TryHackMe
SOC Level 1

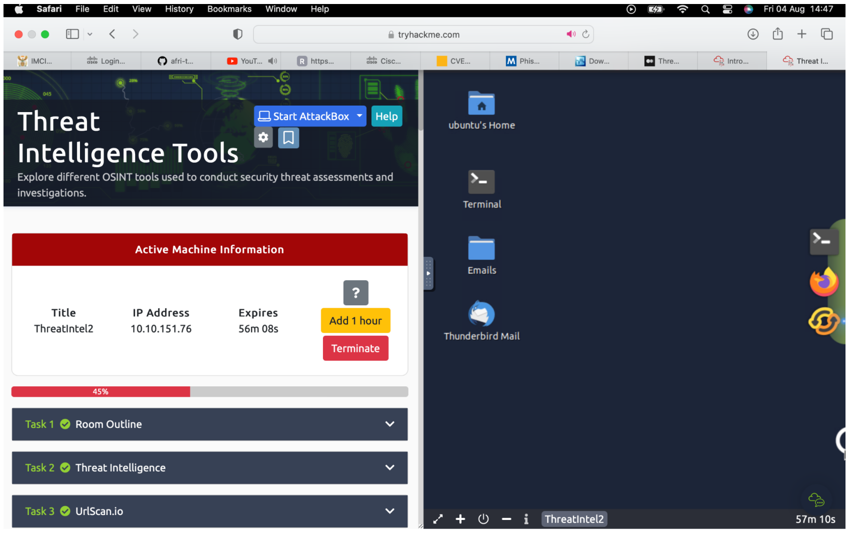
Skills needed to work as a Junior Security Analyst in a Security Operations Centre

- Detect and analyse traffic anomalies
- Monitor endpoints for threats
- Utilise SIEM tools to handle incidents
- Investigate forensic artefacts

Threat Intelligence Tools

I explored different OSINT tools used to conduct security threat assessments and investigations.

Utilised a virtual machine to complete some of the excersises.



Threat Intelligence Tools

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

Active Machine Information

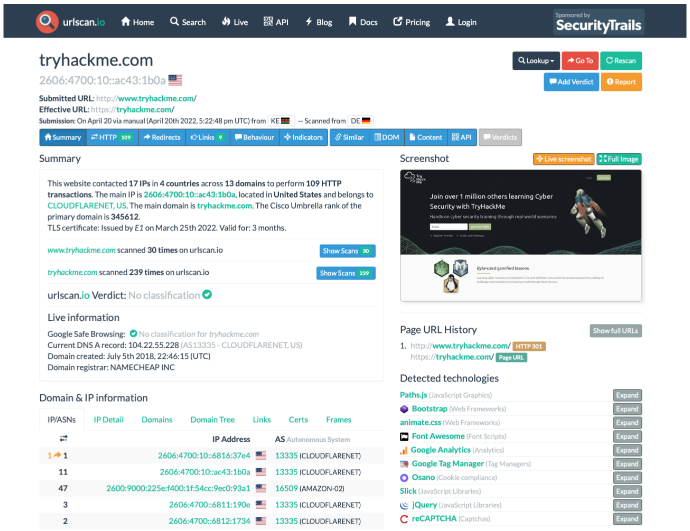
Title	IP Address	Expires
ThreatIntel2	10.10.151.76	56m 08s

Task 1 ✓ Room Outline

Task 2 ✓ Threat Intelligence

Task 3 ✓ UrlScan.io

When a URL is submitted, the information recorded includes the domains and IP addresses contacted, resources requested from the domains, a snapshot of the web page, technologies utilised and other metadata about the website.



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 — Show Scans 30

tryhackme.com scanned **239 times** on urlscan.io — Show Scans 239

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 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)
2	2606:4700::6812:1734	13335 (CLOUDFLARENET)

Screenshot

Page URL History

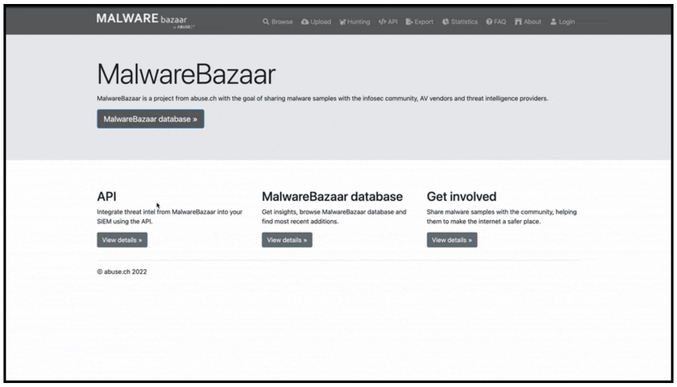
1. http://www.tryhackme.com/ HTTP 301
   https://tryhackme.com/ Page URL

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)
- reCAPTCHA (Captchas)

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).



MalwareBazaar

MalwareBazaar is a project from abuse.ch with the goal of sharing malware samples with the infosec community, AV vendors and threat intelligence providers.

API

Integrate threat intel from MalwareBazaar into your SIEM using the API.

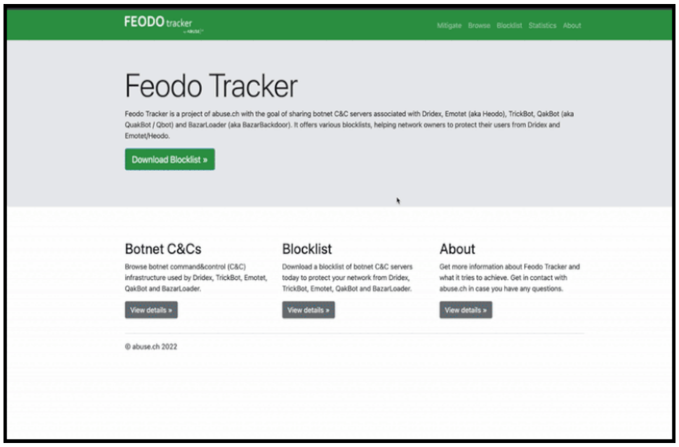
MalwareBazaar database

Get insights, browse MalwareBazaar database and find most recent additions.

Get involved

Share malware samples with the community, helping them to make the internet a safer place.

© abuse.ch 2022



Feodo Tracker

Feodo Tracker is a project of abuse.ch with the goal of sharing botnet C&C servers associated with Dridex, Emotet (aka Heodo), TrickBot, QakBot (aka QuakBot / Qbot) and BazarLoader (aka BazarBackdoor). It offers various blocklists, helping network owners to protect their users from Dridex and Emotet/Heodo.

Botnet C&Cs

Browse botnet command&control (C&C) infrastructure used by Dridex, TrickBot, Emotet, QakBot and BazarLoader.

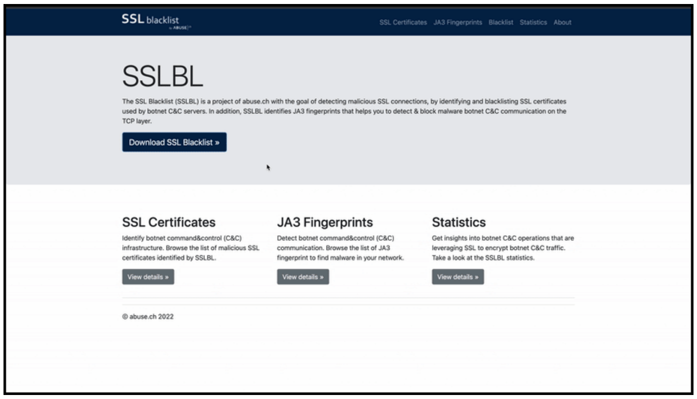
Blocklist

Download a blocklist of botnet C&C servers today to protect your network from Dridex, TrickBot, Emotet, QakBot and BazarLoader.

About

Get more information about Feodo Tracker and what it tries to achieve. Get in contact with abuse.ch in case you have any questions.

© abuse.ch 2022



SSLBL

The SSL Blacklist (SSLBL) is a project of abuse.ch with the goal of detecting malicious SSL connections, by identifying and blacklisting SSL certificates used by botnet C&C servers. In addition, SSLBL identifies JA3 fingerprints that helps you to detect & block malware botnet C&C communication on the TCP layer.

SSL Certificates

Identify botnet command&control (C&C) infrastructure. Browse the list of malicious SSL certificates identified by SSLBL.

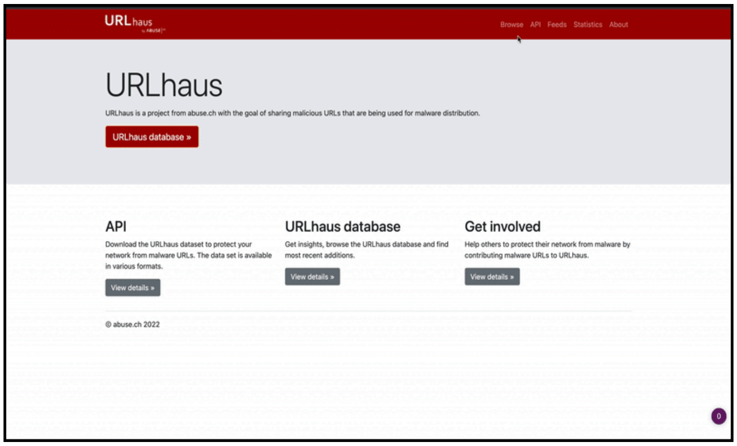
JA3 Fingerprints

Detect botnet command&control (C&C) communication. Browse the list of JA3 fingerprint to find malware in your network.

Statistics

Get insights into botnet C&C operations that are leveraging SSL to encrypt botnet C&C traffic. Take a look at the SSLBL statistics.

© abuse.ch 2022



URLhaus

URLhaus is a project from abuse.ch with the goal of sharing malicious URLs that are being used for malware distribution.

API

Download the URLhaus dataset to protect your network from malware URLs. The data set is available in various formats.

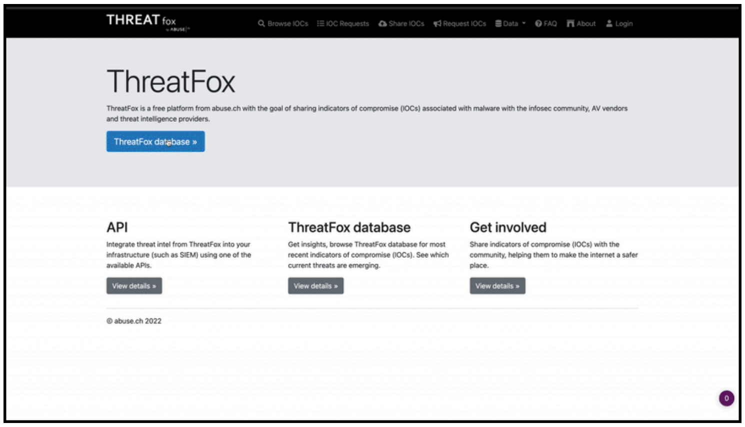
URLhaus database

Get insights, browse the URLhaus database and find most recent additions.

Get involved

Help others to protect their network from malware by contributing malware URLs to URLhaus.

© abuse.ch 2022



ThreatFox

ThreatFox is a free platform from abuse.ch with the goal of sharing indicators of compromise (IOCs) associated with malware with the infosec community, AV vendors and threat intelligence providers.

API

Integrate threat intel from ThreatFox into your infrastructure (such as SIEM) using one of the available APIs.

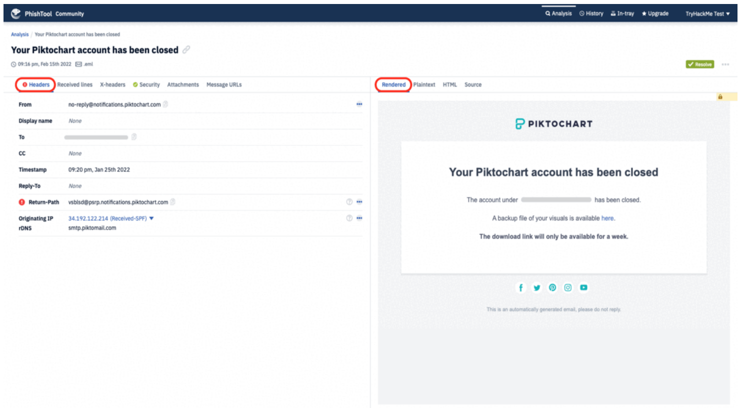
ThreatFox database

Get insights, browse ThreatFox database for most recent indicators of compromise (IOCs). See which current threats are emerging.

Get involved

Share indicators of compromise (IOCs) with the community, helping them to make the internet a safer place.

© abuse.ch 2022



Your Piktochart account has been closed

09:16 pm, Feb 15th 2022 .eml

From	no-reply@notifications.piktochart.com
Display name	None
To	[redacted]
CC	None
Timestamp	09:20 pm, Jan 25th 2022
Reply-To	None
Return-Path	vsblsd@psrp.notifications.piktochart.com
Originating IP	34.192.122.214 (Received-SPF)
rDNS	smtp.piktomail.com

Your Piktochart account has been closed

The account under [redacted] has been closed.

A backup file of your visuals is available here.

The download link will only be available for a week.

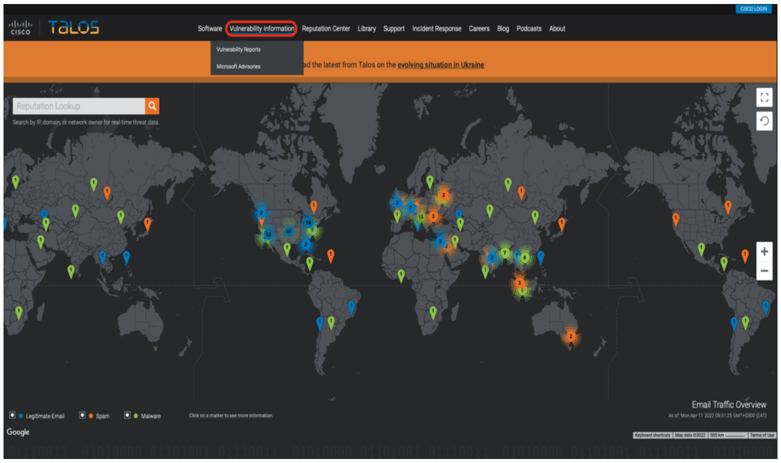
This is an automatically generated email, please do not reply.

PhishTool

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.



ad the latest from Talos on the evolving situation in Ukraine

Search by IP, domain, or network owner for real-time threat data.

Click on a marker to see more information.

Email Traffic Overview

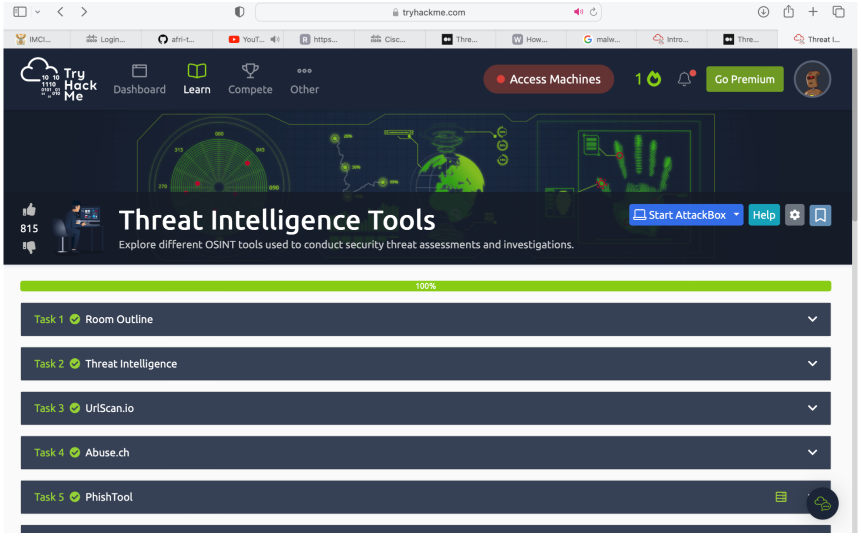
As of: Mon Apr 11 2022 09:31:25 GMT+0300 (EAT)

Cisco Talos Intelligence

Cisco Talos encompasses six key teams:

- Threat Intelligence & Interdiction
- Detection Research
- Engineering & Development
- Vulnerability Research & Discovery
- Communities
- Global Outreach

Completed Threat Intelligence Tools in the TryHackMe SOC Level 1



Threat Intelligence Tools

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

Task 1 ✓ Room Outline

Task 2 ✓ Threat Intelligence

Task 3 ✓ UrlScan.io

Task 4 ✓ Abuse.ch

Task 5 ✓ PhishTool