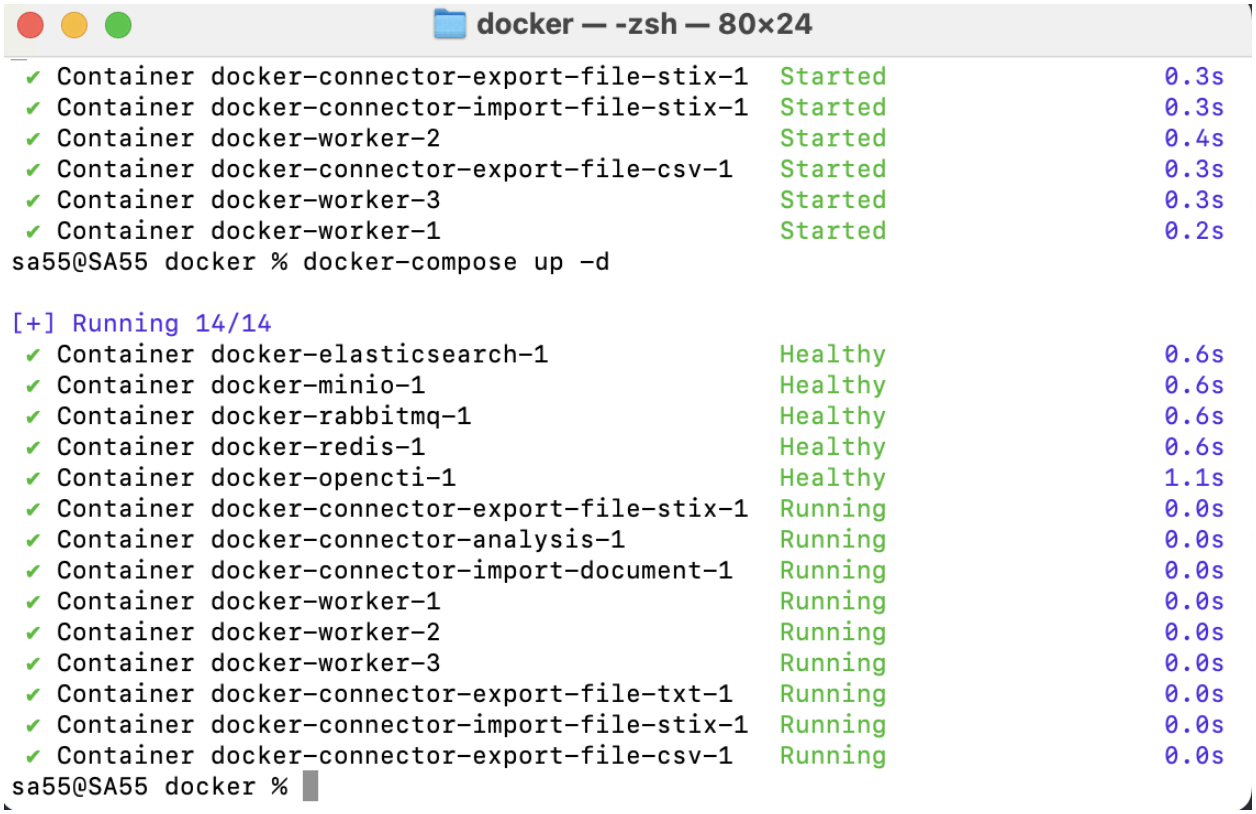
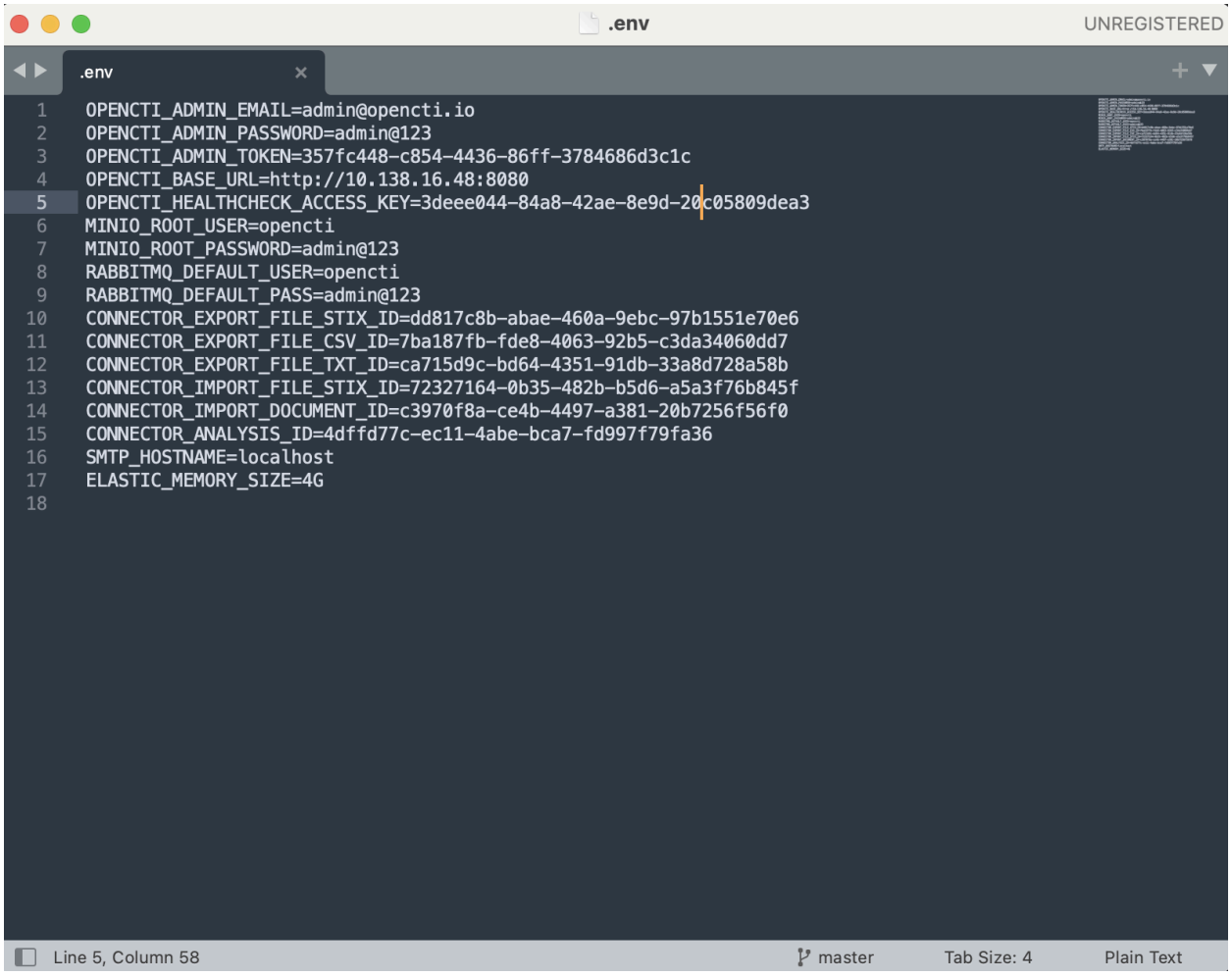
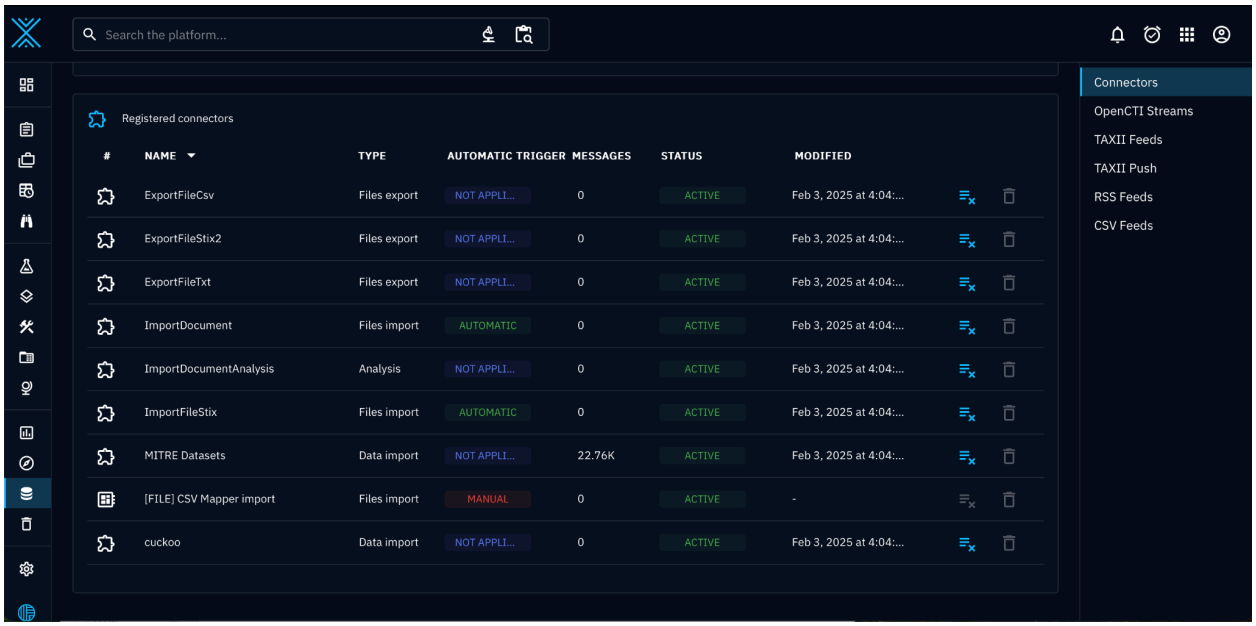
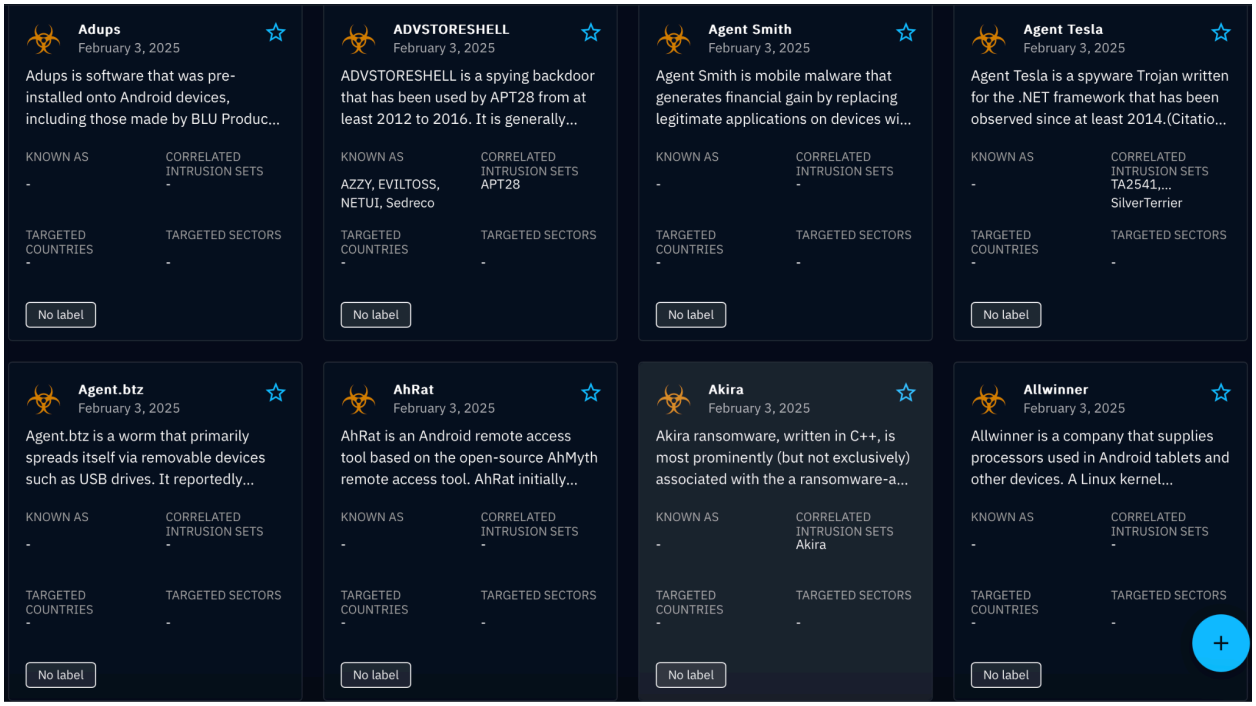
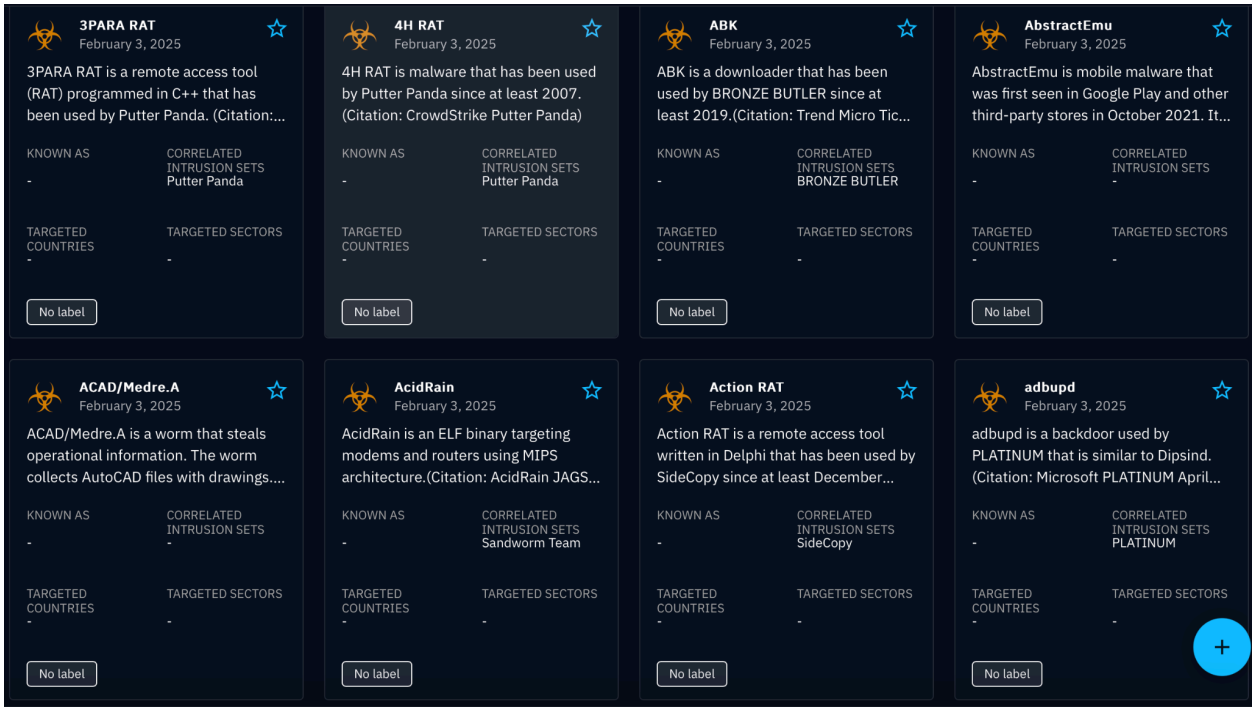
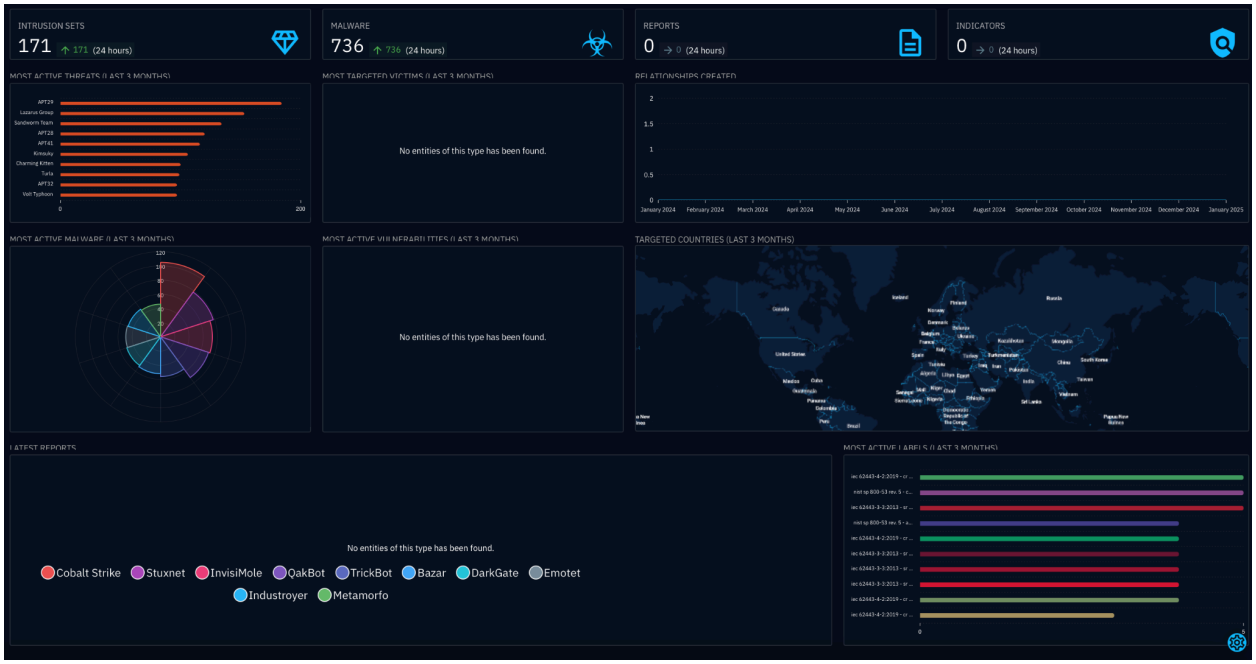

docker — -zsh — 80×24
✔ Container docker-connector-export-file-stix-1 Started 0.3s
✔ Container docker-connector-import-file-stix-1 Started 0.3s
✔ Container docker-worker-2 Started 0.4s
✔ Container docker-connector-export-file-csv-1 Started 0.3s
✔ Container docker-worker-3 Started 0.3s
✔ Container docker-worker-1 Started 0.2s
sa55@SA55 docker % docker-compose up -d
[+] Running 14/14
✔ Container docker-elasticsearch-1 Healthy 0.6s
✔ Container docker-minio-1 Healthy 0.6s
✔ Container docker-rabbitmq-1 Healthy 0.6s
✔ Container docker-redis-1 Healthy 0.6s
✔ Container docker-opencti-1 Healthy 1.1s
✔ Container docker-connector-export-file-stix-1 Running 0.0s
✔ Container docker-connector-analysis-1 Running 0.0s
✔ Container docker-connector-import-document-1 Running 0.0s
✔ Container docker-worker-1 Running 0.0s
✔ Container docker-worker-2 Running 0.0s
✔ Container docker-worker-3 Running 0.0s
✔ Container docker-connector-export-file-txt-1 Running 0.0s
✔ Container docker-connector-import-file-stix-1 Running 0.0s
✔ Container docker-connector-export-file-csv-1 Running 0.0s
sa55@SA55 docker %


.env
UNREGISTERED
.env
1 OPENCTI_ADMIN_EMAIL=admin@opencti.io
2 OPENCTI_ADMIN_PASSWORD=admin@123
3 OPENCTI_ADMIN_TOKEN=357fc448-c854-4436-86ff-3784686d3c1c
4 OPENCTI_BASE_URL=http://10.138.16.48:8080
5 OPENCTI_HEALTHCHECK_ACCESS_KEY=3deee044-84a8-42ae-8e9d-20c05809dea3
6 MINIO_ROOT_USER=opencti
7 MINIO_ROOT_PASSWORD=admin@123
8 RABBITMQ_DEFAULT_USER=opencti
9 RABBITMQ_DEFAULT_PASS=admin@123
10 CONNECTOR_EXPORT_FILE_STIX_ID=dd817c8b-abae-460a-9ebc-97b1551e70e6
11 CONNECTOR_EXPORT_FILE_CSV_ID=7ba187fb-fde8-4063-92b5-c3da34060dd7
12 CONNECTOR_EXPORT_FILE_TXT_ID=ca715d9c-bd64-4351-91db-33a8d728a58b
13 CONNECTOR_IMPORT_FILE_STIX_ID=72327164-0b35-482b-b5d6-a5a3f76b845f
14 CONNECTOR_IMPORT_DOCUMENT_ID=c3970f8a-ce4b-4497-a381-20b7256f56f0
15 CONNECTOR_ANALYSIS_ID=4dffd77c-ec11-4abe-bca7-fd997f79fa36
16 SMTP_HOSTNAME=localhost
17 ELASTIC_MEMORY_SIZE=4G
18
Line 5, Column 58
master
Tab Size: 4
Plain Text


Search the platform...
Registered connectors
NAME TYPE AUTOMATIC TRIGGER MESSAGES STATUS MODIFIED
ExportFileCsv Files export NOT APPLI... 0 ACTIVE Feb 3, 2025 at 4:04:...
ExportFileStix2 Files export NOT APPLI... 0 ACTIVE Feb 3, 2025 at 4:04:...
ExportFileTxt Files export NOT APPLI... 0 ACTIVE Feb 3, 2025 at 4:04:...
ImportDocument Files import AUTOMATIC 0 ACTIVE Feb 3, 2025 at 4:04:...
ImportDocumentAnalysis Analysis NOT APPLI... 0 ACTIVE Feb 3, 2025 at 4:04:...
ImportFileStix Files import AUTOMATIC 0 ACTIVE Feb 3, 2025 at 4:04:...
MITRE Datasets Data import NOT APPLI... 22.76K ACTIVE Feb 3, 2025 at 4:04:...
[FILE] CSV Mapper import Files import MANUAL 0 ACTIVE -
cuckoo Data import NOT APPLI... 0 ACTIVE Feb 3, 2025 at 4:04:...
Connectors
OpenCTI Streams
TAXII Feeds
TAXII Push
RSS Feeds
CSV Feeds


Adups
February 3, 2025
Adups is software that was pre-installed onto Android devices, including those made by BLU Produc...
KNOWN AS
-
CORRELATED INTRUSION SETS
-
TARGETED COUNTRIES
-
TARGETED SECTORS
-
No label
ADVSTORESHELL
February 3, 2025
ADVSTORESHELL is a spying backdoor that has been used by APT28 from at least 2012 to 2016. It is generally...
KNOWN AS
AZZY, EVILTOSS, NETUI, Sedreco
CORRELATED INTRUSION SETS
APT28
TARGETED COUNTRIES
-
TARGETED SECTORS
-
No label
Agent Smith
February 3, 2025
Agent Smith is mobile malware that generates financial gain by replacing legitimate applications on devices wi...
KNOWN AS
-
CORRELATED INTRUSION SETS
-
TARGETED COUNTRIES
-
TARGETED SECTORS
-
No label
Agent Tesla
February 3, 2025
Agent Tesla is a spyware Trojan written for the .NET framework that has been observed since at least 2014.(Citatio...
KNOWN AS
-
CORRELATED INTRUSION SETS
TA2541,...
SilverTerrier
TARGETED COUNTRIES
-
TARGETED SECTORS
-
No label
Agent.btz
February 3, 2025
Agent.btz is a worm that primarily spreads itself via removable devices such as USB drives. It reportedly...
KNOWN AS
-
CORRELATED INTRUSION SETS
-
TARGETED COUNTRIES
-
TARGETED SECTORS
-
No label
AhRat
February 3, 2025
AhRat is an Android remote access tool based on the open-source AhMyth remote access tool. AhRat initially...
KNOWN AS
-
CORRELATED INTRUSION SETS
-
TARGETED COUNTRIES
-
TARGETED SECTORS
-
No label
Akira
February 3, 2025
Akira ransomware, written in C++, is most prominently (but not exclusively) associated with the a ransomware-a...
KNOWN AS
-
CORRELATED INTRUSION SETS
Akira
TARGETED COUNTRIES
-
TARGETED SECTORS
-
No label
Allwinner
February 3, 2025
Allwinner is a company that supplies processors used in Android tablets and other devices. A Linux kernel...
KNOWN AS
-
CORRELATED INTRUSION SETS
-
TARGETED COUNTRIES
-
TARGETED SECTORS
-
No label


3PARA RAT
February 3, 2025
3PARA RAT is a remote access tool (RAT) programmed in C++ that has been used by Putter Panda. (Citation:...
KNOWN AS
-
CORRELATED INTRUSION SETS
Putter Panda
TARGETED COUNTRIES
-
TARGETED SECTORS
-
No label
4H RAT
February 3, 2025
4H RAT is malware that has been used by Putter Panda since at least 2007. (Citation: CrowdStrike Putter Panda)
KNOWN AS
-
CORRELATED INTRUSION SETS
Putter Panda
TARGETED COUNTRIES
-
TARGETED SECTORS
-
No label
ABK
February 3, 2025
ABK is a downloader that has been used by BRONZE BUTLER since at least 2019.(Citation: Trend Micro Tic...
KNOWN AS
-
CORRELATED INTRUSION SETS
BRONZE BUTLER
TARGETED COUNTRIES
-
TARGETED SECTORS
-
No label
AbstractEmu
February 3, 2025
AbstractEmu is mobile malware that was first seen in Google Play and other third-party stores in October 2021. It...
KNOWN AS
-
CORRELATED INTRUSION SETS
-
TARGETED COUNTRIES
-
TARGETED SECTORS
-
No label
ACAD/Medre.A
February 3, 2025
ACAD/Medre.A is a worm that steals operational information. The worm collects AutoCAD files with drawings....
KNOWN AS
-
CORRELATED INTRUSION SETS
-
TARGETED COUNTRIES
-
TARGETED SECTORS
-
No label
AcidRain
February 3, 2025
AcidRain is an ELF binary targeting modems and routers using MIPS architecture.(Citation: AcidRain JAGS...
KNOWN AS
-
CORRELATED INTRUSION SETS
Sandworm Team
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...
KNOWN AS
-
CORRELATED INTRUSION SETS
SideCopy
TARGETED COUNTRIES
-
TARGETED SECTORS
-
No label
adbupd
February 3, 2025
adbupd is a backdoor used by PLATINUM that is similar to Dipsind. (Citation: Microsoft PLATINUM April...
KNOWN AS
-
CORRELATED INTRUSION SETS
PLATINUM
TARGETED COUNTRIES
-
TARGETED SECTORS
-
No label



Threat Intelligence Implementation Report

1. Understanding of Threat Intelligence Principles

This report details the practical implementation of threat intelligence principles. The goal of this project is to analyze two Indicators of Compromise (IoCs), detect potential threats using OpenCTI Threat Intelligence Platform, and demonstrate functionality with proper documentation and evidence.

---

2. Analysis of Indicators of Compromise (IoCs)

IoC 1: 3PARA RAT

- **Description**: 3PARA RAT is a remote access tool programmed in C++ and associated with Putter Panda, a known threat actor.
- **Detection Methods**:
    - **File Hash Analysis**: Use tools like VirusTotal to detect known malicious file hashes associated with 3PARA RAT.
    - **Network Traffic Analysis**: Monitor for unusual communication patterns between endpoints and Command-and-Control (C2) servers.
- **Threat Indication**:
    - Communication to known malicious IP addresses or domains.
    - Unusual user behavior or process execution on affected systems.

IoC 2: Akira Ransomware

- **Description**: Akira ransomware is written in C++ and linked to ransomware attacks targeting Linux and Windows systems.
- **Detection Methods**:
    - **Signature-Based Detection**: Match file signatures against a database of ransomware samples.
    - **Behavioral Analysis**: Monitor file encryption behavior or unauthorized attempts to modify system files.
- **Threat Indication**:
    - Sudden high CPU usage.
    - Creation of ransom note files in compromised directories.

---

3. OpenCTI Platform Implementation

Platform Setup

The OpenCTI Threat Intelligence Platform was deployed using Docker for ease of setup and maintenance. Steps for installation:

1. Install Docker and Docker Compose.
2. Clone the OpenCTI repository:

   ```
   git clone https://github.com/OpenCTI-Platform/opencti-docker.git
   cd opencti-docker
   ```

3. Configure environment variables in the `.env` file, including API keys and database settings.
4. Start the platform using Docker Compose:

   ```
   docker-compose up -d
   ```

Connector Integration

Two connectors were configured and integrated into OpenCTI:

1. **Cuckoo Connector**:
    - **Purpose**: Automates the analysis of malware samples using the Cuckoo sandbox.
    - **Configuration**: Updated the `config.yml` file with Cuckoo server details and OpenCTI API credentials.
    - **Functionality**:
        - Uploaded suspicious files to the Cuckoo sandbox.

        - Cuckoo-generated reports were automatically imported into OpenCTI.
    - **Evidence**: Logs and screenshots show successful sandbox analysis and report integration.
2. **MITRE Datasets Connector**:
    - **Purpose**: Imports datasets from MITRE ATT&CK for enhanced correlation of threat actors, techniques, and tactics.
    - **Configuration**: API key for MITRE ATT&CK was added to the connector configuration file.
    - **Functionality**:
        - Automatically fetched datasets on tactics, techniques, and threat actor profiles.
        - Enabled mapping of IoCs to corresponding ATT&CK techniques.
    - **Evidence**: Screenshots confirm the successful import and mapping of MITRE datasets.

Usage Demonstration

- **Threat Intelligence Analysis**:
    - IoCs such as "3PARA RAT" and "Akira" were searched within the platform.
    - Correlated intrusion sets (e.g., "Putter Panda" and "Akira group") were identified.
- **Connector Logs**:
    - Logs confirmed the successful functionality of the Cuckoo and MITRE Datasets connectors, evidenced by sandbox analysis results and updated datasets.

---

4. Documentation and Evidence

- **Screenshots**:
    - Evidence of connector configuration, sandbox analysis (Cuckoo), and IoC correlation (MITRE datasets) is provided in the attached screenshots.
- **Challenges Encountered**:
    - Initial setup required fine-tuning of environment variables for connector integration.
    - Resolved by reviewing logs and consulting OpenCTI documentation.

---

5. Conclusion

This project successfully demonstrated the implementation of threat intelligence principles using OpenCTI. Two IoCs were analyzed with detection methods, and OpenCTI was deployed with two functional connectors: **Cuckoo** for malware analysis and **MITRE Datasets** for threat actor correlation. Evidence confirms platform functionality and the utility of threat intelligence in detecting and mitigating threats.