

Challenge Writeup: Carnage

This writeup details the approach to solving the Carnage challenge hosted on TryHackMe. This room involves using Wireshark to analyse a PCAP file, however, you could use Brim and other tools to investigate the file.

Scenario: Eric Fischer from the Purchasing Department at Bartell Ltd has received an email from a known contact with a Word document attachment. Upon opening the document, he accidentally clicked on “Enable Content”. The SOC Department immediately received an alert from the endpoint agent that Eric’s workstation was making suspicious connections outbound. The pcap was retrieved from the network sensor and handed to you for analysis. Your task is to investigate the packet capture and uncover the malicious activities.

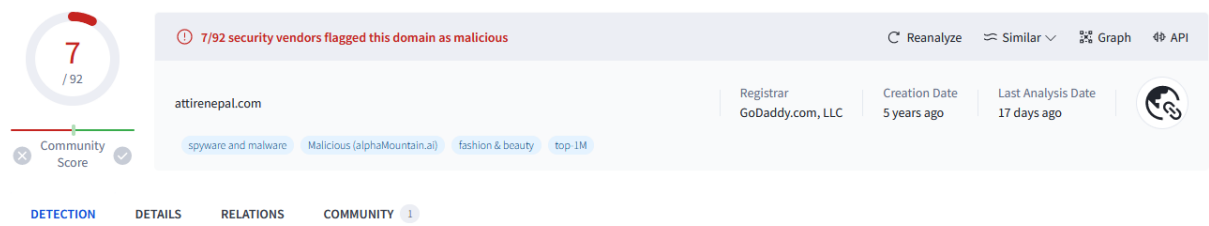
1. What was the date and time for the first HTTP connection to the malicious IP?

I started off this analysis by loading the given PCAP file and using a display filter to filter for tcp port 80 traffic aka HTTP:

- tcp.port == 80

No.	Time	Source	Destination	Protocol	Length	Host	Info
1656	2021-09-24 16:44:38.607114	10.9.23.102	85.187.128.24	TCP	66		62245 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1696	2021-09-24 16:44:38.816464	10.9.23.102	85.187.128.24	TCP	66		52275 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1733	2021-09-24 16:44:38.989165	85.187.128.24	10.9.23.102	TCP	58		80 → 62245 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
1734	2021-09-24 16:44:38.989824	10.9.23.102	85.187.128.24	TCP	54		62245 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
1735	2021-09-24 16:44:38.990412	10.9.23.102	85.187.128.24	HTTP	514	attirenepal.com	GET /incidunt-consequatur/documents.zip HTTP/1.1

What caught my attention is the GET requests made to 85.187.128.24, where a zip file was downloaded (documents.zip). It is common to see malware within a zip archive usually password protected to try and evade endpoint security controls. To verify/confirm my suspicion, I decided to enter the domain into VirusTotal:



As you can see, several vendors flagged the domain as malicious. Therefore, the answer is simply the first HTTP connection which is 2021-09-24 16:44:38.

2. What is the name of the zip file that was downloaded?

This is super easy; you can see the name of the zip file in the image in question 1:

GET /incidunt-consequatur/documents.zip HTTP/1.1

You can also easily find the answer by checking the file logs in Brim:

_path	tx_hosts	rx_hosts	conn_uids	mime_type	filename	md5	sha1
file	10.9.23.102	185.14.56.240	C5p1f21UWOP6qdF5M2	application/zip	=7UTF-87B7Q2xhaW0tNDg2NjkzNjEyLTASmJyQyMDIxLnppcA==?	08be246371e65cac315b868ba397e421	30b5e3723f340bc7fd30b1fdf2292cbf0cf712d5
file	10.9.23.102	93.89.226.88	CILAj2YV5Hh3aB3Ej	application/zip	=7UTF-87B7Q2xhaW0tNDg2NjkzNjEyLTASmJyQyMDIxLnppcA==?	32345f29077eed5d26a27055524245f3	3399db49c34c7a169400d4d85e2b77b178c8dec6e
file	10.9.23.102	177.149.159.181	CxNsb48yYKZf3dZf	application/zip	=7UTF-87B7Q2xhaW0tNDg2NjkzNjEyLTASmJyQyMDIxLnppcA==?	bfd95c78552e86351437b0bf216f30b	909ebb9cb6e6f5ca9e7bf5f3b03c93034f19f9f4
file	85.187.128.24	10.9.23.102	CCkG7q2RshYqc8bC02	application/zip	documents.zip	a7658b33cd0d5289190b58fb62ab3b71	dcd0b4446a46850b95b7a2b776675448faaeb58

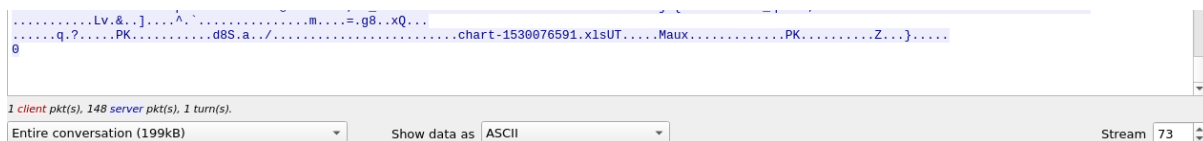
3. What was the domain hosting the malicious zip file?

I decided to add the hostname as a column to Wireshark which allows us to easily see the domain hosting the malicious file:

```
attirenepal.com
```

4. Without downloading the file, what is the name of the file in the zip file?

There is likely multiple ways to do this, however, I went the route of following the TCP stream of the GET request and scrolling down the payload until I found something interesting at the bottom:



As you can see, there is a filename 'chart-1530076591.xls'.

5. What is the name of the webserver of the malicious IP from which the zip file was downloaded?

Using the same TCP stream as the previous question, if you look at the server response header, you can see the name of the webserver:

```
HTTP/1.1 200 OK
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100
x-powered-by: PHP/7.2.34
set-cookie: PHPSESSID=3de638a4b99bd63f8f7b0ca7e3b6f14c; path=/
content-description: File Transfer
content-type: application/octet-stream
content-disposition: attachment; filename=documents.zip
content-transfer-encoding: binary
expires: 0
cache-control: must-revalidate, post-check=0, pre-check=0
pragma: public
transfer-encoding: chunked
date: Fri, 24 Sep 2021 16:44:06 GMT
server: LiteSpeed
strict-transport-security: max-age=63072000; includeSubDomains
x-frame-options: SAMEORIGIN
x-content-type-options: nosniff
```

6. What is the version of the webserver from the previous question?

Similarly, we can see in the above image that the webserver is running PHP version 7.2.34 so the answer is:

x-powered-by: PHP/7.2.34

7. Malicious files were downloaded to the victim host from multiple domains. What were the three domains involved with this activity.

Using the hint, we can enter the following query to find the answer:

- `tls.handshake.type == 1 && frame.time >= "Sep 24, 2021 16:45:11" && frame.time <= "Sep 24, 2021 16:45:30"`
- `tls.handshake.type == 1` simply filters for TLS Client Hello messages, and
- `frame.time >= "Sep 24, 2021 16:45:11" && frame.time <= "Sep 24, 2021 16:45:30"` restricts the display to the specified time range given in the hint.

tls.handshake.type == 1 && frame.time >= "Sep 24, 2021 16:45:11" && frame.time <= "Sep 24, 2021 16:45:30"							
No.	Time	Source	Destination	Protocol	Length	Host	Server Name
3229	2021-09-24 16:45:25.731116	10.0.23.102	148.72.53.144	TLSv1.2	247	new.americold.com	new.americold.com
2427	2021-09-24 16:45:11.840716	10.0.23.102	148.72.192.206	TLSv1.2	247	finejewels.com.au	finejewels.com.au
3009	2021-09-24 16:45:21.314012	10.0.23.102	210.245.90.247	TLSv1.2	244	thietbiagt.com	thietbiagt.com

We are concerned with the highlighted packets so the answer will be:

finejewels.com.au, thietbiagt.com, new.americold.com

8. Which certificate authority issued the SSL certificate to the first domain from the previous question?

Simply follow the TCP stream from the 2 packet seen using the query previously, you will then be able to identify the SSL certificate authority:

\$http://certs.godaddy.com/repository/1301..U...*Go Daddy Secure Certificate Authority - G20..

9. What are the two IP addresses of the Cobalt Strike servers? Use VirusTotal (the Community tab) to confirm if Ips are identified as Cobalt Strike C2 servers.

Seeing as Cobalt Strike communicate through GET and POST requests I will filter for GET requests using the following query:

- `http.request.method == GET`

I then navigated to Statistics -> Conversations and sorted the Packets column to identify IP addresses which have frequently been communicating. I then simply checked through the top IP addresses and entered them into VirusTotal and found both Cobalt Strike C2 servers:



4
/ 92

Community Score

4/92 security vendors flagged this IP address as malicious

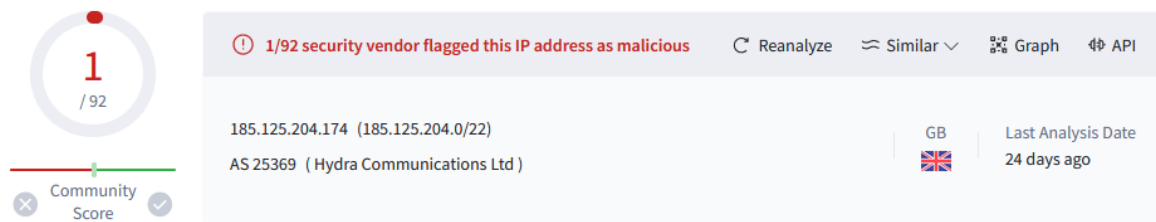
Reanalyze Similar Graph API

185.106.96.158 (185.106.96.0/24)

AS 133619 (DESIVPS)

US

Last Analysis Date
23 days ago



Both are claimed to be Cobalt Strike C2 servers in the community comments:

Cobalt Strike Server Found
 C2: HTTPS @ 185[.]106[.]96[.]158:8888
 C2 Server: survmeter[.]live,/gscp[.]R/,185[.]106[.]96[.]158,/gscp[.]R/
 POST URI: /supprq/sa/
 Country: United States
 ASN: DediPath
 Host Header: ocsp[.]verisign[.]com

10. What is the host header for the first Cobalt Strike IP address from the previous question?

I first started by filtering for the IP address of the first C2 server like as follows:

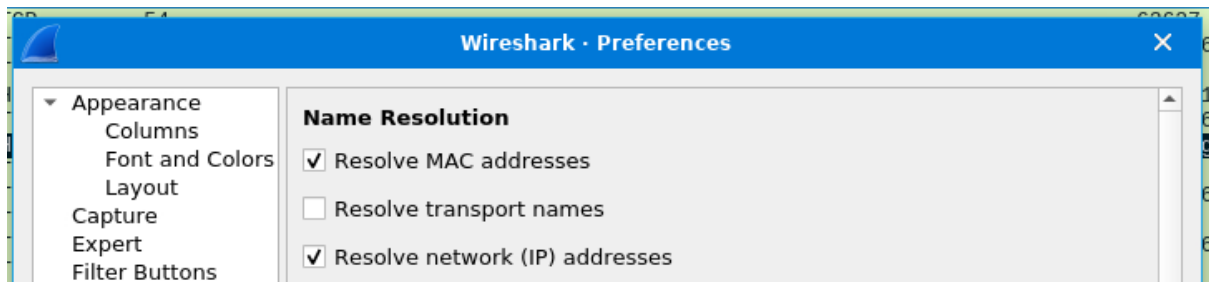
- ocsp.verisign.com

I then found the host header in the packet details pane under HTTP:

```
Frame 26879: 569 bytes on wire
Ethernet II, Src: HewlettP_1c:4
Internet Protocol Version 4, S
Transmission Control Protocol,
Hypertext Transfer Protocol
  [truncated]GET /gscp.R/oapn
  Accept: */*\r\n
  Host: ocsp.verisign.com\r\n
  User-Agent: Mozilla/5.0 (Win
  Connection: Keep-Alive\r\n
  Cache-Control: no-cache\r\n
  \r\n
```

11. What is the domain name for the first IP address of the Cobalt Strike Server? You may use VirusTotal to confirm if it's the Cobalt Strike server.

To answer this, first enable 'Resolve network (IP addresses):



Then filter for the IP address we identified previously:

ip.addr == 185.106.96.158			
No.	Time	Source	Destination
27685	2021-09-24 17:02:25.594617	ip-10-9-23-102.eu-w...	survmeter.live
26909	2021-09-24 17:02:22.333887	ip-10-9-23-102.eu-w...	survmeter.live

You can find the domain name under destination. You can also just look through DNS queries.

12. What is the domain name of the second Cobalt Strike server IP? You may use VirusTotal to confirm if it's the Cobalt Strike server.

For this question, I decided to use VirusTotal by entering the IP address found earlier for the second C2 server (185.125.204.174) and then navigating to the community section:



drb_ra

2 years ago

Cobalt Strike Server Found

C2: HTTPS @ 185[.]125[.]204[.]174:4444

C2 Server: securitybusinpu[.]com, /jquery-3[.]3[.]1[.]min[.]js, 185[.]125[.]204[.]174, /jquery-3[.]3[.]1[.]min[.]js

POST URI: /jquery-3[.]3[.]2[.]min[.]js

Country: N/A

ASN: Hydra Communications Ltd

#c2 #cobaltstrike

The defanged domain name is the answer.

13. What is the domain name of the post-infection traffic?

I started off by filtering for http POST traffic by entering the following display filter:

- http.request.method == POST

You can immediately determine that the domain name of the post-infection traffic is **maldivehost.net**:

No.	Time	Source	Destination	Protocol	Length	Host	Info
4140	2021-09-24 16:51:42.636644	10.9.23.102	208.91.128.6	HTTP	265	maldivehost.net	POST /zLIisQRWZI9/ITIYRX5ZHZJ1fXhkenx9 HTTP/1.1 Continuation
4150	2021-09-24 16:52:07.751878	10.9.23.102	208.91.128.6	HTTP	265	maldivehost.net	POST /zLIisQRWZI9/OhpCfX9lc2V+fGv7e34= HTTP/1.1 Continuation
4162	2021-09-24 16:52:32.848606	10.9.23.102	208.91.128.6	HTTP	273	maldivehost.net	POST /zLIisQRWZI9/DcWZNSYNBRJfFntkcmJ9eGR6fH0= HTTP/1.1 Continuation
4179	2021-09-24 16:52:58.930595	10.9.23.102	208.91.128.6	HTTP	289	maldivehost.net	POST /zLIisQRWZI9/myYfEB/BgeuIAnYGHgkPAMSGdcYQ3p8YXJxeXhemp5 HTTP/1.1 Continuation
4207	2021-09-24 16:53:23.217609	10.9.23.102	208.91.128.6	HTTP	277	maldivehost.net	POST /zLIisQRWZI9/eg17fAgEMAQAakJ7e2J2ZXh4Yn57eA== HTTP/1.1 Continuation
4581	2021-09-24 16:53:48.310036	10.9.23.102	208.91.128.6	HTTP	269	maldivehost.net	POST /zLIisQRWZI9/KQsyKkZ6emV1YX15ZX1/eQ= HTTP/1.1 Continuation
4930	2021-09-24 16:54:13.397897	10.9.23.102	208.91.128.6	HTTP	289	maldivehost.net	POST /zLIisQRWZI9/hh8fPwglJRkuIzgr0jp5HjovOkZ6emV1YX15ZX1/eQ= HTTP/1.1 Continuation
5208	2021-09-24 16:54:38.381382	10.9.23.102	208.91.128.6	HTTP	265	maldivehost.net	POST /zLIisQRWZI9/AjlcFk9lc2V+fGv7e34= HTTP/1.1 Continuation
6227	2021-09-24 16:55:03.473692	10.9.23.102	208.91.128.6	HTTP	265	maldivehost.net	POST /zLIisQRWZI9/OSdCfX9lc2V+fGv7e34= HTTP/1.1 Continuation
6600	2021-09-24 16:55:28.568119	10.9.23.102	208.91.128.6	HTTP	297	maldivehost.net	POST /zLIisQRWZI9/H1YfEtpyPng4KCF4Pzk8EQgQ0kQ0A0PBUJ7e2J2ZXh4Yn57eA== HTTP/1.1 Continuation
7188	2021-09-24 16:55:53.548487	10.9.23.102	208.91.128.6	HTTP	285	maldivehost.net	POST /zLIisQRWZI9/3hANAz16Gw8FBhMABRYGcn9CFX9lc2V+fGv7e34= HTTP/1.1 Continuation

14. What are the first eleven characters that the victim host sends out to the malicious domain involved in the post-infection traffic?

You can see the first eleven characters that the victim host sends to the malicious domain in the first packet display using the query in the previous question:

POST /zLIisQRWZI9/

15. What was the length for the first packet sent out to the C2 server?

We can see the length of the first packet under the length column when using the query from 2 questions ago:

http.request.method == POST						
No.	Time	Source	Destination	Protocol	Length	
3822	2021-09-24 16:46:16.395000	10.9.23.102	208.91.128.6	HTTP	281	

16. What was the sever header for the malicious domain from the previous question?

To find the server header, simply follow the TCP stream for the first packet when using the http.request.method == POST query and look at the server field:

Wireshark · Follow TCP Stream (tcp.stream eq 104) · carnage.pcap	
POST /zLIisQRWZI9/OQsaDixzHTgtfjMcGypGenpldWF5ewV9f3k= HTTP/1.1	
Host: maldivehost.net	
Content-Length: 112	
Dw8YBxsEGmYFAAEJFR4NQkMmLTYqZDk5KyQmOyRGQglxEB04Lzk/EyYrMi1h0T8vIyM7IhcNPzs0KjguFvgkLSIIJCxFRgwFAgIIDQUZGB0FD0JF	
HTTP/1.1 200 OK	
Date: Fri, 24 Sep 2021 16:46:15 GMT	
Server: Apache/2.4.49 (cPanel) OpenSSL/1.1.1l mod_bwlimited/1.4	
X-Powered-By: PHP/5.6.40	
Content-Length: 302	
Strict-Transport-Security: ...max-age=15552000...	
Connection: close	
Content-Type: text/html; charset=UTF-8	

17. The malware used an API to check for the IP address of the victim's machine. What was the date and time when the DNS query for the IP check domain occurred?

You could use a display filter like frame.contains "api", however, I simply queried for all DNS traffic by entering the following display filter:

- udp.port == 53

After scrolling through the requests, you can find a query that resolves an IP address to api.ipify.org which is an API that enables you to get someone's public IP address.

24147	2021-09-24	17:00:04.093354	10.9.23.102	10.9.23.5	DNS	73 api.ipify.org
-------	------------	-----------------	-------------	-----------	-----	------------------

The answer is simply the timestamp.

18. What was the domain in the DNS query from the previous question?

Fortunately for us, the name of the domain can be seen using the query sent previously and also in the image above.

19. Looks like there was some malicious spam (malspam) activity going on. What was the first MAIL FROM address observed in the traffic?

To find the first MAIL FROM address observed in the traffic, I enter the following display filter which filters for SMTP traffic that contains the text "MAIL FROM":

- smtp && frame contains "MAIL FROM"

No.	Time	Source	Destination	Protocol	Length	Name	Info
26576	2021-09-24 17:02:40.770117	10.9.23.102	105.4.29.135	SMTP	85		C: MAIL FROM:<farshin@mailfa.com>
26804	2021-09-24 17:02:40.813592	10.9.23.102	177.149.159.181	SMTP	93		C: MAIL FROM:<ho3ein.sharifi@mailfa.com>
39985	2021-09-24 17:03:30.417353	10.9.23.102	93.89.226.88	SMTP	112		C: MAIL FROM:<cristianodummar@cultura.com.br> BODY=8BITIME
46434	2021-09-24 17:03:59.536388	10.9.23.102	185.14.56.249	SMTP	95		C: MAIL FROM:<info@tanrıverdinakiliyat.com>
67182	2021-09-24 17:04:45.764101	10.9.23.102		SMTP	101		C: MAIL FROM:<roser@barcelo.com> BODY=8BITIME

You can see the first from address in the first packet. You can also follow the TCP traffic of the first packet to see the from address:

```
220 mail.mailfa.com
EHLO localhost
250-mail.mailfa.com
250-SIZE 300000000
250 AUTH LOGIN
AUTH LOGIN
334 VXNlcm5hbWU6
ZmFyc2hpbkBTYWlsZmEuY29t
334 UGFzc3dvcmQ6
ZGluYW1pdA==
235 authenticated.
MAIL FROM:<farshin@mailfa.com>
550 Your SMTP Service is disable please check by your mailservice provider.
```

20. How many packets were observed for the SMTP traffic?

To find the number of SMTP packets, you can simply use the 'smtp' display filter and check the bottom right-hand corner of the Wireshark window to see the displayed packets:

Packets: 70873 · Displayed: 1439

Conclusion

This writeup analysed a pcap file which contains traffic of a malicious campaign involving multiple domains and IP addresses, including Cobalt Strike C2 servers. The initial infection vector was a malicious Word document. Utilising Wireshark and cross-referencing with VirusTotal I was able to answer all of the questions and complete the room. I really enjoyed completing this room and hope my writeup can be of use to someone out there.