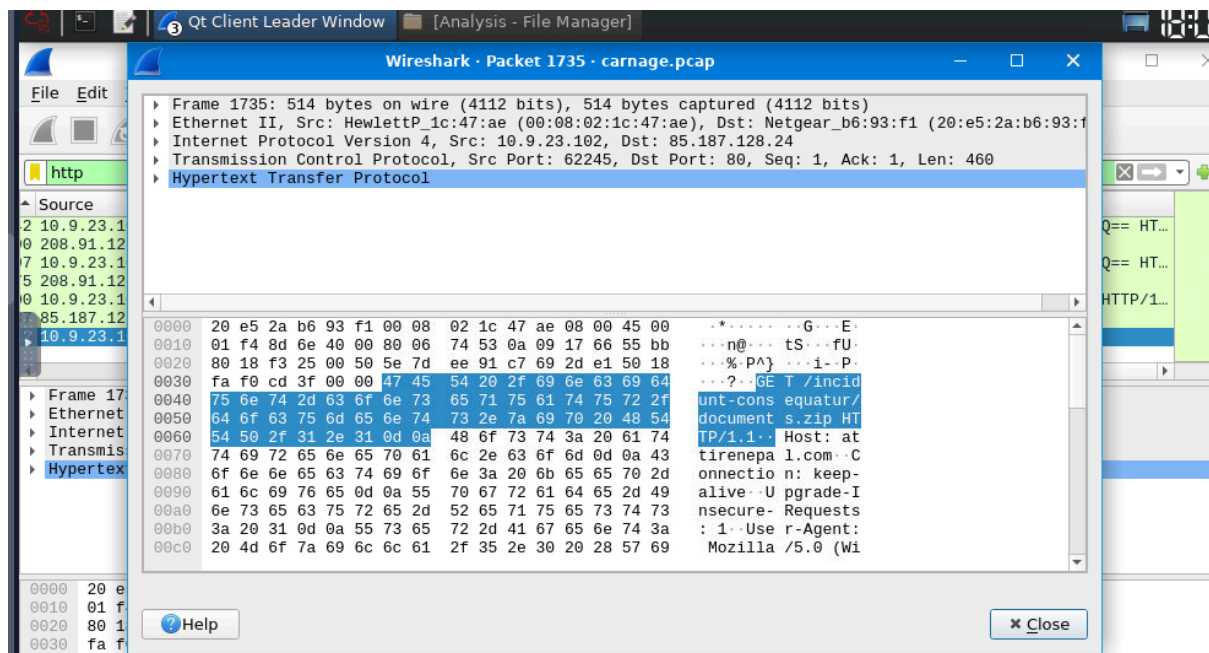


Network analysis traffic using wireshark

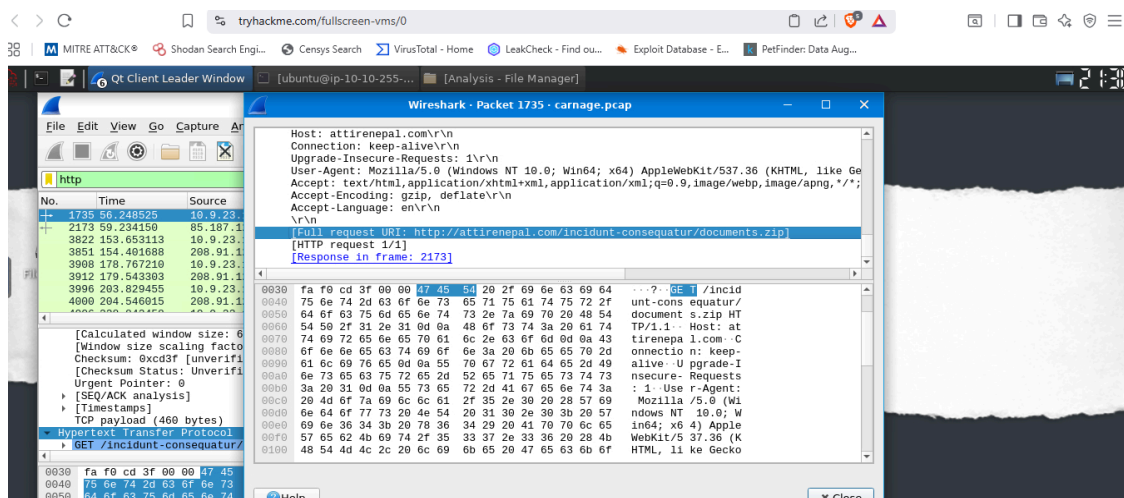
In this THM virtual environment we need to investigate an endpoint that was making suspicious connections outbound .

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 .

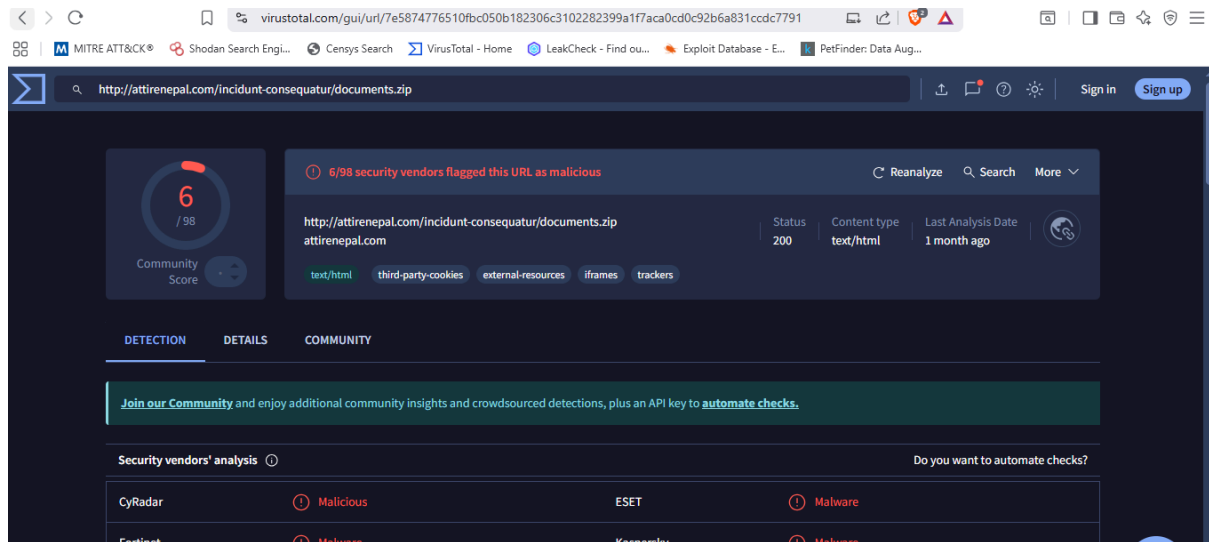
In order to investigate the process that has taken action we'll use wireshark .



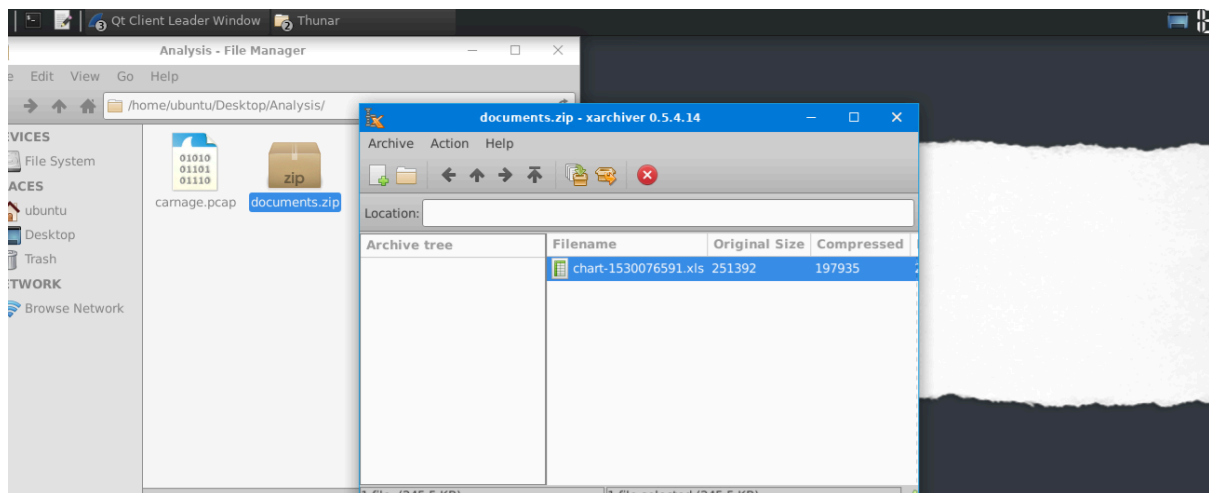
After isolating the suspicious action that occurred at 16:44:38 we can see documents.zip was downloaded and it's host "attirenepal.com"



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

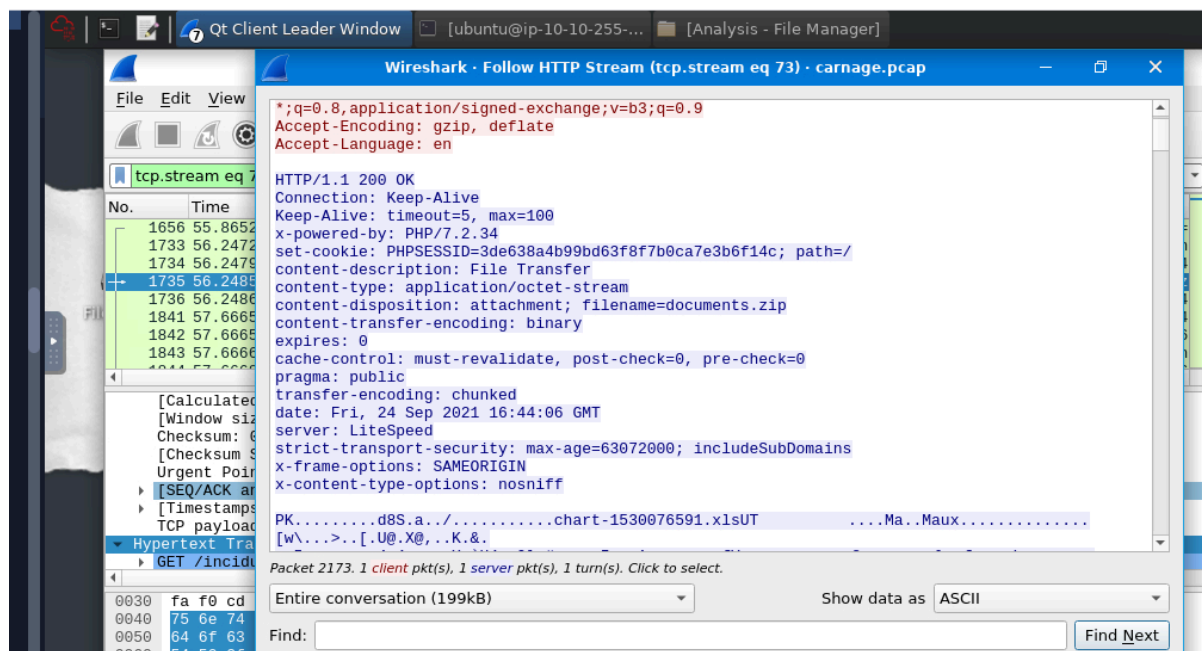


This confirms the malicious activity and that the alert is a true positive , further investigations need to take place .



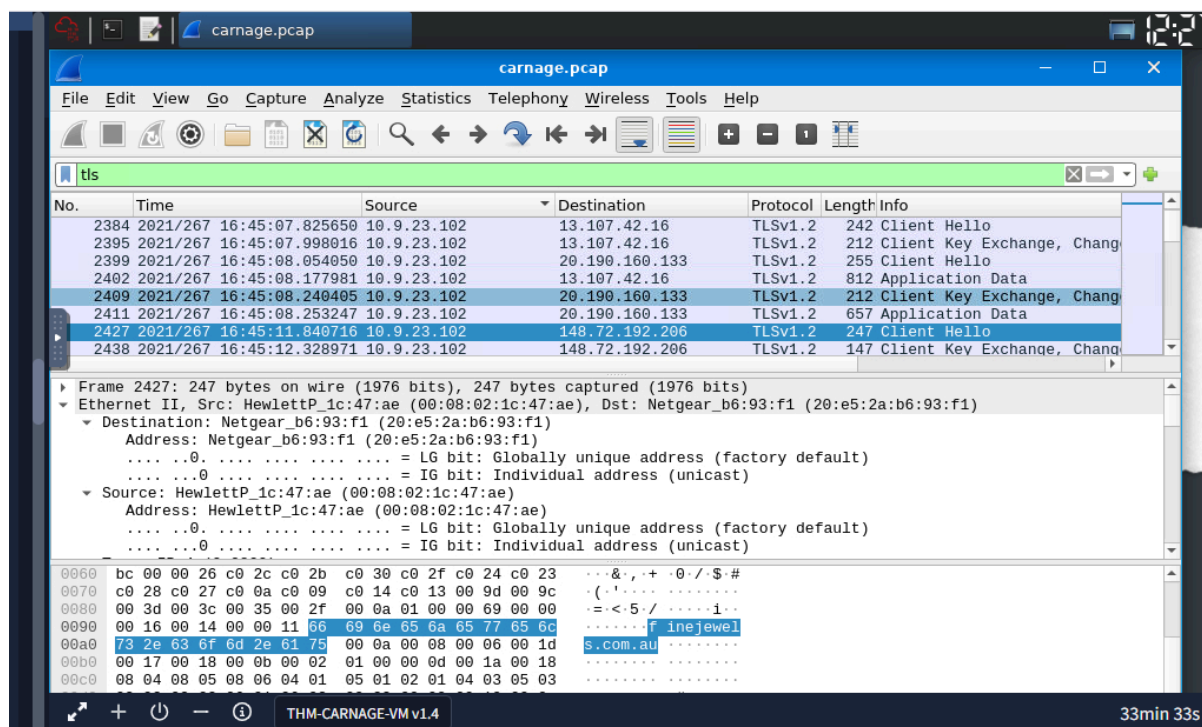
After extracting the malicious file in a sandbox we can notice that it's in xls format , it's possible to escalate this to a malware analyst in order to acquire more details .

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 web interface for the URL `http://finejewels.com.au/`. At the top, a red banner indicates that 4/98 security vendors flagged this URL as malicious. Below this, a table lists the security vendors and their respective detections:

Security Vendor	Detection
CyRadar	Malicious
Kaspersky	Malware
alphaMountain.ai	Suspicious
Fortinet	Malware
SOCradar	Phishing
Forcepoint ThreatSeeker	Suspicious

The interface also shows a 'Community Score' of 4/98 and a 'Last Analysis Date' of 24 days ago. The URL is categorized as 'text/html' with a 'Content type' of 'text/html; charset=utf-8'.

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

The screenshot shows a Wireshark packet capture of a TLS connection. The packet list on the left shows several packets, with packet 3009 selected. The packet details pane on the right shows the structure of the TLS Client Hello message:

- Frame 3009: 244 bytes on wire (1952 bits), 244 bytes captured (1952 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)
- Source: HewlettP_1c:47:ae (00:08:02:1c:47:ae)

The packet bytes pane at the bottom shows the raw data of the TLS Client Hello message, including the domain name `thietbiagt.com` in the 'Server Name' field.

MITRE ATT&CK® Shodan Search Engi... Censys Search VirusTotal - Home LeakCheck - Find ou... Exploit Database - E... PetFinder: Data Aug...

thietbiagt.com

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

3 / 95 Community Score

3/95 security vendors flagged this domain as malicious

Reanalyze Similar More

thietbiagt.com

Registrar: MAT BAO CORPORATION

Creation Date: 6 years ago

Last Analysis Date: 16 days ago

top-1M

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

carnage.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tls

No.	Time	Source	Destination	Protocol	Length	Info
3009	2021/267	16:45:21.314012	10.9.23.102	TLSv1.2	244	Client Hello
3018	2021/267	16:45:21.749716	10.9.23.102	TLSv1.2	147	Client Key Exchange, Chang
3022	2021/267	16:45:22.149523	10.9.23.102	TLSv1.2	141	Application Data
3024	2021/267	16:45:22.149646	10.9.23.102	TLSv1.2	201	Application Data
3028	2021/267	16:45:22.555055	10.9.23.102	TLSv1.2	92	Application Data
3229	2021/267	16:45:25.731116	10.9.23.102	TLSv1.2	247	Client Hello
3242	2021/267	16:45:26.047029	10.9.23.102	TLSv1.2	147	Client Key Exchange, Chang
3246	2021/267	16:45:26.347554	10.9.23.102	TLSv1.2	141	Application Data

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..... = LG bit: Globally unique address (factory default)

.....0..... = IG 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..... = LG bit: Globally unique address (factory default)

.....0..... = IG bit: Individual address (unicast)

41 00 00 26 c0 2c c0 2b c0 30 c0 2f c0 24 c0 23 A . & , + 0 / \$ #

c0 28 c0 27 c0 0a c0 09 c0 14 c0 13 00 0d 00 9c ((

00 3d 00 3c 00 35 00 2f 00 0a 01 00 00 69 00 00 . = < 5 / i . .

00 16 00 14 00 00 11 6e 65 77 2e 61 6d 65 72 69 n ew . amer i

63 6f 6c 64 2e 63 6f 6d 00 0a 00 08 00 06 00 1d cold . com

00 17 00 18 00 0b 00 02 01 00 00 0d 00 1a 00 18

08 04 08 05 08 06 04 01 05 01 02 01 04 03 05 03

THM-CARNAGE-VM v1.4 17min 59s

MITRE ATT&CK® Shodan Search Engi... Censys Search VirusTotal - Home LeakCheck - Find ou... Exploit Database - E... PetFinder: Data Aug...

new.americold.com

1 / 95 Community Score

1/95 security vendor flagged this domain as malicious

Reanalyze Similar More

new.americold.com

Registrar: CSC Corporate Domains, Inc.

Creation Date: 30 years ago

Last Analysis Date: 15 hours ago

DETECTION DETAILS RELATIONS COMMUNITY 2

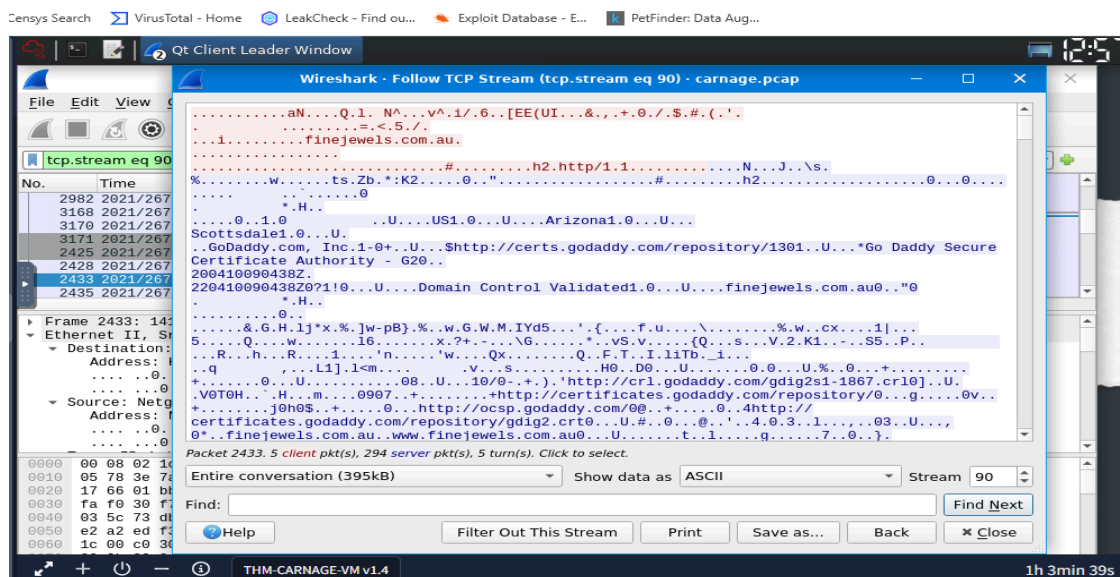
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

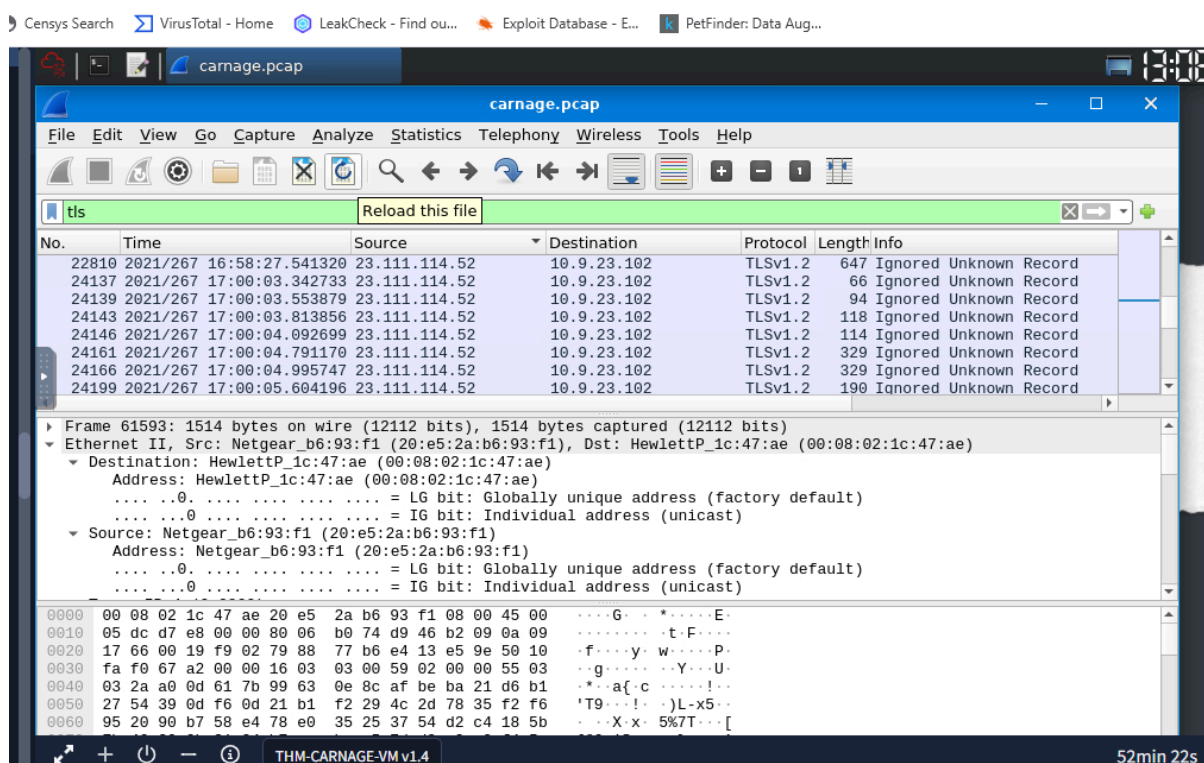
Fortinet	Malware	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AILabs (MONITORAPP)	Clean	AlienVault	Clean

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



MITRE ATT&CK® Shodan Search Engi... Censys Search VirusTotal - Home LeakCheck - Find ou... Exploit Database - E... PetFinder: Data Aug...

23.111.114.52

13 / 95
Community Score -49

13/95 security vendors flagged this IP address as malicious

Reanalyze Similar More

23.111.114.52 (23.111.96.0/19)
AS 39134 (Edinaya Set Limited Liability Company)

RU Last Analysis Date 3 days ago

DETECTION DETAILS RELATIONS COMMUNITY 14

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	ArcSight Threat Intelligence	Malware
BitDefender	Phishing	CyRadar	Malicious
ESET	Malware	Fortinet	Malware

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 and validating by using external resources such as virus total .