TRY HACK ME: Threat Intelligence Tools Write-Up

Threat Intelligence Tools
Explore different OSINT tools used to conduct security threat assessments and investigations.

Task 1 Room Outline-

Concepts of Threat Intelligence and various open-source tools that are useful. The learning objectives include:

- Understanding the basics of threat intelligence & its classifications.
- Using UrlScan.io to scan for malicious URLs.
- Using Abuse.ch to track malware and botnet indicators.
- Investigate phishing emails using PhishTool
- Using Cisco's Talos Intelligence platform for intel gathering

Answer to the questions of this section-

No Answer needed

Task 2 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.

Threat Intelligence Classifications:

Threat Intel is geared towards understanding the relationship between your operational environment and your adversary. With this in mind, we can break down threat intel into the following classifications:

Strategic Intel: High-level intel that looks into the organisation's threat landscape and maps out the risk areas based on trends, patterns and emerging threats that may impact business decisions.

Technical Intel: Looks into evidence and artefacts of attack used by an adversary. Incident Response teams can use this intel to create a baseline attack surface to analyse and develop defence mechanisms.

Tactical Intel: Assesses adversaries' tactics, techniques, and procedures (TTPs). This intel can strengthen security controls and address vulnerabilities through real-time investigations.

Operational Intel: Looks into an adversary's specific motives and intent to perform an attack. Security teams may use this intel to understand the critical assets available in the organisation (people, processes, and technologies) that may be targeted

Answer to the questions of this section-

No Answer needed

Task 3 UrlScan.io-

Urlscan.io is a free service developed to assist in scanning and analysing websites. It is used to automate the process of browsing and crawling through websites to record activities and interactions.

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.

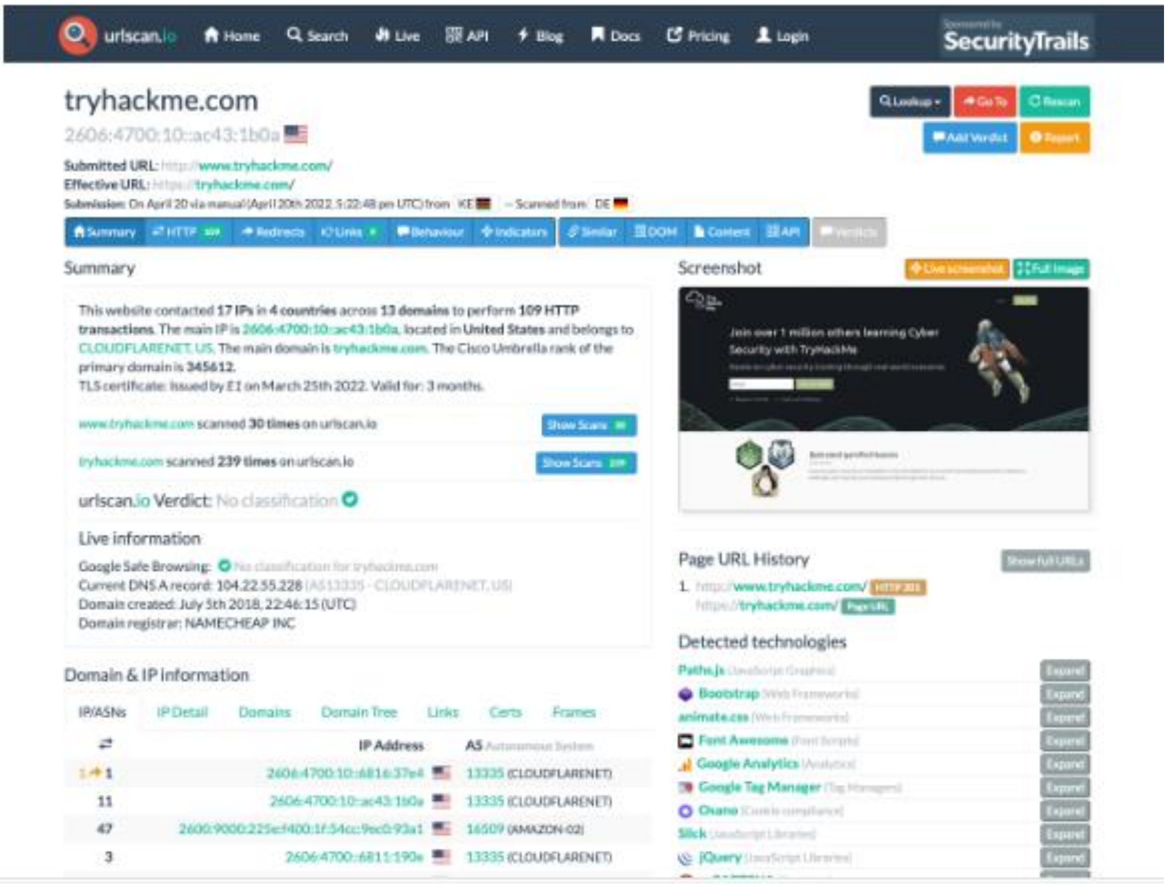
Links: Shows all the identified links outgoing from the site's homepage.

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.

Scenario

You have been tasked to perform a scan on TryHackMe's domain. The results obtained are displayed in the image below. Use the details on the image to answer the questions:



tryhackme.com

2606:4700:10::ac43:1b0a

Submitted URL: http://www.tryhackme.com/
Effective URL: https://tryhackme.com/
Submission: On April 20 via manual (April 20th 2022 5:22:48 pm UTC) from KE — Scanned from DE

Summary

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**.
TLS certificate: Issued by *E1* on March 25th 2022. Valid for: 3 months.

www.tryhackme.com scanned **30 times** on urlscan.io

tryhackme.com scanned **239 times** on urlscan.io

urlscan.io Verdict: No classification

Live information

Google Safe Browsing: No 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

Domain & IP information

IP/ASNs IP Detail Domains Domain Tree Links Certs Frames

⇄	IP Address	AS Autonomous System
1 → 1	2606:4700:10::6816:37e4	13335 (CLOUDFLARENET)
11	2606:4700:10::ac43:1b0a	13335 (CLOUDFLARENET)
47	2600:9000:225e:f400:1f:54cc:9ec0:93a1	16509 (AMAZON-02)
3	2606:4700::6811:190e	13335 (CLOUDFLARENET)

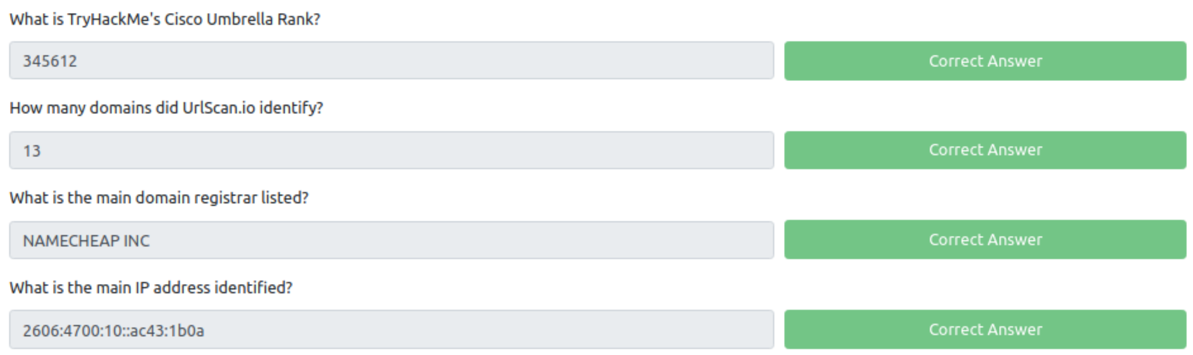
Page URL History

1. http://www.tryhackme.com/ HTTP 301
https://tryhackme.com/ Page URL

Detected technologies

Paths.js (JavaScript Graphics)
Bootstrap (Web Frameworks)
animate.css (Web Frameworks)
Font Awesome (Font Scripts)
Google Analytics (Analytics)
Google Tag Manager (Tag Managers)
Osano (Cookie compliance)
Slick (JavaScript Libraries)
jQuery (JavaScript Libraries)

Answer to the questions of this section-



What is TryHackMe's Cisco Umbrella Rank?

345612 — Correct Answer

How many domains did UrlScan.io identify?

13 — Correct Answer

What is the main domain registrar listed?

NAMECHEAP INC — Correct Answer

What is the main IP address identified?

2606:4700:10::ac43:1b0a — Correct Answer

Task 4 Abuse.ch-

Abuse.ch is a research project hosted by the Institue for Cybersecurity and Engineering at the Bern University of Applied Sciences in Switzerland. It was developed to identify and track malware and botnets through several operational platforms developed under the project. These platforms are:

Malware Bazaar: A resource for sharing malware samples.

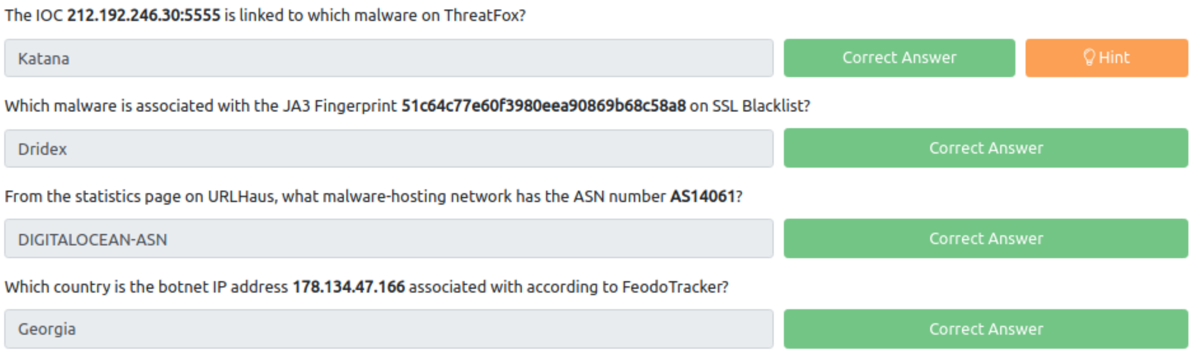
Feodo Tracker: A resource used to track botnet command and control (C2) infrastructure linked with Emotet, Dridex and TrickBot.

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).

Answer to the questions of this section-



The IOC **212.192.246.30:5555** is linked to which malware on ThreatFox?

Katana

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

Dridex

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

DIGITALOCEAN-ASN

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

Georgia

Task 5 PhishTool-

PhishTool seeks to elevate the perception of phishing as a severe form of attack and provide a responsive means of email security. Through email analysis, security analysts can uncover email IOCs, prevent breaches and provide forensic reports that could be used in phishing containment and training engagements.

PhishTool has two accessible versions: Community and Enterprise. We shall mainly focus on the Community version and the core features in this task. Sign up for an account via this link to use the tool.

The core features 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.

Additional features are available on the Enterprise version:

- 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.

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).

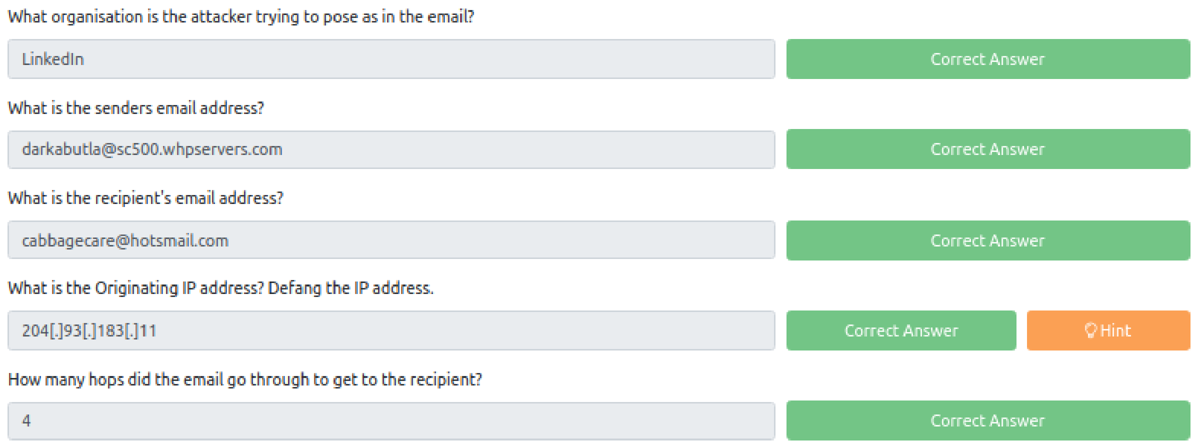
Attachments: Lists any file attachments found in the email.

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. Use the tool and skills learnt on this task to answer the questions.

Answer to the questions of this section-



What organisation 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@hotmail.com

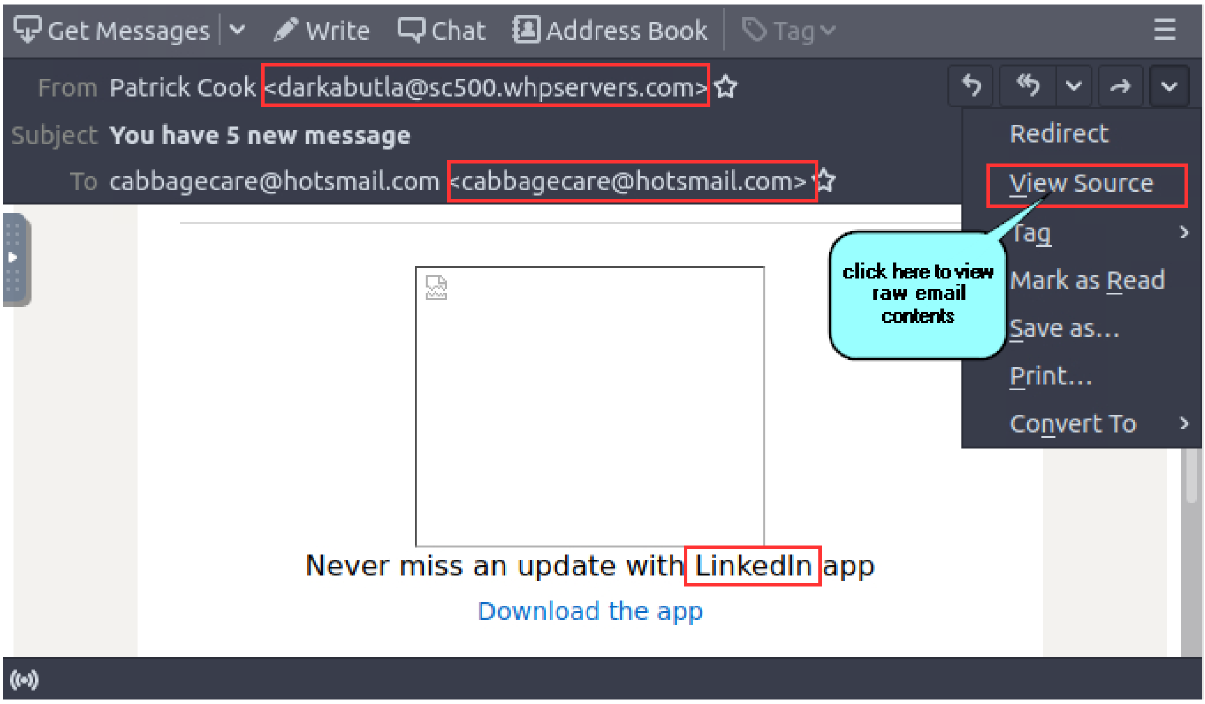
What is the Originating IP address? Defang the IP address.

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

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

4

Answers-



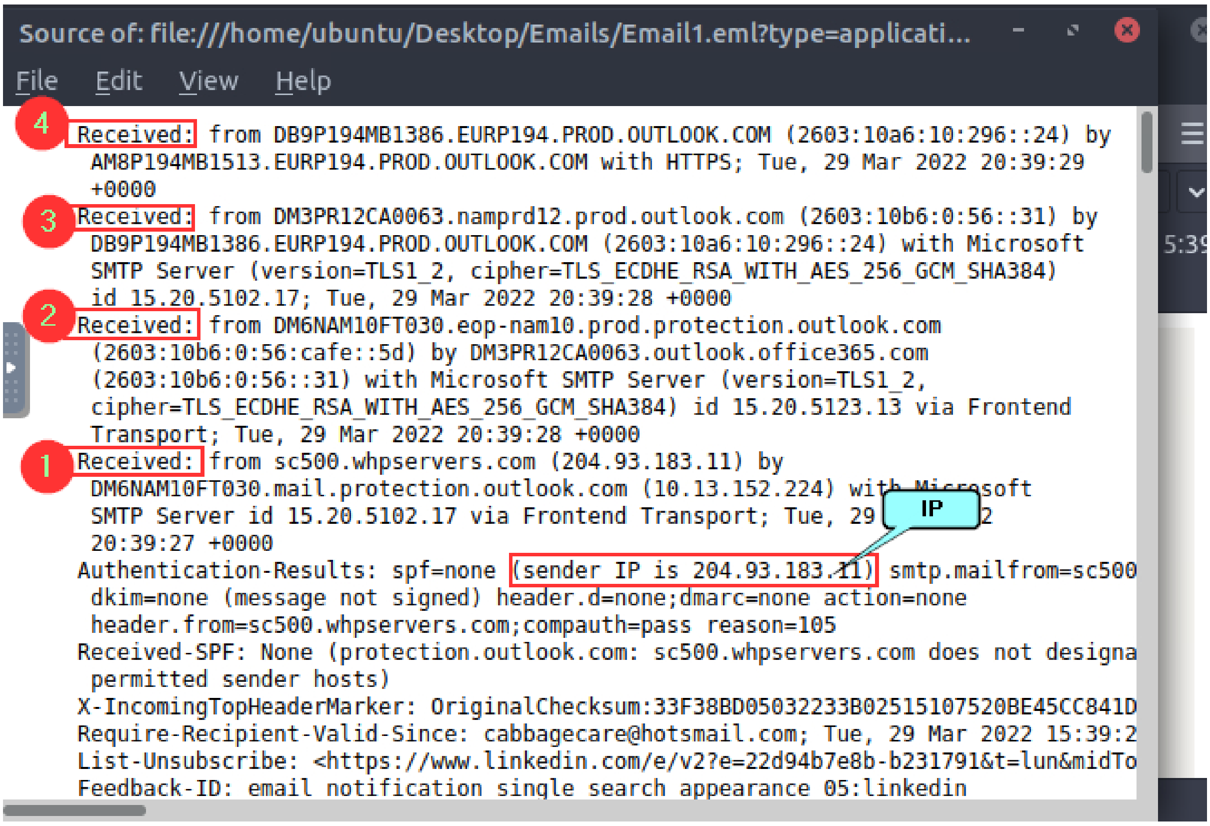
From Patrick Cook <darkabutla@sc500.whpservers.com>

Subject **You have 5 new message**

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

Never miss an update with LinkedIn app

Download the app


Source of: file:///home/ubuntu/Desktop/Emails/Email1.eml?type=applicati…
File
Edit
View
Help
4
3
2
1
IP

```
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           2
 20:39:27 +0000
Authentication-Results: spf=none (sender IP is 204.93.183.11) smtp.mailfrom=sc500
 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 designa
 permitted sender hosts)
X-IncomingTopHeaderMarker: OriginalChecksum:33F38BD05032233B02515107520BE45CC841D
Require-Recipient-Valid-Since: cabbagecare@hotsmail.com; Tue, 29 Mar 2022 15:39:2
List-Unsubscribe: <https://www.linkedin.com/e/v2?e=22d94b7e8b-b231791&t=lun&midTo
Feedback-ID: email notification single search appearance 05:linkedin
```

Task 6 Cisco Talos Intelligence-

IT and Cybersecurity companies collect massive amounts of information that could be used for threat analysis and intelligence. Being one of those companies, Cisco assembled a large team of security practitioners called Cisco Talos to 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.

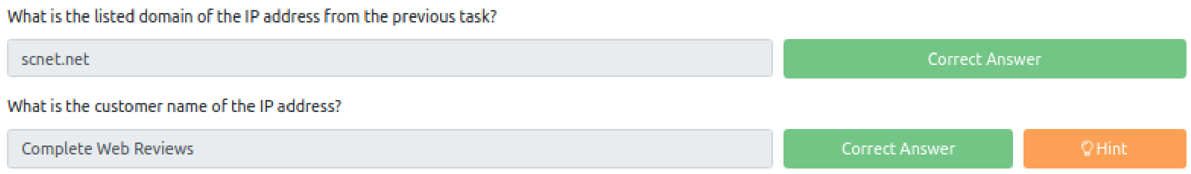
Global Outreach: Disseminates intelligence to customers and the security community through publications.

More information about Cisco Talos can be found on their White Paper

Task

Use the .eml file you've downloaded in the previous task, PhishTool, to answer the following questions.

Answer to the questions of this section-



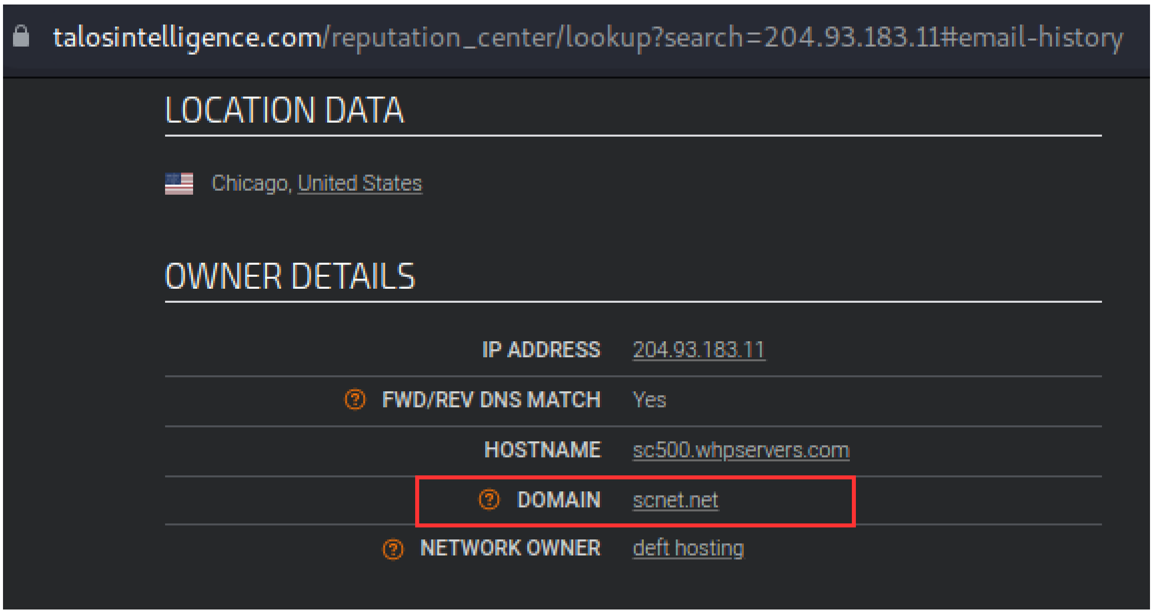
What is the listed domain of the IP address from the previous task?

scnet.net

What is the customer name of the IP address?

Complete Web Reviews

Answers-



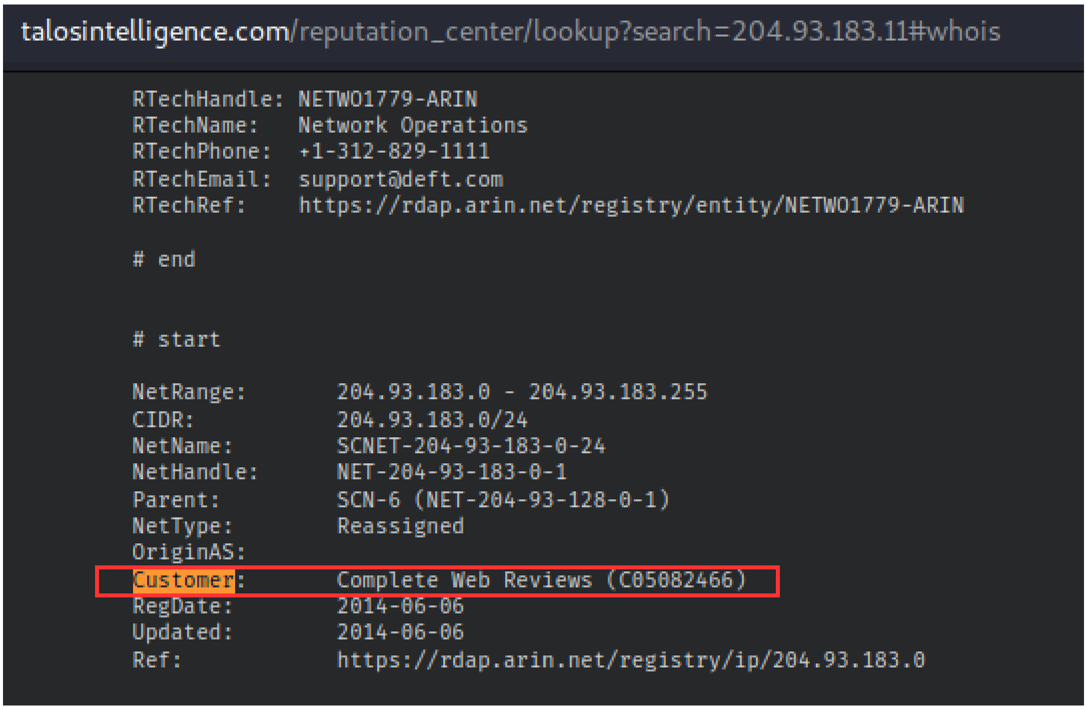
talosintelligence.com/reputation_center/lookup?search=204.93.183.11#email-history

LOCATION DATA

Chicago, United States

OWNER DETAILS

IP ADDRESS	204.93.183.11
FWD/REV DNS MATCH	Yes
HOSTNAME	sc500.whpservers.com
DOMAIN	scnet.net
NETWORK OWNER	deft hosting



talosintelligence.com/reputation_center/lookup?search=204.93.183.11#whois

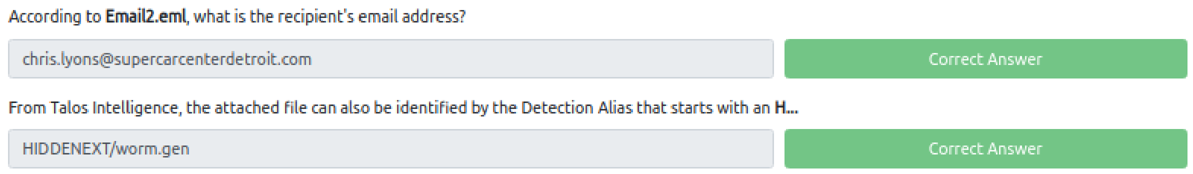
```
RTechHandle: NETWO1779-ARIN
RTechName:   Network Operations
RTechPhone:  +1-312-829-1111
RTechEmail:  support@deft.com
RTechRef:    https://rdap.arin.net/registry/entity/NETWO1779-ARIN

# end


# start

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
```

Task 7 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 discussed throughout this room (or use your resources) to help you analyze Email2.eml and use the information to answer the questions.

Answer to the questions of this section-



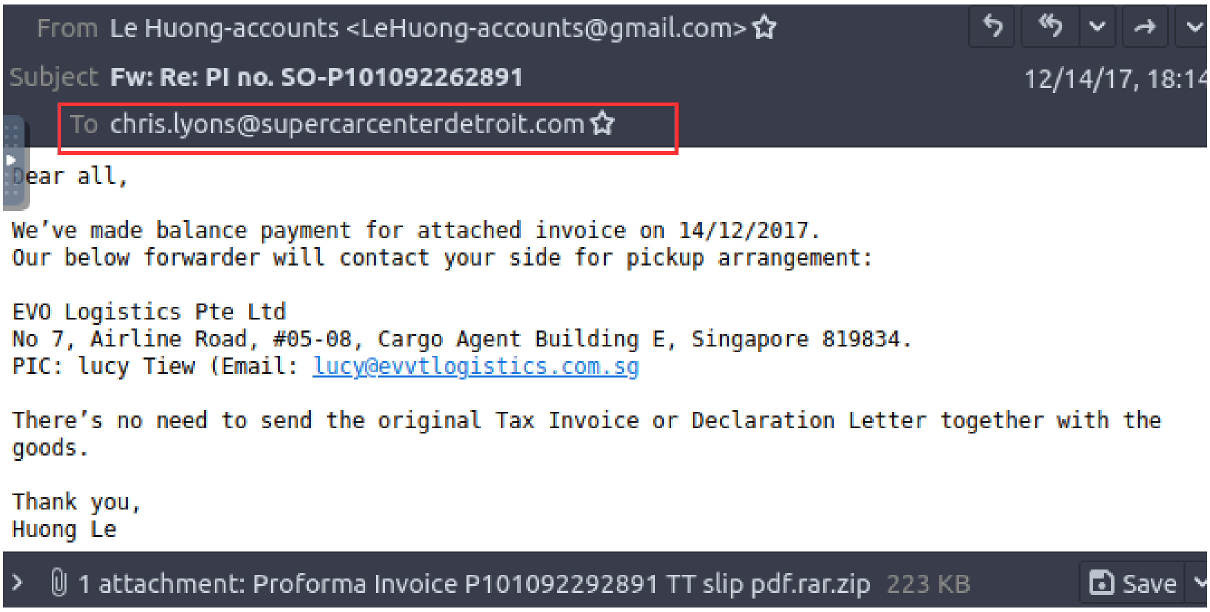
According to **Email2.eml**, what is the recipient's email address?

chris.lyons@supercarcenterdetroit.com

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

HIDDENEXT/worm.gen

Answers- steps



From Le Huong-accounts <LeHuong-accounts@gmail.com>

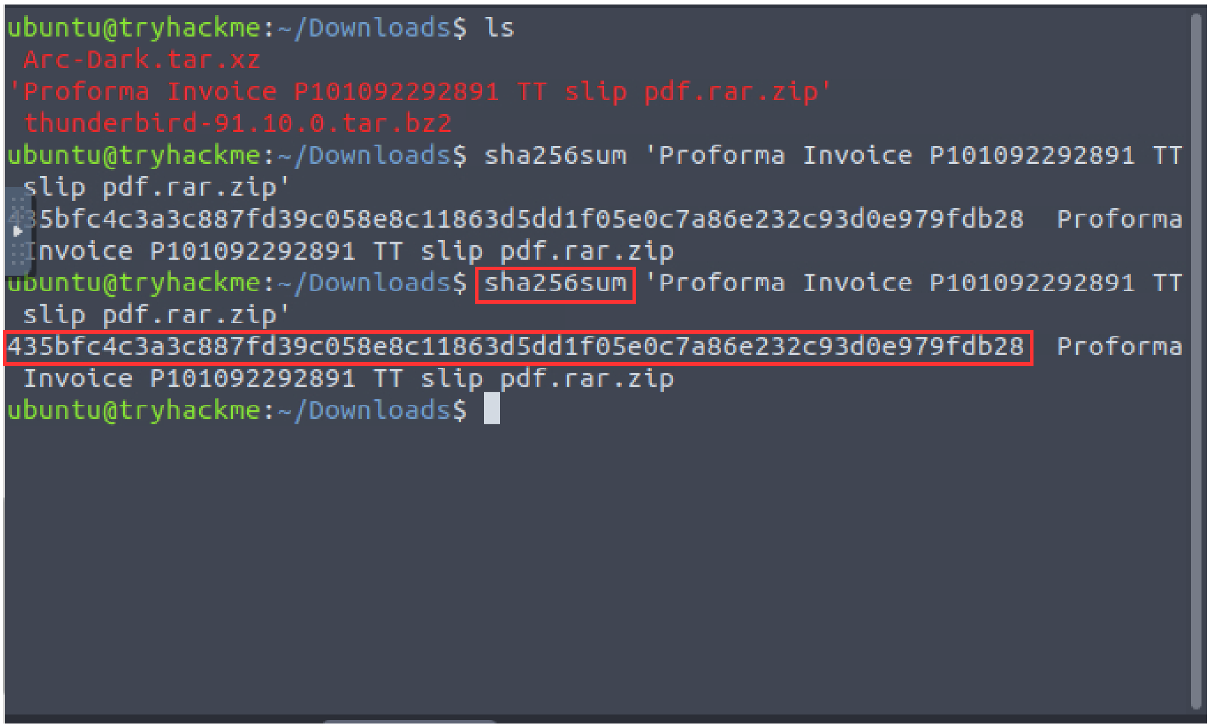
Subject **Fw: Re: PI no. SO-P101092262891**

12/14/17, 18:14

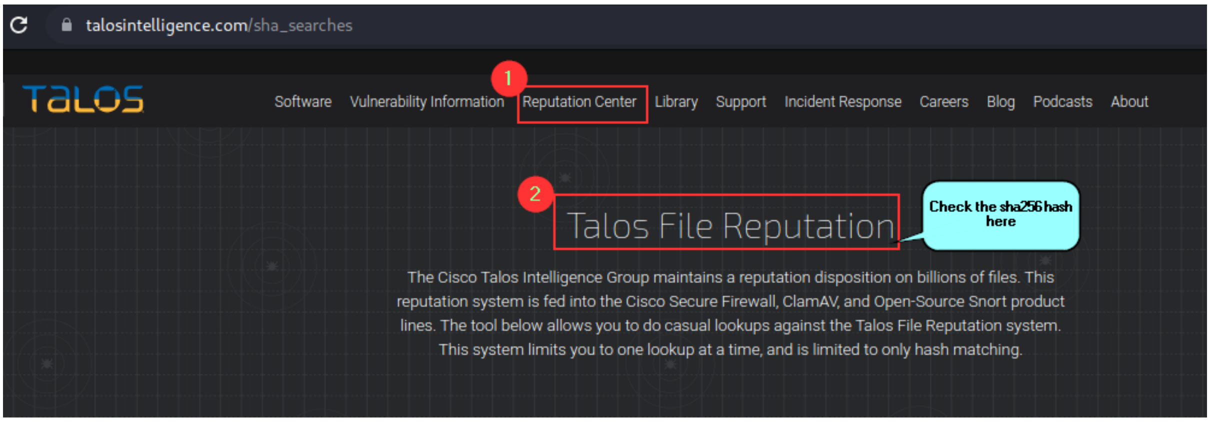
To chris.lyons@supercarcenterdetroit.com

```
Dear all,

We’ve made balance payment for attached invoice on 14/12/2017.
Our below forwarder will contact your side for pickup arrangement:

EVO Logistics Pte Ltd
No 7, Airline Road, #05-08, Cargo Agent Building E, Singapore 819834.
PIC: lucy Tiew (Email: lucy@evvtlogistics.com.sg

There’s no need to send the original Tax Invoice or Declaration Letter together with the
goods.

Thank you,
Huong Le
```

1 attachment: Proforma Invoice P101092292891 TT slip pdf.rar.zip 223 KB

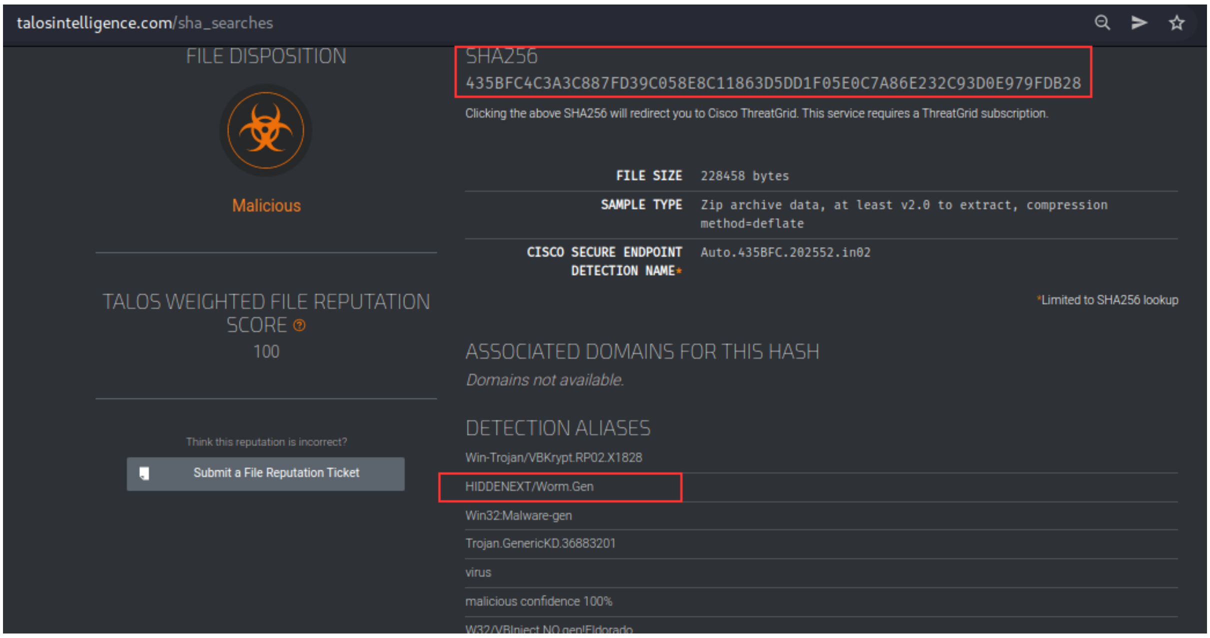


```
ubuntu@tryhackme:~/Downloads$ ls
 Arc-Dark.tar.xz
'Proforma Invoice P101092292891 TT slip pdf.rar.zip'
 thunderbird-91.10.0.tar.bz2
ubuntu@tryhackme:~/Downloads$ sha256sum 'Proforma Invoice P101092292891 TT
 slip pdf.rar.zip'
435bfc4c3a3c887fd39c058e8c11863d5dd1f05e0c7a86e232c93d0e979fdb28  Proforma
Invoice P101092292891 TT slip pdf.rar.zip
ubuntu@tryhackme:~/Downloads$ sha256sum 'Proforma Invoice P101092292891 TT
 slip pdf.rar.zip'
435bfc4c3a3c887fd39c058e8c11863d5dd1f05e0c7a86e232c93d0e979fdb28  Proforma
 Invoice P101092292891 TT slip pdf.rar.zip
ubuntu@tryhackme:~/Downloads$
```



Talos File Reputation

The Cisco Talos Intelligence Group maintains a reputation disposition on billions of files. This reputation system is fed into the Cisco Secure Firewall, ClamAV, and Open-Source Snort product lines. The tool below allows you to do casual lookups against the Talos File Reputation system. This system limits you to one lookup at a time, and is limited to only hash matching.



FILE DISPOSITION

Malicious

TALOS WEIGHTED FILE REPUTATION SCORE

100

Think this reputation is incorrect?

Submit a File Reputation Ticket

SHA256

435BFC4C3A3C887FD39C058E8C11863D5DD1F05E0C7A86E232C93D0E979FDB28

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

FILE SIZE	228458 bytes
SAMPLE TYPE	Zip archive data, at least v2.0 to extract, compression method=deflate
CISCO SECURE ENDPOINT DETECTION NAME*	Auto.435BFC.202552.in02

*Limited to SHA256 lookup

ASSOCIATED DOMAINS FOR THIS HASH

Domains not available.

DETECTION ALIASES

Win-Trojan/VBKrypt.RP02.X1828

HIDDENEXT/Worm.Gen

Win32:Malware-gen

Trojan.GenericKD.36883201

virus

malicious confidence 100%

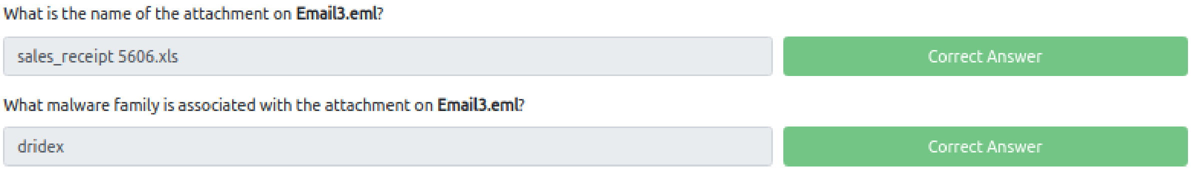
W32/VBInject.NQ.gen!Eldorado

Task 8 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 discussed throughout this room (or use your resources) to help you analyze Email3.eml and use the information to answer the questions.

Answer to the questions of this section-



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

sales_receipt 5606.xls

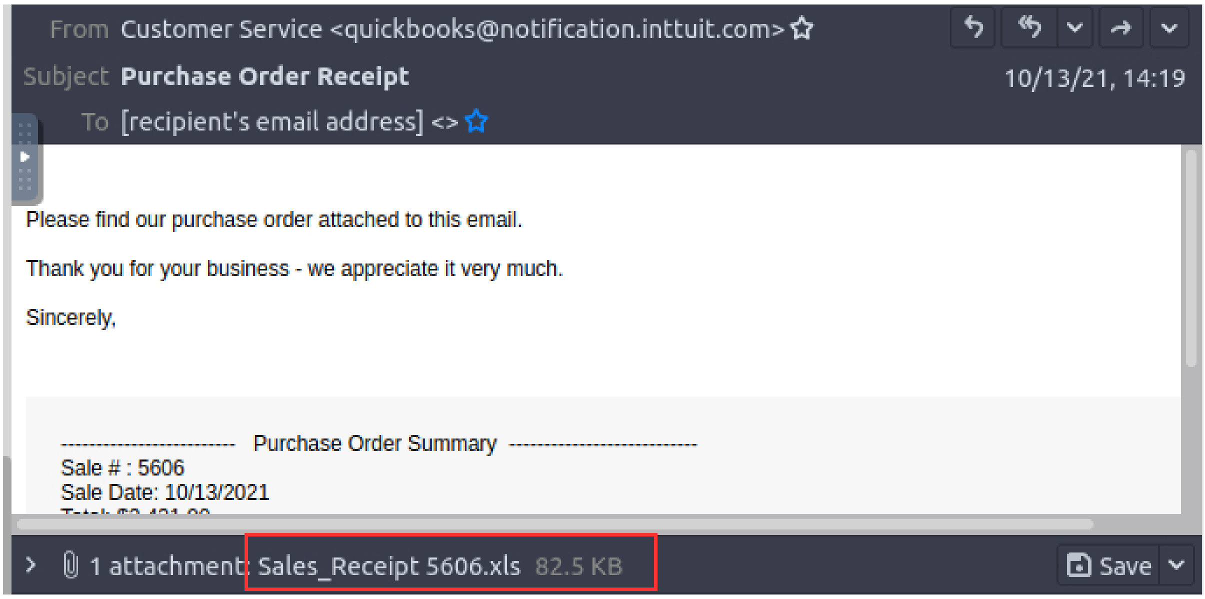
Correct Answer

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

dridex

Correct Answer

Answers-



From Customer Service <quickbooks@notification.inttuit.com>

Subject **Purchase Order Receipt** 10/13/21, 14:19

To [recipient's email address] <>

Please find our purchase order attached to this email.

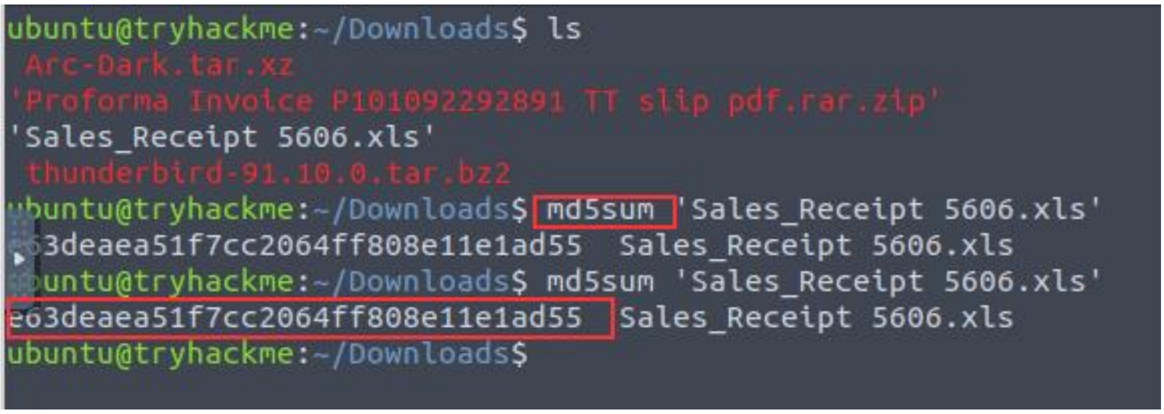
Thank you for your business - we appreciate it very much.

Sincerely,

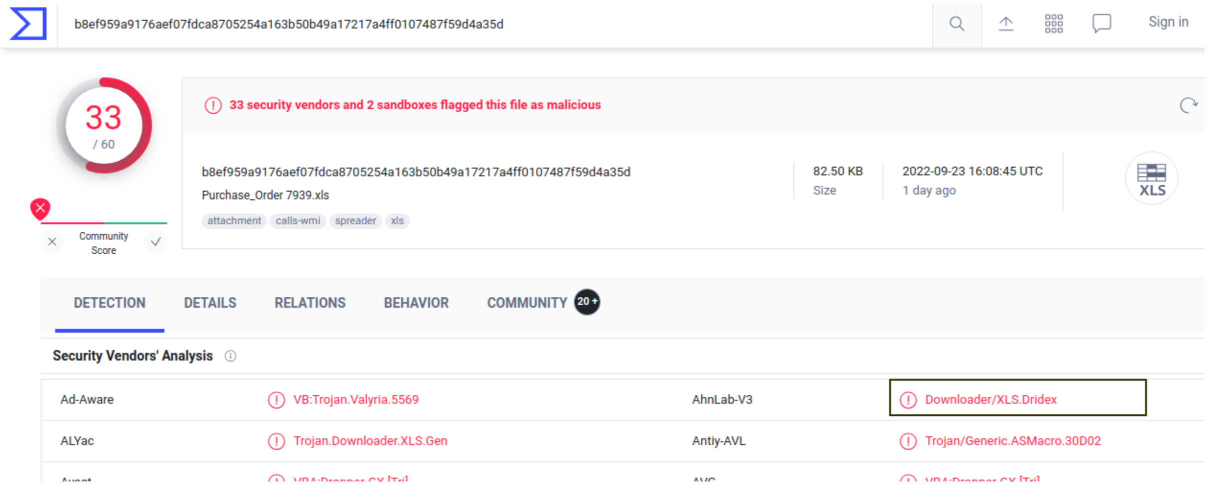
------------------------- Purchase Order Summary ---------------------------

Sale # : 5606
Sale Date: 10/13/2021
Total: $2,421.00

1 attachment: Sales_Receipt 5606.xls 82.5 KB



```
ubuntu@tryhackme:~/Downloads$ ls
 Arc-Dark.tar.xz
'Proforma Invoice P101092292891 TT slip pdf.rar.zip'
'Sales_Receipt 5606.xls'
 thunderbird-91.10.0.tar.bz2
ubuntu@tryhackme:~/Downloads$ md5sum 'Sales_Receipt 5606.xls'
e63deaea51f7cc2064ff808e11e1ad55  Sales_Receipt 5606.xls
ubuntu@tryhackme:~/Downloads$ md5sum 'Sales_Receipt 5606.xls'
e63deaea51f7cc2064ff808e11e1ad55  Sales_Receipt 5606.xls
ubuntu@tryhackme:~/Downloads$
```



b8ef959a9176aef07fdca8705254a163b50b49a17217a4ff0107487f59d4a35d

33 / 60

33 security vendors and 2 sandboxes flagged this file as malicious

b8ef959a9176aef07fdca8705254a163b50b49a17217a4ff0107487f59d4a35d
Purchase_Order 7939.xls
attachment calls-wmi spreader xls

82.50 KB Size

2022-09-23 16:08:45 UTC 1 day ago

Security Vendors' Analysis

Ad-Aware	VB:Trojan.Valyria.5569	AhnLab-V3	Downloader/XLS.Dridex
ALYac	Trojan.Downloader.XLS.Gen	Antiy-AVL	Trojan/Generic.ASMacro.30D02
Avast	VBA:Dropper-GX [Trj]	AVG	VBA:Dropper-GX [Trj]

That is all for this Write-up, hoping this will help you in solving the challenges of Threat Intelligence Tools. Have Fun and Enjoy Hacking! Do visit other rooms and modules on TryHackMe for more learning.

-by Shefali Kumai

For more cyber security learning follow me here-

https://github.com/ctf-time

https://www.youtube.com/channel/UCf-F-eATCUXYaUVk8Xl7OOQ

https://www.instagram.com/cybersecurity.cyber_seek/

https://twitter.com/Shefali37920461