Project Charter

Blue-Team Intelligence Capstone

Student: Kyle Hathaway

Working Title: Malvertising: A Small SOC Implementation

Repository: kylehathaway-champlain/capstone

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 a playbook to turn OSINT into detections and a response drill.

Goal

A thorough and reproducible blue team package using OSINT investigation to create detections and a demonstration with 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.

Objectives

The objectives of this project are to deploy Security Onion and ingest logs from a Cisco ASA, an Aruba switch, and Windows 10 machines. Collect IOCs for one malvertising campaign and build a timeline and ATT&CK mapping. Implement three detections and confirm them with three controlled simulations. Run a timed drill and achieve detection and response metrics.

Scope

In scope for this project is ingesting logs from the Aruba switch, Cisco ASA firewall, and Windows event logs from the Windows 10 machines into Security Onion. One OSINT case investigation and three simulations. Authoring and tuning three rules with a small FP/TP matrix

Out or scope for this project is internet scanning, engaging with live threat infrastructure, production EDR rollout, and multi-brand campaigns.

Architecture

- Network: Aruba switch, Cisco ASA.
- Sensor: Security Onion.
- Hosts: Two Windows 10 machines and three Windows 10 VMs.

Milestones

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

Milestone B at the end of week six consists of two sims executed, one rule created, and OSINT intelligence 50% completed.

Milestone C at the end of week nine consists of all sims executed, rules 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 completed GitHub repository.

Risks & Mitigations

The risk of scope creep will be managed by keeping the OSINT investigation to one campaign, three sims, and three detection rules. 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 weekly progress reports with digital evidence. Digital evidence will be screenshots, IOCs.csv, rule files, FP/TP tables, PCAP files and config files.