### THREAT-INTELLIGENCE-TOOLS

#### **INTRODUCTION**

- # **Threat Intelligence** is the analysis of data and information using tools and techniques to generate meaningful patterns on how to mitigate against potential risks associated with existing or emerging threats targeting organizations, industries, sectors or governments.
- #This room will cover the concepts of Threat Intelligence and various open-source tools that are useful.
- #I came to have a grep of the various classification of threat intelligence namely;
  - Strategic Intel: High-level intelligence focused on the broader trends and patterns in
- the threat landscape.
- Tactical Intel: Intelligence that provides specific information on tactics, techniques, and procedures (TTPs) used by threat actors.
- Operational Intel: ntelligence focused on the details of specific, imminent threats or incidents.
- # Now here are the questions and how I solved them.

Read the description! Continue to the next task.



Looking closely on the screenshot provided in this room, the rank was 345612. And this can be prooven from the image below.

This website contacted 17 IPs in 4 countries across 13 domains to perform 109 HTTP transactions. The main IP is 2606:4700:10::ac43:1b0a, located in United States and belongs to CLOUDFLARENET, US. The main domain is tryhackme.com. The Cisco Umbrella rank of the primary domain is 345612.

How many domains did UrlScan.io identify on the screenshot?

13 Correct

This website contacted 17 IPs in 4 countries across 13 domains to perform 109 HTTP

NAMECHEAP INC



The domain registrar is NAMECHEAP INC as it can be seen from the image below.

### Live information

Google Safe Browsing: ONo classification for tryhackme.com

Current DNS A record: 104.22.55.228 (AS13335 - CLOUDFLARENET, US)

Domain created: July 5th 2018, 22:46:15 (UTC)

Domain registrar: NAMECHEAP INC

What was the main IP address identified for TryHackMe on the screenshot?

2606:4700:10::ac43:1b0a



This website contacted 17 IPs in 4 countries across 13 domains to perform 109 HTTP transactions. The main IP is 2606:4700:10::ac43:1b0a, located in United States and belongs to

The IOC 212.192.246.30:5555 is identified under which malware alias name on ThreatFox?

Katana



For this question, I did some little google search and the results were as shown below.

15 Mar 2022 — **IOC** ID: 395319. **IOC**: **212.192.246.30:5555**. **IOC** Type : ip:port. Threat Type : botnet\_cc. Malware: Mirai. Malware alias: Katana.

Which malware is associated with the JA3 Fingerprint 51c64c77e60f3980eea90869b68c58a8 on SSL Blacklist?

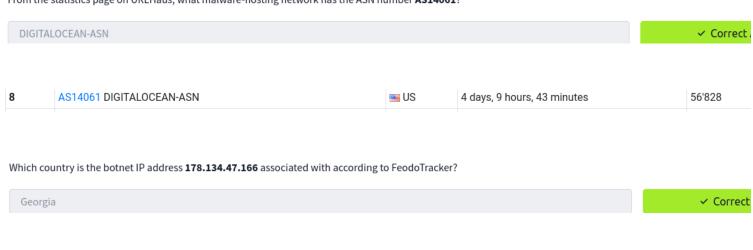
Dridex



Dridex, is the malware as you can see from the image below.

JA3 Fingerprint:	51c64c77e60f3980eea90869b68c58a8
First seen:	2018-08-30 21:04:57 UTC
Last seen:	2021-08-11 08:13:08 UTC
Status:	Blacklisted
Malware samples:	227'014
Destination IPs:	5'216
Malware:	Dridex @
Listing date:	2018-12-17 07:47:19

From the statistics page on URLHaus, what malware-hosting network has the ASN number AS14061?



Status

♣ Offline

Network (ASN)

AS35805 SILKNET-AS

↑↓ Country

**∷** GE

# What social media platform is the attacker trying to pose as in the email?

Malware

🕏 TrickBot



I used to the phish tools and talos to analyse for this information and the screenshots below summarizes how I got the answers.

This email was intended for CabbageCare. Learn why we included this.

You are receiving LinkedIn notification emails.

↑↓ Host

178.134.47.166

Firstseen (UTC)

2021-04-22 22:04:30

### What is the senders email address?

darkabutla@sc500.whpservers.com

✓ Correct Answer

By simply looking at the header information, I was able to retrieve the senders email.

From Patrick Cook <darkabutla@sc500.whpservers.com>☆

What is the recipient's email address?

cabbagecare@hotsmail.com

✓ Correct Answer

By simply looking at the header information, I was able to retrieve the recipient's email.

To cabbagecare@hotsmail.com <cabbagecare@hotsmail.com>☆

What is the Originating IP address? Defang the IP address.

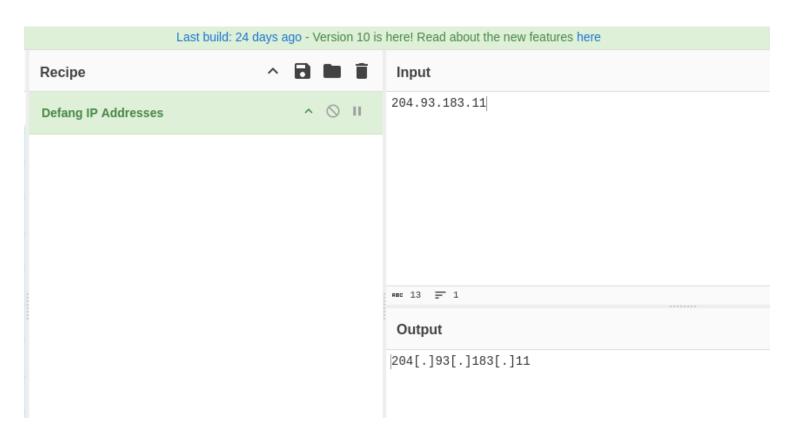
204[.]93[.]183[.]11

✓ Correct Answer

Q Hint

I used the phishtool to analyse the email and got this information (basically the IP). Visited the cyberchef and to defang the ip address as shown in the image below.

Received: from sc500.whpservers.com (204.93.183.11) by DM6NAM10FT030.mail.protection.outlook.com (10.13.152.224) with Microsoft SMTP Server id 15.20.5102.17 via Frontend Transport; Tue, 29 Mar 2022 20:39:27 +0000



How many hops did the email go through to get to the recipient?

4 Correct Answer

What is the listed domain of the IP address from the previous task?

scnet.net Correct Answer 9 Hint

NetRange: 204.93.183.0 - 204.93.183.255

CIDR: 204.93.183.0/24

NetName: SCNET-204-93-183-0-24 NetHandle: NET-204-93-183-0-1

Parent: SCN-6 (NET-204-93-128-0-1)

NetType: Reassigned

OriginAS:

Customer: Complete Web Reviews (C05082466)

RegDate: 2014-06-06 Updated: 2014-06-06

Ref: https://rdap.arin.net/registry/ip/204.93.183.0

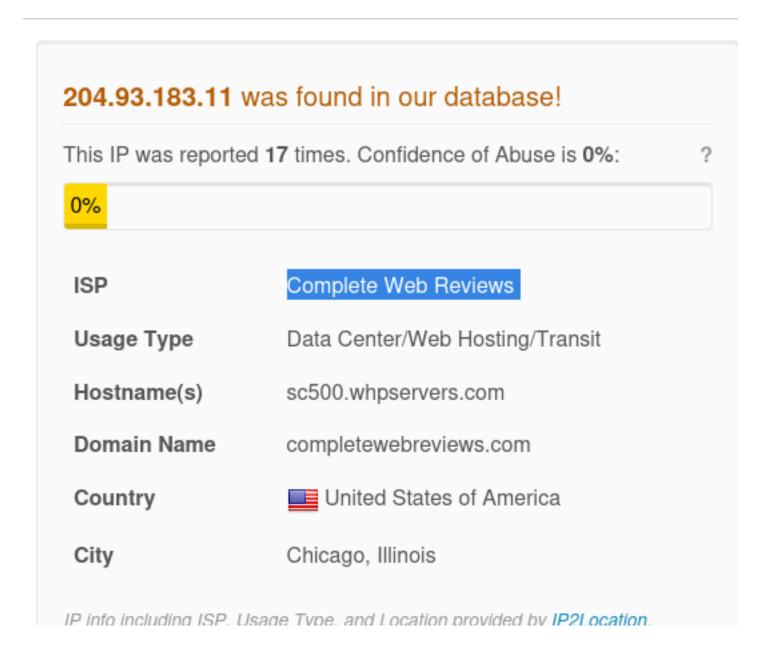
### What is the customer name of the IP address?

Complete Web Reviews

✓ Correct Answer

♀ Hint

I visited the whois.org to extract this information just as shown in the screenshot below.

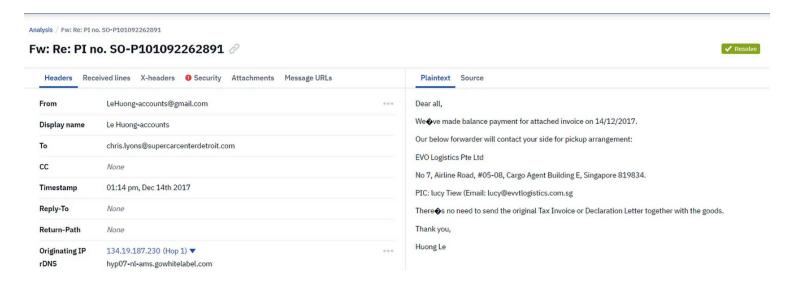


# According to **Email2.eml**, what is the recipient's email address?

ris.lyons@supercarcenterdetroit.com

✓ Correct Answer

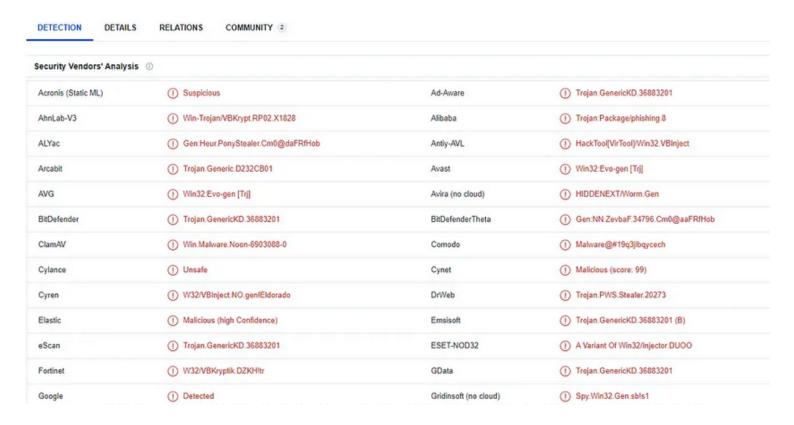
I uploaded the email to the phishtool and did some analysis on the analysis tab. And below was the output.



From Talos Intelligence, the attached file can also be identified by the Detection Alias that starts with an **H...** 



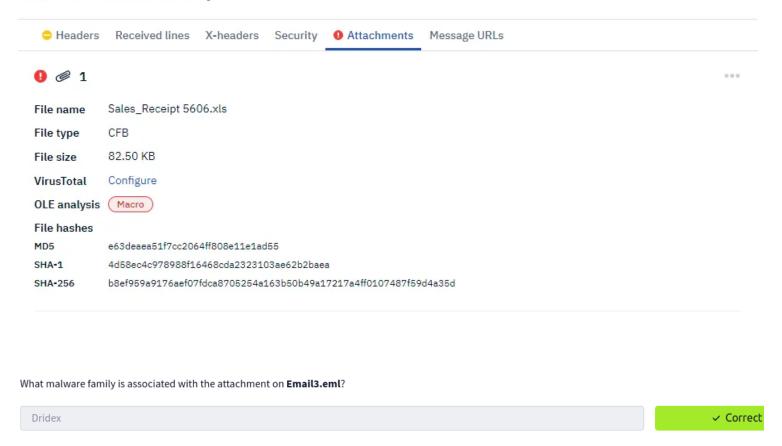
I went to the attachments and copied the SHA-256 hash. I Opened Cisco Talos and checked the reputation of the file. I then got the alias name



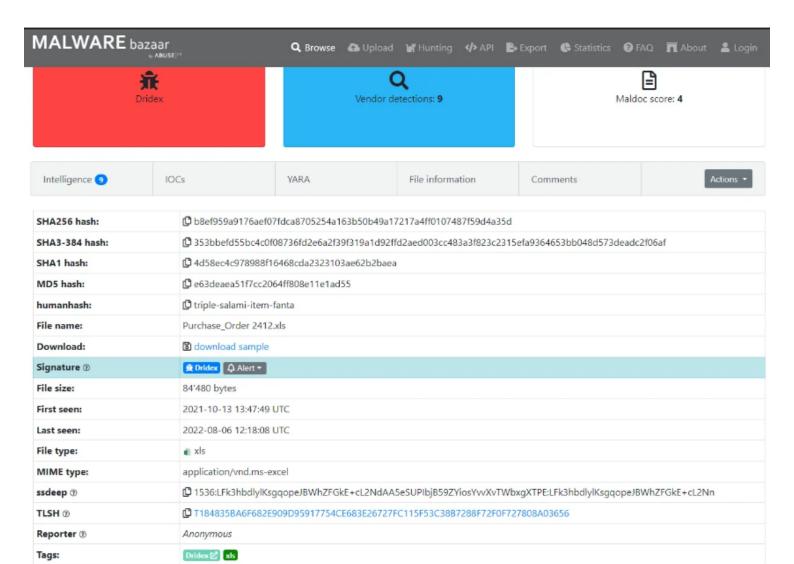
What is the name of the attachment on Email3.eml?

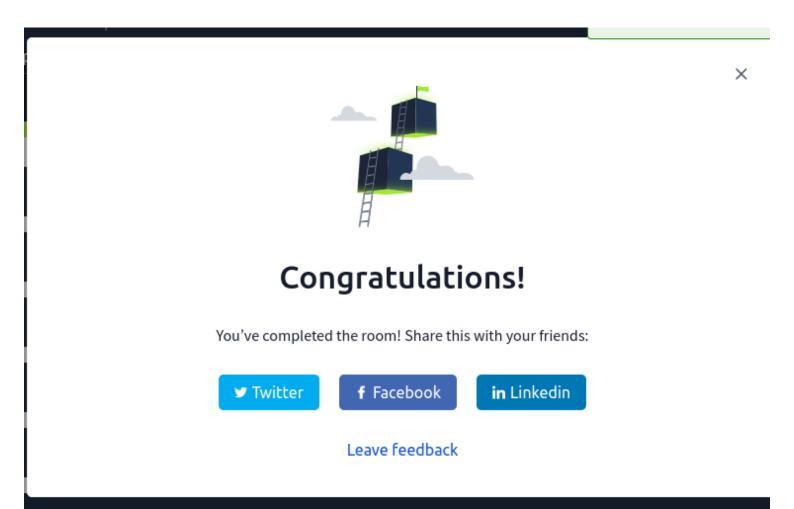
On the phishtool, I uploaded the email, analysed it and then checked on the attachments tab for detailed information pertaining this email. And it can be seen fromt the image below the file name is Sales\_Receipt 5606.xls

## Purchase Order Receipt 🔗



For this question, I used the MalwareBazaar tool. I provided the hash and analyzed it and here there were intel of importance as shown in the image below. The malware family is dridex.





https://tryhackme.com/r/room/threatinteltools

#### **CONCLUSION**

This room majorly was to introduce me to the various threat intelligence tools to analyse data and information to generate meaningful patterns to mitigate potential threats to the organisations systems and operations.