Technical CTI Workshop

Paralus LLC

paralus.co

Course Overview

The Paralus Technical Cyber Threat Intelligence (CTI) Workshop is designed as a highly interactive, hands-on training exercise. Taking theoretical concepts from the Paralus Operational Threat Intelligence Course, attendees will perform technical analysis of recent samples or artifacts as well as utilize available resources for further enrichment and sample identification.

Course Schedule

The Workshop is broken into five, two-hour sessions roughly covering the following topics:

- Session One: Network Infrastructure Hunting
    - Discussion of what makes up a domain, an IP address, and a SSL/TLS certificate
    - Identifying malicious network infrastructure
    - Hunting and pivoting techniques
    - DomainTools Iris walkthrough
- Session Two: Malicious Document Files and Droppers
    - Malicious document types and delivery mechanisms
    - Understanding macros
    - Understanding template injection
    - Understanding ActiveX objects
    - Parsing and analyzing files
- Session Three: Malware Analysis
    - PE file types: EXE and DLL
    - Initial static analysis and file examination
    - Controlled malware execution
- Session Four: Hunting and Pivoting
    - Identifying samples and characteristics
    - Leveraging tools and resources for further identification
    - VirusTotal query walkthrough
- Session Five: Detections and Rule Creation
    - Introduction to YARA
    - Differentiating between YARA rule types
    - VirusTotal-specific YARA possibilities
    - Background into Network Security Monitoring (NSM) rule concepts

Course Technical Requirements

- Computer with virtualization software (VMWare, VirtualBox, etc.) capable of capturing snapshots.
    - Windows Virtual Machine (7 or 10) with the following tools installed:
        - Windows Sysinternals suite (https://docs.microsoft.com/en-us/sysinternals/), at minimum Process Monitor (ProcMon) and System Monitor (SysMon).
        - FakeNet (https://github.com/fireeye/flare-fakenet-ng)
    - Linux Virtual Machine, either Remnux (https://remnux.org/) or with the following tools installed:
        - PE Analyzer script (https://github.com/serrastusbear/PE_Analyzer)
        - OLETools (https://www.decalage.info/python/oletools)
- Access to the following tools is preferable, but not necessary:
    - VirusTotal Intelligence
    - DomainTools Iris
    - Censys.io
    - Urlscan.io

Course Author & Instructor

Joe Slowik has emphasized the operational significance of threat intelligence through multiple roles: through leading intelligence and detection teams at Gigamon and Huntress; as an industrial control system (ICS) focused analyst for Dragos; leading the incident response team at Los Alamos National Laboratory; and serving as a Cryptologic Warfare Officer in the U.S. Navy. Ultimately Joe seeks to focus cyber threat intelligence as providing actionable, relevant guidance to day-to-day security operations to ensure robust, adaptable defense.

In addition to his work at Dragos and at Paralus, Joe also writes extensively on his website, Pylos. Joe is a frequent speaker and author of multiple papers covering threat intelligence and ICS concepts.