

COMP 3010 CW1

1) Introduction

The report presents a comprehensive intrusion analysis of a social engineering attack observed in a captured PCAP file, in which a victim downloaded a malicious ZIP file disguised as a legitimate document. As a security analyst, the aim is to analyze the breach by interpreting intrusion detection alerts, identifying the threat, and explaining how the attacker compromised the system. The report is structured as follows: Section 2 explains the investigation methodology, Section 3 presents the findings with supporting packet evidence, and Section 4 gives recommendations for prevention.

2) Methodology

The investigation was carried out in Wireshark with the following steps taken to identify the infected system information, an indicator of the infection, and how the system got infected:

2a) Infected System Information

IP Address and MAC Address:

- The analysis began by isolating HTTP traffic in Wireshark to find suspicious downloads and identify the source IP.

No.	Time	Source	Destination	Protocol	Length	Info
1735	56.248525	10.9.23.102	85.187.128.24	HTTP	514	GET /incident-consequatur/documents.zip HTTP/1.1
2173	59.234150	85.187.128.24	10.9.23.102	HTTP	580	HTTP/1.1 200 OK
3822	153.653113	10.9.23.102	208.91.128.6	HTTP	281	POST /zLiisQRNZI9/OQsaDixzHTgtfjMcGypGenpldwF5eWV9f3k= HTTP/1.1 Continuation
3851	154.401688	208.91.128.6	10.9.23.102	HTTP	634	HTTP/1.1 200 OK (text/html)
3908	178.767210	10.9.23.102	208.91.128.6	HTTP	285	POST /zLiisQRNZI9/ASk5kx0SPR8lJje5eTg9GKn6fGFyZh1/YXp6eQ== HTTP/1.1 Continuation
3912	179.543303	208.91.128.6	10.9.23.102	HTTP	634	HTTP/1.1 200 OK (text/html)
3996	203.829455	10.9.23.102	208.91.128.6	HTTP	285	POST /zLiisQRNZI9/FxMKNg0nKzN/DA15DggB10N6fGFyZh1/YXp6eQ== HTTP/1.1 Continuation
4000	204.546015	208.91.128.6	10.9.23.102	HTTP	634	HTTP/1.1 200 OK (text/html)
4006	228.842458	10.9.23.102	208.91.128.6	HTTP	273	POST /zLiisQRNZI9/eDkKAAbInx9Rnp6ZXVheX1lfX95 HTTP/1.1 Continuation
4010	229.568579	208.91.128.6	10.9.23.102	HTTP	634	HTTP/1.1 200 OK (text/html)
4017	254.037243	10.9.23.102	208.91.128.6	HTTP	293	POST /zLiisQRNZI9/LjI+JSoqJQ4lBiwyAhR7KngvHgopKBhFfntkcmJ9eGR6fH0= HTTP/1.1 Continuation
4021	254.776306	208.91.128.6	10.9.23.102	HTTP	634	HTTP/1.1 200 OK (text/html)
4027	279.063986	10.9.23.102	208.91.128.6	HTTP	289	POST /zLiisQRNZI9/HDN9NScAAw8PKwEFMi0/JTI5PEZ6emV1YX15ZX1/eQ== HTTP/1.1 Continuation

- The first malicious HTTP GET request was isolated and inspected at packet level.

No.	Time	Source	Destination	Protocol	Length	Info
1735	56.248525	10.9.23.102	85.187.128.24	HTTP	514	GET /incident-consequatur/documents.zip HTTP/1.1

- Expansion of packet 1735's Ethernet II and IPv4 headers revealed the internal system's IP and MAC address. This establishes which host initiated the download and will be used to tie all subsequent activity back to that same machine.

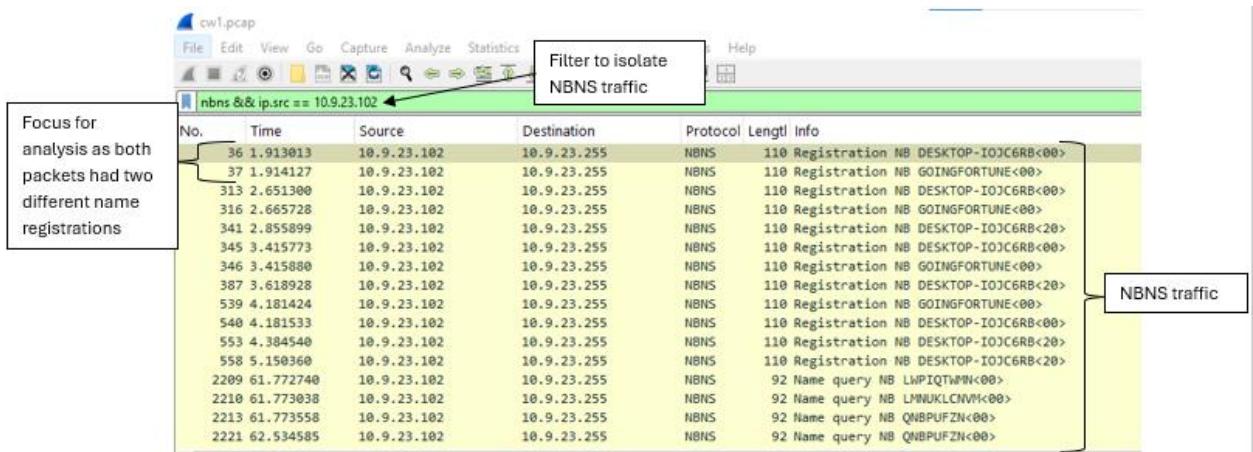
Infected system's IP address

Infected system's MAC address

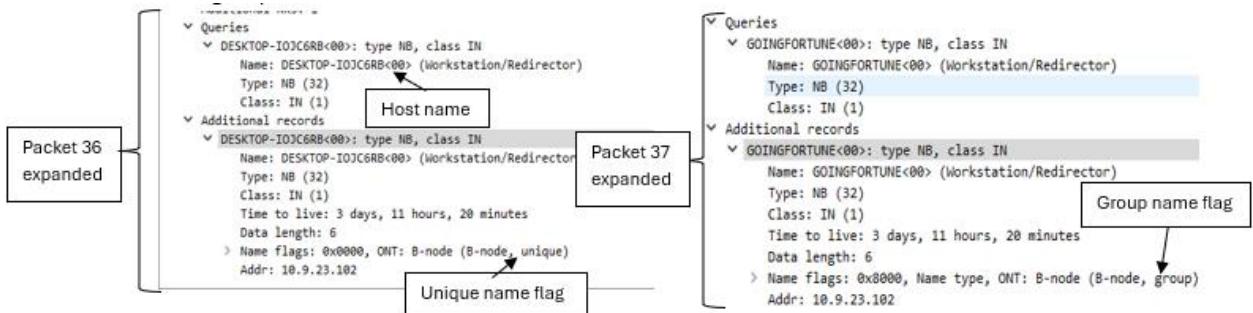
```
> Frame 1735: 514 bytes on wire (4112 bits), 514 bytes captured (4112 bits)
> Ethernet II, Src: HewlettPacka_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
> Internet Protocol Version 4, Src: 10.9.23.102, Dst: 85.187.128.24
▼ Transmission Control Protocol, Src Port: 62245, Dst Port: 80, Seq: 1, Ack: 1, Len: 460
```

Host Name:

- Next, NBNS traffic was filtered as NetBIOS Name Service packets contain name registration data that exposes a Windows system's hostname.

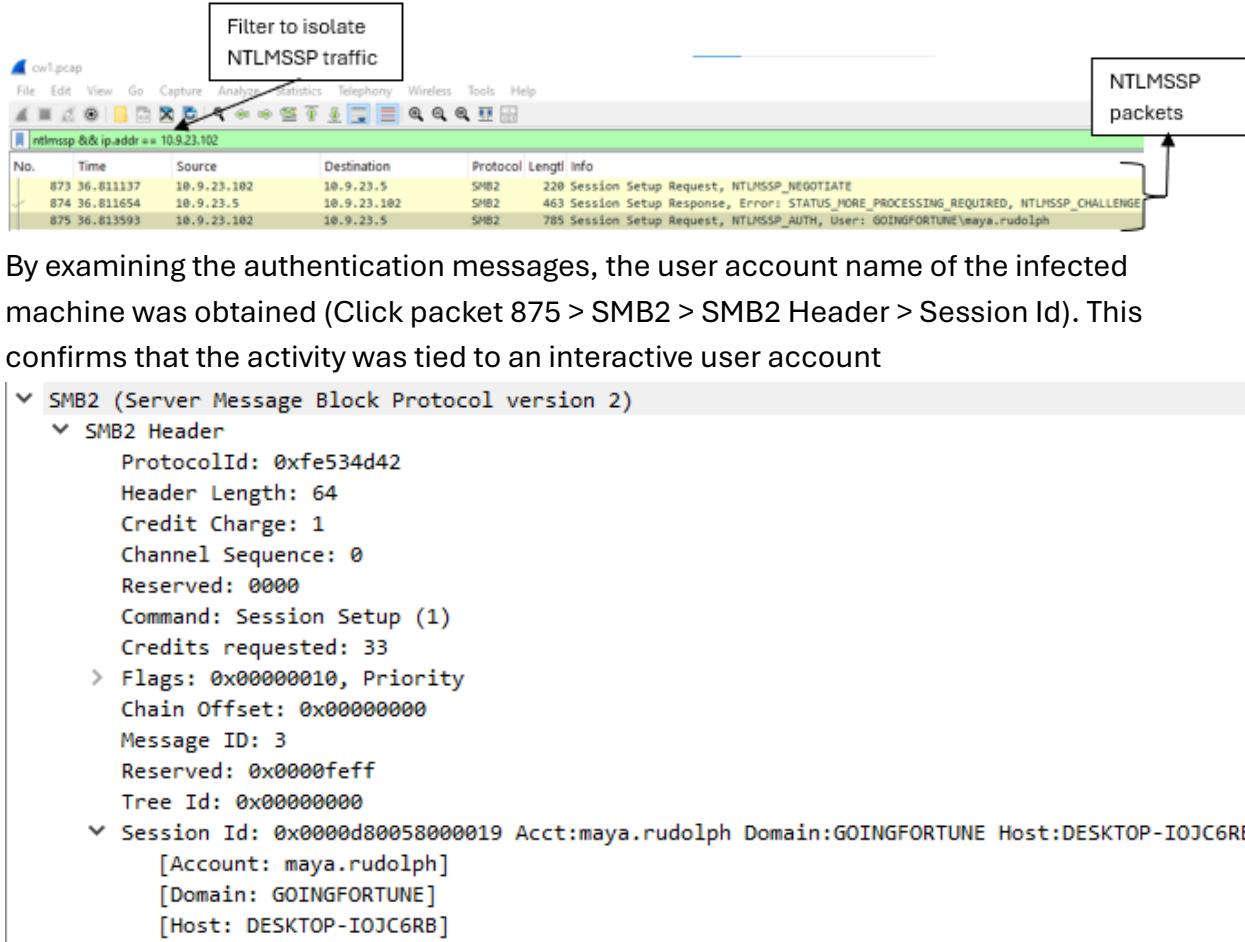


- By reviewing those packets, the workstation name of the host was recovered and distinguished from any broadcast group/domain names.



User Account Name:

- To identify the user account name, NTLMSSP traffic was inspected because it displays packets that often carry user authentication data such as usernames and domains (Blin n.d.).



2b) Indicator of Infection

- To find an lol, http traffic from the victim's IP was analyzed. This revealed multiple HTTP POST requests to an external IP address containing randomized data.

http && ip.src == 10.9.23.102

No.	Time	Source	Destination	Protocol	Length	Info
1735	56.248525	10.9.23.102	85.187.128.24	HTTP	514	GET /incidentund-consequatur/documents.zip HTTP/1.1
3822	153.653113	10.9.23.102	208.91.128.6	HTTP	281	POST /zLiisQRWZI9/QQsaDixHtgefjMcGyGenpldwF5ewV9f3k= HTTP/1.1 Continuation
3908	178.767210	10.9.23.102	208.91.128.6	HTTP	285	POST /zLiisQRWZI9/ASk5Kx0SPR81ljE5etfg9GKnGfGfyZH1/Vxp6eQ== HTTP/1.1 Continuation
3996	203.829455	10.9.23.102	208.91.128.6	HTTP	285	POST /zLiisQRWZI9/FXwKNg0nKzN/DA15DgBGIoNGfGfyZH1/Vxp6eQ== HTTP/1.1 Continuation
4006	228.842458	10.9.23.102	208.91.128.6	HTTP	273	POST /zLiisQRWZI9/eDkKA0bInx9Rp6ZXVheX1fx95 HTTP/1.1 Continuation
4017	254.037243	10.9.23.102	208.91.128.6	HTTP	293	POST /zLiisQRWZI9/LjI+J5eqJQ4lBiwyAhR7KngvHgopK8hFfnkcm9eGR6fH0= HTTP/1.1 Continuation
4027	279.06398	10.9.23.102	208.91.128.6	HTTP	289	POST /zLiisQRWZI9/HDN9NSCAAw8PKwEFM10/JTISPEZ6emV1YX152XL/eQ== HTTP/1.1 Continuation
4037	304.108570	10.9.23.102	208.91.128.6	HTTP	273	POST /zLiisQRWZI9/CaZDz1/MEJ9f2VzX58ZXt7fg= HTTP/1.1 Continuation
4046	329.217819	10.9.23.102	208.91.128.6	HTTP	285	POST /zLiisQRWZI9/DC1zfTsJDgA/AicrERgXChsERX57ZHjifXhken9 HTTP/1.1 Continuation
4099	354.299575	10.9.23.102	208.91.128.6	HTTP	293	POST /zLiisQRWZI9/EgwEcw0hNhk+BQkuH38nHQUTIy4GLwpFFntkcm9eGR6fH0= HTTP/1.1 Continuation
4099	379.469159	10.9.23.102	208.91.128.6	HTTP	269	POST /zLiisQRWZI9/G80tLyckJq3p8YXjkeX9henp HTTP/1.1 Continuation
4109	404.557049	10.9.23.102	208.91.128.6	HTTP	269	POST /zLiisQRWZI9/EgwSFkZ6emV1YX15ZX1/eQ== HTTP/1.1 Continuation
4118	429.544248	10.9.23.102	208.91.128.6	HTTP	285	POST /zLiisQRWZI9/CxvgNgIIIXleQkPHYCOUN6fGfyZH1/Vxp6eQ== HTTP/1.1 Continuation
4131	454.726221	10.9.23.102	208.91.128.6	HTTP	277	POST /zLiisQRWZI9/FskCegEtcg8Vkw95Qn1/ZXNlfnxle3t+ HTTP/1.1 Continuation
4140	479.894757	10.9.23.102	208.91.128.6	HTTP	265	POST /zLiisQRWZI9/ITIYRX57ZHjifXhken9 HTTP/1.1 Continuation
4150	505.009991	10.9.23.102	208.91.128.6	HTTP	265	POST /zLiisQRWZI9/OhpCfx91c2V+fGv7e34= HTTP/1.1 Continuation

- These POST requests were reviewed and I discovered they all occurred repeatedly in short intervals as seen in the arrival times of the first 3 packets with POST requests below.

```

▼ Frame 3822: 281 bytes on wire (2248 bits), 281 bytes captured (2248 bits)
  Encapsulation type: Ethernet (1)
  Arrival Time: Sep 24, 2021 17:46:16.395000000 W. Central Africa Standard Time
  UTC Arrival Time: Sep 24, 2021 16:46:16.395000000 UTC

▼ Frame 3908: 285 bytes on wire (2280 bits), 285 bytes captured (2280 bits)
  Encapsulation type: Ethernet (1)
  Arrival Time: Sep 24, 2021 17:46:41.509097000 W. Central Africa Standard Time
  UTC Arrival Time: Sep 24, 2021 16:46:41.509097000 UTC

▼ Frame 3996: 285 bytes on wire (2280 bits), 285 bytes captured (2280 bits)
  Encapsulation type: Ethernet (1)
  Arrival Time: Sep 24, 2021 17:47:06.571342000 W. Central Africa Standard Time
  UTC Arrival Time: Sep 24, 2021 16:47:06.571342000 UTC

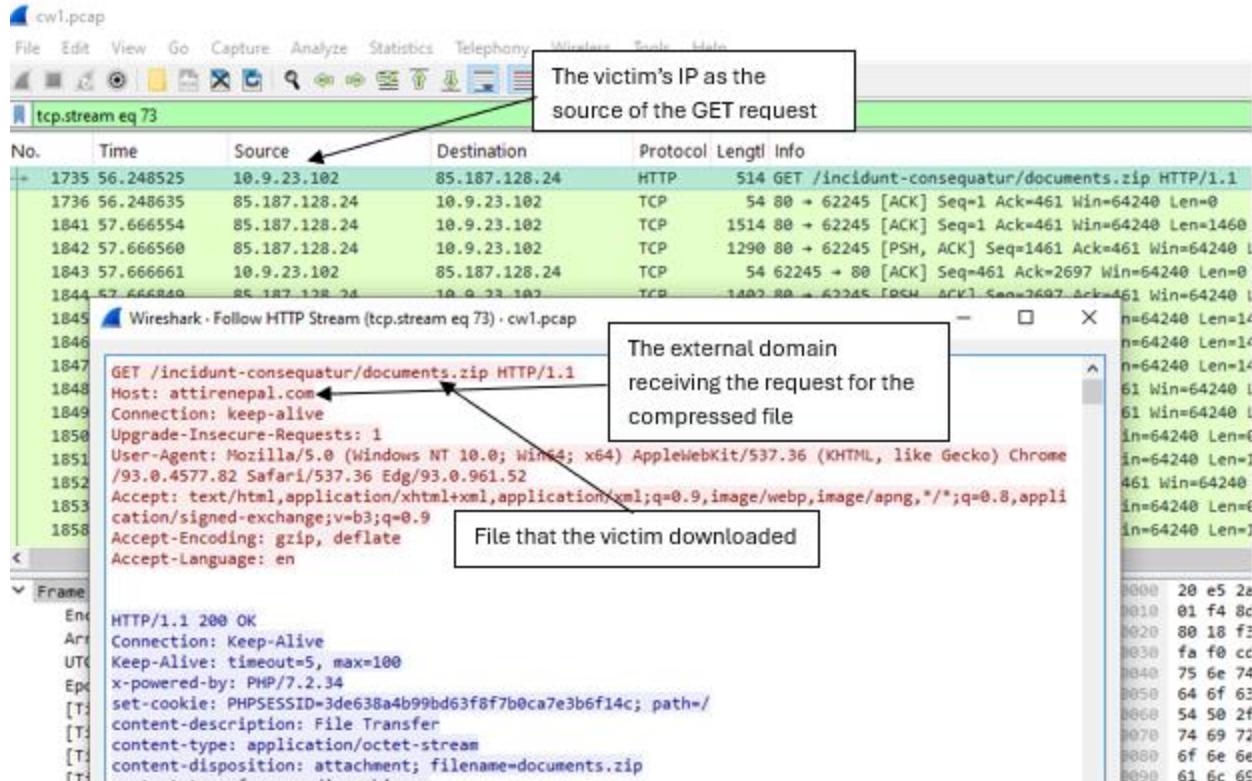
```

- This encoded communication and repetition pattern indicates malware command-and-control activity, confirming the system is infected.



2c) How the system got infected

- Following the HTTP stream of packet 1735, where the initial malicious HTTP connection occurred, the HTTP response headers confirmed that a ZIP archive was downloaded.



- The archive contained a macro-enabled Excel file. Opening this file triggered malicious code on the victim host and led to outbound command-and-control traffic to attacker infrastructure.

documents.zip (evaluation copy)

File Commands Tools Favorites Options Help

Add Extract To Test View Delete Find Wizard Info VirusScan Commer

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
chart-153007659...	251,392	197,935	Microsoft Excel 97...	9/24/2021 10:3...	F6EE61FC

3) Results

This section presents findings from the analysis and supporting evidence that explain the quiz answers:

3a) Initial Infection & File Transfer

The victim host made an HTTP GET request for documents.zip from attirenepal.com at 2021-09-24 16:44:38 UTC. A ZIP file containing chart-1530076591.xls was sent with the response. LiteSpeed was recognized with PHP/7.2.34 in the Server header, suggesting that a PHP-based shared server was probably compromised. The downloaded Excel file was opened by the user, and its macro started post-exploitation actions and became more persistent by establishing external connections.

```
Frame 1735: 514 bytes on wire (4112 bits), 514 bytes captured (4112 bits)
Encapsulation type: Ethernet (1)
Arrival Time: Sep 24, 2021 17:44:38.990412000 W. Central
UTC Arrival Time: Sep 24, 2021 16:44:38.990412000 UTC
Time of initial HTTP connection
```

Wireshark · Follow TCP Stream (tcp.stream eq 73) - cw1.pcap

```
GET /incident-consequatur/documents.zip HTTP/1.1
Host: attirenepal.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome /93.0.4577.82 Safari/537.36 Edg/93.0.961.52
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en

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; include
x-frame-options: SAMEORIGIN
x-content-type-options: nosniff
```

Malicious compressed file that the victim downloaded

Domain that hosted the malicious compressed file

The version number of the web server

The specific web server software running on the malicious IP address that served the compressed file.

After initial infection, inspection of subsequent DNS traffic within the 16:45:11 – 16:45:30 UTC range revealed three additional domains were involved in downloading malicious files to the victim host.

Filter to inspect traffic in the timeframe after the initial infection

First additional domain

Second additional domain

Third additional domain

No.	Time	Source	Destination	Protocol	Length	Info
2422	88.698693	10.9.23.102	10.9.23.5	DNS	77	Standard query 0x84b5 A finejewels.com.au
2423	88.698996	10.9.23.5	10.9.23.102	DNS	93	Standard query response 0x84b5 A finejewels.com.au A 148.72.192.206
2612	94.171723	10.9.23.102	10.9.23.5	DNS	90	Standard query 0xf3e8 A self.events.data.microsoft.com
2613	94.317927	10.9.23.5	10.9.23.102	DNS	212	Standard query response 0xf3e8 A self.events.data.microsoft.com CNAME
2878	97.520753	10.9.23.102	10.9.23.5	DNS	128	Standard query 0x68ce SRV _ldap._tcp.Default-First-Site-Name._sites.d
2878	97.521104	10.9.23.5	10.9.23.102	DNS	196	Standard query response 0x68ce SRV _ldap._tcp.Default-First-Site-Name
2983	97.745236	10.9.23.102	10.9.23.5	DNS	74	Standard query 0xa024 A thieltbiagt.com
2998	98.213955	10.9.23.5	10.9.23.102	DNS	90	Standard query response 0xa024 A thieltbiagt.com A 210.245.90.247
3224	102.715616	10.9.23.102	10.9.23.5	DNS	77	Standard query 0x65b4 A new.americold.com
3225	102.716106	10.9.23.5	10.9.23.102	DNS	93	Standard query response 0x65b4 A new.americold.com A 148.72.53.144

3b) Command & Control Activity

Post-execution, the host initiated encrypted sessions to 185.106.96.158 and 185.125.204.174, conversations analysis flagged these as top candidates by packet count/bytes. TLS certificate inspection of the first additional domain using its IP showed issuer GoDaddy as the CA.

C2 server IP addresses

Conversation Settings

- Name resolution
- Absolute start time
- Limit to display filter

Ethernet · 1 IPv4 · 5 IPv6 TCP · 106 UDP

Address A	Address B	Packets	Bytes	Stream ID	Total Packets	P
10.9.23.102	185.125.204.174	1	2 kB	49	2,923	
10.9.23.102	185.106.96.158	152	71 kB	57	1,973	
10.9.23.102	208.91.128.6	52	24 kB	46	244	
10.9.23.102	85.187.128.24	2	1 kB	34	225	
10.9.23.102	104.83.124.33	4	806 bytes	50	25	

Copy

Follow Stream...

Graph...

Host header/SNI evidence included ocsp.verisign.com, and DNS answers associated the C2 IPs with these domains: survmeter.live (185.106.96.158) and securitybusinpuff.com (185.125.204.174).

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns && dns.a == 185.106.96.158

No.	Time	Source	Destination	Protocol	Length	Info
6511	688.066449	10.9.23.5	10.9.23.102	DNS	90	Standard query response 0xe5da A survmeter.live A 185.106.96.158

```
> Frame 6511: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
> Ethernet II, Src: Dell_c2:09:6a (a4:1f:72:c2:09:6a), Dst: HewlettPacka_1c:47:ae (00:08:02:1c:47:ae)
> Internet Protocol Version 4, Src: 10.9.23.5, Dst: 10.9.23.102
> User Datagram Protocol, Src Port: 53, Dst Port: 58930
└ Domain Name System (response)
    Transaction ID: 0xe5da
    > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
    > Queries
    < Answers
        survmeter.live: type A, class IN, addr 185.106.96.158
            Name: survmeter.live
            Type: A (1) (Host Address)
            Class: IN (0x0001)
            Time to live: 1798 (29 minutes, 58 seconds)
            Data length: 4
            Address: 185.106.96.158
    [Request In: 6510]
    [Time: 0.013337000 seconds]
```

First C2 server's domain name

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns && dns.a == 185.125.204.174

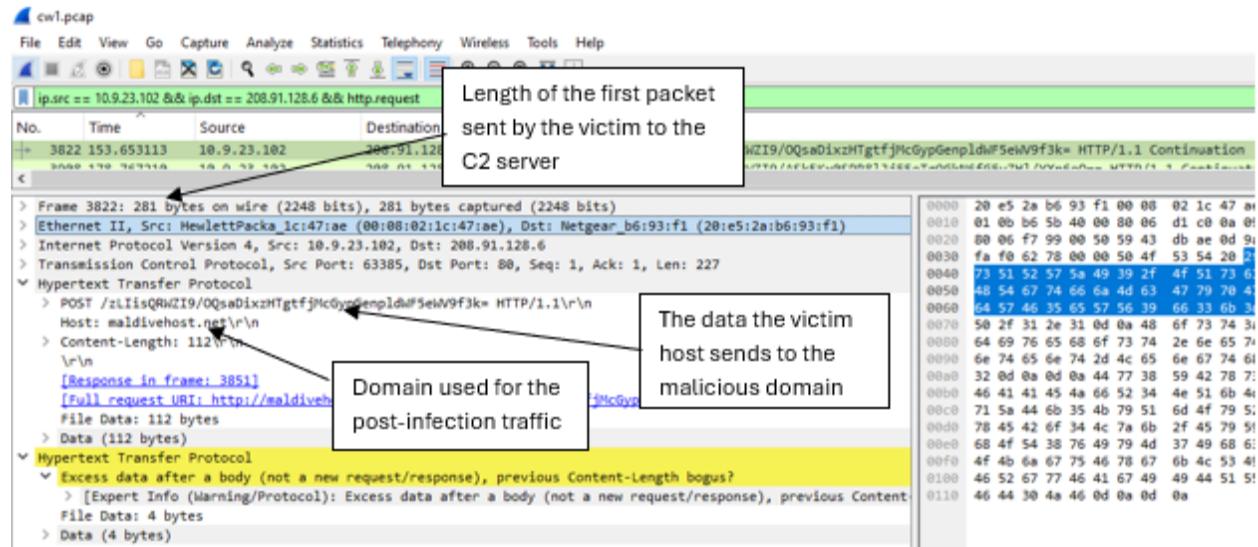
No.	Time	Source	Destination	Protocol	Length	Info
4494	585.263709	10.9.23.5	10.9.23.102	DNS	97	Stand

```
> Frame 4494: 97 bytes on wire (776 bits), 97 bytes captured (776 bits)
> Ethernet II, Src: Dell_c2:09:6a (a4:1f:72:c2:09:6a), Dst: HewlettPacka_1c:47:ae (00:08:02:1c:47:ae)
> Internet Protocol Version 4, Src: 10.9.23.5, Dst: 10.9.23.102
> User Datagram Protocol, Src Port: 53, Dst Port: 62353
└ Domain Name System (response)
    Transaction ID: 0xc042
    > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
    > Queries
    < Answers
        securitybusinpuff.com: type A, class IN, addr 185.125.204.174
            Name: securitybusinpuff.com
            Type: A (1) (Host Address)
            Class: IN (0x0001)
            Time to live: 300 (5 minutes)
            Data length: 4
            Address: 185.125.204.174
    [Request In: 4493]
    [Time: 0.169967000 seconds]
```

Second C2 server's domain name

HTTP POST requests exhibited short, periodic payloads with total packet length around 281 bytes, consistent with Cobalt Strike beaconing (Rahman 2021). Lack of standard HTML

body supports the interpretation of automated beacon traffic rather than normal user browsing.



3c) Final Exfiltration

At 2021-09-24 17:00:04 UTC, the infected host queried api.ipify.org. This service is commonly used by malware to discover the victim's external/public IP address before it reports back to its operator (Ipify.org, 2014).

After this IP check, the host initiated SMTP traffic. The first SMTP transaction in the pcap shows MAIL FROM:<farshin@mailfa.com>. In a later SMTP session from the same host, the client performed AUTH LOGIN and supplied Base64-encoded credentials. Decoding those values reveals the password 13691369 for the user ho3ein.sharifi@mailfa.com. The server responded with 235 authenticated., and the client then attempted to send mail using MAIL FROM:<ho3ein.sharifi@mailfa.com>.

This demonstrates that the host is attempting to authenticate to an external mail service using exposed credentials and then send outbound email.

No.	Time	Source	Destination	Protocol	Length	Info
28506	1143.222457	10.9.23.102	185.4.29.135	SMTP	70	C: EHLO localhost
28521	1143.450341	185.4.29.135	10.9.23.102	SMTP	110	S: 250-mail.mailfa.com SIZE 30000000 AUTH LOGIN
28524	1143.456304	185.4.29.135	10.9.23.102	SMTP	74	S: 235 authenticated.
28576	1144.036130	10.9.23.102	185.4.29.135	SMTP	86	C: MAIL FROM:<farshin@mailfa.com>

Wireshark - Follow TCP Stream (tcp.stream eq 387) · cw1.pcap

```

220 mail.mailfa.com
EHLO localhost
250-mail.mailfa.com
250-SIZE 30000000
250 AUTH LOGIN
AUTH LOGIN
334 VXNlc3dvcnQ6
aG8zZWluLnNoYXJpZmlAbWFpbGZhLmNvbQ==
334 UGFzc3dvcnQ6
MTM2OTEzNjk= → ho3ein.sharifi's password
235 authenticated.
MAIL FROM:<ho3ein.sharifi@mailfa.com> → Attempt to send mail
550 Your SMTP Service is disable please check by your mailservice provider.

```

4) Conclusion

The captured traffic shows a successful compromise of an internal Windows host, followed by command-and-control communication and credentialled outbound activity. The attacker didn't just breach the victim's system but achieved post-exploitation control and attempted to move data out of the environment.

To reduce the impact of similar incidents, the organization should:

- Use network-based intrusion detection systems (NIDS) to detect odd patterns such as anomalous outbound traffic, executable macro-enabled attachments, and enable email gateway filtering in order to stop similar instances.
- Train its users on the dangers of opening unexpected attachments.
- Use Intrusion prevention systems (IPS) to actively stop malicious sessions or block traffic before it reaches important assets.
- Use EDR, XDR, and SIEM solutions to enhance visibility across hosts, networks, and cloud environments, supporting the integration of threat intelligence and automated response capabilities which is useful for the early detection of C2 activity.

Open challenges remain because most of the post infection traffic is encrypted or encoded and blends in with normal HTTPS and SMTP. Attackers rely on this more to evade traditional defense systems. Future work should integrate real-time threat intelligence feeds and sandboxing environments to improve early detection and response to similar threats.

5) References

- Blin, K. (n.d.) Implementing the NTLM Secure Service Provider for Wine.
- Rahman, A. (2021) ‘Defining Cobalt Strike Components So You Can BEA-CONFIDENT in Your Analysis.’ *Mandiant*.
- Ipify.org. (2014). *ipify - A Simple Public IP Address API*. [online] Available at: <https://www.ipify.org/>.

6) Github

<https://github.com/ukashley/COMP-3010-Security-Operations-Incident-Management->

7) Appendix

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.	<input type="checkbox"/>
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.	<input type="checkbox"/>
	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.	<input type="checkbox"/>
	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.	<input type="checkbox"/>
	A4 – Research Assistance	<input type="checkbox"/>

	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.	<input type="checkbox"/>
	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.	<input type="checkbox"/>
	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.	<input type="checkbox"/>
	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.	<input type="checkbox"/>
	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.	<input type="checkbox"/>
	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.	<input type="checkbox"/>
	A11 - Other uses not listed above Please specify: I used AI for critical feedback and grading simulation.	<input type="checkbox"/>

Partnered Work	<p>P1 - Generative AI tool usage has been used integrally for this assessment</p> <p>Students can adopt approaches that are compliant with instructions in the assessment brief.</p> <p>Please Specify:</p> <p>I used generative AI to assist with a small part of the investigative analysis, report structuring and summarization, research assistance and technical language improvement. It helped me critically assess my methodology, clarify grammar, and simulate grading feedback to improve the quality of my submission. All documentation, explanations, analysis of results and screenshots were performed independently as per assignment instructions.</p>	<input checked="" type="checkbox"/>
-----------------------	--	-------------------------------------

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

Generative AI was used to support the development of this coursework. It assisted with structuring the report, improving technical phrasing, and clarifying grammar. Specific elements where AI was used include the Methodology and Results sections, where it helped articulate packet analysis findings and streamline explanations.

I understand that the ownership and responsibility for the academic integrity of this submitted assessment falls with me, the student.	<input checked="" type="checkbox"/> 
I confirm that all details provide above are an accurate description of how AI was used for this assessment.	<input checked="" type="checkbox"/> 