaha.edu

Todd McDonald
University of South Alabama,
jtmcdonald@southalabama.edu

Abstract

As technology integrates into all aspects of life, cyber operations, defenses, and digital forensics resolutions intensify in importance. The escalation necessitates the development of innovative real-world managerial, technological, and strategic analysis solutions. Hence, this mini-track presents research that addresses these needs. The papers in the mini-track investigate the 'Security Operations Centers: A Holistic View on Problems and Solutions'; 'Lantern to the Underworld - Following User Actions Using Bing URL Parameters When Child Exploitation Terms Are Suggested by the Search Engine' and 'HESPIDS: A Hierarchical and Extensible System for Process Injection Detection using Sysmon.' The contributions presented in these papers highlight the escalating need for cyber operations, defense, and forensics research.

1. Introduction

The constant evolution of technology demands creative, out-of-the-box administrative, scientific, and tactical solutions to secure and investigate digitalized societies. This mini-track is dedicated to reporting advancements that focus on these emerging and critically important topics. Each paper submission went through a rigorous peer-review process. A summary of each paper is provided below.

2. Security Operations Centers

The paper 'Security Operations Centers: A Holistic View on Problems and Solutions' presents a literature review that focuses on identifying current and ongoing challenges that security operation centers face in today's highly connected world [1]. More specifically, the authors examine operations and layout, as well as challenges that include staffing issues, automation, tool integration, and leveraging machine learning in security operations centers.

3. Lantern to the Underworld

In the paper, the 'Lantern to the Underworld - Following User Actions Using Bing URL Parameters When Child Exploitation Terms Are Suggested by the Search Engine' presents an approach for tracing user activity through Bing URL parameters based on a documented case overseen by the authors [2].

The authors use a virtual reenactment of the case to demonstrate the value of the approach. They have developed a tool creating as output a timeline of probable search events. This case shows how the offender can start with a generic search term and reach CEM without typing the specific search terms. The reenactment chronicles actions that are either directly typed searches, user clicks, or suggestion-based clicks.

4. A Hierarchical and Extensible System for Process Injection Detection using Sysmon

Advanced persistent threats continue to escalate in today's networked world. Couple this with living-off-the-land cyberattack techniques that are implemented to avoid detection, and the problem space becomes more complicated. Hence, the authors of 'HESPIDS: A Hierarchical and Extensible System for Process Injection Detection using Sysmon' present a hierarchical graph-based detection tool to capture several different process injection attacks. Furthermore, the tool allows for the specification of different graphs to handle different attacks [3].

5. Research roadmap

The papers presented in this mini-track contribute to addressing challenges in Cyber Operations, Defence, and Forensics. However, numerous research challenges remain in these evolving areas.

URI: https://hdl.handle.net/10125/80246
978-0-9981331-5-7

Future research in these areas includes technology investigations, technical integration, solution impact, and the abuse of technology through attacks, along with the practical analysis and evaluation of proposed solutions. Hence, identifying and validating technical solutions to secure data from new and emerging technologies, investigating the impact that these solutions have on the industry, and understanding how technologies can be abused are crucial to the viability of commercial, government, and legal communities.

7. References

[1] Shutock, M. and G. Dietrich. *Security Operations Centers: A Holistic View on Problems and Solutions*. in *55th Hawaii International Conference on System Sciences*. 2022. Hawaii: Hawaii International Conference on System Sciences.

[2] Spear, N., D. Hawbecker, and B. McElyea. *Lantern to the Underworld - Following User Actions Using Bing URL Parameters When Child Exploitation Terms Are Suggested by the Search Engine*. in *55th Hawaii International Conference on System Sciences*. 2022. Hawaii: Hawaii International Conference on System Sciences.

[3] Thomas, R., S. Steiner, and D.C.d. Leon. *HESPIDS: A Hierarchical and Extensible System for Process Injection Detection using Sysmon*. in *55th Hawaii International Conference on System Sciences*. 2022. Hawaii: 55th Hawaii International Conference on System Sciences.