**Nwachukwu Edumanichukwu**

**CYBR 440 - Incident Detection and Response  
Module 11 Lab – Leveraging Threat Intelligence**

In this eleventh lab, we will look at some open-source threat intelligence platforms and the data that they provide. We will then look at an open-source on-premise threat intelligence platform that you can use to integrate multiple sources of intelligence on one platform. Finally, we will use Mandiant’s Open IOC editor to create an IOC file based on the previous week’s case study. This IOC file can then be shared with other professionals and organizations to allow defenders to quickly identify and stop threats using the same tools and techniques.

**You will be required to submit the following graded items as part of this lab:**

* Answer all questions listed in **BOLD**
* Provide screenshots when asked

Part 1 - AlienVault OTX

AlienVault produces an open-source SIEM, a commercial cloud-hosted SIEM, and has created the most popular and used open-source threat intelligence community. AlienVault’s threat intelligence community is called OTX. It provides API integrations using web API’s, STIX, and TAXII. These are protocols for sharing cyber-threat intelligence between different systems. OTX is also integrated into several other open-source and freely available tools such as Graylog SIEM and TheHive, as we have previously seen.

1. Navigate to <https://otx.alienvault.com/> and sign up for a free OTX account. You can use your Bellevue email, personal email, or Google/Facebook integrated authentication. Make sure you activate your account via the email you receive.

Graphical user interface, application

Description automatically generated

1. Navigate to <https://otx.alienvault.com/> and sign in. Your initial page will be a dashboard that shows a list of Pulses. Pulses are unique self-contained intelligence entries that have unique information attached. This data includes descriptions of the threat, tags, industries targeted, malware family, MITRE ATT&CK Framework, and Indicators of Compromise.
2. Click on a Pulse you find interesting. Explore the intelligence and then answer the following questions.

**What type of threat is this?**

Trojan:Win32/Urelas

Pulse: gagnob.com/cl/73c395f8c4c84f9c?p1&p2&source&site

**What MITRE ATT&CK Framework IDs are being used?**

T1071 - Application Layer Protocol, T1083 - File and Directory Discovery , T1105 - Ingress Tool Transfer , T1140 - Deobfuscate/Decode Files or Information , T1555 - Credentials from Password Stores

**What Indicators of compromise are provided with this Pulse?**

Domain (4), Hostname (8), URL (43), FileHash-SHA256(118), FileHash-MD5 (83) and other (66)

1. Click on the Scan Endpoints tab at the top of the page. OTX provides endpoints for a variety of platforms and allows you to scan for IOCs on those endpoints. We will not install this endpoint or scan for the endpoint in this lab but you should download and use the endpoint on your own systems when you have the chance.
2. Click on API Integrations tab at the top of the page. This page shows you the different API integrations available. Pulses will often include Zeek and Suricata rules to help you detect badness with your network intrusion detection and prevention systems. Look on the right of the page. You should see your API Key that allows you automate the access and use of OTX threat intel.

**Paste your OTX Key below:**

8927c6784bced246627e0f7091fce0a41fe534c0067dfeacb6782b8f41fedc08

Part 2 - Open CTI

In this second section of the lab, we will briefly look at an open-source threat intelligence platform. Threat intel platforms are systems that are designed to integrate multiple threat sources or streams into one integrated system. We will look at a free and open-source platform called OpenCTI.

1. Open a browser and navigate to <https://www.opencti.io/en/>. On the main page, click on the Demonstration link. On the next page, click Sign In with Citeum Collective.
2. Register as a New User on this page or sign in with a Google, Facebook, or Github account. Acknowledge the email if necessary and log into the OpenCTI demo.
3. Examine the default threat dashboard and answer the following questions:

**What are the top threat labels for the last three months?**

Phishing, PowerShell, email, block or filter, osint, html file, phishing-as-a-service, trojan, backdoor

**What countries have been the top targets over the last three months?**

United States, Canada, United Kingdom, Germany, Ukraine, Kazakhstan, Belarus, Italy, Afghanistan, Kyrgyzstan, Tajikistan, India, Russia, Brazil

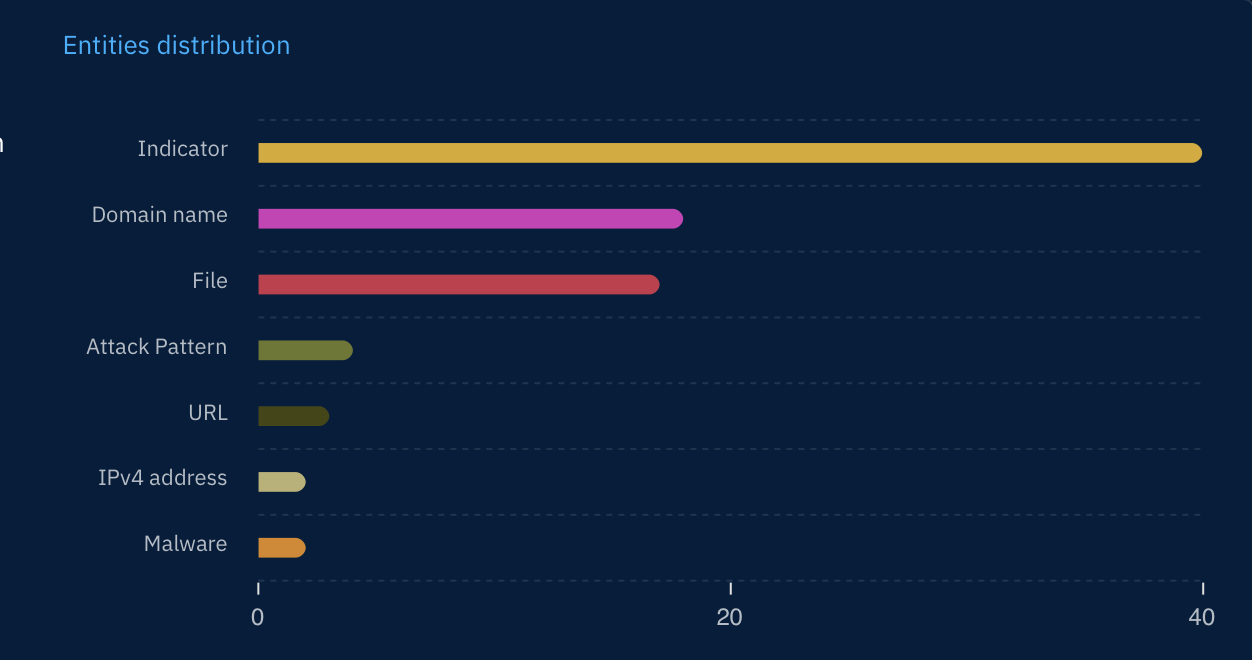
**What are the top 10 entities (tools & groups) for the last three months?**

Email, Trojan, Cobalt Strike, Redline, WarzoneRAT, Vidar, Ursnif, RAT, APT137, IcedID

1. Navigate to Activities -> Analysis on the left side of the screen. This will bring up a list of reports for different threats. Click on a threat of interest. This brings up a second set of tabs that contains detailed information on a threat. Review the Knowledge, Content, Entities, Observables, and Data tabs and answer the following questions.

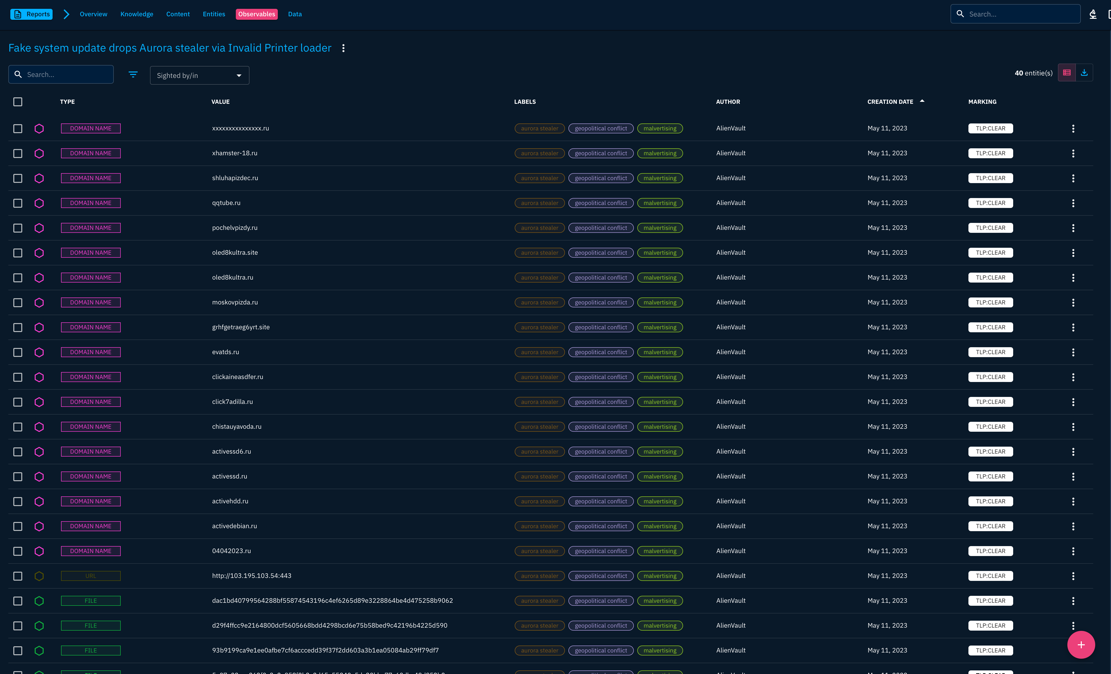
**Who is the author of this information (threat source)?**

ALIENVAULT

**Take a screenshot for the Entity Details distribution pie chart and paste it below?**

**What are some of the entities and observables associated with this threat?A screenshot of a computer

Description automatically generated with medium confidence**

****

Malware, IP4v4 address, URL, Attack Pattern, File, Domain name, Indicator.

1. Navigate to the left side of the screen to Data. Then open the Connectors tab on the top of the page. Connectors are the mechanism to import and enrich data from threat intel sources like OTX.

**Which Connectors do you see that seem like they would be most valuable?**

AlienVault, MISP Limeo, MITRE ATT&CK and OpenCTI Datasets.

**What are the different types of connectors available? What do you think each does?**

Data import, Files export, and Enrichment.

Accessing the Lab

This lab is hosted in the university IS Lab and requires special instructions to access it. If you are not familiar with accessing the IS Lab, please see the document in this course that walks you through accessing the Cybersecurity Desktop. You can access the Cybersecurity Desktop through the Web or using VMWare’s Horizon client. It would be best if you used the native Horizon client when possible as it provides better performance. The web client can be accessed at <https://workspace.bellevue.edu>. Make sure you log in to this interface with your Bellevue student ID and password.

After accessing workspace.bellevue.edu and selecting the IS Lab desktop, open a browser and navigate to <https://10.98.100.11>. The first time you access this site, you will see a warning in the browser. Make sure to click advanced and then Proceed to 10.98.100.11 (Unsafe). Next, you should see the following remote access page.

Graphical user interface, application, Word

Description automatically generated

After accessing Bellevue Bank and Trust’s Remote Management Portal, login in using the following information:

* Username: analyst# - Where # is the number provided to you by your instructor
* Password: An@lyst#!! - Where # is the number provided to you by your instructor

After logging in, you should see the following page:

Graphical user interface, application

Description automatically generated

You should have three available connections, RDP Kali #, RDP Workstation#, and SSH Kali #. These are the three analyst tools you will use throughout this course.

You will be using the Windows 10 RDP Workstation# connection for this lab. Therefore, it would be best to open each new RDP or SSH connection in a new tab.

Part 3 - Creating Shareable IOCs with Mandiant’s Open IOC Editor

In this third section of the lab, we will use Mandiant’s OpenIOC editor to create a shareable set of IOCs in the OpenIOC format. We will use the IOCs from our previous module’s cast study.

1. After accessing your analyst workstation, double-click the Mandiant IOC Editor icon on the desktop. Alternatively, navigate with Windows Explorer to C:\Program File (x86)\Mandiant\Mandiant IOCe.exe. When IOCe opens, select This PC -> C:\ -> CYBR 440 as the IOC directory.
2. On the File menu click New -> Indicator. This brings up a new indicator window which allows you to add specific metadata to the indicator. In this case we will add all the metadata to a single indicator.

Table

Description automatically generated

1. In metadata screen that simply has an --OR, right click the OR and select Add Item -> FileItem -> File MD5. Add the first MD5 hash from the case study to the blank textbox that appears in the metadata pane. Repeat until you have added all seven of the MD5 hashes.

Graphical user interface, text, application

Description automatically generated

1. In the metadata screen that now has an --OR with MD5 hashes underneath, select Add Item -> DnsEntryItem -> DNS Host. Add the 11 domain names found as part of the case study incident.

Table

Description automatically generated

1. In the metadata screen hat now has -OR with MD5 hashes and DNS Hosts underneath, select Add Item -> DNS Record Data IPv4 Address. Add the 6 IP addresses found as part of the case study incident.

Text

Description automatically generated with medium confidence

1. In the metadata screen that now has -OR with MD5 hashes, DNS Hosts, and DNS IP addresses. Add the three email addresses found as part of the case study incident.

Graphical user interface, text

Description automatically generated

**Paste a screenshot of your IOCe Description and Metadata below**

**A screenshot of a computer

Description automatically generated with medium confidence**

Public IOC files are available. The OpenIOC format used in the files created by IOC Editor can be used in Redline (which we’ve previously used) to check memory images for indicators of compromise. In this case, forensics performed in the case study could automate the detection of any of the indicators you added in IOC Editor when opening a memory dump. These IOCs can also be shared on intelligence streams or platforms like OTX and uploaded to certain EDR tools like Fireeye HX.