Malvertising: A Small SOC Implementation

CMIT-450-80: Senior Seminar Project

Instructor Michael Atwood

Kyle Hathaway

12.11.2025

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 a detection and test it in a lab simulation.

The product of this project will be an attempt at an example of a 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 malvertising with an IOC table. With one detection rule created from the brief. A SOC evidence bundle consisting of configs and dashboards. All of this will be presented in a GitHub repository with a 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: Working through the initial OSINT and beginning a more refined second investigation.
- Digital Evidence: OSINT v1.

Week 7

- SOC Lab: Finish SOC lab.
- OSINT: Work on the second OSINT investigation and begin building the IOC table.
- Digital Evidence: OSINT v2, IOC.csv v1.

Week 8

- OSINT: Draft OSINT v2.
- Digital Evidence: OSINT v2.

Week 9

- OSINT: Continue to work on intel brief.
- Digital Evidence: OSINT v2.

Week 10

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

Week 11

- SOC Lab: Troubleshoot issues with the SOC lab.
- OSINT: Publish IOC.csv v1.0 in repo.
- Digital Evidence: GitHub.

Week 12

- SOC Lab: Begin detection rule testing.
- Digital Evidence: Detection rule screenshots.

Week 13

- OSINT: Polish report.
- Digital Evidence: Complete readmes.

Week 14

- SOC Lab: Final time for tweaks, notes.
- OSINT: Final polish.
- Digital Evidence: Filled out GitHub repository containing all evidence

Lab Construction

The construction of the lab consisted of scavenged components. The Cisco firewall, Aruba switch, and mini desktops were all gathered from devices that were scheduled for recycling. I began to prep the environment by resetting the firewall and switching to factory settings, wiping whatever configuration their previous users had. I did the same with the host mini desktops. I loaded Windows 10 on them. On each machine, I had to check whether they were set to run Hyper-V, as that's what I would use to run virtual machines in the environment.

After getting the basic network up, I began to spin up virtual machines. The three Windows 10 virtual machines on Host 2 came up without issue. Spinning up Security Onion on Host 1 was a struggle. There were a couple of physical limitations that I hadn't accounted for. The device would need two network interfaces. Luckily, I found an Ethernet-to-USB adapter that worked for my needs. The other limitation was that the device didn't have enough RAM to run Security Onion. Digging through my spare parts, I found a RAM stick that I could add to the device.

Spinning up Security Onion was a challenge as well. I went through the installation multiple times. Each time, I learned something new in the process. A few key points in the setup are to define which NIC is going to monitor the network and to define at which IP address the management dashboard can be reached. Once Security Onion was installed, I was able to access the management dashboard at the specified IP. To finish out the lab buildout, I assigned each device a static IP and constructed a network diagram. This helped me have a better visual of how my network was laid out.

OSINT Investigation

My initial OSINT investigation was more exploratory than anything else. I had to discover what sort of tools were at my disposal and which, if any, of them were going to be helpful. In the initial investigation, I began to learn what to look for, how to construct queries, and how to structure what I found. I wasn't sure what I was going to need to document what I found, and I wasn't sure what was going to be necessary for the rule design.

My second OSINT investigation had more direction and purpose. I found ways to use the tools better. I found three domains that fit what I was looking for. They were impersonating legitimate sites that serve IT support tools. These downloads gave the desired software, but also malware. By impersonating common tools used in IT, the attackers were trying to increase the odds that their malware ended up on more desirable endpoints. I was able to document several Indicators of Compromise, and I figured I would be able to use them to build detection rules.

Complications

Toward the mid-semester mark, I experienced a power failure in the lab. I had to rebuild the lab at this point, as I couldn't get anything to communicate with each other. As the weeks went on, the failure happened a few more times. After the last time, I was not able to reestablish the connection, internal or external. At this point, I needed to rescope the project. Between the issues in the lab and my own time constraints, I was going to be able to reach the goals I set out to achieve. I shifted from trying to do a full validation of detection rules in the lab to just building out some plausible rules.

Rules

The rules were the simplest ones I could think of creating. The first one alerts on a DNS query attempting to resolve the malicious domain. The other alerts on outbound traffic to the malicious IP address. These were never able to be tested in the lab, but their creation is based directly on data found in the OSINT investigation. After scaling back the project, building detection rules based on the OISNT was the goal.

Conclusion

This project didn't turn out how I thought it would. It ended up being much harder to work through than I imagined. I learned a lot about myself. One of my biggest takeaways is that I make a lot of assumptions about how something's going to go. This may have served me well in my previous career, where I had a lot of experience, but right now it doesn't serve me well because I don't know what I am doing, and assuming that everything is going to go smoothly is only setting myself up for failure. The other lesson I learned was that I greatly overestimated how much I would be able to do each week. My project would have been hard to pull off even if everything had gone according to plan. In building out a timeline for a project, I need to leave more room for things to change or go wrong.

Despite all of the challenges, I learned a lot along the way, and I really enjoyed my project. This idea was something I had been thinking about for a while, and I am glad I had an excuse to attempt it. I had hoped to validate my detections and build out a whole playbook to create a full Blue Team Intelligence loop, but it was more than I could handle in the time I had available. I will keep the lab up, and I'll see if I can fix the network in the new year.