Threat Intelligence Report

Project Overview

This report documents the practical implementation of threat intelligence principles.

The project is divided into three main sections:

1. Analysis of Indicators of Compromise (IoCs): Identification, analysis, and detection methods for two specific IoCs.
2. OpenCTI Threat Intelligence Platform Implementation: Setup and configuration of the platform using Docker or system installation, including the integration of two connectors.
3. Demonstration of Platform Usage: A walkthrough of basic platform functionality with supporting evidence.

Section 1: Indicators of Compromise (IoCs) Analysis

IoC 1: "LOWBALL" Malware

- Description: LOWBALL is a malware used by the "admin@338" China-based cyber threat group. It delivers malicious payloads by exploiting newsworthy events as lures.
- Detection Methods:
    - File Hash Analysis: Identifying unique file hashes related to LOWBALL samples.
    - Network Traffic Monitoring: Observing abnormal traffic patterns linked to known LOWBALL command-and-control (C2) servers.
- Threat Indication:
    - Connections to LOWBALL C2 servers indicate potential compromise.

IoC 2: "Pink Sandstorm"

- Description: Pink Sandstorm is a ransomware and wiper malware associated with the "Agrius" Iranian threat actor group. This malware has been active in Middle Eastern regions.
- Detection Methods:
    - Endpoint Detection: Monitoring endpoints for encrypted files and wiper activity.
    - Log Analysis: Reviewing system logs for traces of unauthorized encryption tools or scripts.

- Threat Indication:
    - Sudden appearance of encrypted files and the deletion of system recovery tools suggest ransomware activity.

Section 2: OpenCTI Threat Intelligence Platform Implementation
Installation Process

The OpenCTI platform was implemented using Docker for containerized deployment.

Below are the steps:

1. System Preparation:
    - Installed Docker and Docker Compose on the host system.
    - Allocated required resources (CPU, RAM, and storage).
2. OpenCTI Setup:
    - Pulled the official OpenCTI Docker images.
    - Configured the `docker-compose.yml` file with environment variables.
    - Started the services using `docker-compose up`.

Configuration of Connectors

Two connectors were integrated to enrich threat intelligence data:

1. VirusTotal Connector:
    - Configured with an API key for retrieving IoC data from VirusTotal.
    - Enabled automated ingestion of malware hashes and associated metadata.
2. MISP Connector:
    - Linked to a MISP instance to sync threat reports and enrich OpenCTI datasets.

Documentation of Setup and Integration

- Screenshots demonstrate the platform interface, showing active connectors and ingested data.
- Logs confirm successful integration of connectors and data flow between systems.

Section 3: Demonstration of Basic Platform Usage Evidence of Functionality

1. IoC Search:
    - LOWBALL and Pink Sandstorm IoCs were queried within the platform.
    - Detailed metadata, including associated threat actors and related malware, were retrieved.
2. Visualization:
    - Generated a graph to visualize relationships between intrusion sets, malware, and targeted sectors.
3. Analytics Dashboard:
    - Monitored the dashboard for statistics on the most active threats and malware over the last three months (refer to screenshots).

Supporting Evidence

Screenshots provided illustrate:

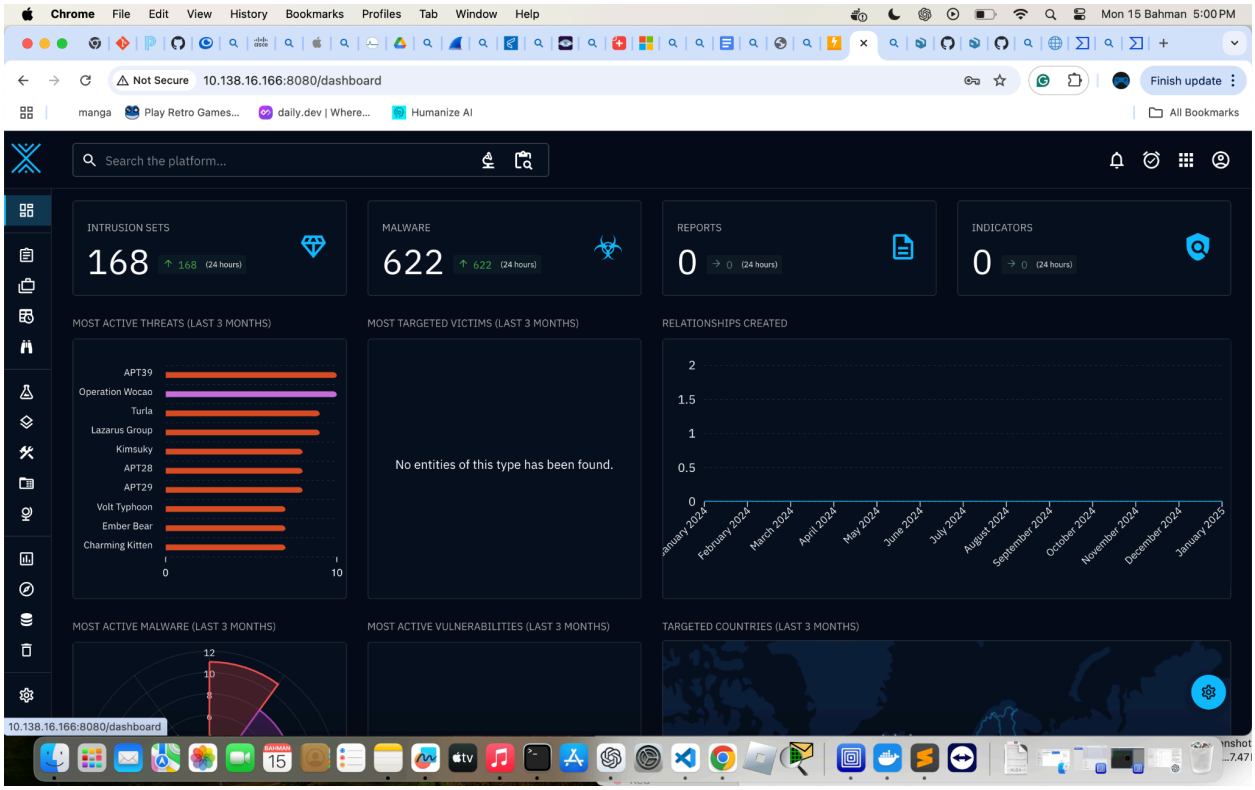
- The "Intrusion Sets" section showcasing profiles such as "admin@338" and "Agrius."
- The "Malware" section with entries like "LOWBALL" and "Pink Sandstorm."
- The dashboard displaying metrics on active threats and malware.

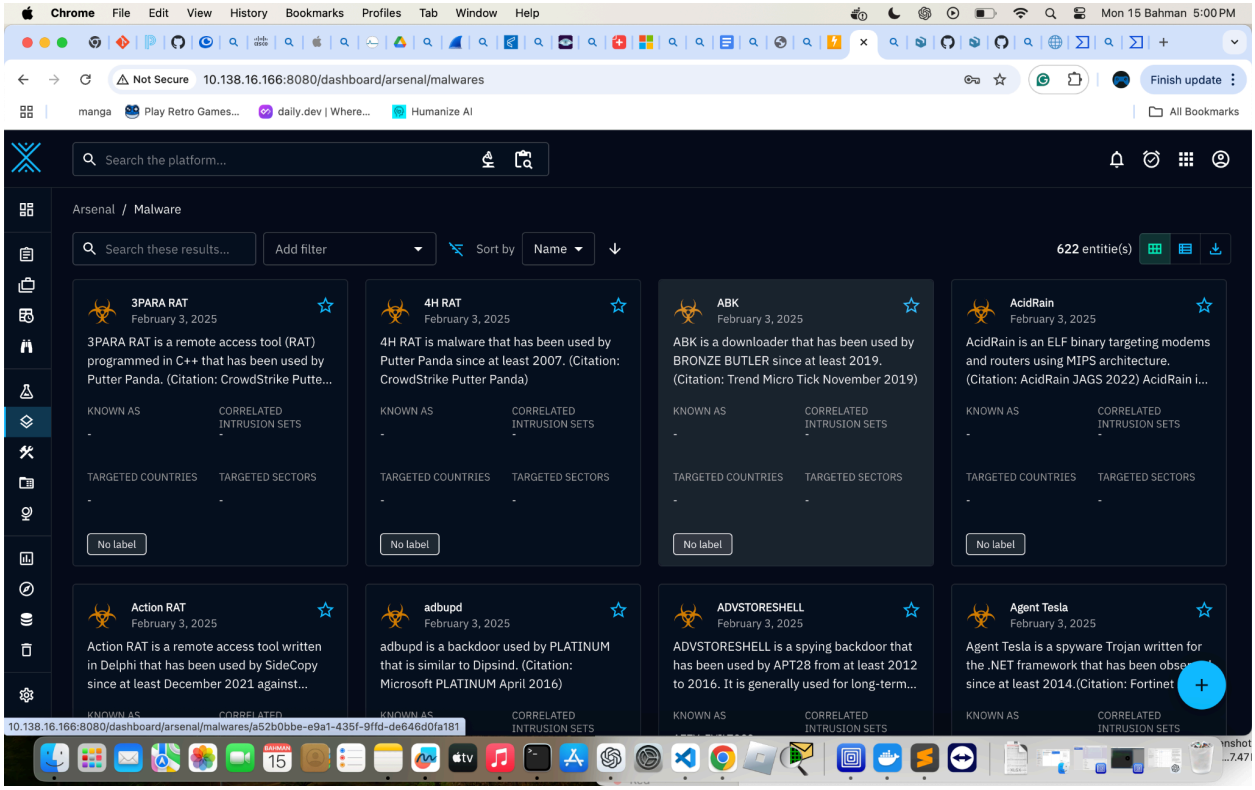
Conclusion

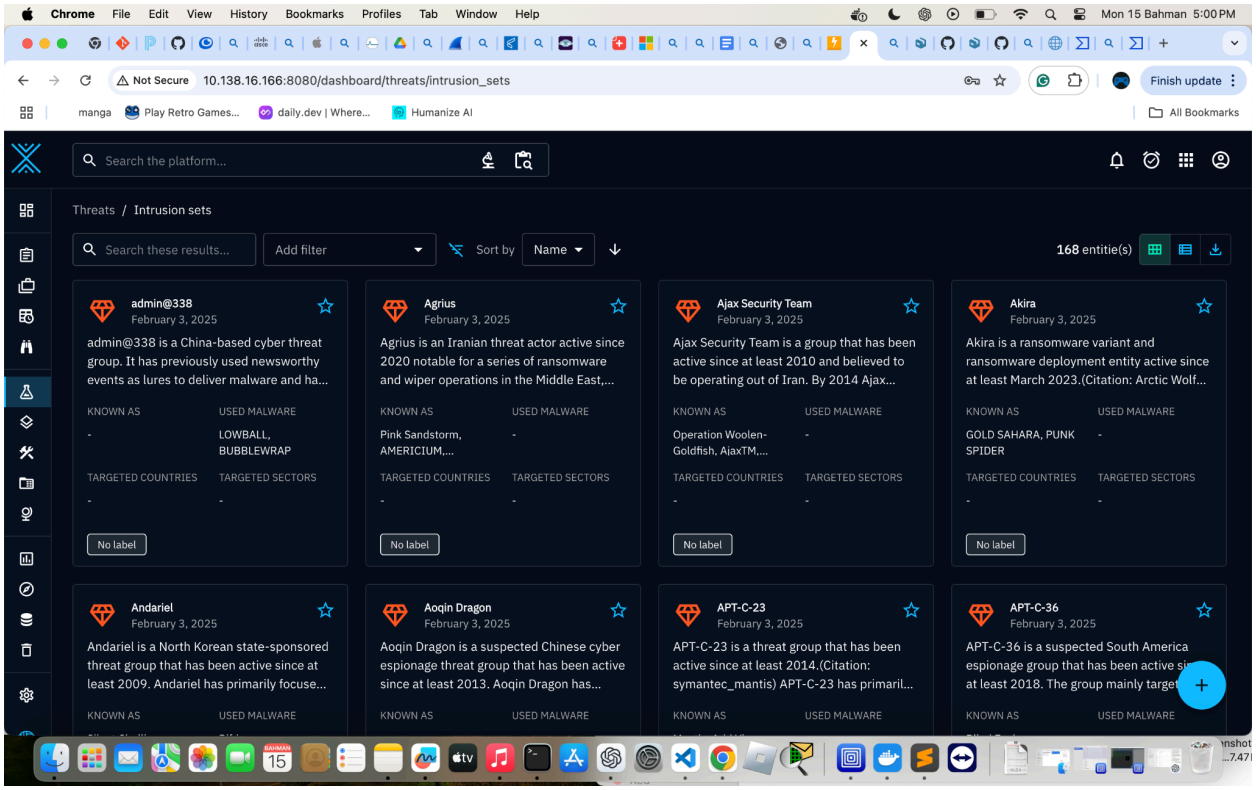
This project successfully demonstrates an understanding of threat intelligence principles through:

1. Detailed analysis of two IoCs with detection methodologies.
2. Implementation and configuration of the OpenCTI platform with two operational connectors.
3. Demonstration of platform usage, supported by screenshots and functional evidence.

The insights gained through this implementation highlight the critical role of threat intelligence in proactive cybersecurity efforts.


Chrome File Edit View History Bookmarks Profiles Tab Window Help
Mon 15 Bahman 5:00 PM
Not Secure
10.138.16.166:8080/dashboard
Finish update
manga
Play Retro Games...
daily.dev | Where...
Humanize AI
All Bookmarks
Search the platform...
INTRUSION SETS
168
168 (24 hours)
MALWARE
622
622 (24 hours)
REPORTS
0
0 (24 hours)
INDICATORS
0
0 (24 hours)
MOST ACTIVE THREATS (LAST 3 MONTHS)
APT39
Operation Wocao
Turla
Lazarus Group
Kimsuky
APT28
APT29
Volt Typhoon
Ember Bear
Charming Kitten
0
10
MOST TARGETED VICTIMS (LAST 3 MONTHS)
No entities of this type has been found.
RELATIONSHIPS CREATED
2
1.5
1
0.5
0
January 2024
February 2024
March 2024
April 2024
May 2024
June 2024
July 2024
August 2024
September 2024
October 2024
November 2024
December 2024
January 2025
MOST ACTIVE MALWARE (LAST 3 MONTHS)
MOST ACTIVE VULNERABILITIES (LAST 3 MONTHS)
TARGETED COUNTRIES (LAST 3 MONTHS)
10.138.16.166:8080/dashboard


Chrome File Edit View History Bookmarks Profiles Tab Window Help
Mon 15 Bahman 5:00 PM
Not Secure
10.138.16.166:8080/dashboard/arsenal/malwares
Finish update
manga
Play Retro Games...
daily.dev | Where...
Humanize AI
All Bookmarks
Search the platform...
Arsenal / Malware
Search these results...
Add filter
Sort by
Name
622 entitie(s)
3PARA RAT
February 3, 2025
3PARA RAT is a remote access tool (RAT) programmed in C++ that has been used by Putter Panda. (Citation: CrowdStrike Putte...
4H RAT
February 3, 2025
4H RAT is malware that has been used by Putter Panda since at least 2007. (Citation: CrowdStrike Putter Panda)
ABK
February 3, 2025
ABK is a downloader that has been used by BRONZE BUTLER since at least 2019. (Citation: Trend Micro Tick November 2019)
AcidRain
February 3, 2025
AcidRain is an ELF binary targeting modems and routers using MIPS architecture. (Citation: AcidRain JAGS 2022) AcidRain i...
KNOWN AS
CORRELATED INTRUSION SETS
TARGETED COUNTRIES
TARGETED SECTORS
No label
Action RAT
February 3, 2025
Action RAT is a remote access tool written in Delphi that has been used by SideCopy since at least December 2021 against...
adbupd
February 3, 2025
adbupd is a backdoor used by PLATINUM that is similar to Dipsind. (Citation: Microsoft PLATINUM April 2016)
ADVSTORESHELL
February 3, 2025
ADVSTORESHELL is a spying backdoor that has been used by APT28 from at least 2012 to 2016. It is generally used for long-term...
Agent Tesla
February 3, 2025
Agent Tesla is a spyware Trojan written for the .NET framework that has been obse... since at least 2014.(Citation: Fortinet
10.138.16.166:8080/dashboard/arsenal/malwares/a52b0bbe-e9a1-435f-9ffd-de646d0fa181


Chrome File Edit View History Bookmarks Profiles Tab Window Help
Mon 15 Bahman 5:00 PM
Not Secure
10.138.16.166:8080/dashboard/threats/intrusion_sets
Finish update
manga
Play Retro Games...
daily.dev | Where...
Humanize AI
All Bookmarks
Search the platform...
Threats / Intrusion sets
Search these results...
Add filter
Sort by
Name
168 entitie(s)
admin@338
February 3, 2025
admin@338 is a China-based cyber threat group. It has previously used newsworthy events as lures to deliver malware and ha...
KNOWN AS
USED MALWARE
LOWBALL, BUBBLEWRAP
TARGETED COUNTRIES
TARGETED SECTORS
No label
Agrius
February 3, 2025
Agrius is an Iranian threat actor active since 2020 notable for a series of ransomware and wiper operations in the Middle East,...
KNOWN AS
Pink Sandstorm, AMERICIUM,...
USED MALWARE
TARGETED COUNTRIES
TARGETED SECTORS
No label
Ajax Security Team
February 3, 2025
Ajax Security Team is a group that has been active since at least 2010 and believed to be operating out of Iran. By 2014 Ajax...
KNOWN AS
Operation Woolen-Goldfish, AjaxTM,...
USED MALWARE
TARGETED COUNTRIES
TARGETED SECTORS
No label
Akira
February 3, 2025
Akira is a ransomware variant and ransomware deployment entity active since at least March 2023.(Citation: Arctic Wolf...
KNOWN AS
GOLD SAHARA, PUNK SPIDER
USED MALWARE
TARGETED COUNTRIES
TARGETED SECTORS
No label
Andariel
February 3, 2025
Andariel is a North Korean state-sponsored threat group that has been active since at least 2009. Andariel has primarily focuse...
KNOWN AS
USED MALWARE
Aoqin Dragon
February 3, 2025
Aoqin Dragon is a suspected Chinese cyber espionage threat group that has been active since at least 2013. Aoqin Dragon has...
KNOWN AS
USED MALWARE
APT-C-23
February 3, 2025
APT-C-23 is a threat group that has been active since at least 2014.(Citation: symantec_mantis) APT-C-23 has primaril...
KNOWN AS
USED MALWARE
APT-C-36
February 3, 2025
APT-C-36 is a suspected South America espionage group that has been active si
at least 2018. The group mainly target
KNOWN AS
USED MALWARE