Project Charter v1.0

Blue-Team Intelligence Capstone

Kyle Hathaway

Malvertising Intelligence and Detection Design

Repository: kylehathaway-champlain/Capstone

Contents

Background and Problem

Malvertising, sponsored search ads leading to look-alike sites, is a common initial access path for attackers and ransomware. Small businesses typically don't have the time, staff, or processes needed to take publicly available information and turn it into reliable detection rules.

Earlier versions of the project had the goal of implementing a fully validated detection pipeline. Changes to the lab environment made reliable detection testing and ATT&CK based analysis inaccessible. This final version changes the scope of the project to the design and documentation of OSINT driven detections, with a focus on accuracy and transparency over completeness.

Project Goal

To develop a reproducible blue-team intelligence workflow that demonstrates how OSINT can be converted into detection logic.

Objectives

1. Build a home security lab.
2. Conduct an OSINT investigation.
3. Identify and document Indicators of Compromise from the OSINT investigation.
4. Build detection rules based on the IOCs from the OSINT investigation.
5. Document expected behavior and limitations.
6. Present everything in a GitHub repository for review.

Scope

In scope:

- OSINT investigation.
- Collection and documentation of IOCs.
- Design and documentation of detection rules.
- Documentation justifying why live detection testing was not possible.

Out of Scope:

- MITRE ATT&CK mapping.
- Live execution of detection rules.
- Active assessment of live threat infrastructure.
- Internet wide scanning.
- Production security deployment.

Architecture

Network Devices: Cisco ASA firewall, Aruba switch.

Analysis Platform: Security Onion VM.

Endpoints: Two Windows 10 Hosts, 3 Windows 10 VMs.

Milestones

Milestone A at the end of week three consists of Security Onion spun up, an OSINT case selected, a screenshot of the GitHub repository, and network configuration files.

Milestone B at the end of week six consists of completing OSINT investigations and creating one rule.

Milestone C at the end of week nine consists of one sim executed, rule tuned, and an OSINT intelligence brief in the finalization stage.

Milestone D at the end of week twelve consists of the final package write-up and a complete GitHub repository.

Risks & Mitigations

The risk of scope creep will be managed by keeping the OSINT investigation to a single campaign, a single sim, and a single detection rule. Keeping the log ingestion to the ASA, switch, and Windows events. Passive OSINT only. No execution of unknown binaries. Use VM snapshots and harmless payloads for simulation.

Reporting

Reporting will consist of progress reports with digital evidence. Digital evidence will be screenshots, IOCs.csv, rule files, and config files.