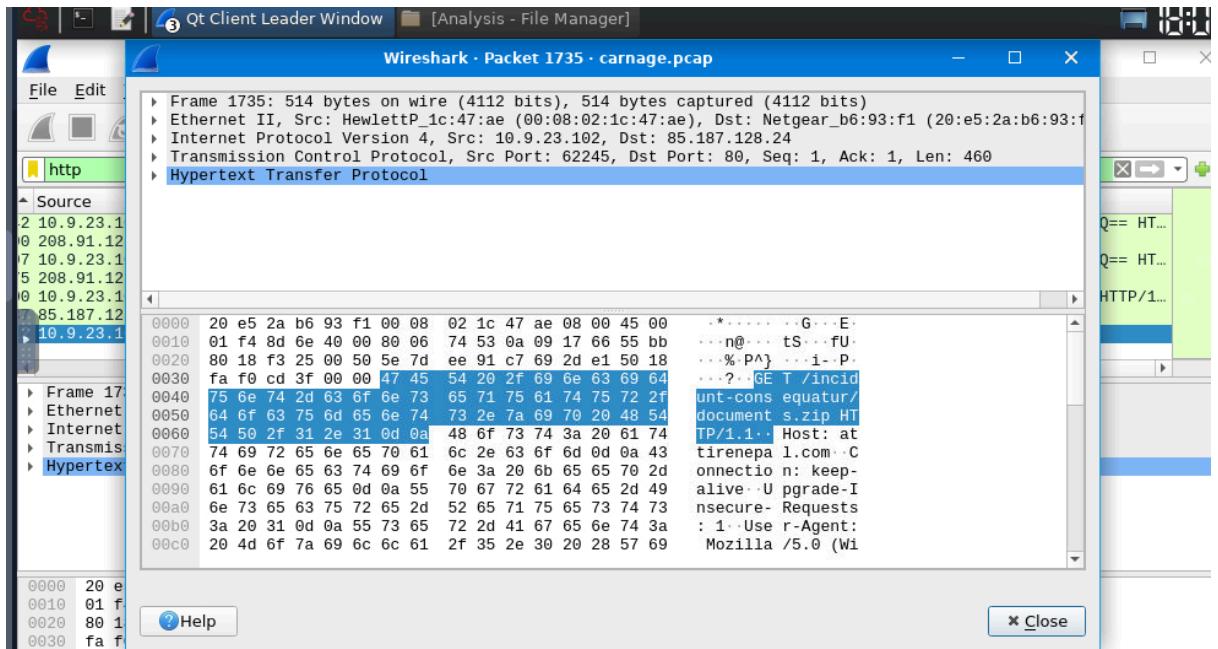


Network analysis traffic using wireshark

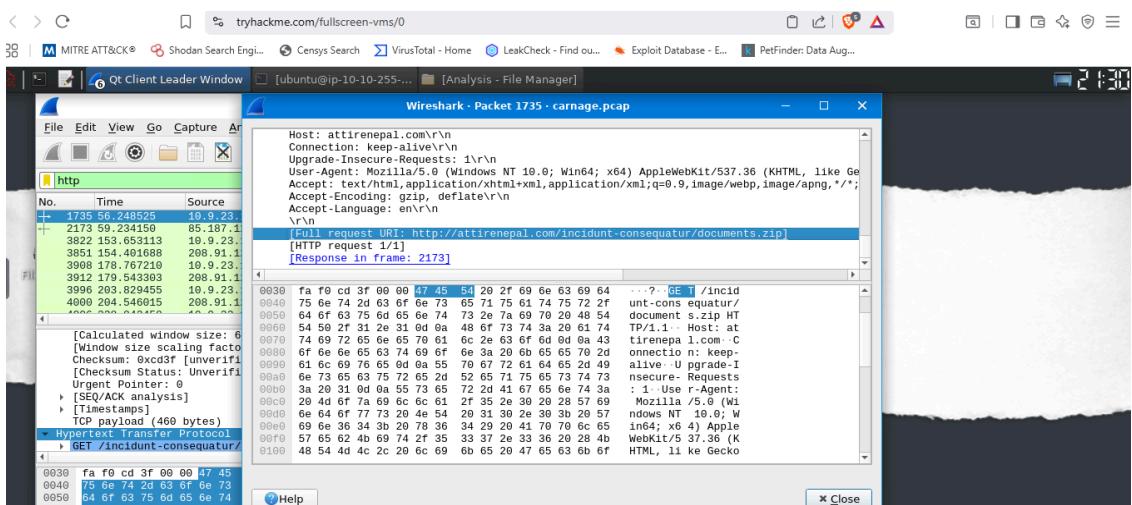
In this THM virtual environment we need to investigate an endpoint that was making suspicious connections outbound .

The alert was triggered when the user of this endpoint opened an attached document that was received with an email , which could mean the possibility of a phishing attack .

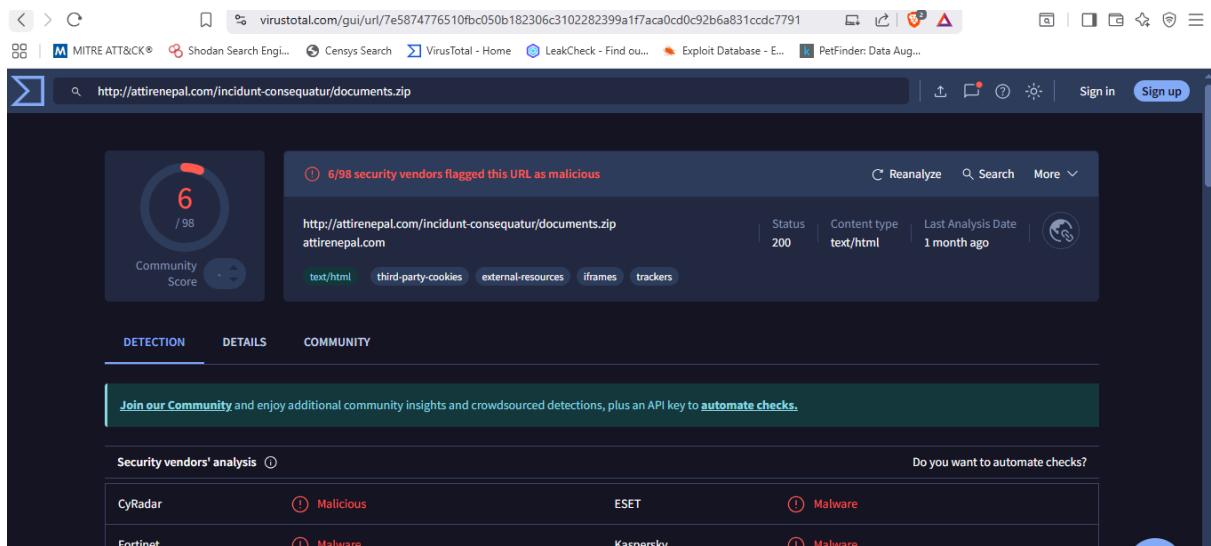
In order to investigate the process that has taken action we'll use wireshark .



After isolating the suspicious action that occurred at 16:44:38 we can see documents.zip was downloaded and it's host “attirenepal.com”

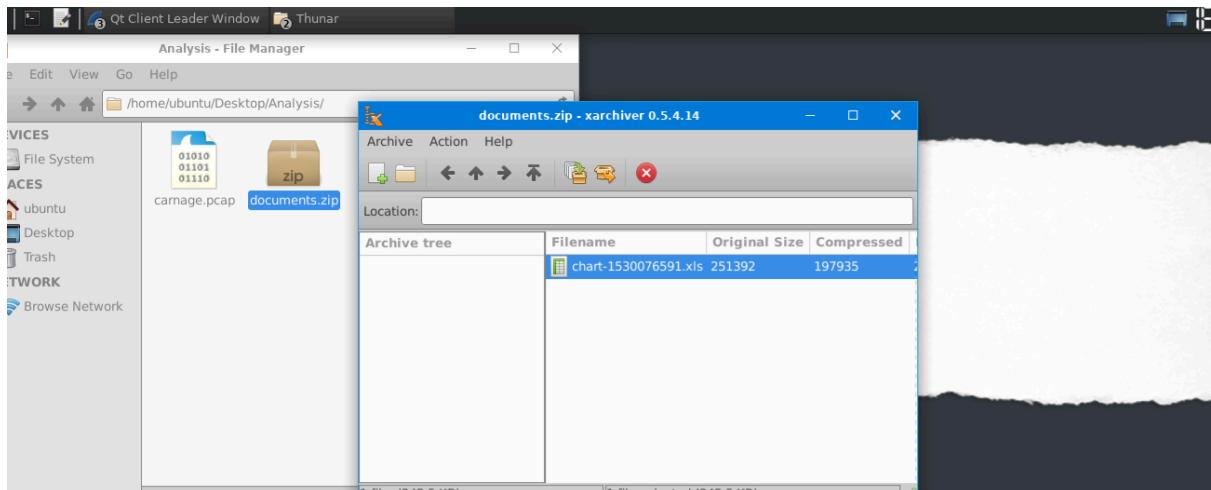


After finding the suspicious URL , a common procedure is to test it using external tools and websites such as Virus total



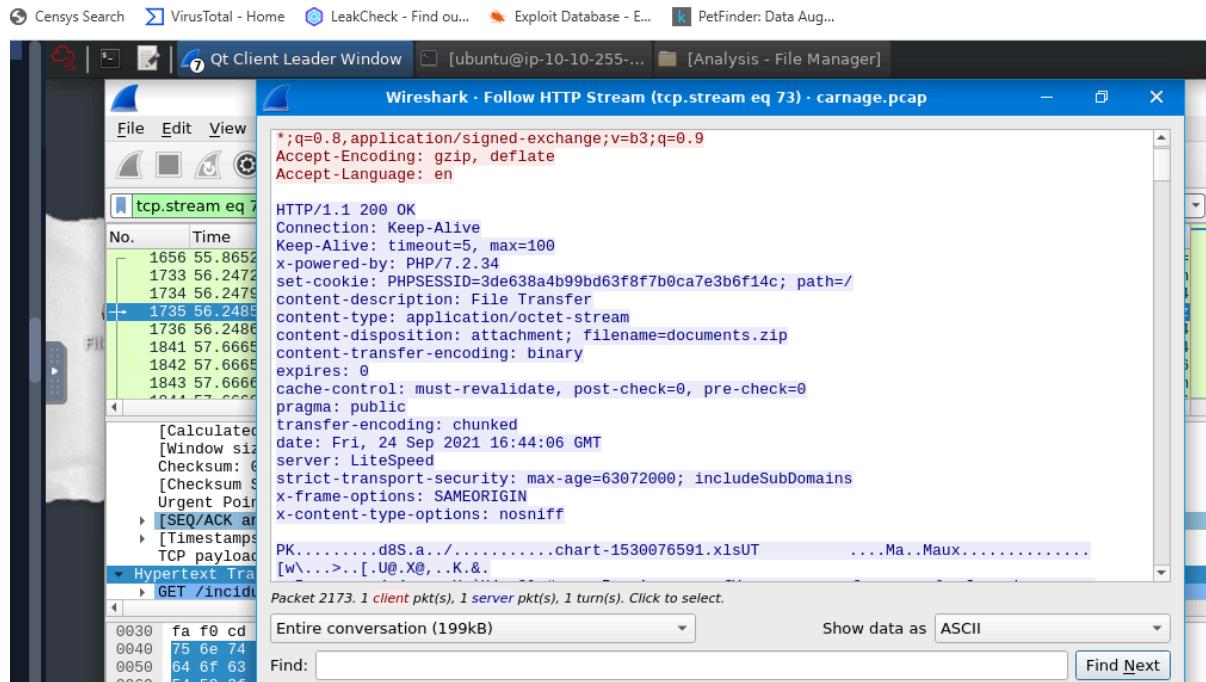
The screenshot shows the VirusTotal analysis interface for the URL <http://attirenepal.com/incidunt-consequatur/documents.zip>. The main summary indicates that 6 out of 98 security vendors flagged the URL as malicious. Below this, detailed information is provided: Status 200, Content type text/html, and Last Analysis Date 1 month ago. The interface includes tabs for DETECTION, DETAILS, and COMMUNITY, and a call-to-action to join the community for additional insights. A section titled "Security vendors' analysis" lists vendor results: CyRadar (Malicious), ESET (Malware), Fortinet (Malware), and Kaspersky (Malware).

This confirms the malicious activity and that the alert is a true positive , further investigations need to take place .



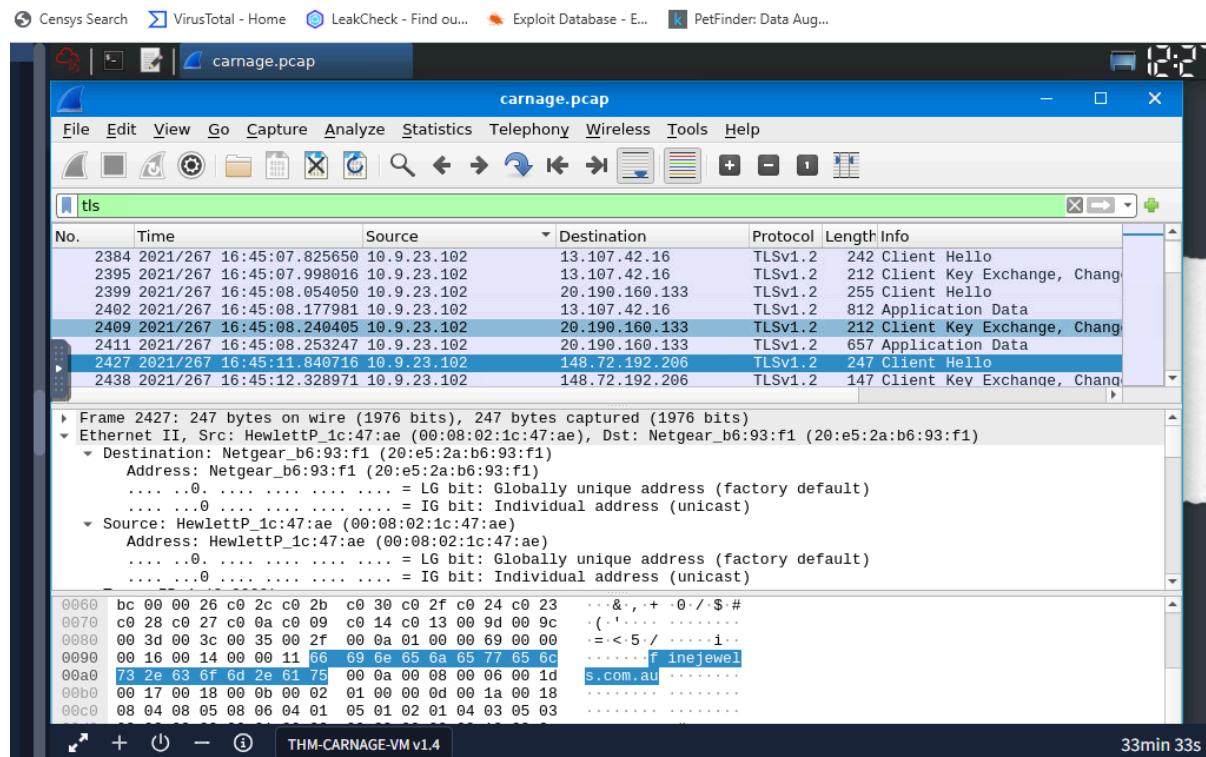
After extracting the malicious file in a sandbox we can notice that it's in xls format , it's possible to escalate this to a malware analyst in order to acquire more details .

Also we should block the malicious ip address 85.187.128.24



After following the HTTP stream we can acquire additional information such as the webserver of the malicious ip which is Litespeed / version PHP/7.2.34 .

Now we should look at the outbound connections from the targeted machine 10.9.23.102 after the first malicious connection at 16:44:38 to check for any additional downloads and other suspicious activities .



After filtering to TLS and examining the traffic before encryption we can notice some connections happening with microsoft edge and other safe connections until we reach the second malicious connection at 16.45.11 with the domain “finejewels.com.au” and IP address 148.72.192.206 .

The screenshot shows the VirusTotal analysis page for the URL <http://finejewels.com.au/>. The page displays a community score of 4/98, indicating that 4 out of 98 security vendors flagged the URL as malicious. The status is 200, the content type is text/html; charset=utf-8, and the last analysis date was 24 days ago. Below the main summary, there are tabs for DETECTION, DETAILS, and COMMUNITY. A green banner encourages joining the community for additional insights and automation checks. The SECURITY VENDORS' ANALYSIS section lists vendor findings: CyRadar (Malicious), Fortinet (Malware), Kaspersky (Malware), SOC Radar (Phishing), alphaMountain.ai (Suspicious), and Forcepoint ThreatSeeker (Suspicious). A blue button on the right allows users to automate checks.

The third malicious connection occurred at 16.45.21 with the domain “thietbiagt.com” IP address 210.245.90.247

The screenshot shows the Wireshark interface displaying a packet capture named "carnage.pcap". The packet list view shows several TLS frames, with frame 3009 highlighted. The details pane shows the structure of the Client Hello message, including fields like Version (TLSv1.2), Ciphersuites (244), and Compression Methods (147). The bytes pane shows the raw hex and ASCII data of the message. The timeline pane shows the sequence of frames over time. The status bar at the bottom indicates the session duration is 23min 24s.

Did you intend to search across the file corpus instead? [Click here](#)

3 / 95 security vendors flagged this domain as malicious

thietbiagt.com

Registrar: MAT BAO CORPORATION

Creation Date: 6 years ago

Last Analysis Date: 16 days ago

Community Score: top-1M

Reanalyze Similar More

DETECTION DETAILS RELATIONS COMMUNITY 5

Join our 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?	
alphaMountain.ai	Malicious	CyRadar	Malicious
Fortinet	Malware	Forcepoint ThreatSeeker	Suspicious
Abusix	Clean	Acronis	Clean

The fourth connection occurred at 16.45.25 with the domain "new.americold.com" IP address 140.72.53.144

The screenshot shows a Wireshark capture of a TLS handshake. The timeline pane displays frames from 3009 to 3246. The details pane shows the following sequence:

- Frame 3229: 247 bytes on wire (1976 bits), 247 bytes captured (1976 bits)
- Ethernet II, Src: HewlettP_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
 - Destination: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
 - Address: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
 -0. = L6 bit: Globally unique address (factory default)
 -0. = I6 bit: Individual address (unicast)
 - Source: HewlettP_1c:47:ae (00:08:02:1c:47:ae)
 - Address: HewlettP_1c:47:ae (00:08:02:1c:47:ae)
 -0. = L6 bit: Globally unique address (factory default)
 -0. = I6 bit: Individual address (unicast)

The bytes pane shows the raw hex and ASCII data for each frame, with frame 3229 highlighted.

1/95 security vendor flagged this domain as malicious

new.americold.com
americold.com

Registrar: CSC Corporate Domains, Inc.

Creation Date: 30 years ago

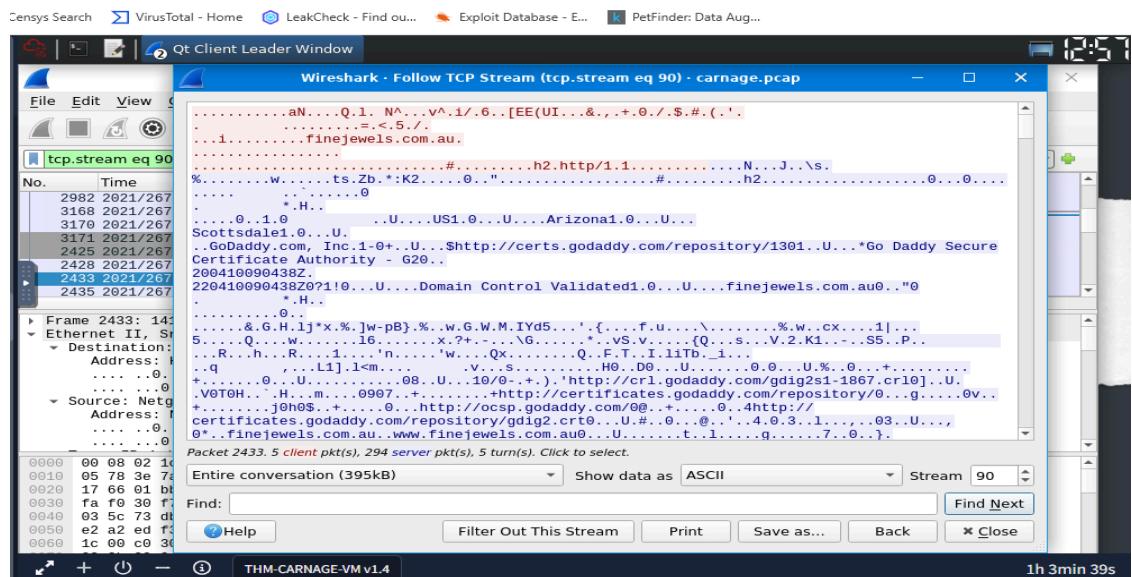
Last Analysis Date: 15 hours ago

Community Score: 1 / 95

DETECTION DETAILS RELATIONS COMMUNITY 2

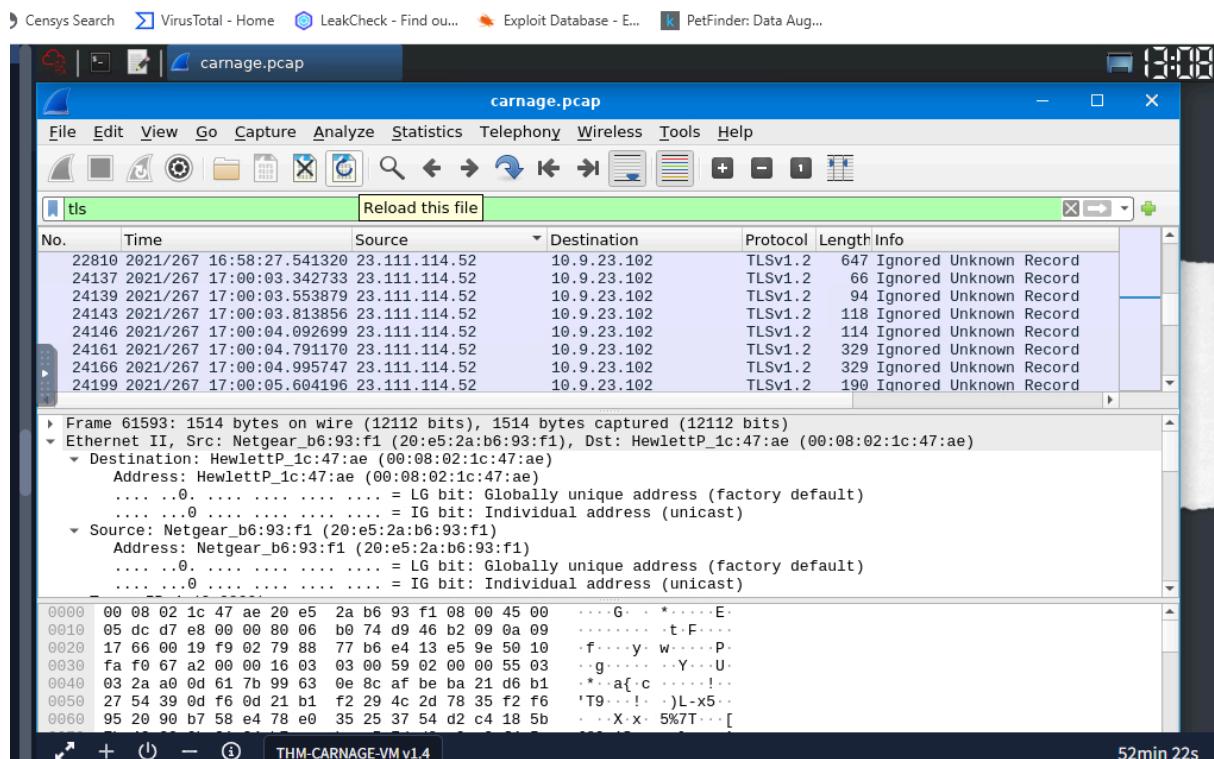
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

We should block these IP addresses to prevent future connections .



After following the connection with the second malicious domain we can see that the SSL certificate was issued by GoDaddy

In addition , we have this suspicious ip address making unusual connections with the endpoint



The screenshot shows the VirusTotal analysis interface for the IP address 23.111.114.52. The main header includes links to MITRE ATT&CK, Shodan Search Engine, Censys Search, VirusTotal - Home, LeakCheck - Find ou..., Exploit Database - E..., and PetFinder: Data Aug... A search bar at the top contains the IP address. To the right are buttons for Sign in and Sign up, along with various navigation icons.

Key information displayed on the page:

- A large circular icon on the left shows a "Community Score" of 13 / 95, with a "-49" indicator below it.
- A message above the main content area states: "13/95 security vendors flagged this IP address as malicious".
- The IP address is listed as 23.111.114.52 (23.111.96.0/19) and belongs to AS 39134 (Edinaya Set Limited Liability Company).
- A RU flag indicates the country of origin.
- The last analysis date is 3 days ago.
- Below the main content, there's a banner encouraging users to "Join our Community" and automate checks.
- A table titled "Security vendors' analysis" lists vendor names, their findings, and a column for "Do you want to automate checks?".

Vendor	Findings	Action
alphaMountain.ai	Malicious	ArcSight Threat Intelligence
BitDefender	Phishing	CyRadar
ESET	Malware	Fortinet

We can confirm that the IP address is malicious .

Additional investigations can be performed using the same procedures that I used such as inspecting suspicious ip addresses and connections like GET/POST and reading the hello client packets before encryption , isolating time frames and validating by using external resources such as virus total .