COMP3010HK Security Operations and Incident Management 2025/2026
Coursework 1: Set Exercises - PCAP Analysis

Github repo: https://github.com/aka331/COMP3010HK/tree/main/CW1

Section 1 – Introduction

This report presents a network traffic investigation based on the provided PCAP file and associated quiz questions. The objective is to identify the infected system, understand how the infection occurred, and determine the nature of the malware or attack involved.

The structure of this report is as follows:
Section 2 describes the tools and methodology used to analyse the PCAP and extract key indicators of compromise (IOCs).
Section 3 presents the main findings, drawing on the quiz answers and supporting evidence from the traffic analysis.
Section 4 concludes with prevention techniques, open challenges, and relevant references.

Section 2 – Methodology

Wireshark was used to investigate the PCAP. I filtered HTTP GET traffic to find the first malicious download and extracted the timestamp, domain, file name, and server headers. I exported the downloaded archive via Export Objects to confirm the embedded file. I then used DNS/TLS evidence and Conversations statistics to identify C2 IPs and map them to domains/Host headers. Lastly, I followed the SMTP TCP stream and decoded Base64 authentication data to obtain the required email and password details.

```
http.request
```

Expression 1. Filtering only HTTP request traffic

```
http.request.method == "GET"
```

Expression 2. Filtering only HTTP GET requests

```
ip.src==10.9.23.102 && dns
```

Expression 3. Filtering only the source IP from 10.9.23.102 and the DNS protocol traffic

```
ip.addr == 185.106.96.158 && http
```

Expression 4. Filtering only the source IP from 185.106.96.158 and the HTTP traffic

```
ip.addr == 185.125.204.174 && tcp.port == 8080
```

Expression 5. Filtering only the source IP from 185.125.204.174 and the port 8080 protocol traffic

```
ip.addr==10.9.23.102 && http.request.method=="POST"
```

Expression 6. Filtering only the source IP from the user computer and the HTTP POST traffic

```
ip.addr==10.9.23.102 && dns && frame contains "api"
```

Expression 7. Filtering only the source IP from the user computer, the DNS protocol traffic, and containing “api”

```
ip.addr==10.9.23.102 && smtp && frame contains "FROM"
```

Expression 8. Filtering only the source IP from the user computer, the SMTP protocol traffic, and containing “FROM”

Section 3 – Results

Infected system identification: The compromised host is the primary internal client observed initiating the earliest suspicious HTTP download and subsequent repeated C2 communications. Key identifiers captured include IP address [victim IP], MAC address [victim MAC] (from ARP/Ethernet headers), and (if present) hostname/user context from relevant traffic.

Initial infection & file transfer: At **2021-09-24 16:44:38** (Figure 1), the victim made an HTTP GET request to **attirenepal.com,** retrieving **documents.zip** (Figure 2&3).

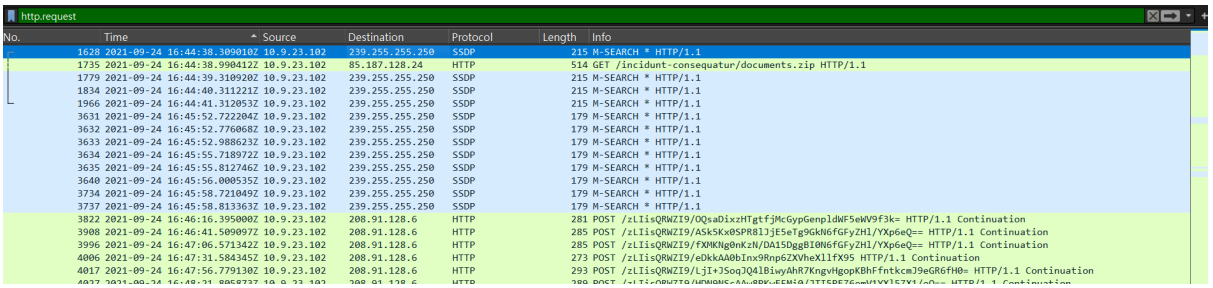


Figure 1. First HTTP request

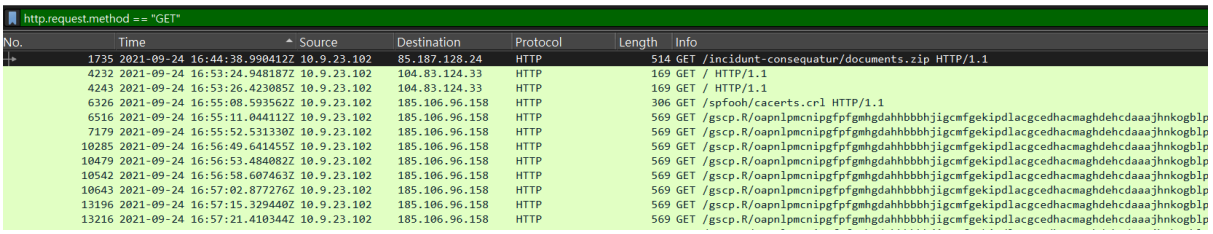


Figure 2. HTTP GET request that discovers document.zip

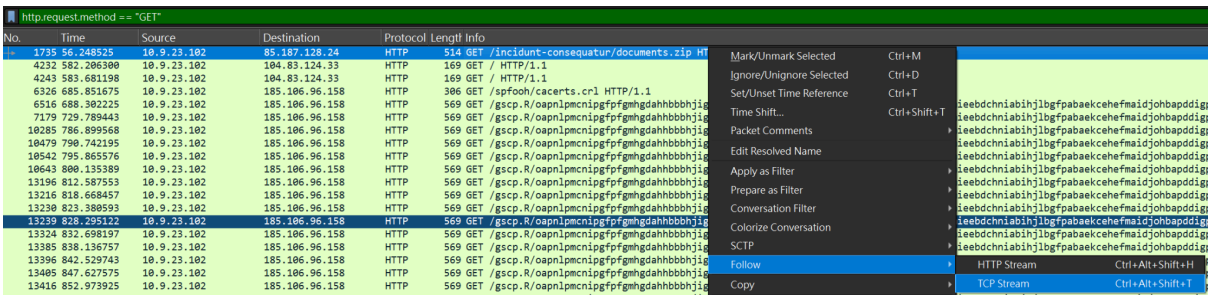


Figure 3. Select TCP Stream to view the dedicated traffic from GET /incidunt-consequatur/documents.zip HTTP/1.1

Exporting HTTP objects confirmed the archive contained **chart-1530076591.xls** (Figures 4 & 5). The malicious web server responded with Server: **LiteSpeed** with **PHP/7.2.34** (Figure 6), indicating the attacker-controlled infrastructure delivering the initial payload.

Figure 4. TCP Stream for /incidunt-consequatur/documents.zip

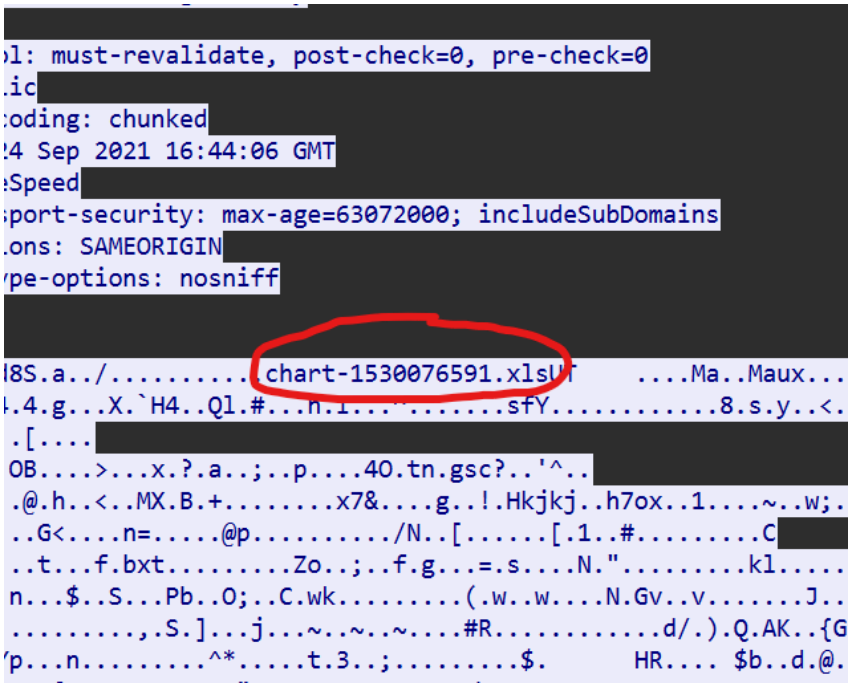


Figure 5. chart-1530076591.xls inside the stream

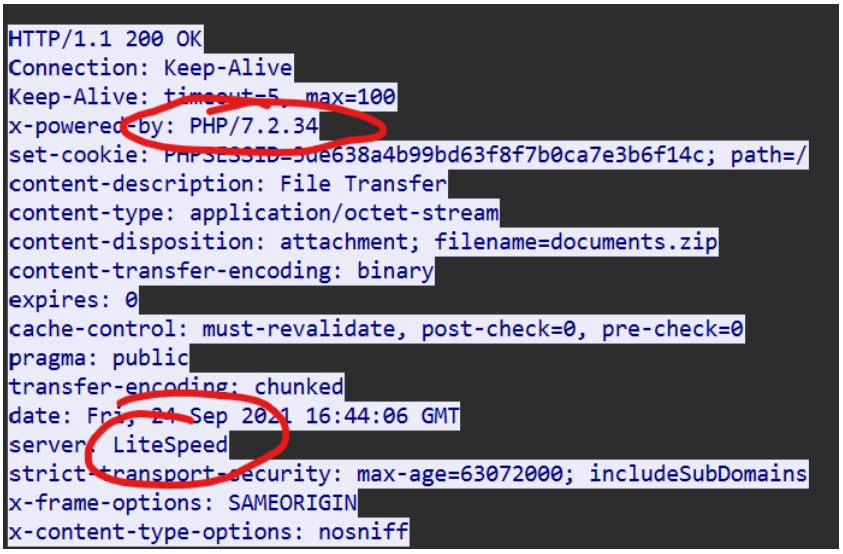


Figure 6. Web server and version

Additional download infrastructure: Within 16:45:11–16:45:30 UTC, additional domains contacted by the victim were **finejewels.com.au**, **thietbiagt.com**, and **new.americold.com,** as shown via DNS/TLS evidence (Figure 7). For the first domain, the TLS certificate issuer (CA) was **GoDaddy** (Figure 8).

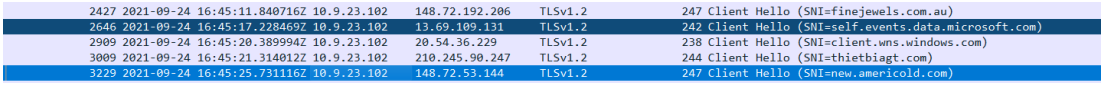


Figure 7. DNS traffic

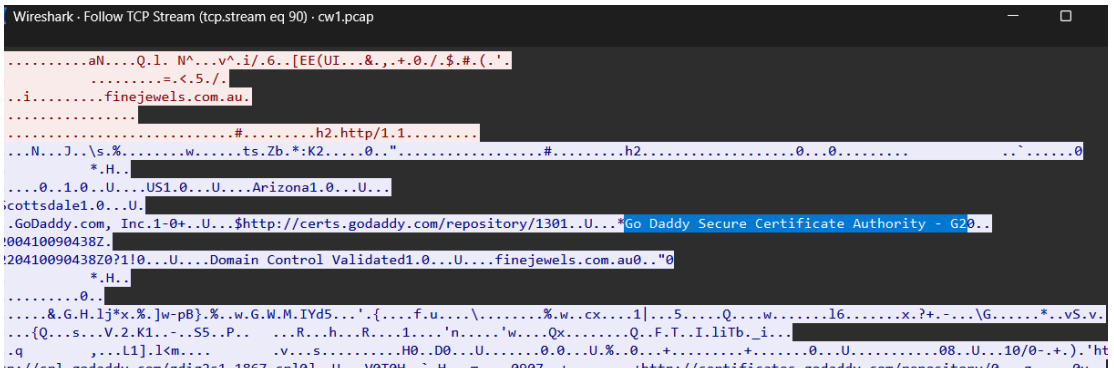
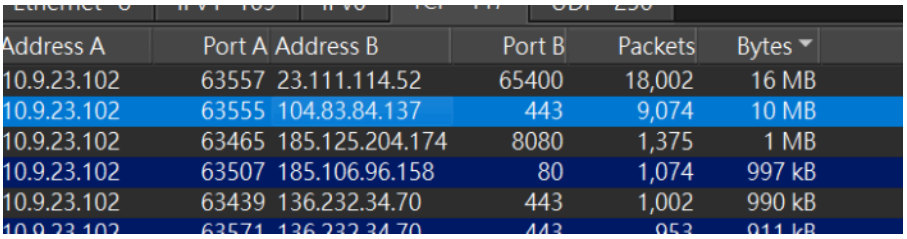


Figure 8. CA issuer

C2 activity (Cobalt Strike): Using Statistics → Conversations, two C2 candidate servers were identified: **185.125.204.174** (Port 8080) and **185.106.96.158** (Port 80) (Figures 9 & 10 & 11).

DNS analysis linked **185.106.96.158** (Port 80) to **survmeter.live** (Figure 12), and the Host/SNI value observed for this infrastructure was **ocsp.verisign.com** (Figure 13).

For **185.125.204.174**, HTTP POST traffic revealed an association with **securitybusinpuff.com** (Figure 14).



Address A	Port A	Address B	Port B	Packets	Bytes
10.9.23.102	63557	23.111.114.52	65400	18,002	16 MB
10.9.23.102	63555	104.83.84.137	443	9,074	10 MB
10.9.23.102	63465	185.125.204.174	8080	1,375	1 MB
10.9.23.102	63507	185.106.96.158	80	1,074	997 kB
10.9.23.102	63439	136.232.34.70	443	1,002	990 kB

Figure 9. TCP stream statistics in order of packets

Figure 10. Virustotal review (1)

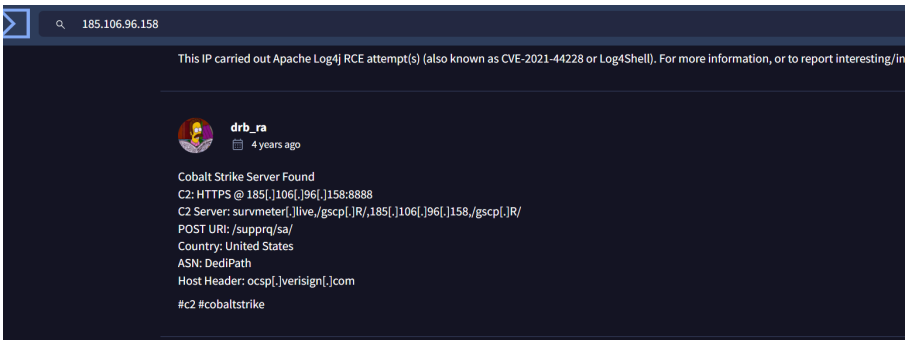
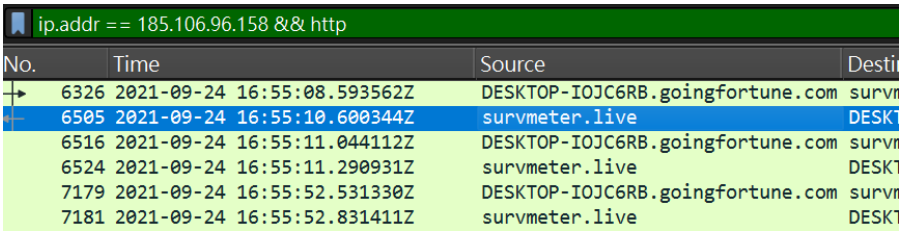


Figure 11. Virustotal review (2)



ip.addr == 185.106.96.158 && http

No.	Time	Source	Desti
6326	2021-09-24 16:55:08.593562Z	DESKTOP-IOJC6RB.goingfortune.com	survm
6505	2021-09-24 16:55:10.600344Z	survmeter.live	DESK
6516	2021-09-24 16:55:11.044112Z	DESKTOP-IOJC6RB.goingfortune.com	survm
6524	2021-09-24 16:55:11.290931Z	survmeter.live	DESK
7179	2021-09-24 16:55:52.531330Z	DESKTOP-IOJC6RB.goingfortune.com	survm
7181	2021-09-24 16:55:52.831411Z	survmeter.live	DESK

Figure 12. Domain linked to 185.106.96.158

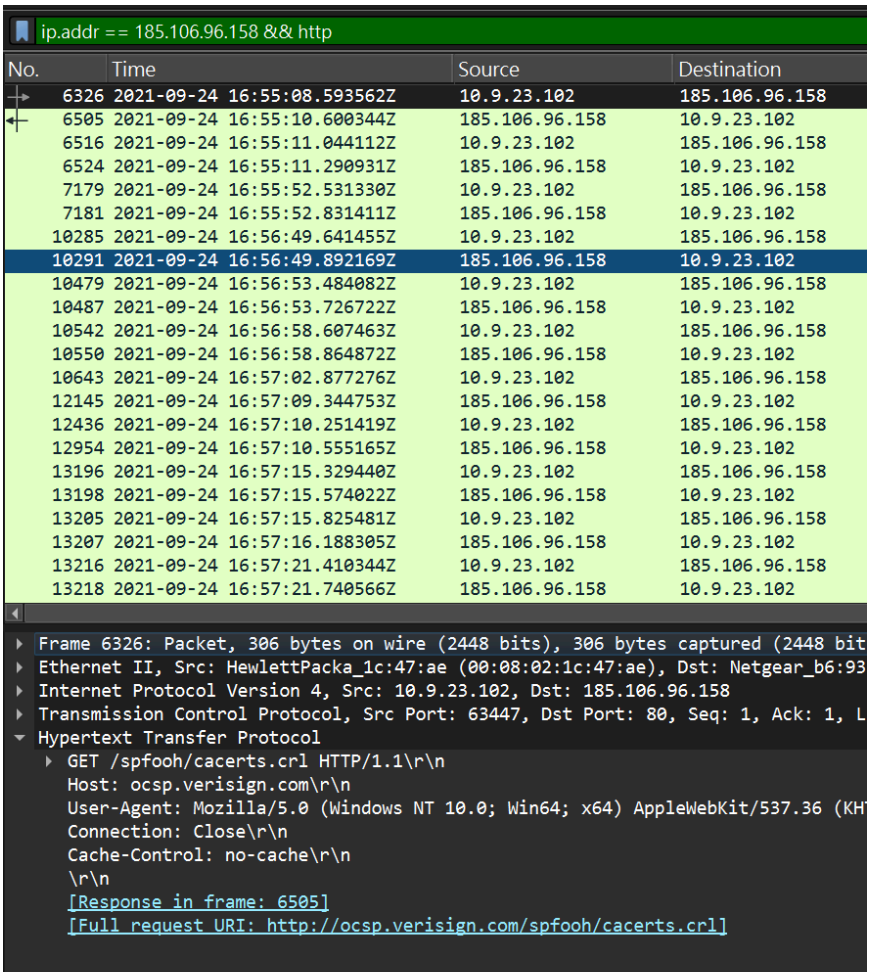


Figure 13. Request URL for 185.106.96.158

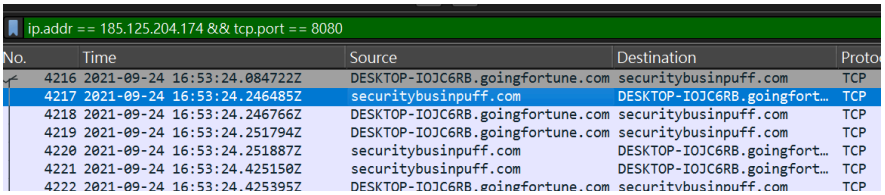


Figure 14. Domain linked to 185.125.204.174

Post-infection beaconing traffic was primarily directed to **maldivehost.net** (Figure 15), with the victim sending data beginning with **zLIisQRWZI9** (Figure 16). The first packet from the victim to the C2 server had a frame length of **281** bytes (Figure 16). Server-side response headers from **maldivehost.net** indicated Server: **Apache/2.4.49 (cPanel) OpenSSL/1.1.1l mod_bwlimited/1.4** (Figure 17), which further supports that this domain was attacker-controlled and actively responding to client beacons.

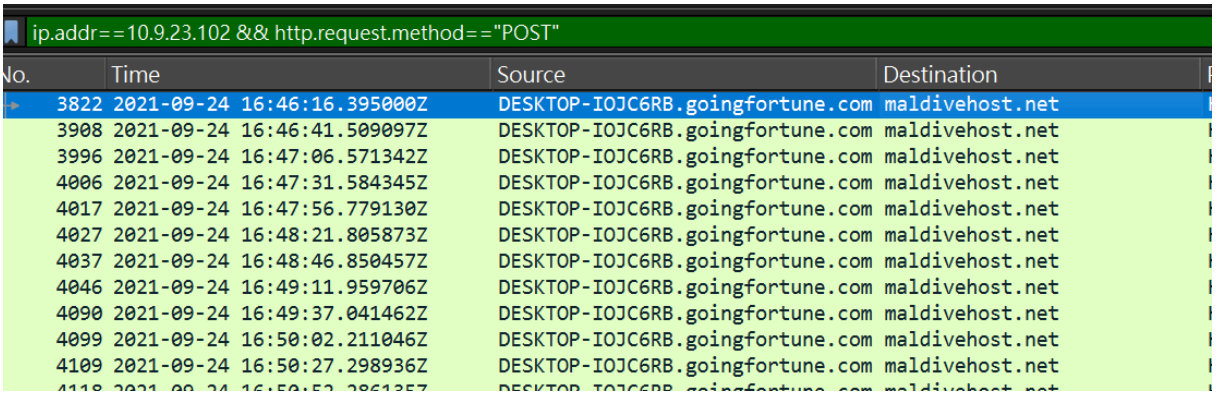


Figure 15. Post-infection beaconing traffic

Figure 16. Post-infection beaconing traffic

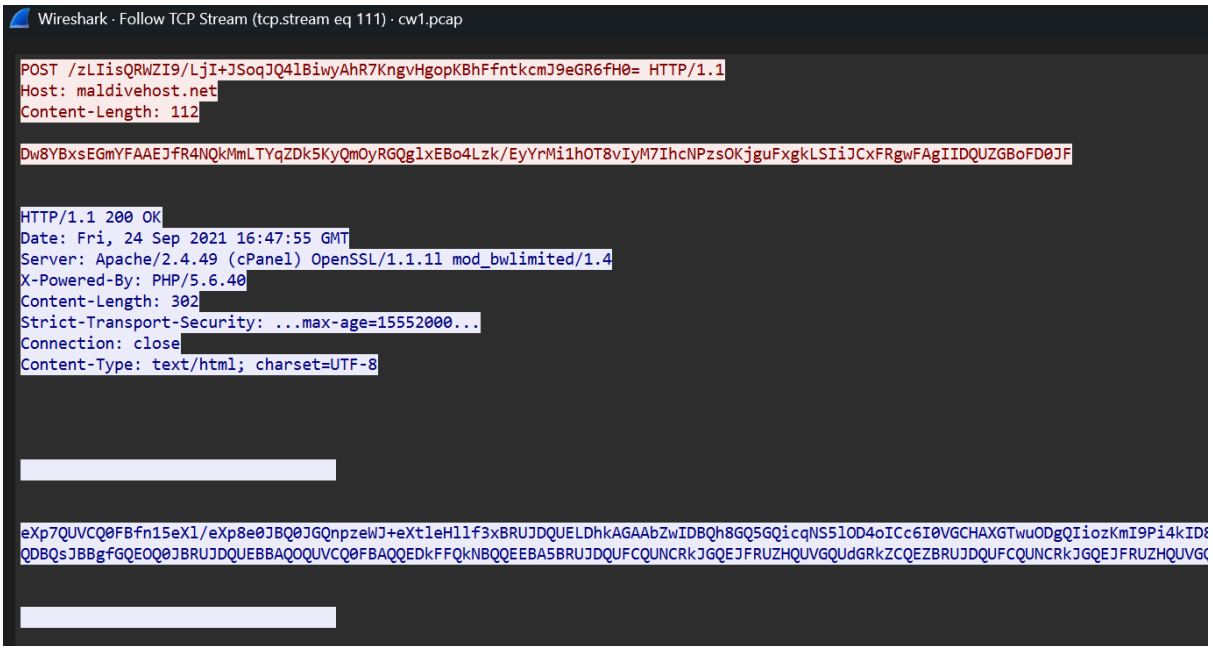


Figure 17. Server header

Final exfiltration/check-in: The malware performed an external IP check via DNS at **2021-09-24 17:00:04**, querying **api.ipify.org** (Figure 18). SMTP traffic showed the first MAIL FROM address as **farshin@mailfa.com** (Figure 19). Following the same TCP stream, the password was transmitted using AUTH LOGIN (Base64), and the password associated with ho3ein.sharifi's password is **13691369** (Figures 20 & 21).

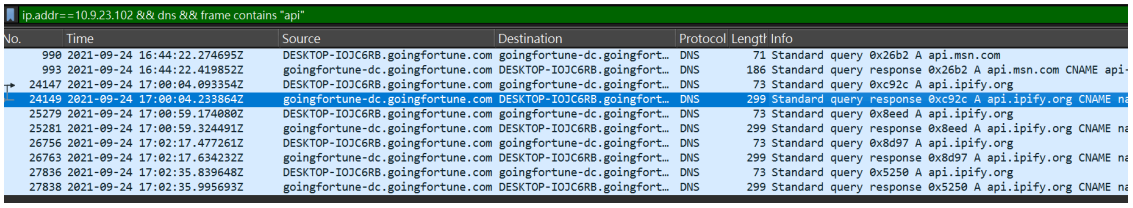


Figure 18. A DNS query occurred for the domain used by the malware

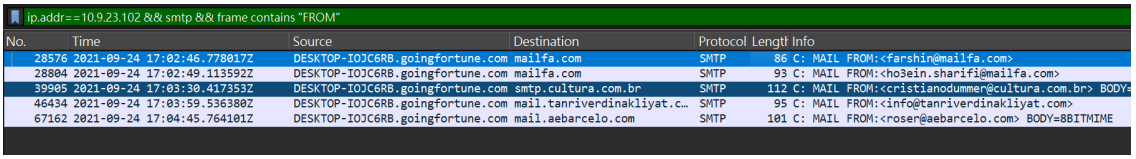


Figure 19. SMTP traffic

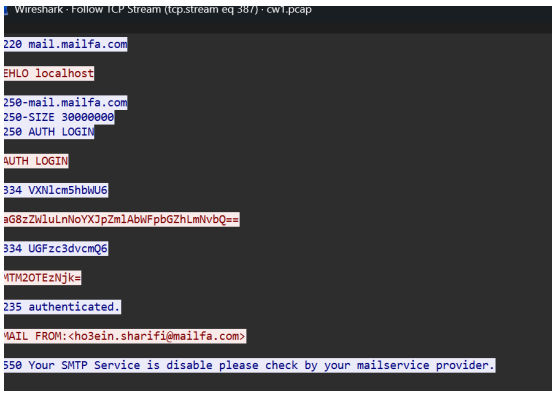


Figure 20. Packet content

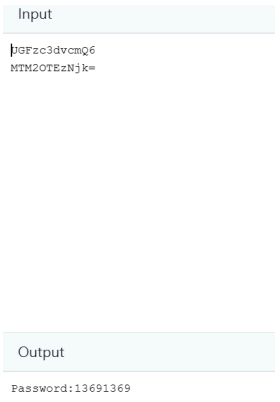


Figure 21. BASE64 decryption

Section 4 – Conclusion and References

The investigation successfully identified the infected system, reconstructed the initial infection vector, and characterised the C2 infrastructure and final exfiltration behaviour observed in the PCAP. The combination of protocol filtering, conversation analysis, and correlation with the quiz questions enabled a coherent incident narrative from initial compromise to attacker objectives.

To prevent similar incidents in the future, organisations should enforce secure web gateways, robust endpoint protection, and strict email filtering, as well as monitor network traffic for abnormal HTTP/HTTPS patterns and known malicious domains. Implementation of network intrusion detection systems (NIDS), regular patching, least-privilege access, and multi-factor authentication can further reduce the risk of successful compromise and lateral movement.

Open challenges remain around detecting encrypted C2 traffic, identifying zero-day malware, and distinguishing benign from malicious use of legitimate cloud and web services. Continued improvement of threat intelligence integration, behavioural analytics, and incident response processes is essential for enhancing situational awareness and resilience.

Reference

1. Palo Alto Networks Unit 42：

   Unit 42. (n.d.). Using Wireshark display filter expressions. Palo Alto Networks. https://unit42.paloaltonetworks.com/using-wireshark-display-filter-expressions/

2. Wireshark User’s Guide：

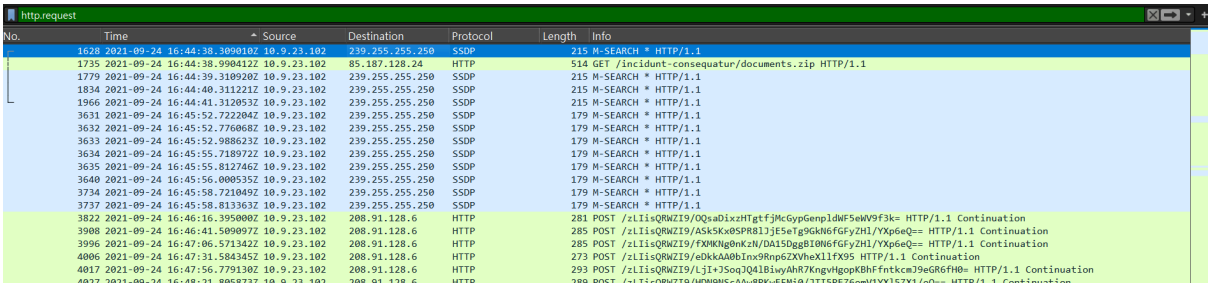
   Wireshark Foundation. (2019). Wireshark user’s guide (Version 4.7.0). https://www.wireshark.org/docs/wsug_html_chunked/

Appendix

Part 1: Initial Infection & File Transfer

1. When did the initial malicious HTTP connection occur? (Provide the date and time in yyyy-mm-dd hh:mm:ss format).

Ans:



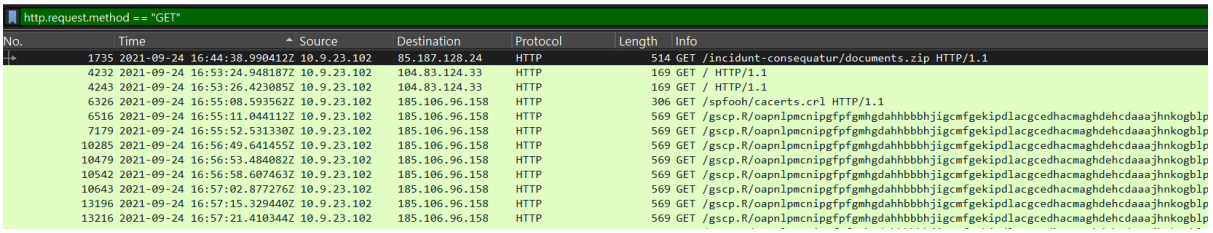
1735 2021-09-24 16:44:38.990412Z 10.9.23.102 85.187.128.24 HTTP 514 GET /incidunt-consequatur/documents.zip HTTP/1.1

UTC Arrival Time: Sep 24, 2021 16:44:38.309010000 UTC

2021-09-24 16:44:38

2. What is the name of the compressed file that the victim downloaded?

Ans:



[Full request URI: http://attirenepal.com/incidunt-consequatur/documents.zip]

documents.zip

3. Which domain hosted the malicious compressed file?

Ans:

attirenepal.com

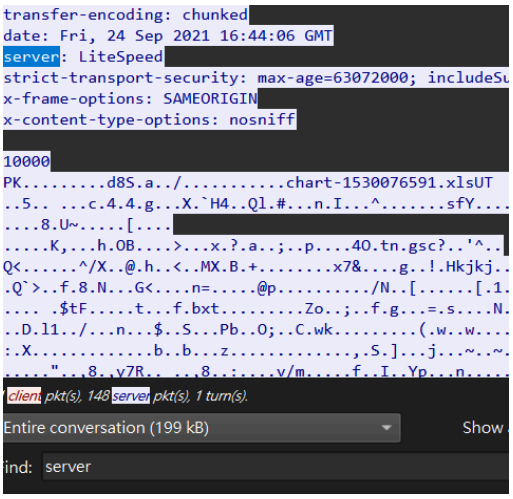
4. What is the name of the file located inside the compressed archive?

Ans:

chart-1530076591.xls

5. Identify the specific web server software (Server header) running on the malicious IP address that served the compressed file.

Ans:



LiteSpeed

6. What is the version number of the web server identified in the previous question?

Ans:
PHP/7.2.34

7. Identify the three additional domains that were involved in downloading malicious files to the victim host.
Hint: Inspect HTTPS traffic and focus on the time window between 16:45:11 and 16:45:30. Note this range is in UTC, not BST.

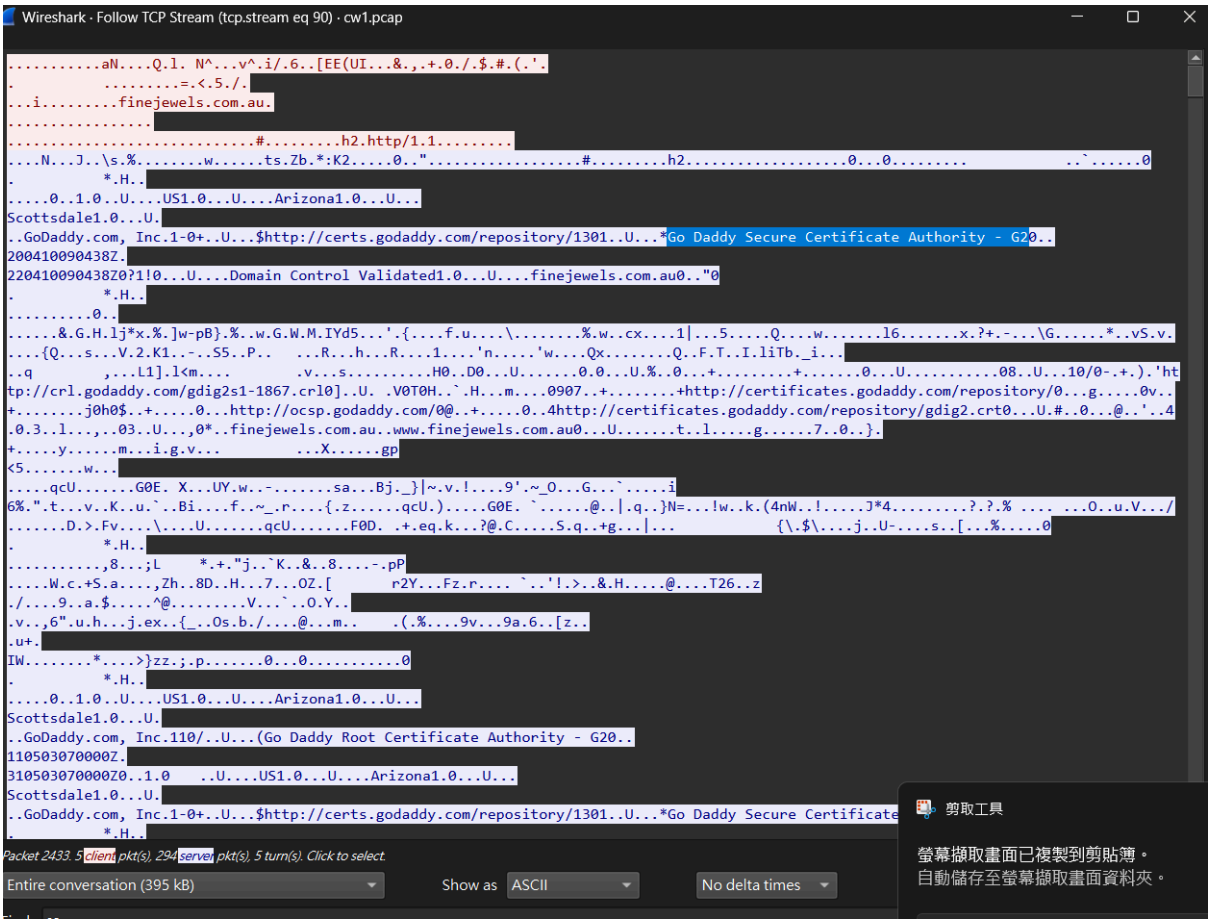
Ans:

2427	2021-09-24 16:45:11.840716Z	10.9.23.102	148.72.192.206	TLSv1.2	247 Client Hello (SNI=finejewels.com.au)
2646	2021-09-24 16:45:17.228469Z	10.9.23.102	13.69.109.131	TLSv1.2	242 Client Hello (SNI=self.events.data.microsoft.com)
2909	2021-09-24 16:45:20.389994Z	10.9.23.102	20.54.36.229	TLSv1.2	238 Client Hello (SNI=client.wns.windows.com)
3009	2021-09-24 16:45:21.314012Z	10.9.23.102	210.245.90.247	TLSv1.2	244 Client Hello (SNI=thietbiagt.com)
3229	2021-09-24 16:45:25.731116Z	10.9.23.102	148.72.53.144	TLSv1.2	247 Client Hello (SNI=new.americold.com)

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

Part 2: Command and Control (C2) Activity
8. Which Certificate Authority (CA) issued the SSL certificate for the first domain identified in question 7?

Ans:



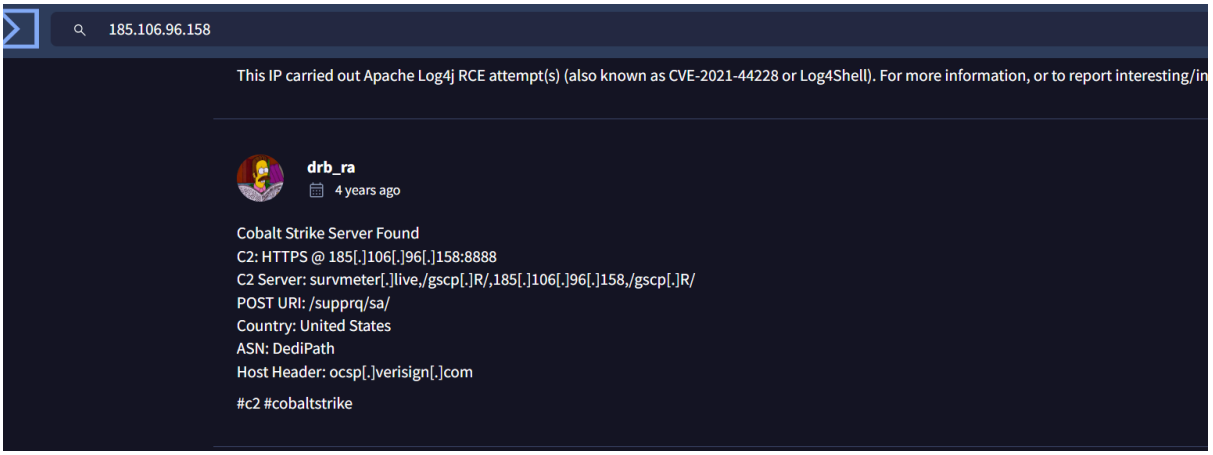
GoDaddy

9. What are the two IP addresses of the Cobalt Strike servers? (Provide them in sequential order).
Hint: Inspect the Conversations menu option

Ans:

Address A	Port A	Address B	Port B	Packets	Bytes
10.9.23.102	63557	23.111.114.52	65400	18,002	16 MB
10.9.23.102	63555	104.83.84.137	443	9,074	10 MB
10.9.23.102	63465	185.125.204.174	8080	1,375	1 MB
10.9.23.102	63507	185.106.96.158	80	1,074	997 kB
10.9.23.102	63439	136.232.34.70	443	1,002	990 kB

Virustotal



185.106.96.158
185.125.204.174

10.What is the value of the Host header for the first Cobalt Strike IP address?
Hint: Apply a filter to isolate DNS queries.

Ans:
ocsp.verisign.com

11.What is the domain name associated with the first Cobalt Strike IP address?
Hint: Take a closer look at HTTPS (443)

Ans:
survmeter.live

12.What is the domain name associated with the second Cobalt Strike IP address?
Hint: Apply a filter to capture HTTP POST requests.

Ans:
securitybusinpuff.com

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

Ans:
maldivehost.net

14.What are the first eleven characters of the data the victim host sends to the malicious domain identified in the previous question?

Ans:
zLIisQRWZI9

15.What was the length of the first packet the victim sent to the C2 server?

Ans:
281

16.What was the Server header value for the malicious domain from question 13?

Ans:
Apache/2.4.49 (cPanel) OpenSSL/1.1.1l mod_bwlimited/1.4

Part 3: Final Exfiltration/Check-in
17.What was the date and time (in yyyy-mm-dd hh:mm:ss UTC format) when the DNS query occurred for the domain used by the malware to check the victim's external IP address?

Ans:
2021-09-24 17:00:04

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

Ans:
api.ipify.org

19.What was the first email address observed in the SMTP traffic in the pcap file (the MAIL FROM address)?

Ans:
28576 2021-09-24 17:02:46.778017Z 10.9.23.102 185.4.29.135 SMTP 86 C: MAIL FROM:<farshin@mailfa.com>

farshin@mailfa.com

20.Follow the stream from Q19. What is ho3ein.sharifi’s password?

Ans:
220 mail.mailfa.com

EHLO localhost

250-mail.mailfa.com
250-SIZE 30000000
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.

Due to the communication using BASE64, which is decryptable, the password was found in the decrypt output.

Password:**13691369**

Student Declaration of AI Tool use in this Assessment

Please indicate your level of usage of generative AI for this assessment - please tick the appropriate category(s).

If the "Assisted Work" or "Partnered Work" category is selected, please expand on the usage and in which elements of the assignment the usage refers to.

Solo Work	**S1 - Generative AI tools have not been used for this assessment.**	☐
Assisted Work	**A1 – Idea Generation and Problem Exploration** Used to generate project ideas, explore different approaches to solving a problem, or suggest features for software or systems. Students must critically assess AI-generated suggestions and ensure their own intellectual contributions are central.	☐
	A2 - Planning & Structuring Projects AI may help outline the structure of reports, documentation and projects. The final structure and implementation must be the student's own work.	☐
	A3 – Code Architecture AI tools maybe used to help outline code architecture (e.g. suggesting class hierarchies or module breakdowns). The final code structure must be the student's own work.	☐
	A4 – Research Assistance Used to locate and summarise relevant articles, academic papers, technical documentation, or online resources (e.g. Stack Overflow, GitHub discussions. The interpretation and integration of research into the assignment remain the student's responsibility.	☐
	A5 - Language Refinement Used to check grammar, refine language, improve sentence structure in documentation not code. AI should be used only to provide suggestions for improvement. Students must ensure that the documentation accurately reflects the code and is technically correct.	☐

	A6 – Code Review AI tools can be used to check comments within the code and to suggest improvements to code readability, structure or syntax. AI should be used only to provide suggestions for improvement. Students must ensure that the code accurately reflects their knowledge and is technically correct.	☐
	A7 - Code Generation for Learning Purposes Used to generate example code snippets to understand syntax, explore alternative implementations, or learn new programming paradigms. Students must not submit AI-generated code as their own and must be able to explain how it works.	☐
	A8 - Technical Guidance & Debugging Support AI tools can be used to explain algorithms, programming concepts, or debugging strategies. Students may also help interpret error messages or suggest possible fixes. However, students must write, test, and debug their own code independently and understand all solutions submitted.	☐
	A9 - Testing and Validation Support AI may assist in generating test cases, validating outputs, or suggesting edge cases for software testing. Students are responsible for designing comprehensive test plans and interpreting test results.	☐
	A10 - Data Analysis and Visualization Guidance AI tools can help suggest ways to analyse datasets or visualize results (e.g. recommending chart types or statistical methods). Students must perform the analysis themselves and understand the implications of the results.	☐
	A11 - Other uses not listed above Please specify:	☐

Partnered Work	**P1 - Generative AI tool usage has been used integrally for this assessment** Students can adopt approaches that are compliant with instructions in the assessment brief. Please Specify: - The analysis of the pcap file to verify the answer of founding - README.md - report drafting and improvement - generate suggested expression in Wireshark	☒

Please provide details of AI usage and which elements of the coursework this relates to:

improve the report, pcap analysis

I understand that the ownership and responsibility for the academic integrity of this submitted assessment falls with me, the student.	☒
I confirm that all details provide above are an accurate description of how AI was used for this assessment.	☒