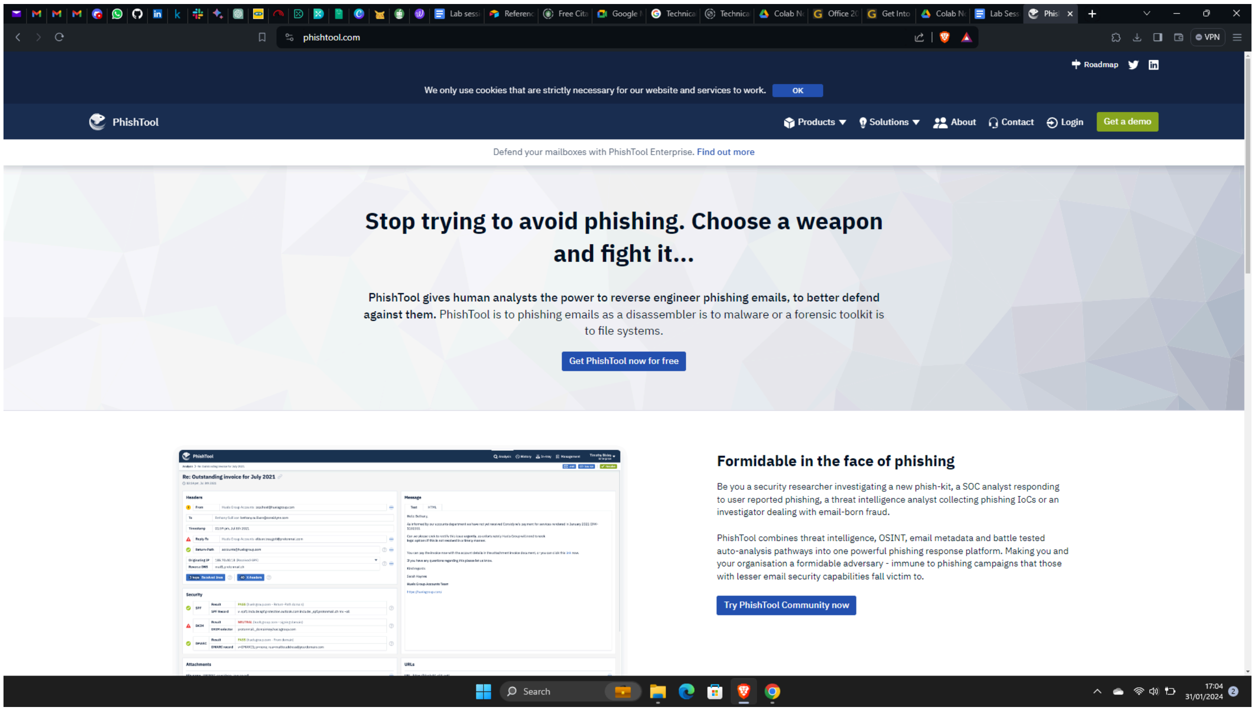
INTRODUCTION

In the realm of Incident Response, Business Continuity, and Disaster Recovery, one of the crucial aspects involves forensic email analysis. This process is integral for uncovering potential threats, ensuring the security of digital communication, and fortifying the resilience of an organization's information infrastructure. Below is a detailed report on the steps undertaken during the forensic email analysis assignment.

Accessing Phishtool Website and Account Creation

The initial step involved accessing the Phishtool website through the provided link (!link). This platform serves as a valuable resource for email analysis. Upon reaching the website, an account was created to facilitate the analysis process. Account creation is a standard security measure to ensure authenticated access and maintain a record of user activities.



We only use cookies that are strictly necessary for our website and services to work.

Defend your mailboxes with PhishTool Enterprise. Find out more

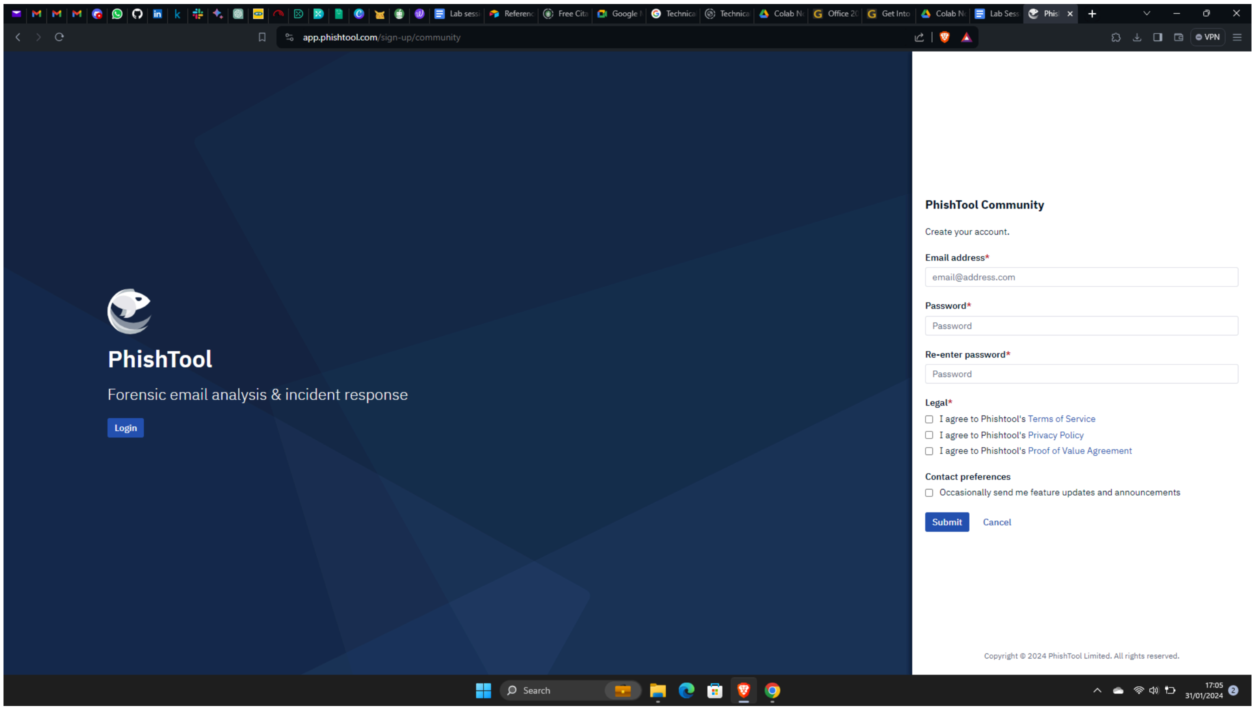
Stop trying to avoid phishing. Choose a weapon and fight it...

PhishTool gives human analysts the power to reverse engineer phishing emails, to better defend against them. PhishTool is to phishing emails as a disassembler is to malware or a forensic toolkit is to file systems.

Formidable in the face of phishing

Be you a security researcher investigating a new phish-kit, a SOC analyst responding to user reported phishing, a threat intelligence analyst collecting phishing IoCs or an investigator dealing with email-born fraud.

PhishTool combines threat intelligence, OSINT, email metadata and battle tested auto-analysis pathways into one powerful phishing response platform. Making you and your organisation a formidable adversary - immune to phishing campaigns that those with lesser email security capabilities fall victim to.


app.phishtool.com/sign-up/community
PhishTool
Forensic email analysis & incident response
Login

PhishTool Community

Create your account.

Email address*
email@address.com

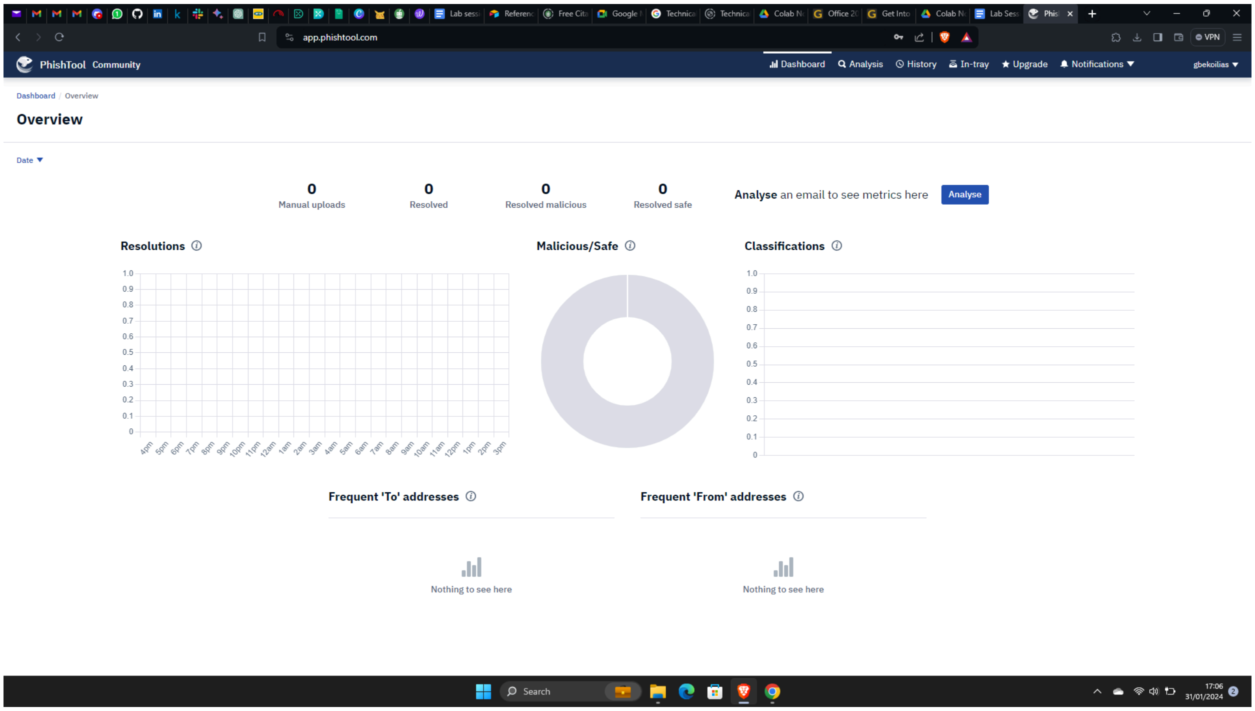
Password*
Password

Re-enter password*
Password

Legal*
□ I agree to Phishtool's Terms of Service
□ I agree to Phishtool's Privacy Policy
□ I agree to Phishtool's Proof of Value Agreement

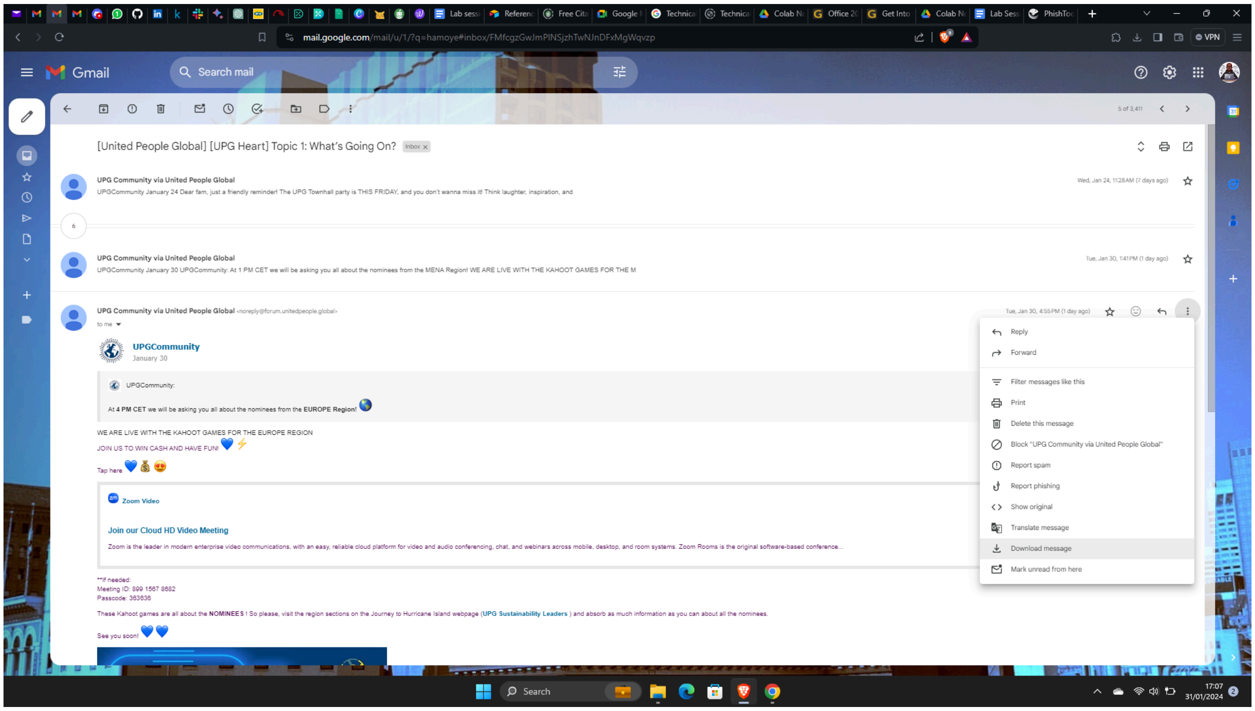
Contact preferences
□ Occasionally send me feature updates and announcements

Submit
Cancel
Copyright © 2024 PhishTool Limited. All rights reserved.
17:05
31/01/2024



Sample Selection and Download

To commence the analysis, a random email from the inbox was selected. This email served as the sample for the forensic analysis. It is essential to choose a representative sample to glean insights into potential threats that might be lurking within the broader communication channels.



[United People Global] [UPG Heart] Topic 1: What's Going On?

UPG Community via United People Global — Wed, Jan 24, 11:28 AM (7 days ago)
UPGCommunity January 24 Dear fam, just a friendly reminder! The UPG Townhall party is THIS FRIDAY, and you don't wanna miss it! Think laughter, inspiration, and

6

UPG Community via United People Global — Tue, Jan 30, 1:41 PM (1 day ago)
UPGCommunity January 30 UPGCommunity: At 1 PM CET we will be asking you all about the nominees from the MENA Region! WE ARE LIVE WITH THE KAHOOT GAMES FOR THE M

UPG Community via United People Global <noreply@forum.unitedpeople.global> — Tue, Jan 30, 4:55 PM (1 day ago)
to me

UPGCommunity
January 30

> UPGCommunity:
>
> At **4 PM CET** we will be asking you all about the nominees from the **EUROPE Region!** 🌎

WE ARE LIVE WITH THE KAHOOT GAMES FOR THE EUROPE REGION

JOIN US TO WIN CASH AND HAVE FUN! 💙 ⚡

Tap here 💙 💰 😍

Zoom Video

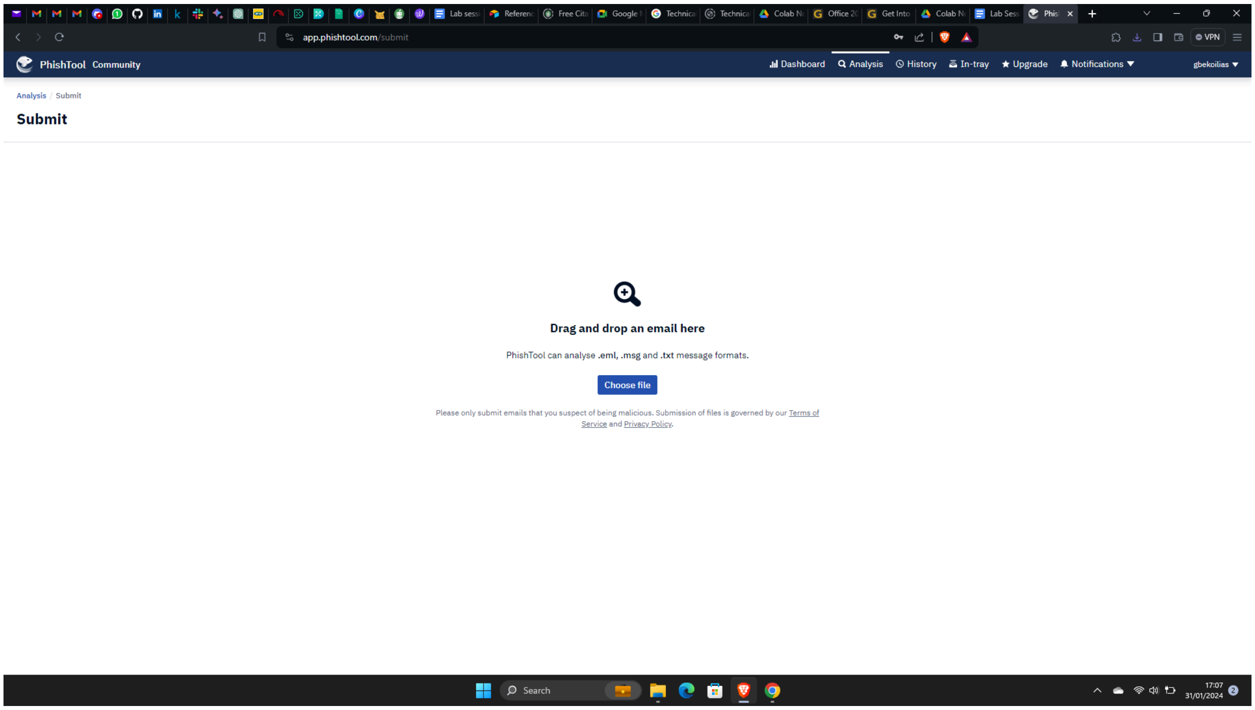
Join our Cloud HD Video Meeting

Zoom is the leader in modern enterprise video communications, with an easy, reliable cloud platform for video and audio conferencing, chat, and webinars across mobile, desktop, and room systems. Zoom Rooms is the original software-based conference...

**If needed:
Meeting ID: 899 1567 8682
Passcode: 363636

These Kahoot games are all about the **NOMINEES** ! So please, visit the region sections on the Journey to Hurricane Island webpage (UPG Sustainability Leaders) and absorb as much information as you can about all the nominees.

See you soon! 💙 💙



Submit

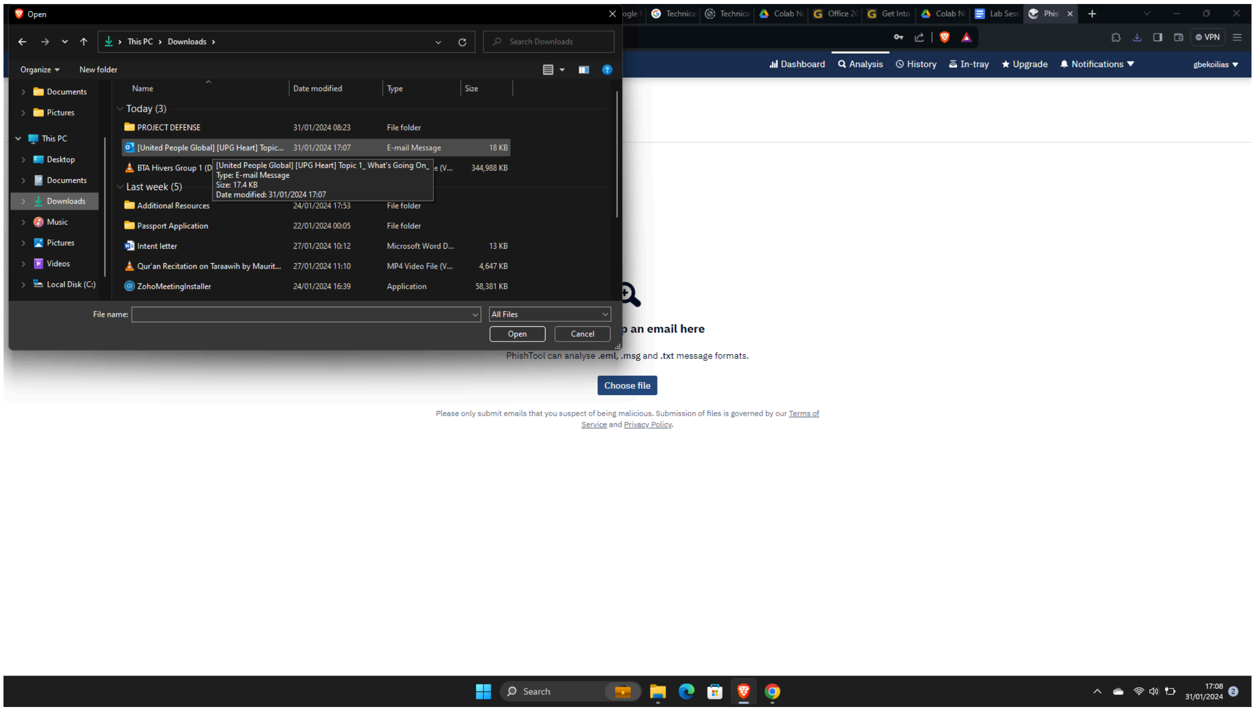
Drag and drop an email here

PhishTool can analyse .eml, .msg and .txt message formats.

Please only submit emails that you suspect of being malicious. Submission of files is governed by our Terms of Service and Privacy Policy.

Uploading Mail File to Phishtool for Analysis

Following the selection of the email sample, the file was downloaded successfully. The next step involved uploading the mail file onto the analysis page of the Phishtool website. This is a critical phase as it initiates the automated analysis process, unraveling the intricacies of the email content.



Name	Date modified	Type	Size
Today (3)			
PROJECT DEFENSE	31/01/2024 08:23	File folder	
[United People Global] [UPG Heart] Topic...	31/01/2024 17:07	E-mail Message	18 KB
BTA Hivers Group 1 (D		…e (V...	344,988 KB
Last week (5)			
Additional Resources	24/01/2024 17:53	File folder	
Passport Application	22/01/2024 00:05	File folder	
Intent letter	27/01/2024 10:12	Microsoft Word D...	13 KB
Qur'an Recitation on Taraawih by Maurit...	27/01/2024 11:10	MP4 Video File (V...	4,647 KB
ZohoMeetingInstaller	24/01/2024 16:39	Application	58,381 KB

[United People Global] [UPG Heart] Topic 1_ What's Going On_
Type: E-mail Message
Size: 17.4 KB
Date modified: 31/01/2024 17:07

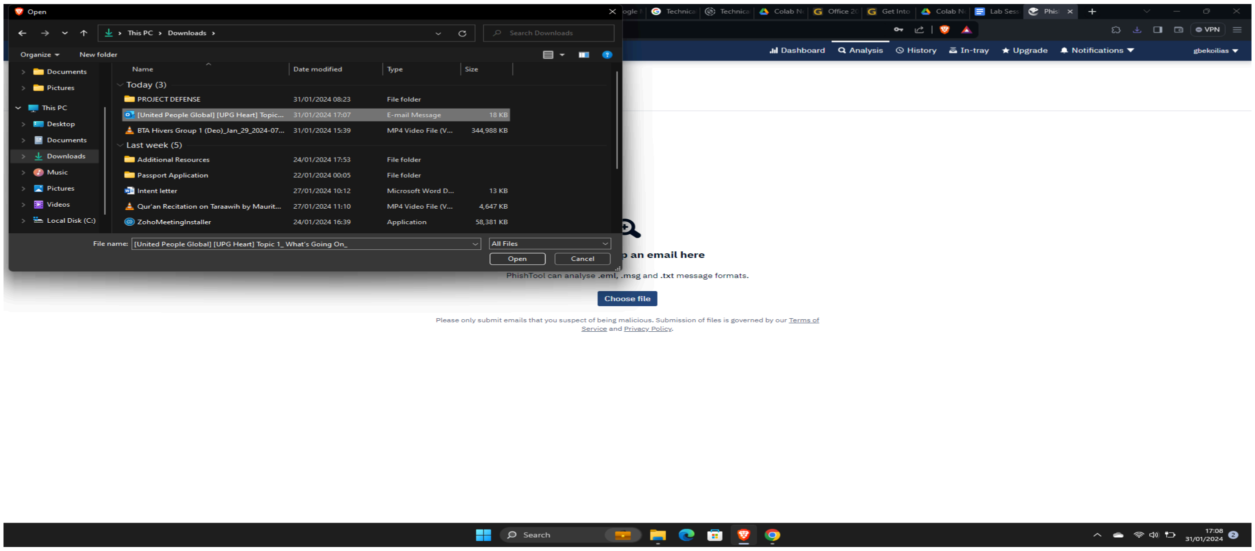
File name:
All Files

…p an email here

PhishTool can analyse .eml, .msg and .txt message formats.

Please only submit emails that you suspect of being malicious. Submission of files is governed by our Terms of Service and Privacy Policy.

17:08
31/01/2024



Name	Date modified	Type	Size
Today (3)			
PROJECT DEFENSE	31/01/2024 08:23	File folder	
[United People Global] [UPG Heart] Topic...	31/01/2024 17:07	E-mail Message	18 KB
BTA Hivers Group 1 (Deo)_Jan_29_2024-07...	31/01/2024 15:39	MP4 Video File (V...	344,988 KB
Last week (5)			
Additional Resources	24/01/2024 17:53	File folder	
Passport Application	22/01/2024 00:05	File folder	
Intent letter	27/01/2024 10:12	Microsoft Word D...	13 KB
Qur'an Recitation on Taraawih by Maurit...	27/01/2024 11:10	MP4 Video File (V...	4,647 KB
ZohoMeetingInstaller	24/01/2024 16:39	Application	58,381 KB

File name: [United People Global] [UPG Heart] Topic 1_ What's Going On_
All Files

…p an email here

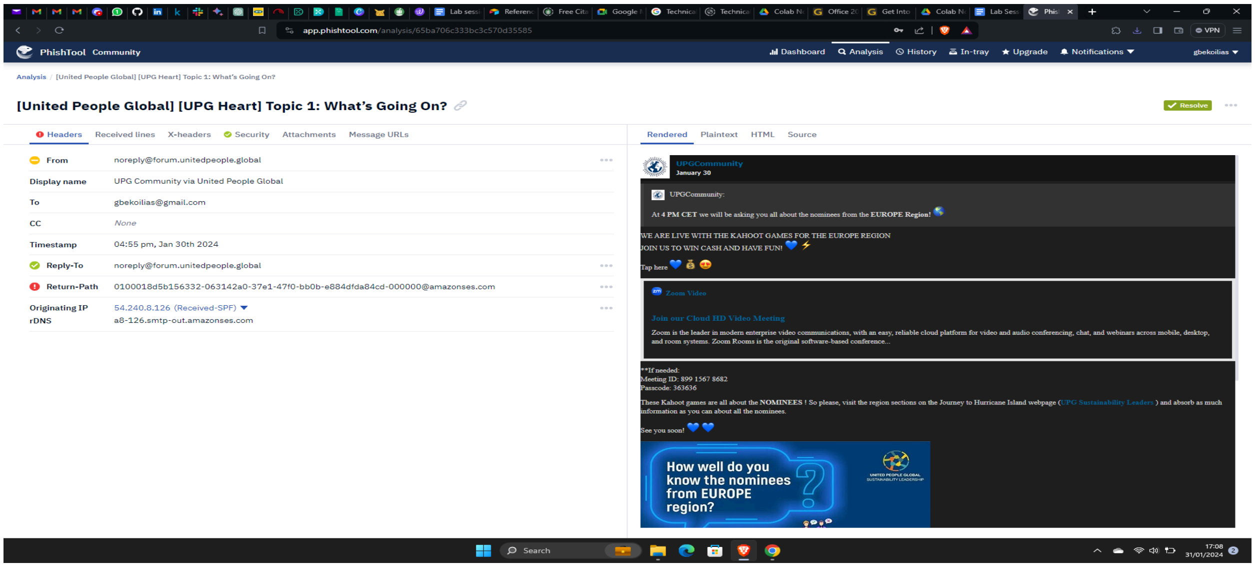
PhishTool can analyse .eml, .msg and .txt message formats.

Please only submit emails that you suspect of being malicious. Submission of files is governed by our Terms of Service and Privacy Policy.

17:08
31/01/2024

Analysis Results on Phishtool Portal

Post-upload, the Phishtool portal swiftly executed the analysis, presenting a comprehensive analysis page. This page included fundamental details of the file, offering valuable insights into the nature of the email. The information obtained from this step forms the basis for further evaluation and investigation.



[United People Global] [UPG Heart] Topic 1: What's Going On?

From	noreply@forum.unitedpeople.global
Display name	UPG Community via United People Global
To	gbekoilias@gmail.com
CC	*None*
Timestamp	04:55 pm, Jan 30th 2024
Reply-To	noreply@forum.unitedpeople.global
Return-Path	0100018d5b156332-063142a0-37e1-47f0-bb0b-e884dfda84cd-000000@amazonses.com
Originating IP rDNS	54.240.8.126 (Received-SPF) a8-126.smtp-out.amazonses.com

UPGCommunity
January 30

UPGCommunity:

At **4 PM CET** we will be asking you all about the nominees from the **EUROPE Region!** 🌍

WE ARE LIVE WITH THE KAHOOT GAMES FOR THE EUROPE REGION
JOIN US TO WIN CASH AND HAVE FUN! 💙 ⚡

Tap here 💙 💰 😍

Zoom Video

Join our Cloud HD Video Meeting

Zoom is the leader in modern enterprise video communications, with an easy, reliable cloud platform for video and audio conferencing, chat, and webinars across mobile, desktop, and room systems. Zoom Rooms is the original software-based conference...

**If needed:
Meeting ID: 899 1567 8682
Passcode: 363636

These Kahoot games are all about the **NOMINEES** ! So please, visit the region sections on the Journey to Hurricane Island webpage (UPG Sustainability Leaders) and absorb as much information as you can about all the nominees.

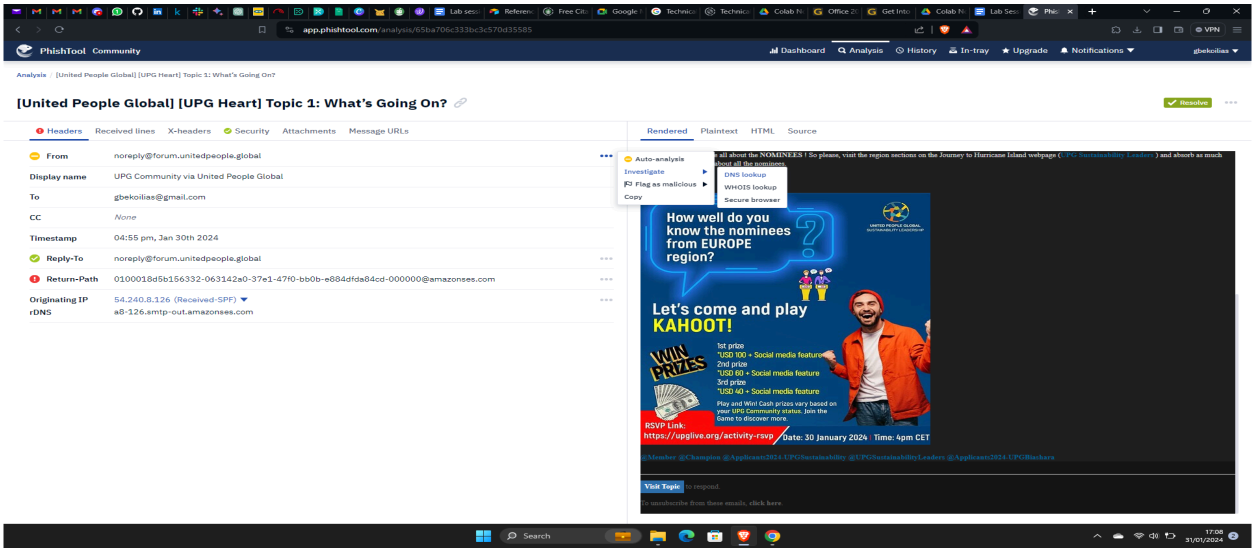
See you soon! 💙 💙

How well do you know the nominees from EUROPE region?

UNITED PEOPLE GLOBAL SUSTAINABILITY LEADERSHIP

Obtaining Originating IP rDNS for Deeper Insight

To enhance the assessment of the email's legitimacy, the Originating IP rDNS (Reverse DNS) was sought. This involved copying the address from the DNS lookup tab, providing additional information regarding the DNS associated with the email. This step is crucial for tracing the origin of the communication and identifying any anomalies.


app.phishtool.com/analysis/65ba706c333bc3c570d35585
PhishTool Community
Dashboard
Analysis
History
In-tray
Upgrade
Notifications
gbekoilias
Resolve
Headers
Received lines
X-headers
Security
Attachments
Message URLs
Rendered
Plaintext
HTML
Source
Auto-analysis
Investigate
Flag as malicious
Copy
DNS lookup
WHOIS lookup
Secure browser
How well do you know the nominees from EUROPE region?
UNITED PEOPLE GLOBAL SUSTAINABILITY LEADERSHIP
Let's come and play KAHOOT!
WIN PRIZES
1st prize
*USD 100 + Social media feature
2nd prize
*USD 60 + Social media feature
3rd prize
*USD 40 + Social media feature
Play and Win! Cash prizes vary based on your UPG Community status. Join the Game to discover more.
RSVP Link: https://upglive.org/activity-rsvp
Date: 30 January 2024 | Time: 4pm CET
Visit Topic
17:08
31/01/2024

Analysis / [United People Global] [UPG Heart] Topic 1: What's Going On?

[United People Global] [UPG Heart] Topic 1: What's Going On?

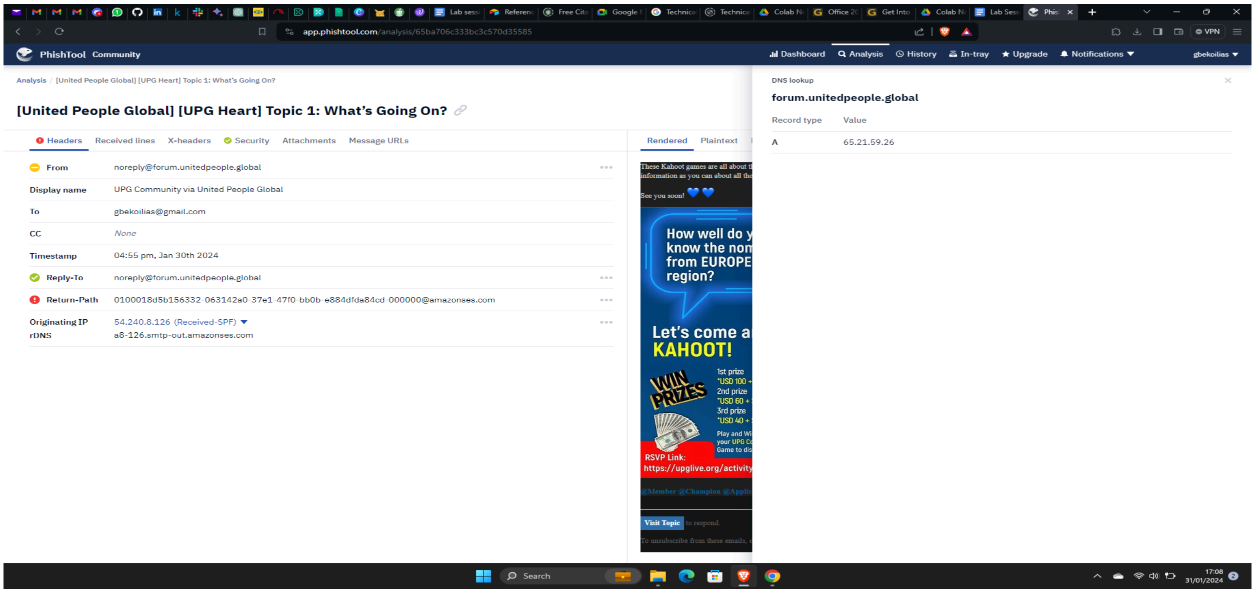
From	noreply@forum.unitedpeople.global
Display name	UPG Community via United People Global
To	gbekoilias@gmail.com
CC	*None*
Timestamp	04:55 pm, Jan 30th 2024
Reply-To	noreply@forum.unitedpeople.global
Return-Path	0100018d5b156332-063142a0-37e1-47f0-bb0b-e884dfda84cd-000000@amazonses.com
Originating IP	54.240.8.126 (Received-SPF)
rDNS	a8-126.smtp-out.amazonses.com

…e all about the NOMINEES ! So please, visit the region sections on the Journey to Hurricane Island webpage (UPG Sustainability Leaders) and absorb as much …about all the nominees.

@Member @Champion @Applicants2024-UPGSustainability @UPGSustainabilityLeaders @Applicants2024-UPGBiashara

Visit Topic to respond.

To unsubscribe from these emails, click here.



Analysis / [United People Global] [UPG Heart] Topic 1: What's Going On?

[United People Global] [UPG Heart] Topic 1: What's Going On?

From	noreply@forum.unitedpeople.global
Display name	UPG Community via United People Global
To	gbekoilias@gmail.com
CC	*None*
Timestamp	04:55 pm, Jan 30th 2024
Reply-To	noreply@forum.unitedpeople.global
Return-Path	0100018d5b156332-063142a0-37e1-47f0-bb0b-e884dfda84cd-000000@amazonses.com
Originating IP	54.240.8.126 (Received-SPF)
rDNS	a8-126.smtp-out.amazonses.com

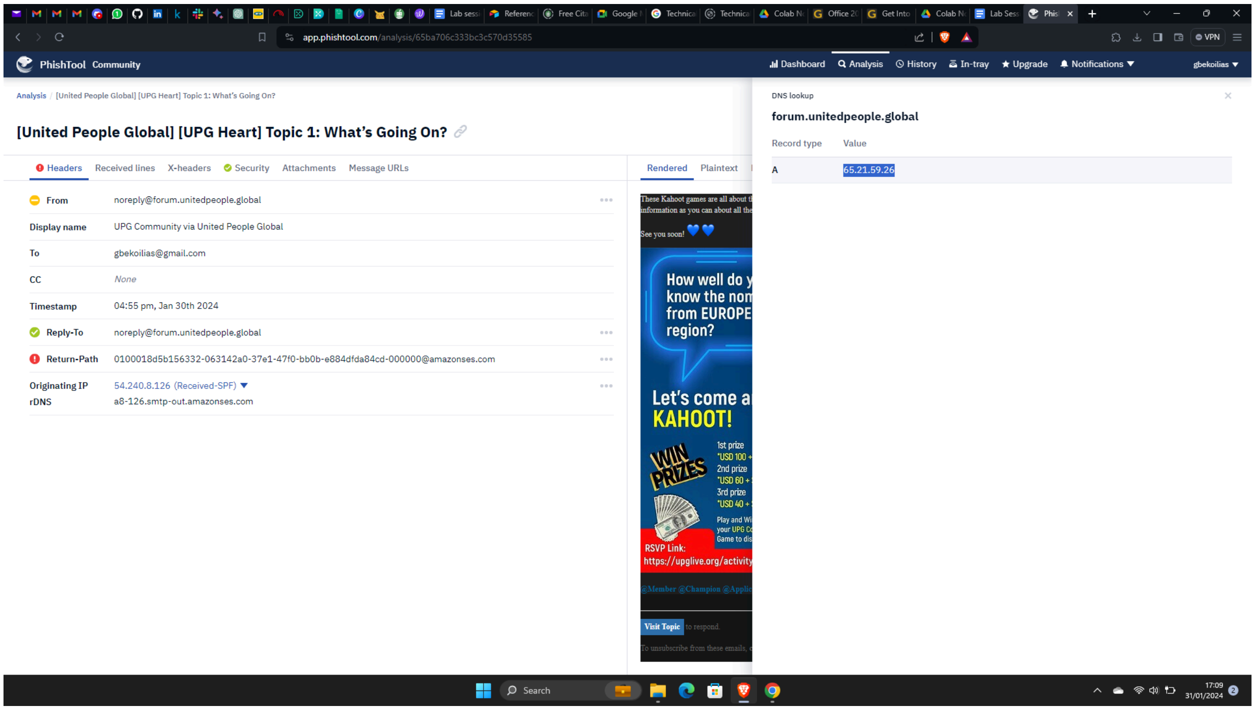
These Kahoot games are all about t… information as you can about all the…

See you soon! 💙 💙

DNS lookup

forum.unitedpeople.global

Record type	Value
A	65.21.59.26



Analysis / [United People Global] [UPG Heart] Topic 1: What's Going On?

[United People Global] [UPG Heart] Topic 1: What's Going On?

From	noreply@forum.unitedpeople.global
Display name	UPG Community via United People Global
To	gbekoilias@gmail.com
CC	*None*
Timestamp	04:55 pm, Jan 30th 2024
Reply-To	noreply@forum.unitedpeople.global
Return-Path	0100018d5b156332-063142a0-37e1-47f0-bb0b-e884dfda84cd-000000@amazonses.com
Originating IP rDNS	54.240.8.126 (Received-SPF) a8-126.smtp-out.amazonses.com

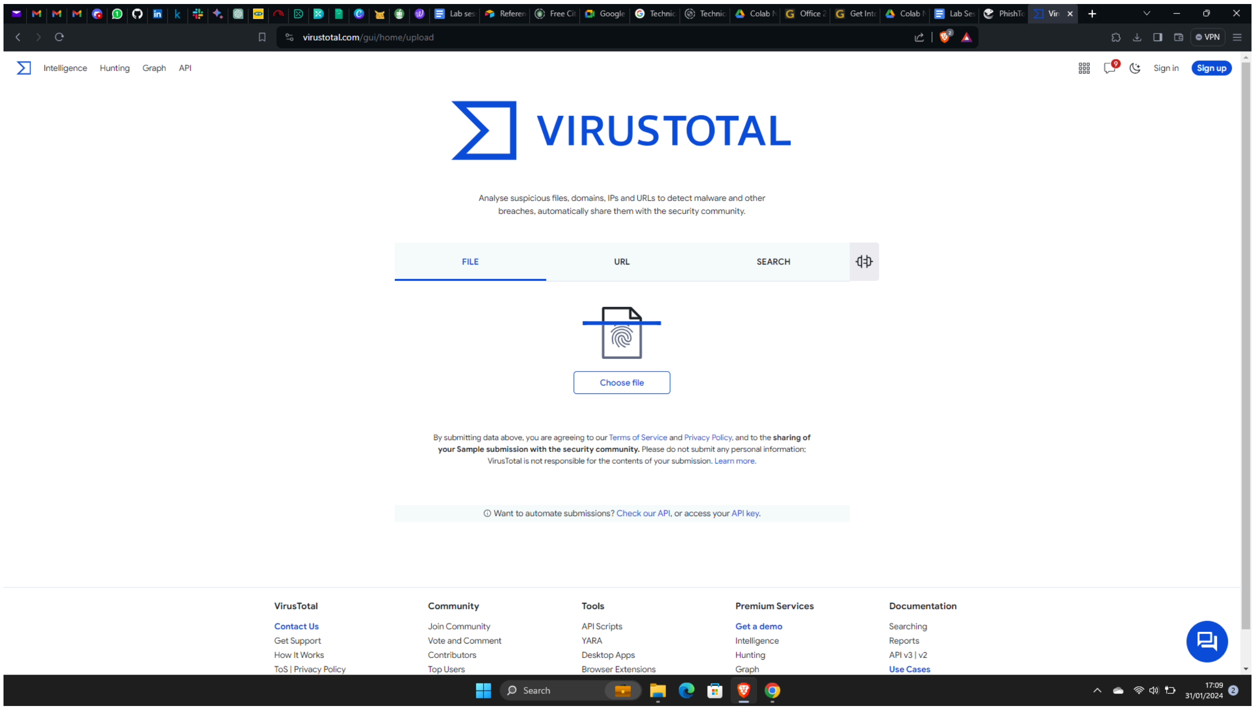
DNS lookup

forum.unitedpeople.global

Record type	Value
A	65.21.59.26

VirusTotal Analysis for Malicious Link Detection

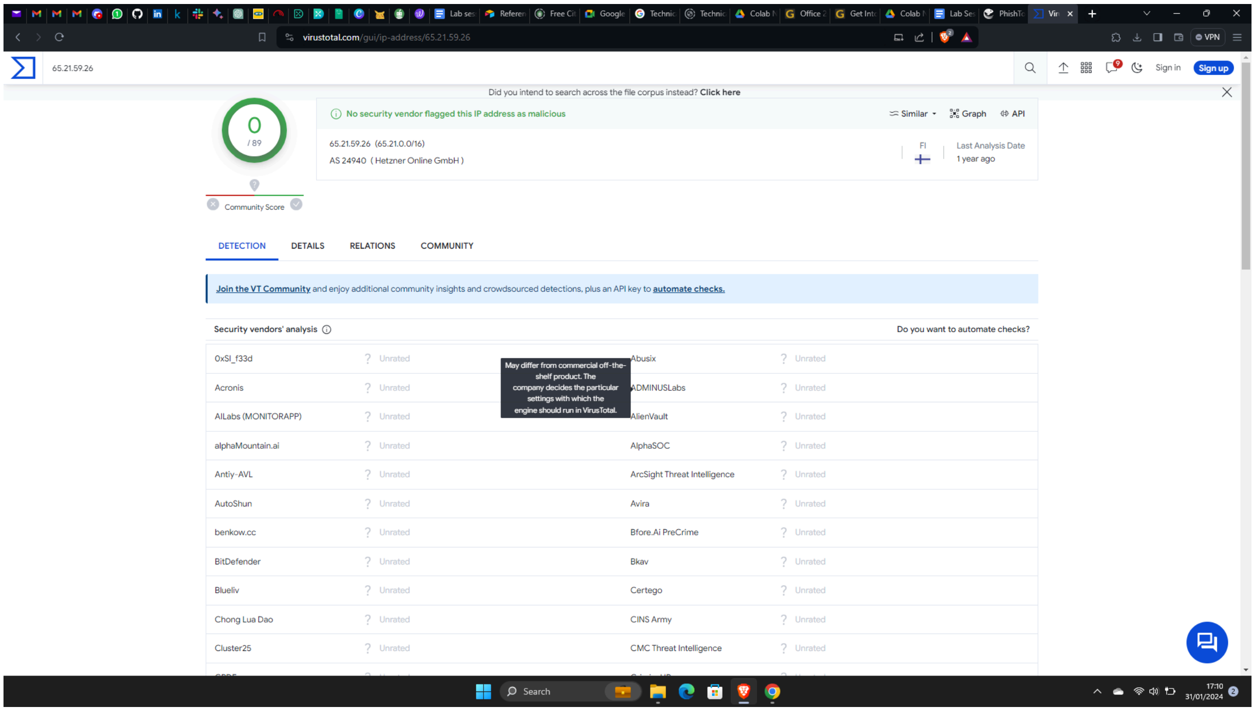
Armed with the Originating IP rDNS, the next step involved using it as a search key on the VirusTotal homepage (!link). This platform specializes in malware detection and virus analysis. The link was run through VirusTotal, unleashing a comprehensive examination of the address. The results encompassed a wealth of information, shedding light on potential threats and vulnerabilities.



Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

By submitting data above, you are agreeing to our Terms of Service and Privacy Policy, and to the **sharing of your Sample submission with the security community.** Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.

ⓘ Want to automate submissions? Check our API, or access your API key.



Did you intend to search across the file corpus instead? **Click here**

ⓘ No security vendor flagged this IP address as malicious

65.21.59.26 (65.21.0.0/16)

AS 24940 (Hetzner Online GmbH)

Last Analysis Date
1 year ago

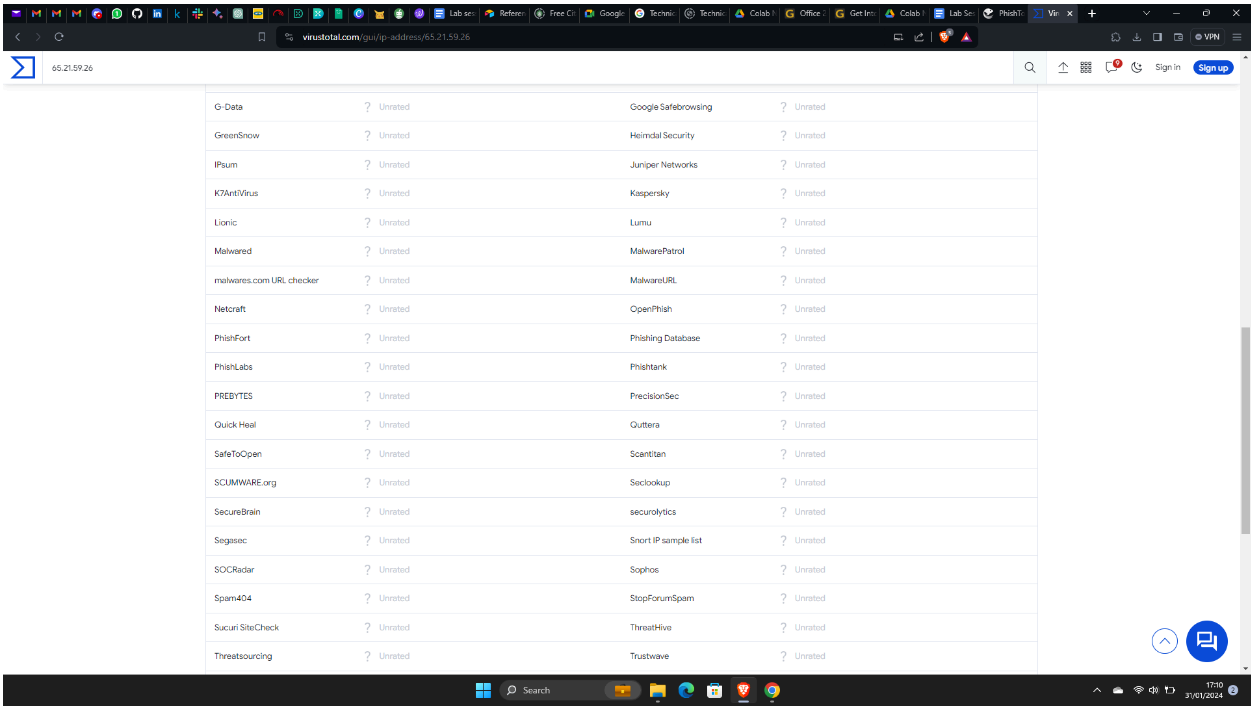
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis ⓘ

Do you want to automate checks?

May differ from commercial off-the-shelf product. The company decides the particular settings with which the engine should run in VirusTotal.

0xSI_f33d	? Unrated	Abusix	? Unrated
Acronis	? Unrated	ADMINUSLabs	? Unrated
AILabs (MONITORAPP)	? Unrated	AlienVault	? Unrated
alphaMountain.ai	? Unrated	AlphaSOC	? Unrated
Antiy-AVL	? Unrated	ArcSight Threat Intelligence	? Unrated
AutoShun	? Unrated	Avira	? Unrated
benkow.cc	? Unrated	Bfore.Ai PreCrime	? Unrated
BitDefender	? Unrated	Bkav	? Unrated
Blueliv	? Unrated	Certego	? Unrated
Chong Lua Dao	? Unrated	CINS Army	? Unrated
Cluster25	? Unrated	CMC Threat Intelligence	? Unrated



G-Data	? Unrated	Google Safebrowsing	? Unrated
GreenSnow	? Unrated	Heimdal Security	? Unrated
IPsum	? Unrated	Juniper Networks	? Unrated
K7AntiVirus	? Unrated	Kaspersky	? Unrated
Lionic	? Unrated	Lumu	? Unrated
Malwared	? Unrated	MalwarePatrol	? Unrated
malwares.com URL checker	? Unrated	MalwareURL	? Unrated
Netcraft	? Unrated	OpenPhish	? Unrated
PhishFort	? Unrated	Phishing Database	? Unrated
PhishLabs	? Unrated	Phishtank	? Unrated
PREBYTES	? Unrated	PrecisionSec	? Unrated
Quick Heal	? Unrated	Quttera	? Unrated
SafeToOpen	? Unrated	Scantitan	? Unrated
SCUMWARE.org	? Unrated	Seclookup	? Unrated
SecureBrain	? Unrated	securolytics	? Unrated
Segasec	? Unrated	Snort IP sample list	? Unrated
SOCRadar	? Unrated	Sophos	? Unrated
Spam404	? Unrated	StopForumSpam	? Unrated
Sucuri SiteCheck	? Unrated	ThreatHive	? Unrated
Threatsourcing	? Unrated	Trustwave	? Unrated