Threat Intelligence Tools

In this room, we learn about different OSINT tools that are used in the real world to conduct security threat assessments

Threat Intelligence
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 organisations, industries, sectors or governments

UrlScan.io

UrlScan.io is a website service that helps scan and analyse websites, it is used for the process of browsing and crawling websites to record activities and interactions

When searching for a website on UrlScan.io it records the data of the website you are searching for such as:

- Domains
- IP Addresses
- Resources requested from domains
- Snapshot of the page
- Technologies used by the site
- Metadata

UrlScan.io has two views:

- Recent scans
- Live scans

Scan Results

URL scan results provide ample information, with the following key areas being essential to look at:

- **Summary:** Provides general information about the URL, ranging from the identified IP address, domain registration details, page history and a screenshot of the site.
- **HTTP:** Provides information on the HTTP connections made by the scanner to the site, with details about the data fetched and the file types received.
- **Redirects:** Shows information on any identified HTTP and client-side redirects on the site.
- **Links:** Shows all the identified links outgoing from the site's homepage.
- **Behaviour:** Provides details of the variables and cookies found on the site. These may be useful in identifying the frameworks used in developing the site.
- **Indicators:** Lists all IPs, domains and hashes associated with the site. These indicators do not imply malicious activity related to the site.

We have to use UrlScan.io on Tryhackme's domain

What is TryHackMe's Cisco Umbrella Rank?

As this answer will vary many times due to it going up and down at the current time of writing this the answer is 248110 but on the site

it is 345612

Apex Domain

Subdomains

66 tryhackme.com

tryhackme.com – Cisco Umbrella Rank: 248110

assets.tryhackme.com – Cisco Umbrella Rank: 388138

If we click on the domain we can see how many domains there is:

Recently observed hostnames on 'tryhackme.com'

Searching for newly observed domains and hostnames is possible on our urlscan Pro platform.

newhelp.tryhackme.com | 2023-02-15 resources.tryhackme.com | 2022-06-10 help.tryhackme.com | 2021-01-08

monitoring.tryhackme.com | 2020-07-31 remote-us-west-1.tryhackme.com | 2020-07-01 assets.tryhackme.com | 2020-

remote-eu-1.tryhackme.com | 2020-05-26 store.tryhackme.com | 2020-04-29 docs.tryhackme.com | 2020-03-03

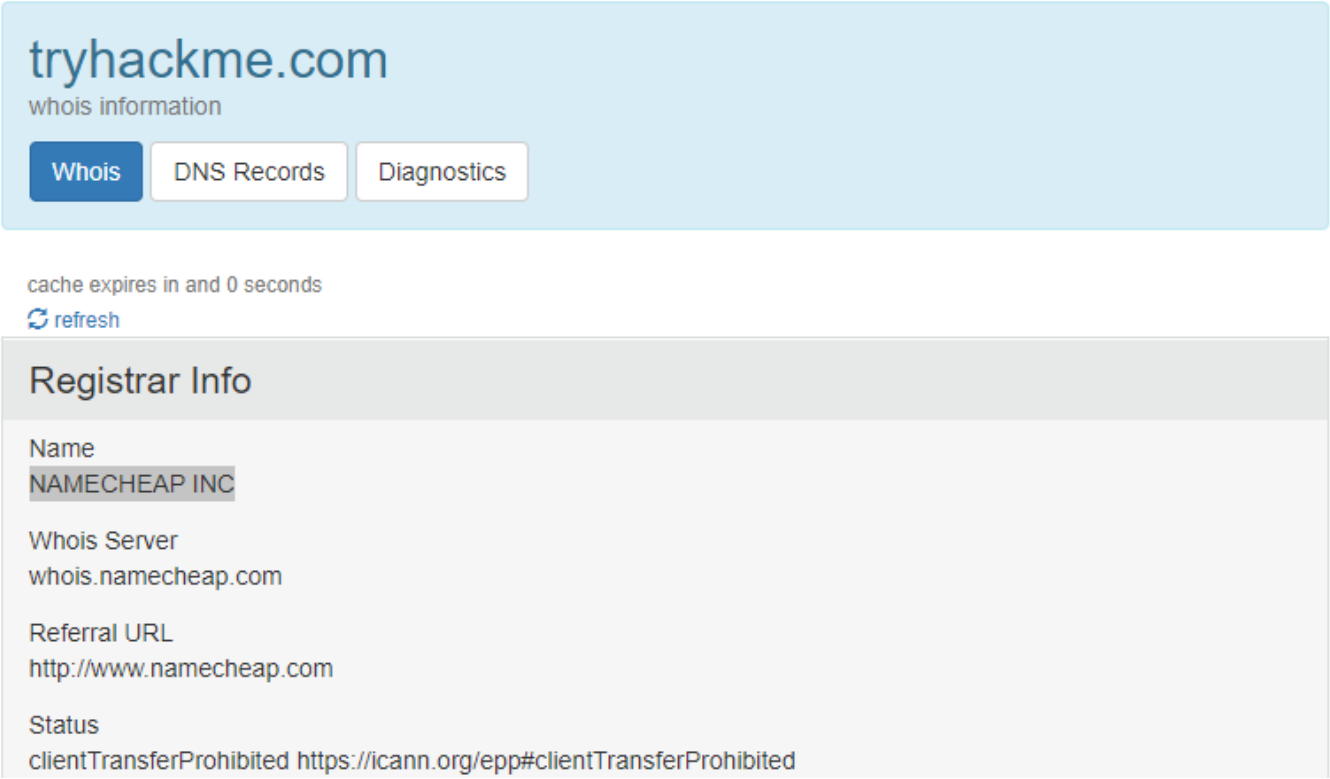
remote.tryhackme.com | 2019-09-22 blog.tryhackme.com | 2018-11-27 www.tryhackme.com | 2018-11-21

tryhackme.com | 2018-08-24

How many domains did UrlScan.io identify?

13

As I could not find it on UrlScan.io I did a whois lookup and found the main domain registar:



What is the main domain registrar listed?

NAMECHEAP INC

What is the main IP address identified?

As of the time writing this, the main IP has changed to # 2606:4700:10::6816:37e4 when the room was created the IP was 2606:4700:10::ac43:1b0a

Abuse.ch

Abuse.ch is a project that was created by the Bern University of Applied Sciences in Switzerland. This project is designed to identify and track botnets through several platforms that include:

- Malware Bazaar: A resource for sharing malware samples
- FeodoTracker: A resource used to track botnet command and control (C2) infrastructure linked with Emotet, Dridex and TrickBot

- SSL Blacklist: A resource for collecting and providing a blocklist for malicious SSL certificates and JA3/JA3s fingerprints
- URL Haus: A resource for sharing malware distribution sites
- Threat Fox: A resource for sharing indicators of compromise (IOCs)

MalwareBazaar

This is an all in one malware collection and analysis database. MalwareBazaar supports the following:

- **Malware Samples Upload:** Security analysts can upload their malware samples for analysis and build the intelligence database. This can be done through the browser or an API.
- **Malware Hunting:** Hunting for malware samples is possible through setting up alerts to match various elements such as tags, signatures, YARA rules, ClamAV signatures and vendor detection.

FeodoTracker

This helps share information on botnet Command & Control servers associated with many known malware such as Dridex, Emotes, Trickbot, Qakbot and much more
FeodoTracker also offers various IP and IOC blocklists and mitigation information to be used to prevent botnet infections

SSL Blacklist

Abuse.ch designed this to detect malicious SSL connections. If a malicious SSL connection was identified it would be updated on a deny list, which the deny list is also used to identify JA3

fingerprints that would help detect and block malware botnet C2 communications

URLhaus

This tool allows you to find malicious URLs used for malware distribution. This is a database for domains, URLs, hashes and filetypes that are suspected to be malicious and validate your investigations

ThreatFox

With ThreatFox, security analysts can search for, share and export indicators of compromise associated with malware. IOCs can be exported in various formats such as MISP events, Suricata IDS Ruleset, Domain Host files, DNS Response Policy Zone, JSON files and CSV files.

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

In ThreatFox search with `ioc: 212.192.246.30:5555`

THREAT fox by ABUSE.ch | Browse IOCs | IOC Requests | Share IOCs | Request IOCs | Data | FAQ | About | Login

ThreatFox IOC Database

You are viewing the ThreatFox database entry for ip:port **212.192.246.30:5555**.

Database Entry

Actions

IOC ID:	395319
IOC:	212.192.246.30:5555
IOC Type:	ip:port
Threat Type:	botnet_cc
Malware:	Mirai
Malware alias:	Katana
Confidence Level:	Confidence level is elevated (75%)
First seen:	2022-03-15 07:20:31 UTC
Last seen:	never
UUID:	65d0f100-a430-11ec-a022-42010aa4000a
Reporter	abuse_ch
Reward	5 credits from **ThreatFox**
Tags:	Mirai

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

SSL blacklist by ABUSE.ch

SSL Certificates JA3 Fingerprints Blacklist Statistics About

JA3 Fingerprint / Browse

JA3 Fingerprints

You can find further information about the JA3 fingerprint 51c64c77e60f3980eea90869b68c58a8, including the corresponding malware samples as well as the associated botnet C&Cs.

Database Entry

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:	222'008
Destination IPs:	4'708
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?****

https://urlhaus.abuse.ch/asn/14061/

URLhaus by ABUSE.ch

Browse API Feeds Statistics About

Database Entry

AS number:	AS14061
AS name:	DIGITALOCEAN-ASN
Country:	DE
Total IPs observed ⓘ:	1'003
Online malware site ⓘ:	54 (0%)
Offline malware site ⓘ:	57'231 (100%)
Oldest active malware site ⓘ:	2018-10-04 23:26:01 UTC (Age: 4 years, 11 months, 24 days, 22 hours, 54 minutes)
Newest active malware site ⓘ:	2023-08-25 16:38:05 UTC
Average takedown time ⓘ:	4 days, 14 hours, 35 minutes - That's a very poor abuse desk reaction time! 😮
First seen:	2018-03-14 07:54:01 UTC
Last seen:	2023-09-03 21:32:05 UTC
Data export:	URLhaus ASN feed

****Which country is the botnet IP address 178.134.47.166 associated with according to FeodoTracker?****

Malware Botnet C&C

You are currently viewing the database entry for the malware botnet command&control server (C&C) hosted at 178.134.47.166 . You can get additional information about this C&C here, such as first seen, last seen and associated malware samples.

Database Entry

IP address:	178.134.47.166
Hostname:	178-134-47-166.dsl.utg.ge
AS number:	AS35805
AS name:	SILKNET-AS
Country:	GE
First seen:	2021-04-22 22:04:30 UTC
Last online:	2022-04-04 12:xx:xx UTC

PhishTool

Email phishing is one of the main precursors of any cyber attack. Unsuspecting users get duped into opening and accessing malicious files and links sent to them by email, as they appear to be legitimate. As a result, adversaries infect their victims’ systems with malware, harvesting their credentials and personal data

and performing other actions such as financial fraud or conducting ransomware attacks

PhishTool is an email phishing analysis tool that allows us to dive deeper into a phishing email and provide email security. The core Features of PhishTool include:

- **Perform email analysis:** PhishTool retrieves metadata from phishing emails and provides analysts with the relevant explanations and capabilities to follow the email's actions, attachments, and URLs to triage the situation.
- **Heuristic intelligence:** OSINT is baked into the tool to provide analysts with the intelligence needed to stay ahead of persistent attacks and understand what TTPs were used to evade security controls and allow the adversary to social engineer a target.

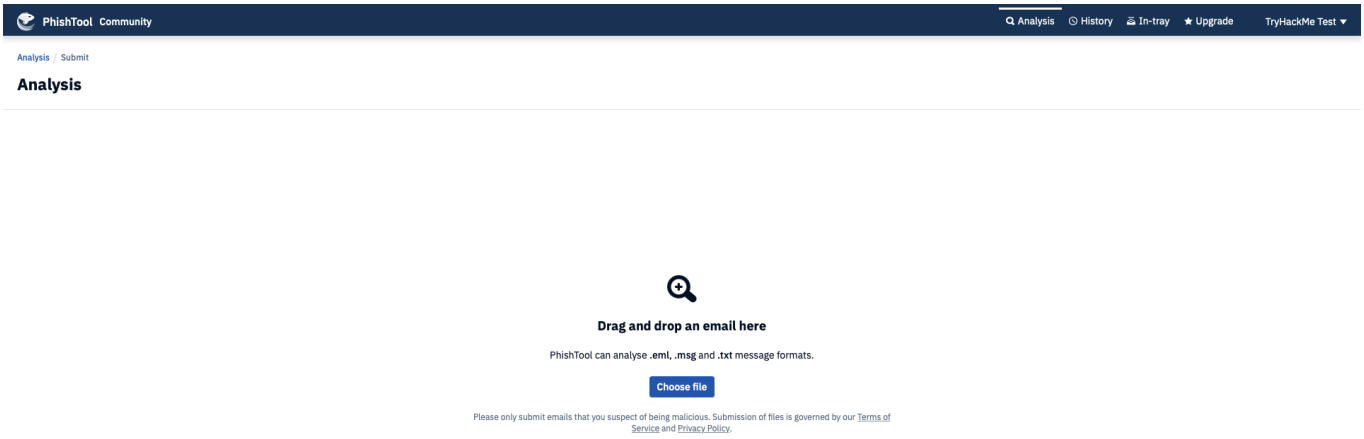
- **Classification and reporting:** Phishing email classifications are conducted to allow analysts to take action quickly. Additionally, reports can be generated to provide a forensic record that can be shared.

The enterprise PhishTool has extra features:

- Manage user-reported phishing events
- Report phishing email findings back to users and keep them engaged in the process
- Email stack integration with Microsoft 365 and Google Workspace

We are presented with an upload file screen from the Analysis tab on login. Here, we submit our email for analysis in the stated file formats. Other tabs include:

- **History:** Lists all submissions made with their resolutions.
- **In-tray:** An Enterprise feature used to receive and process phish reports posted by team members through integrating Google Workspace and Microsoft 365.



Analysis Tab

Once uploaded, we are presented with the details of our email for a more in-depth look. Here, we have the following tabs:

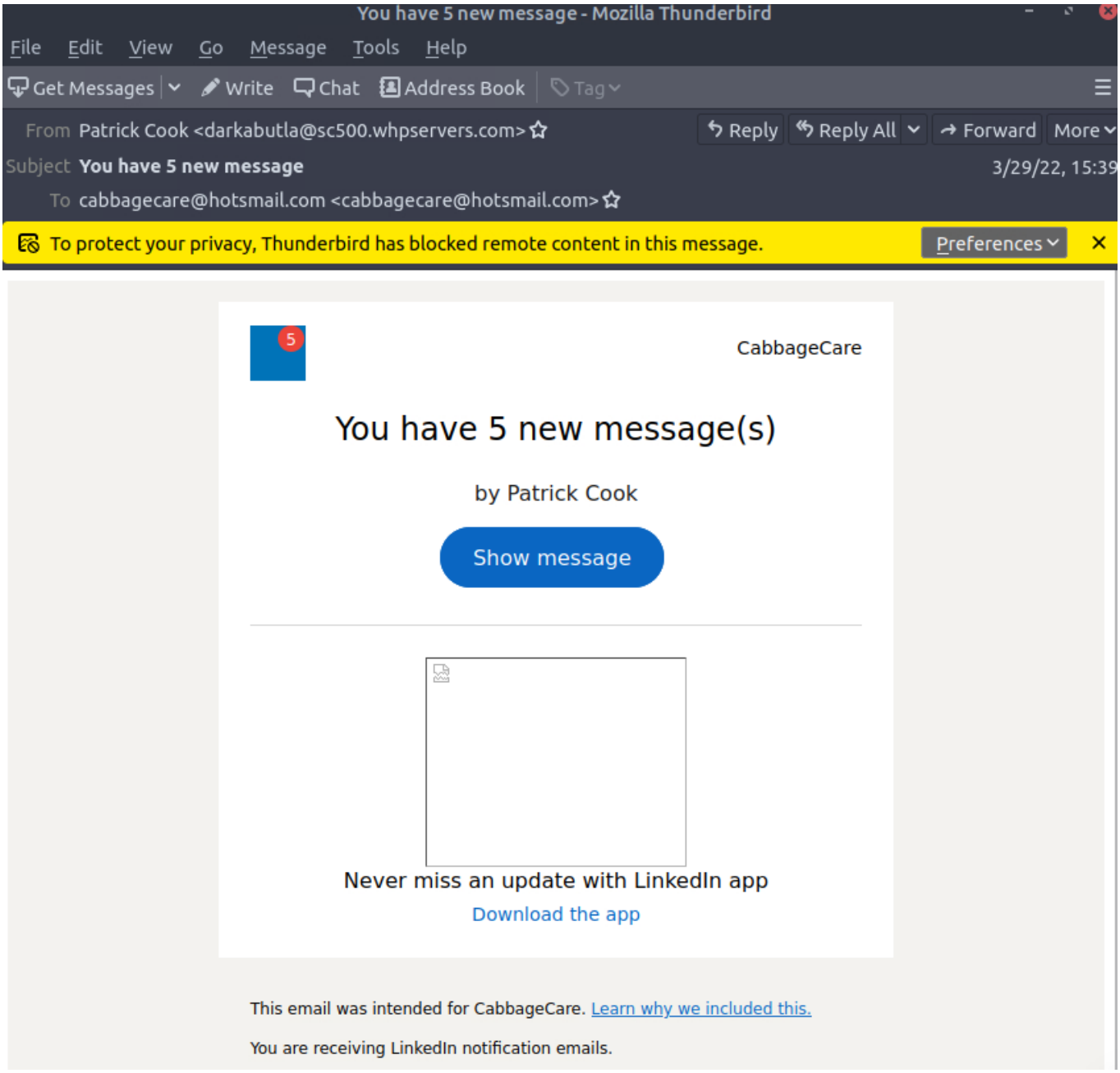
- **Headers:** Provides the routing information of the email, such as source and

destination email addresses, Originating IP and DNS addresses and Timestamp.

- **Received Lines:** Details on the email traversal process across various SMTP servers for tracing purposes.
- **X-headers:** These are extension headers added by the recipient mailbox to provide additional information about the email.
- **Security:** Details on email security frameworks and policies such as Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting and Conformance (DMARC).
- **Attachments:** Lists any file attachments found in the email.
- **Message URLs:** Associated external URLs found in the email will be found here.

Scenario

You are a SOC Analyst and have been tasked to analyse a suspicious email, **Email1.eml**. To solve the task, open the email using **Thunderbird** on the attached VM, analyse it and answer the questions below.



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

LinkedIn

What is the senders email address?

darkabutla@sc500.whpservers.com

What is the recipient's email address?

cabbagecare@hotsmail.com

ile Edit View Help

```
Received: from DB9P194MB1386.EURP194.PROD.OUTLOOK.COM (2603:10a6:10:296::24) by
 AM8P194MB1513.EURP194.PROD.OUTLOOK.COM with HTTPS; Tue, 29 Mar 2022 20:39:29
 +0000
Received: from DM3PR12CA0063.namprd12.prod.outlook.com (2603:10b6:0:56::31) by
 DB9P194MB1386.EURP194.PROD.OUTLOOK.COM (2603:10a6:10:296::24) with Microsoft
 SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)
 id 15.20.5102.17; Tue, 29 Mar 2022 20:39:28 +0000
Received: from DM6NAM10FT030.eop-nam10.prod.protection.outlook.com
 (2603:10b6:0:56:cafe::5d) by DM3PR12CA0063.outlook.office365.com
 (2603:10b6:0:56::31) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.5123.13 via Frontend
 Transport; Tue, 29 Mar 2022 20:39:28 +0000
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
Authentication-Results: spf=none (sender IP is 204.93.183.11) smtp.mailfrom=sc500.whps
 dkim=none (message not signed) header.d=none;dmarc=none action=none
 header.from=sc500.whpservers.com;compauth=pass reason=105
Received-SPF: None (protection.outlook.com: sc500.whpservers.com does not designate
```

Download CyberChef

Last build: 2 months ago - Version 10 is here! Read about the new features

Operations

defang

- Defang URL
- Defang IP Addresses
- Favourites
- Data format
- Encryption / Encoding
- Public Key
- Arithmetic / Logic
- Networking
- Language
- Utils
- Date / Time
- Extractors
- Compression
- Hashing
- Code tidy
- Forensics

Recipe

Defang IP Addresses

Input

204.93.183.11

Output

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

What is the Originating IP address? Defang

the IP address

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

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

4

Cisco Talos Intelligence
Cisco Talos helps provide actionable intelligence, visibility on indicators, and protection against emerging threats through data collected from their products. The solution is accessible as Talos Intelligence.

Cisco Talos encompasses six key teams:

- **Threat Intelligence & Interdiction:** Quick correlation and tracking of threats provide a means to turn simple IOCs into context-rich intel.
- **Detection Research:** Vulnerability and malware analysis is performed to create

rules and content for threat detection.

- **Engineering & Development:** Provides the maintenance support for the inspection engines and keeps them up-to-date to identify and triage emerging threats.
- **Vulnerability Research & Discovery:** Working with service and software vendors to develop repeatable means of identifying and reporting security vulnerabilities.
- **Communities:** Maintains the image of the team and the open-source solutions.
- **Global Outreach:** Disseminates intelligence to customers and the security community through publications.

Talos dashboard shows a world map with an overview of email traffic. Talos determines if these emails are safe, spam or phishing

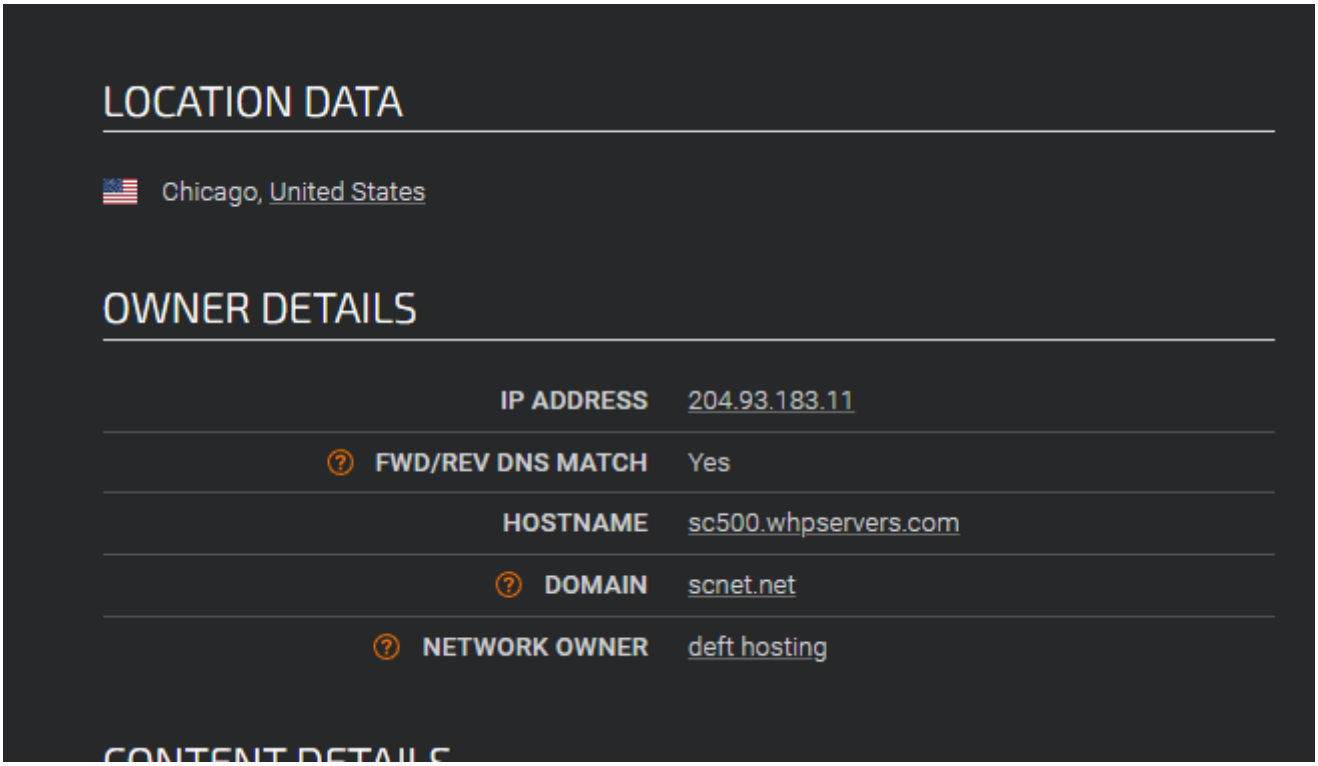
Here are two of Talos Features:

- **Vulnerability Information:** Disclosed and zero-day vulnerability reports marked with CVE numbers and CVSS scores. Details of the vulnerabilities reported are provided when you select a specific report, including the timeline taken to get the report published. Microsoft vulnerability advisories are also provided, with the applicable snort rules that can be used
- **Reputation Center:** Provides access to searchable threat data related to IPs and files using their SHA256 hashes. Analysts would rely on these options to conduct their investigations. Additional email and spam data can be found under the Email & Spam Data tab.

Task

Use the information gathered from inspecting the **Email1.eml** file from Task 5 to answer the

following questions using Cisco Talos Intelligence. Please note that the VM launched in Task 5 would not have access to the Internet.



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

scnet.net

Go over to the Whois Tab on Talos and search for customer

```
# start

NetRange:       204.93.183.0 - 204.93.183.25
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 (C05082
RegDate:        2014-06-06
Updated:        2014-06-06
Ref:            https://rdap.arin.net/regist


CustName:       Complete Web Reviews
```

What is the customer name of the IP address?

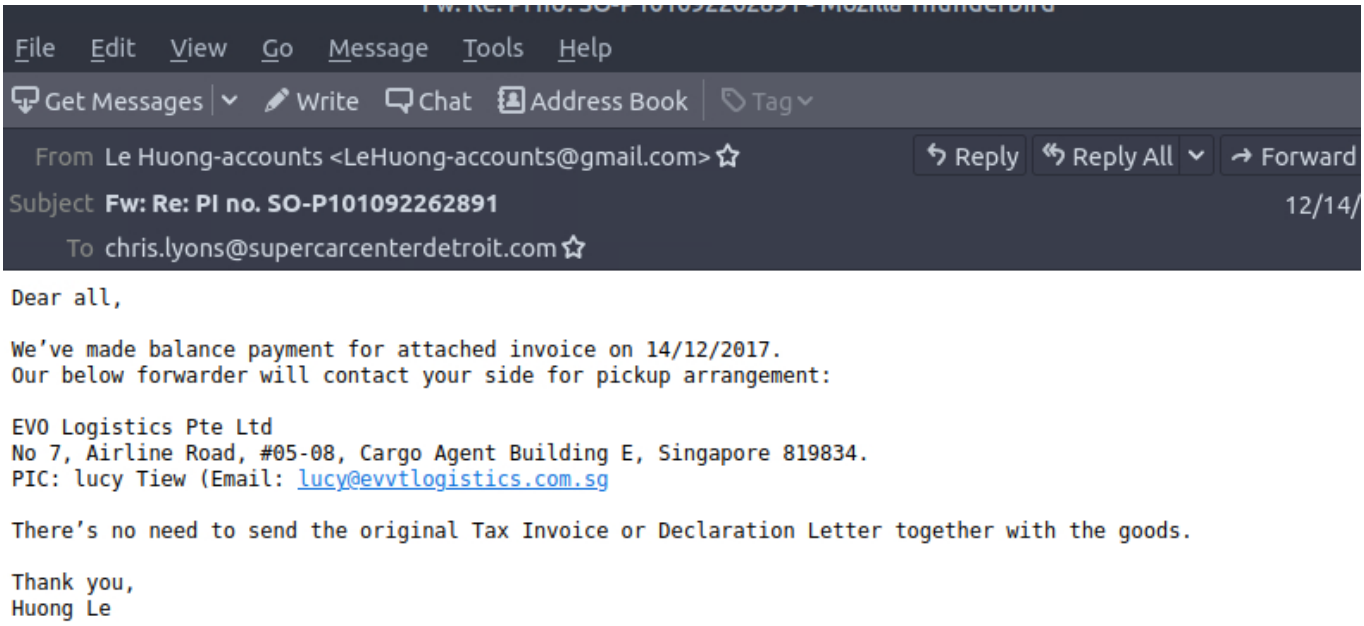
Complete Web Reviews

Scenario 1

Scenario: You are a SOC Analyst. Several suspicious emails have been forwarded to you from other coworkers. You must obtain details from each email to triage the incidents reported.

Task: Use the tools and knowledge discussed throughout this room (or use your resources) to help you analyze **Email2.eml** found on

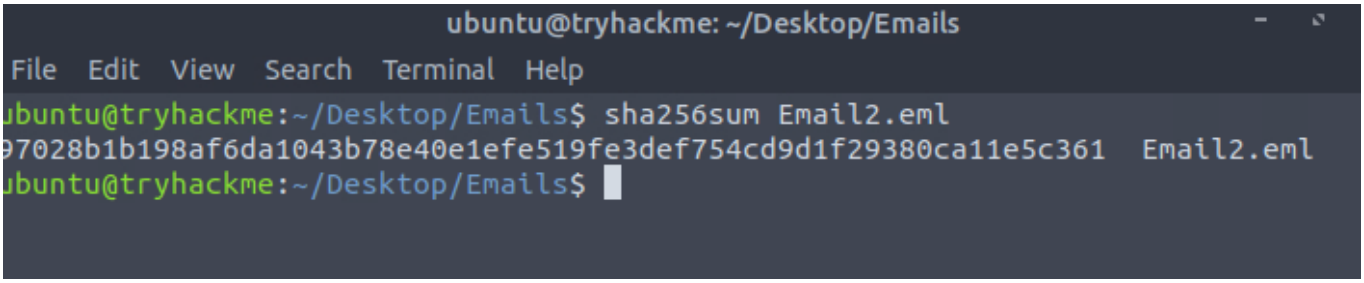
the VM attached to **Task 5** and use the information to answer the questions.



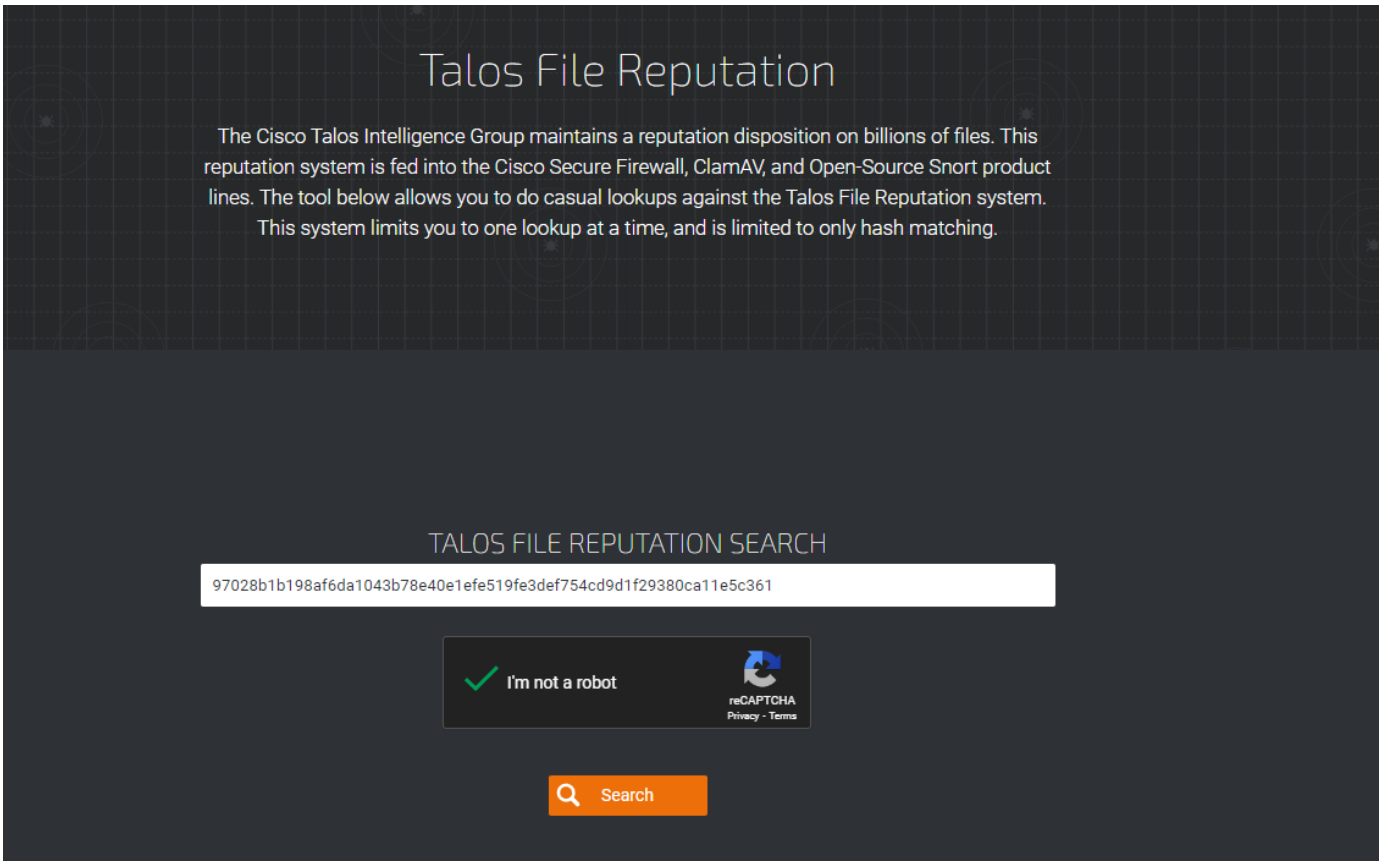
According to Email2.eml, what is the recipient's email address?

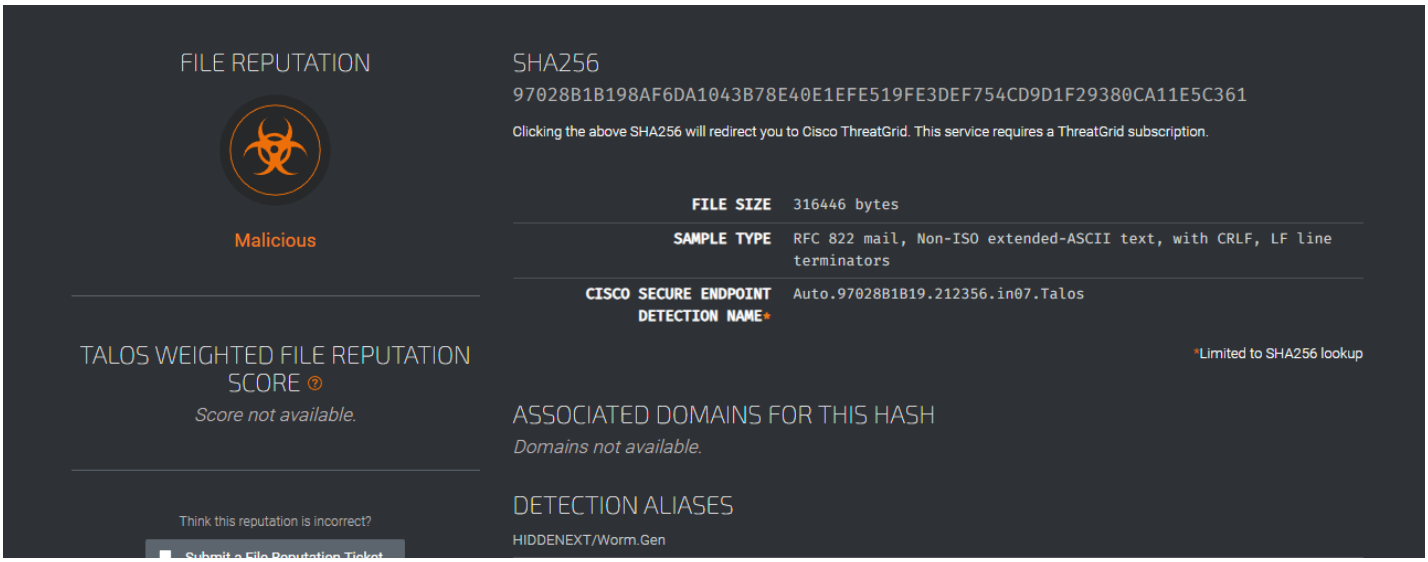
chris.lyons@supercarcenterdetroit.com

Run `sha256sum Email2.eml` this will give use the sha256 hash



Run it in Talos





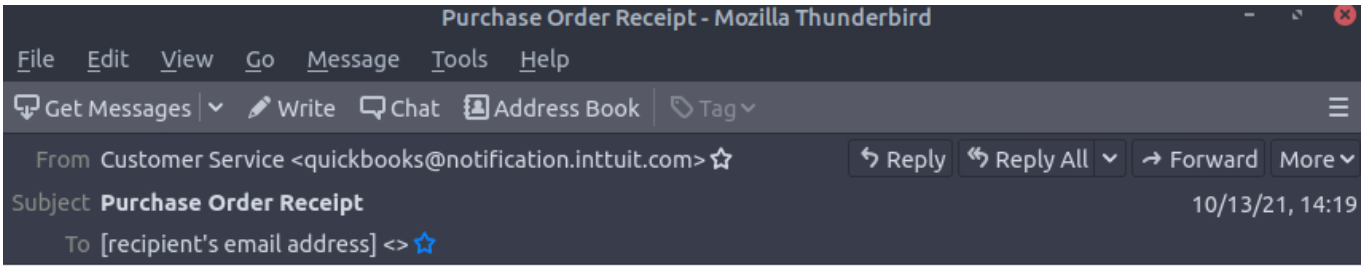
From Talos Intelligence, the attached file can also be identified by the Detection Alias that starts with an H...?**

HIDDENEXT/Worm.Gen

Scenario 2

Scenario: You are a SOC Analyst. Several suspicious emails have been forwarded to you from other coworkers. You must obtain details from each email to triage the incidents reported.

Task: Use the tools and knowledge discussed throughout this room (or use your resources) to help you analyze **Email3.eml** found on the VM attached to **Task 5** and use the information to answer the questions.



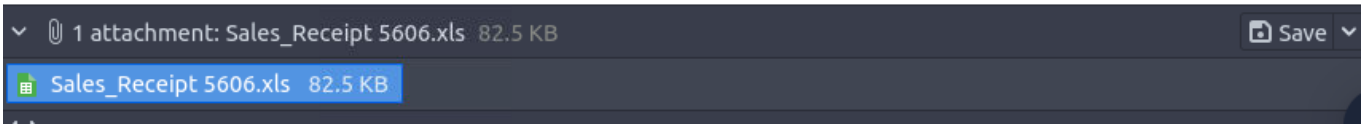
Please find our purchase order attached to this email.

Thank you for your business - we appreciate it very much.

Sincerely,

---------- Purchase Order Summary ----------
Sale # : 5606
Sale Date: 10/13/2021
Total: $3,431.00

The complete version has been provided as an attachment to this email.



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

Sales_Receipt 5606.xls

Run the same command that was run on Email2 and will get the SHA-256 hash

Search it in Talos and you will be able to find the malware family

FILE REPUTATION

Malicious

5 WEIGHTED FILE REPUTATION SCORE

Score not available.

Think this reputation is incorrect?

Submit a File Reputation Ticket

SHA256

F4D97603256A36E81BFE7EF5E0CCAEE44F77DE6BB041FA41F0B3A0DB53F4ABA9

Clicking the above SHA256 will redirect you to Cisco ThreatGrid. This service requires a ThreatGrid subscription.

FILE SIZE	117299 bytes
SAMPLE TYPE	RFC 822 mail, ASCII text
CISCO SECURE ENDPOINT DETECTION NAME*	Auto.F4D9760325.252139.in07.Talos

*Limited to SHA256 lookup

ASSOCIATED DOMAINS FOR THIS HASH

Domains not available.

DETECTION ALIASES

W97M/Agent.2325811

Other:Malware-gen [Trj]

X97M/Dridex.A.gen!Eldorado

Trojan.GenericKD.47173557

VBA/Agent.AD55!tr

Trojan-Downloader.VBA.Agent

HEUR:Trojan-Downloader.MSOffice.SLoad.gen

X97M/Downloader.lu (trojan)

TrojanDownloader:O97M/Dridex.AL!MTB

Ole.Trojan.A2304487

W97M.Downloader

What malware family is associated with the attachment on Email3.eml?

Dridex