# Plantilla de respuestas
# Ejercicio ciberinteligencia

| | |
|---|---|
| Módulo | CIBERINTELIGENCIA |
| Nombre y apellidos | David Fernández Alejo |
| Fecha entrega | 07/10/2024 |

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:**

Tras analizar los ficheros adjuntos en el caso número 1, el ataque realizado es un phishing. Un phishing se define como el fraude en el que se realiza una suplantación de un sitio web o de una aplicación con el objetivo de obtener, de forma ilegítima, cualquier tipo de información sensible o confidencial de un usuario.

La estructura general de un phising, cuenta con varios puntos comunes, entre los que podemos destacar la copia de la estructura de la página web a la que se quiere suplantar. En este caso, se adjunta el index.code de la página web a la que redirige el link indicado en el cuerpo del correo. Dicho índice tiene como referencia la página de “login” de Outlook, la cual no es la original.
Además, como segundo elemento característico de un phising, se incluye un fichero php, el cual tras introducir las credenciales en dicha web, envía mediante las credenciales a un correo electrónico, indicado en la variable “recipient” de dicho script.
Además tras realizar el envió de credenciales al correo electrónico indicado en la variable “recipient”, en la etiqueta “header” del script en PHP, se incluye la información sobre el paso que se hará tras el envío, es decir, hacía dónde se redireccionará la información del usuario tras el envío del formulario, en este caso al sitio web legítimo suplantado.

También se podría decir que al ataque incluye un ataque de tipo cyberstquatting ya que el correo que se envía a **m.walker.franch@fictiy.de** proviene de verify@microfoft.com , el cual intenta simula un dominio legítimo : verify@microsoft.com .

**Pregunta 2 (0,5 puntos):**

**En el caso 1, ¿qué correo es el origen del ataque?**

**Respuesta:**

El correo origen del ataque es verify@microfoft.com ,recibido el día 23 de noviembre de 2017 a las 9:40 , 20 minutos antes del envio del correo de **m.walker.franch@fictic y.de** al resto de compañeros. Dicho correo se hace pasar por verify@microsoft.com , para que el usuario crea que está haciendo loggin contra la página oficial, sin embargo, está siendo objeto de un phishing como se indica en la pregunta anterior. Además, en el registro de acceso de la cuenta, se puede ver que a las 9:45, 5 minutos después del correo de verify@microfoft.com a **m.walker.franch@fictic y.de** se produce un acceso a dicha cuenta de correo desde una ip desde la cual nunca se había accedido a dicha cuenta de correo. Previamente todos los accesos a la cuenta **m.walker.franch@fictic y.de** habían sido dentro de la misma red 172.16.10.XX , sin embargo el acceso de las 9:45 es desde la ip 77.72.83.26 y ha sido aceptado el acceso, con lo cual habían obtenido previamente las credenciales del usuario.

**Pregunta 3 (1 punto):**

**En el caso 1, ¿dónde se envían los datos comprometidos?**

**Respuesta:**

Teniendo en cuenta que dentro de la página web tenemos un formulario, se puede comprobar que al rellenar y mandar los datos se ejecuta el script “post.php”. Dicha acción es un POST de los datos introducidos previamente por el usuario.

En ese caso los datos comprometidos se envían a un correo electrónico indicado en el script php.

En el script se indican los distintos datos que se obtienen del usuario que intenta hacer log-in en el sitio web, en este caso, se obtiene la dirección ip del usuario, así como las credenciales introducidas previamente por el usuario. Además, se indican el destinatario y el asunto del correo, mediante las etiquetas “recipient” y “subjetct”.

A su vez, mediante el método “mail” envía un correo electrónico a la dirección especificada anteriormente, indicando el correo destino, el asunto, el mensaje, el cual incluye la ip del usuario, el usuario y la contraseña.

Después de enviar al correo electrónico la información previamente obtenida, el usuario el redirigido a la página principal de Hotmail.

Por lo tanto, se puede concluir que se envía por mail los datos guardaos en la variable “mensaje” a la dirección indicada en el “recipient”, es decir al correo 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@fictity.de"? ¿Desde dónde es posible que haya sido el ataque?**

**Respuesta:**

Teniendo en cuenta que estamos ante un caso de phishing, se revisará la bandeja de entrada de m.wlaker.franch@fictity.de para analizar el tráfico de correos entrante.

Teniendo en cuenta que los correos bloqueados, no han llegado a su destino ya que han sido bloqueados por el sistema de seguridad de la empresa, nos centraremos en los que han sido aceptados.

Se deben tener en cuenta correos que hayan sido enviados a la cuenta de m.walker.franch@fictity.de antes de las 10 del día 23 de noviembre y con estado "approved", ya que a esa hora se ha enviado un correo sospechoso desde dicha cuenta al resto de cuentas de la organización.

Los correos electrónicos a tener en cuenta son los siguientes:

15574,20171120.11:10:14,j.roman.stelso@fictity.co.uk,m.walker.franch@fictity.de,Private sector,50KB,n,approved

15576,20171120.175915,m.wils.keicher@fictity.de,m.walker.franch@fictity.de,freund,85KB,n,approved

15577,20171121.13:10:14,esitsecurity@fictity.de,m.walker.franch@fictity.de,neues Konto,125KB,n,approved

15578,20171121.17:15:08,j.roman.stelso@fictity.co.uk,m.walker.franch@fictity.de,RE: Private sector,55KB,n,approved

15580,20171122.104554,esitsecurity@fictity.de,m.walker.franch@fictity.de,Aktualisierungen,33KB,n,approved

15581,20171122.182514,s.mick.resce@fictity.de,m.walker.franch@fictity.de,diese Aufgabe,33KB,n,approved

15582,20171123.063056,s.mick.resce@fictity.de,m.walker.franch@fictity.de,RE: diese Aufgabe,360KB,y,approved

15583,20171123.094000,verify@microfoft.com,m.walker.franch@fictity.de,FW: Validate Email Account,42KB,n,approved

15584,20171123.095121,m.will.smith@fictity.us,m.walker.franch@fictity.de,RE:FW: Validate Email Account,50KB,n,approved

15585,20171123.095621,l.stephan.martin@fictity.co.uk,m.walker.franch@fictity.de,RE:FW: Validate Email Account,121KB,n,approved

15586,20171123.095855,l.martin.fierre@fictity.es,m.walker.franch@fictity.de,RE:FW: Validate Email Account,85KB,n,approved

Dentro de los correos recibidos, todos provienen de cuentas corporativas, pertenecientes el dominio de la empresa, "ficticity", sin embargo el correo de las 09:40 cuyo remitente es verify@microfoft.com , no pertenece al dominio de la empresa. Teniendo esto en cuenta, además de que dicho remitente tiene un dominio muy similar al de Microsoft, podríamos sospechar que dicho correo ha sido el desencadenante del phishing.

Tras analizar el código del sitio web, se puede comprobar que es una página de inicio que replica a la de microsoft, y que como hemos indicado anteriormente, los datos introducidos por el usuario son redirigidos a un email, donde se adjunta toda la información del usuario.

Al acceder a dicha web e introducir los datos de la cuenta de m.walker.franch@ficticity.de , la cuenta de dicho usuario fue comprometida.

A su vez, analizando los registros de acceso se puede observar cómo los accesos a la cuenta de correo electrónico se han realizado en todas las ocasiones dentro de la red de la empresa, 172.16.10.XX, salvo un acceso que re ha realizado a las 9:45, cinco minutos después del correo de phshing , desde la dirección ip 77.72.83.26.

Por lo tanto, se puede concluir que el correo de las 10:00 a. m. se envía desde la cuenta m.walker.franch@ficticy.de porque esta cuenta fue comprometida al interactuar con el enlace malicioso del correo previo enviado desde verify@microfoft.com. Se obtuvieron las credenciales de dicho correo electrónico y se envió un correo con el asunto *FW: Validate Email Account.* al resto de empleados de la organización.

Posiblemente dicho correo haya sido enviado desde la ip 77.72.83.26.

**Pregunta 5 (1 punto):**

**En el caso 1, ¿qué otras cuentas han podido ser comprometidas?**

**Respuesta:**

Para poder analizar que cuentas han sido comprometidas, analizaremos los emails de m.walker.franch@ficticy.de, se revisarán los correos cuyo asunto del correo sea "FW: Validate Email Account".

Teniendo en cuenta lo mencionado anteriormente estos son los correos con el asunto indicado:

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

Tras analizar los emails se puede indicar cuales son las cuentas que han sido a su vez comprometidas, ya que siguen el mismo procedimiento que m.walker, reenvían un correo de confirmación al resto de trabajadores de la empresa para poder obtener sus credenciales.

Las cuentas que han podido ser comprometidas son las siguientes:

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

**Pregunta 6 (0,5 puntos):**

**En el caso 2, indicar el tipo de ataque realizado.**

**Respuesta:**

Primero se analizaran los distintos logs de acceso y correos de las cuentas indicadas.
En este caso, se indica que tanto j.philips.todobene@ficticy.es. , como s.labial.guest@ficticy.es y m.protector.fresco@ficticy.es. tienen perfiles en redes sociales. Teniendo en cuenta que tanto Sofía labial como Juan Philips pertenecen al departamento de pagos y transferencias, el análisis de dicho caso se centrará en ellos. Tras ver los distintos accesos, así como los correos recibidos y los logs del MTA, se puede ver que se han realizado varios intentos de creación de cuentas nuevas.

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

Teniendo en cuenta estos intentos de cuenta con dominios parecidos al correo de ju.philips.stodobene@ficticy.es se puede ver que han intentado averiguar el dominio de dicha cuenta, seguramente teniendo en cuenta los distintos perfiles que tenía el usuario en Facebook, LinkedIn e InfoJobs. Utilizando dicha información recopilada, los atacantes podrían haber enviado correos de phishing personalizados, haciendo creer al usuario que el correo es legítimo. Una vez los atacantes han podido obtener acceso a dicha cuenta, se ha podido hacer un pago a una cuenta inusual.

Por lo tanto se podría concluir que dicho ataque involucró múltiples fases, primero con la ingeniería social, intentando averiguar la cuenta del usuario sabiendo su perfil en redes sociales, posteriormente, se habría realizado un phishing para obtener las credenciales de dicho usuario, para posteriormente desviar pagos mediante dicha cuenta.

**Pregunta 7 (0,5 puntos):**

**En el caso 2, ¿qué correo es el origen del ataque?**

**Respuesta:**

Para analizar los mails entrantes de María Protector Fresco, Juan Philips Todobene y Sofía Labial Guest se tendrá en cuenta en primer lugar que tanto Juan Philips como Sofía Labial pertenecen al departamento de transferencias, sabiendo que se ha realizado una transferencia a una cuenta inusual, se buscarán correos sospechosos especialmente en el mail de ambos trabajadores.

En primer lugar, se tendrán en cuenta los correos que hayan sido anteriores a las 13:00 del 23 de noviembre, sabiendo que es a la hora a la que se ha realizado la transferencia inusual, además se tendrán en cuentas los mails que tengan como asunto cambios de contraseña o creación de nuevas cuentas al saber objetivos comunes en un phishing.

A continuación se indican los correos sospechosos de Sofía Labial:
11346,20171122.085621,b.bastian.garcia@ficticy.es,s.labial.guest@ficticy.es,Nuevas cuentas,125KB,n,approved

11348,20171122.163412,s.ramiro.ochoya@ficticy.es,s.labial.guest@ficticy.es,Cuentas,35KB,n,approved

11349,20171122.165521,s.ramiro.ochoya@ficticy.es,s.labial.guest@ficticy.es,Cambio de cuenta,360KB,y,approved

A continuación se indican los correos sospechosos de Juan Philips:
27657,20171122.085621,b.bastian.garcia@ficticy.es,j.philips.todobene@ficticy.es,Nuevas cuentas,125KB,n,approved
27662,20171122.165521,s.ramiro.ochoya@ficticy.es,j.philips.todobene@ficticy.es,Cambio de cuenta,360KB,y,approved
27664,20171122.174544,s.ramiro.ochoya@ficticy.es,j.philips.todobene@ficticy.es,Nuevo cambio de cuenta,50KB,n,approved
27665,20171122.180035,transfer@mailer.com,j.philips.todobene@ficticy.es,New account,121KB,n,approved
27670,20171123.104543,transfer@mailer.com,j.philips.todobene@ficticy.es,RE: New account,44KB,n,approved

Además, se ha proporcionado los logs de acceso de ambas cuentas, se puede observar que las ips de ambos usuarios cambian diariamente, esto podría ser normal ya que los trabajadores de dicha empresa trabajan sobre una VPN corporativa.
Teniendo en cuenta los logs de acceso y los distintos correos destacados anteriormente, se pueden acotar aun más los correos sospechosos.

En primer lugar, de los correos sospechosos de Sofía Labial, el mail con id 11348 podría ser menos sospechoso ya que el tamaño del adjunto es bastante mas pequeño en comparación con los otros dos, lo que sugiere que es menos probable que se adjunten ficheros maliciosos. Teniendo en cuenta lo mismo para los correos de Juan Philips, se pueden descartar los correos con id 27664 y 27670.

Teniendo en cuenta que hemos descartado algunos correos de ambas cuentas los correos sospechosos de dichos usuarios serían los siguientes:

11346,20171122.085621,b.bastian.garcia@ficticy.es,s.labial.guest@ficticy.es,Nuevas cuentas,125KB,n,approved

11349,20171122.165521,s.ramiro.ochoya@ficticy.es,s.labial.guest@ficticy.es,Cambio de cuenta,360KB,y,approved

27657,20171122.085621,b.bastian.garcia@ficticy.es,j.philips.todobene@ficticy.es,Nuevas cuentas,125KB,n,approved
27662,20171122.165521,s.ramiro.ochoya@ficticy.es,j.philips.todobene@ficticy.es,Cambio de cuenta,360KB,y,approved
27665,20171122.180035,transfer@mailer.com,j.philips.todobene@ficticy.es,New account,121KB,n,approved

Teniendo en cuenta que estos son los mails que podemos considerar más sospechosos, el correo 27665 es el correo más llamativo ya que tiene una dirección de correo sospechoso, la cual, a diferencia del resto de mails, es externo a la organización.

Después de analizar los distintos mails, como se ha indicado anteriormente, el correo origen del ataque es el 27665,20171122.180035,transfer@mailer.com,j.philips.todobene@ficticy.es,New account,approved donde se envía un correo desde el transfer@mailer.com a 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:**

Se ha utilizado un ataque de ingeniería social dónde ha averiguado el usuario de Juan Philips, probando distintas combinaciones, seguramente los nombres de los perfiles de dicho usuario en las distintas redes sociales.
Como se puede ver en los logs del MTA, se han mandado correos desde tranfer@mailer.com a dominios similares al correo de j.philips.todobene@ficticy.es.

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

**Pregunta 9 (1 punto):**

**En el caso 2, ¿cómo ha sido la consecución temporal de los hechos?**

**Respuesta:**

Teniendo en cuenta estos intentos de cuenta con dominios parecidos al correo de ju.philips.stodobene@ficticy.es se puede ver que han intentado averiguar el dominio de dicha cuenta, seguramente teniendo en cuenta los distintos perfiles que tenía el usuario en Facebook, LinkedIn e InfoJobs. Utilizando dicha información recopilada, los atacantes podrían haber enviado correos de phishing personalizados, haciendo creer al usuario que el correo es legítimo. Una vez los atacantes han podido obtener acceso a dicha cuenta, se ha podido hacer un pago a una cuenta inusual.

Por lo tanto se podría concluir que dicho ataque involucró múltiples fases, primero con la ingeniería social, intentando averiguar la cuenta del usuario sabiendo su perfil en redes sociales, posteriormente, se habría realizado un phishing para obtener las credenciales de dicho usuario, para posteriormente desviar pagos mediante dicha cuenta.

**Pregunta 10 (0,5 puntos):**

**En el caso 3, indicar el tipo de ataque realizado.**

**Respuesta:**

Después de realizar un análisis de los registros proporcionados y de examinar los registros del servidor EPO, se han observado una serie de eventos que coinciden con el patrón típico de un ataque de randsonware WannaCry.

Los registros del servidor EPO, revelan que se han tomado una seria de medidas proactivas para abordar la amenzada detectada. Como indican sus registros, se han identificado y eliminado un virus que estaba presente en varios archivos del sistema. Dicho mensaje es el siguiente: "# C:\WINDOWS\mssecsvc.exe # Ransom-WannaCry!7339A0EFC768 # trojan # deleted # 1 # VIRUS_DETECTED_REMOVED # VIRUSCAN8800 # VirusScan Enterprise #".

La presencia de la extensión ".wncry" en los archivos cifrados de varios equipos confirma la naturaleza del ataque. Este comportamiento es coherente con el comportamiento del ransomware WannaCry, que cifra archivos en los sistemas comprometidos y les añade una extensión específica como parte de su estrategia de extorsión.

En conclusión, todos estos indicadores apuntan de manera concluyente hacia un ataque de ransomware WannaCry.

**Pregunta 11 (0,5 puntos):**

**En el caso 3, indicar la vulnerabilidad explotada en los sistemas.**

**Respuesta:**

Teniendo en cuenta que las reglas del firewall que se adjuntan en las capturas de pantalla permiten las conexiones al puerto 445, a su vez, sabiendo que dicho puerto es usado por el SMBv1 (protocolo de red que permite compartir archivos, carpetas e impresoras en la red local entre distintos sistemas operativos) y además en los sistemas de alertas se indica que se ha detectado un randomware Wannacry , se puede concluir que la vulnerabilidad explotada en los sistemas es el EternalBlue (CVE-2017-0144).

Utilizando la vulnerabilidad SMBv1, EternalBlue permite que un atacante ejecute código malicioso en el sistema remoto sin necesidad de autenticación.

**Pregunta 12 (1 punto):**

**En el caso 3, ¿cómo se ha propagado el *malware* a través de la red interna?**

**Respuesta:**

Sabiendo como se propaga el malware WannaCry y después de analizar las pruebas que se han adjuntado, se podría decir que tras infectar la primera máquina mediante un correo de phishing en este caso, desde la primera máquina infectada, se realiza un escáner de puertos de la red, para determinar cuáles son las máquinas que pertenecen a la red interna y que además tienen abierto el puerto 445.

Cuando dicho escáner, detecta dicho puerto abierto en la máquina, explota la vulnerabilidad SMBv1, carga y ejecuta el payload en dicha máquina. Dicha carga como se indica en el caso, incluye el cifrado de los archivos, la propagación a otras máquinas de la red así como otras actividades como la instalación de un randsonware.

**Pregunta 13 (1 punto):**

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

**Respuesta:**

Para evitar el ataque se podría haber tomado las siguientes medidas:

**Aplicación del Parche MS17-010**

Uno de los pasos más cruciales para evitar el ataque WannaCry habría sido la aplicación del parche MS17-010 en todos los dispositivos Windows. Este parche corrige una vulnerabilidad crítica en el protocolo SMBv1 que permite la ejecución remota de código arbitrario. Al aplicar este parche, se habría impedido que los atacantes no autenticados enviaran mensajes SMBv1 maliciosos que explotaran esta vulnerabilidad, evitando así la capacidad de los atacantes para ejecutar código en los sistemas afectados.

**Desactivación del Protocolo SMBv1**

Otra medida importante habría sido desactivar el protocolo SMBv1, que es obsoleto y menos seguro. El uso de SMBv1 deja a los sistemas vulnerables a varias formas de explotación. En su lugar, se debería haber implementado SMBv2 o SMBv3, que ofrecen mejoras significativas en seguridad. Estas versiones más recientes del protocolo SMB incluyen características de seguridad avanzadas que protegen contra varios tipos de ataques.

**Uso de un Antivirus Actualizado**

Como se puede observar en el enunciado del caso práctico, el antivirus detecta la presencia del malware y parece que lo elimina, sin embargo, los archivos terminan siendo cifrados. Es por ello que la utilización de un antivirus actualizado es fundamental. Un buen antivirus no solo detecta la presencia de malware, sino que también puede prevenir el cifrado de archivos y la propagación del malware a otros dispositivos en la red. Asegurarse de que el software antivirus esté siempre actualizado garantiza que el sistema esté protegido contra las últimas amenazas conocidas.

**Segmentación de la Red**

La segmentación de la red es una estrategia efectiva para limitar la propagación de malware. Al dividir la red en segmentos más pequeños y aislados, se puede contener un ataque en una parte específica de la red, evitando que se extienda a todos los dispositivos. Esto se puede lograr mediante el uso de VLANs (redes de área local virtuales) y otras técnicas de segmentación que restringen el movimiento lateral del malware.

**Uso de Sandboxes para Clientes de Correo**

Otra medida útil es ejecutar el cliente de correo electrónico en una sandbox. Una sandbox es un entorno aislado del sistema operativo principal que permite ejecutar, probar y analizar programas de manera segura. Si el cliente de correo estuviera en una sandbox, cualquier intento de ejecución de malware a través de un correo electrónico malicioso sería contenido dentro de este entorno, protegiendo el resto del sistema. Además, esto garantiza que incluso si el malware se ejecuta, no podrá afectar otros archivos personales ni propagarse a otros dispositivos