Malvertising: A Small SOC Implementation

CMIT-450-80: Senior Seminar Project

Instructor Michael Atwood

Kyle Hathaway

11.2.2025

Contents

Introduction

This project's goal is to build a home SOC lab using an Aruba switch, Cisco ASA, two host machines, Security Onion running in a VM, and three Windows 10 VMs. In this environment, I will ingest logs from the various sources into Security Onion. Additionally, I will conduct an OSINT research on a malvertising campaign, creating an intelligence brief with ATT&CK mapping and IOC tables. The OSINT investigation will be used to develop three detection rules and test them in simulations within the lab.

The product of this project will be a thorough and reproducible Blue Team package utilizing OSINT investigation to create detections, along with a demonstration featuring a timed incident drill in a home SOC lab. Deliverables for this project will be an OSINT intelligence brief on WinSCP malvertising with IOC tables and MITRE ATT&CK mapping. A detection pack of three rules created from the brief. A SOC evidence bundle consisting of configs and dashboards. An incident response playbook and timed drill report. All of this will be presented in a GitHub repository with a reproducible README.

Timeline

Week 3

- SOC Lab: Create repo, draft network diagram, spin up Security Onion and VMs, capture ASA baseline config.
- OSINT: Select a case and write the research question.
- Digital Evidence: Charter PDF, repo tree screenshot, network diagram, and ASA baseline config.

Week 4

- SOC Lab: Finish Security Onion config, enable Zeek/Suricata, configure ASA syslog, set up Aruba SPAN, and confirm first logs.
- OSINT: Start collection using URLScan, Virustotal, WHOIS, and create IOC>csv v0.1.
- Digital Evidence: Security Onion dashboard screenshots, Zeek/Suricata events.

Week 5

- SOC Lab: Spin up Windows VMs, forward security, and PowerShell logs.
- OSINT: Draft ATT&CK techniques list.
- Digital Evidence: Event ID samples,

Week 6

- SOC Lab: Finalize three simulations tied to the case.
- OSINT: Complete collection, draft methods, and findings sections.
- Digital Evidence: Simulation design document.

Week 7

- SOC Lab: Execute simulation #1, verify artifacts, and capture timestamps for MTTD.
- OSINT: Expand IOC tables.
- Digital Evidence: PCAP, Suricata alert detail, IOC.csv v0.2.

Week 8

- SOC Lab: Execute simulation #2. Create the first rule, begin building the FP/TP matrix.
- OSINT: Draft ATT&CK mapping.
- Digital Evidence: Rule v0.1 file, FP/TP matrix v0.1.

Week 9

- SOC Lab: Execute simulation #3, create rules two and three. Start the incident response runbook.
- OSINT: Continue to work on intel brief.
- Digital Evidence: Rules v0.2-0.3, runbook draft.

Week 10

- SOC Lab: Consolidate triage dashboards.
- OSINT: Finalize the intel brief.
- Digital Evidence: OSINT PDF v1.0.

Week 11

- SOC Lab: Drill rehearsal across all simulations, time triage steps for MTTR.
- OSINT: Publish IOC.csv v1.0 in repo.
- Digital Evidence: Simulation rehearsal notes.

Week 12

- SOC Lab: Formal timed drill.
- OSINT: Post-mortem on what intel improved and remaining gaps.
- Digital Evidence: Formal drill document.

Week 13

- SOC Lab: Export rules, dashboards, and runbook.
- OSINT: Polish report.
- Digital Evidence: Rules v1.0. README, screenshots.

Week 14

- SOC Lab: Final time for tweaks, notes.
- OSINT: Final polish.
- Digital Evidence: Submission includes an executive one-pager, an OSINT brief, an IOC.csv, a detection pack, an FP/TP matrix, Security Onion dashboard screenshots, an incident response runbook and drill timing table, and a repo README.

Summary

This project, as I have designed it, seems to be larger than I have time or the knowledge to tackle in a reasonable manner. Every step I have taken has been a struggle. Going into this project, I knew that for most of the parts I would be working on, I had no practical knowledge of how to get them done, but I thought it wouldn't be as challenging as it has been. I am quite frustrated with my progress and inability to meet my deadlines. I will have to adjust the deliverables because I cannot extend the deadline. I have some ideas as to what that will look like. But I haven't made any decisions yet. That is mostly because, as I get closer to the end of the project, I am unclear on exactly what the final product will look like.

Putting the struggles I am facing aside, the project itself is coming along, albeit at a pace that I am not happy with. I have completed the second OSINT investigation, which is more focused and coherent. I think that I have gathered interesting examples of malvertising. These malicious sites masquerade as legitimate sites that serve common IT utilities, like WinSCP, Putty, and AnyDesk. I learned a significant amount during the course of both of my OSINT investigations, and I am happy with how the process went.

I built an IOC table using the data gathered from the OSINT investigation. From that, I have a stack of potential detection rules to implement in Security Onion. I haven't included any in this report as I am unsure if any will work, as I am still trying to understand how I need to format them for Security Onion. Looking ahead to the weekend, I would like to get one detection in and tested.

Evidence

The evidence this week will consist of my second and more coherent OSINT investigation, along with an appendix with screenshots of the evidence gathered. I have also included my IOC table.

Conclusion

In the next two weeks, I want to get as close to a bare bones completion of this project. I want to leave enough time to polish it up a bit and stretch to get some of those deliverables that are feeling a bit far off right now. If I cut the detections down to one and remove the timed drill from the deliverables, I believe I can still produce a well-rounded project. Ultimately, this whole project has been incredibly challenging but I have learned so much a long the way.