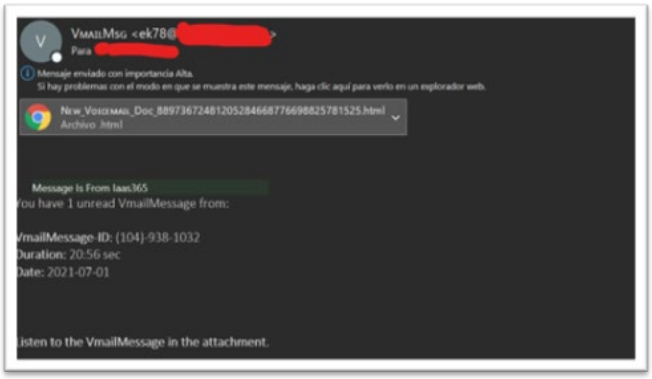
Artículo:

¿Está tu organización preparada ante un ataque de Phishing? Análisis y prevención frente a correos maliciosos



Por: Verónica Berenguer y Juan Pérez de Algaba - Técnicos de Ciberseguridad, CyberSOC365 Analytics.

Los ciberataques han aumentado exponencialmente en la última década, siendo el phishing uno de los más comunes. Este tipo de ataques suplantan una entidad (personas, organizaciones, etc.…) para obtener datos como contraseñas, información bancaria o personal. El objetivo de estas acciones criminales es usarlas para su propio beneficio, venderlo a otra entidad o publicarlas en la Deep Web para obtener rédito económico.

Es interesante mencionar que hay muchos tipos distintos de phishing como el vishing (a través de llamadas de teléfono), smishing (SMS) y el típico correo electrónico, entre otros.

Muchas veces, estos correos de Phishing vienen con archivos adjuntos que les ayudan a realizar su ataque. En este artículo, vamos a analizar uno de estos archivos y vamos a ofrecer posibles remediaciones para estos ataques.

En este caso, vamos a analizar un posible ataque en el que, aunque el correo recibido por el usuario no estuviese muy elaborado, el archivo adjunto que incluía sí lo estaba. Este hecho es bastante común ya que los ciberdelincuentes siempre buscan atacar al eslabón más débil de la cadena, en este caso los empleados menos concienciados con la ciberseguridad.

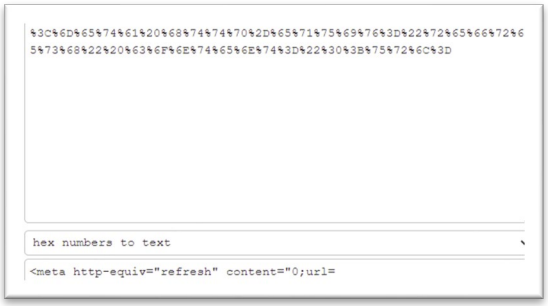
Obviamente, un usuario hábil sabrá detectar al momento que este correo se trata de Phishing, pero habrá muchos otros que no. Podemos ver que el correo tiene adjunto un archivo .html. Un tanto extraño, ¿verdad?

Si echamos un ojo a este documento, veremos lo siguiente:

Como podemos ver, este archivo no tiene un formato muy habitual para ser una página web. En el mismo sólo podemos ver cómo se carga un script de Javascript en el

que se ejecuta una función llamada “unescape()”. El argumento que se le pasa a esta función es bastante extraño y está claro que ha sido codificado (probablemente en hexadecimal) para tratar de ocultar algún tipo de comportamiento anómalo.

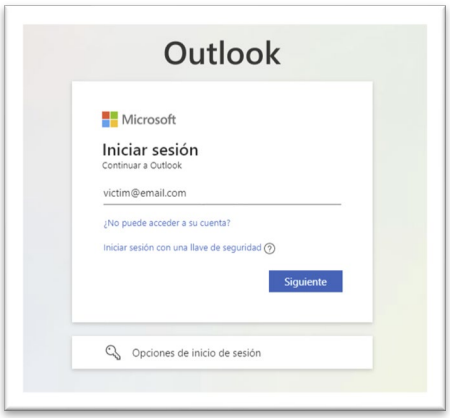
Si tratamos de convertir este texto hexadecimal a un formato legible usando algunos recursos online, podemos ver lo siguiente:



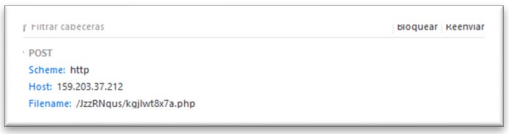
Sabiendo esto, ya podemos encontrar el código real del archivo:

Viendo el código de la web, podemos ver que se va a cargar una página web con un parámetro llamado “referrer”. Este parámetro parece un poco extraño, lo bueno es que está codificado en base-64:

Si lo decodificamos, podemos ver el correo de la persona que ha recibido el mail. Qué raro. Una vez hecho el análisis estático, podemos proceder a abrir la página web para realizar un análisis dinámico. Si abrimos la web, podemos ver un clon exacto de la página web del login de Outlook:



Esta web viene precargada con el correo del usuario, usando esto para engañar al mismo y que crea que es la web legítima. Una vez que el usuario introduce sus contraseñas, éstas se mandan a la web de los atacantes y ya podrían tener un vector de entrada a la red de la empresa:



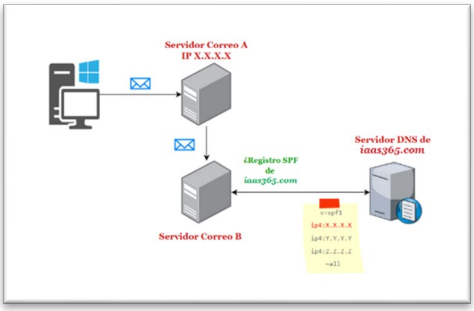
Una vez que se ha analizado y confirmado que el correo anterior se trata de un ataque Phishing, dejamos una cuestión pendiente. ¿Cómo hace nuestro servidor de correo para protegernos frente a estos ataques? La clave está en los protocolos **SPF**, **DKIM** Y **DMARC**. Las herramientas **SPF**, **DKIM** y **DMARC** tienen la misión conjunta de comprobar la autenticidad y veracidad de los correos entrantes. De esta forma se garantiza, en la medida de lo posible, la suplantación de identidad.

La **protección SPF** se encarga de comprobar los servidores autorizados para enviar correos electrónicos a nombre de un dominio. Para ello, el servidor receptor comprobará en el DNS del dominio la lista de equipos permitidos para dicho fin.

El registro se almacenaría en el DNS de tu dominio, cuyo formato sería el siguiente:

```
v=spf1  ip4:X.X.X.X  ip4:Y.Y.Y.Y
        ip4:Z.Z.Z.Z  ~all
```

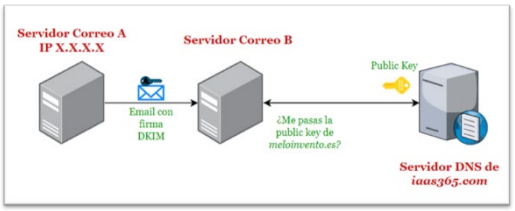
Para entenderlo mejor, podemos ver el proceso que sigue este protocolo en el siguiente esquema.



La **protección DKIM** se encarga de firmar el mensaje para autenticar el emisor, haciendo uso de un par de claves pública-privada. A parte de ello, pretende garantizar la integridad del mensaje, es decir, que no sea modificado por ninguna entidad intermedia. Para que pueda llevarse a cabo la comprobación DKIM, la persona encargada de gestionar el dominio debe generar un par de claves pública-privada. Una vez creadas, se procede a insertar la clave pública en el DNS del dominio. Por su parte, la clave privada será utilizada para firmar el correo que se envíe. Para ello el remitente, antes de enviar el mensaje, elige las cabeceras del email que quiere incluir en la firma DKIM, como por ejemplo los campos *To, From, Reply-To* y *Subject*. De esta forma, en caso de que estos parámetros sean modificados durante el trayecto, la integridad del mensaje no será válida.

Una vez elegidas las cabeceras, el remitente configurará su plataforma de correo electrónico para crear automáticamente un hash de estas cabeceras, convirtiendo el texto legible en una cadena de texto única, conformada por caracteres alfanuméricos. Antes de enviar el correo electrónico, esa cadena de hash es codificada utilizando la clave privada que generamos con anterioridad. De esta forma, cuando se realice la consulta DKIM con la clave privada, se podrá verificar la autenticación.

A continuación, se puede visualizar el proceso de este protocolo en el siguiente esquema.



La **protección DMARC** se encarga de indicar al servidor destinatario qué hacer con el correo si las valoraciones dadas por SPF y DKIM han determinado que el mensaje es una suplantación de identidad. Por lo tanto, para que un mensaje sea validado por DMARC, debe pasar la autenticación SPF y/o la autenticación DKIM. En cambio, si ambas fallan, el mensaje será rechazado. Al contrario que podríamos pensar, esta decisión no la toma exclusivamente el servidor destino. Si yo soy el propietario del dominio *iaas365.com*, configuro un registro DMARC en el DNS indicando qué acción quiero que tome un servidor que reciba un correo suplantando mi identidad. Por lo tanto, al igual que los protocolos anteriores, se debe registrar primero en el DNS la configuración DMARC. Un ejemplo de formato de este registro sería el siguiente:

```
_dmarc.iaas365.com IN TXT "v=DMARC1;
    p=quarantine; sp=quarantine;
rua=mailto:admin@iaas365.com; adkim=r;
                aspf=r;"
```

Los posibles valores para determinar el destino del correo son los siguientes:

NONE

Le indica al servidor que no haga nada con el mensaje y siga sus propias políticas para determinar el destino del mismo. Le va a indicar una cuenta de correo a la que quiere que se le notifique con un informe del mensaje sospechoso, indicada en el parámetro rua. Este es el valor por defecto.

QUARANTINE

Le indica al servidor que marque los mensajes como spam y que los mantenga en cuarentena a la espera de seguir tratándolos. También se enviaría notificación a la entidad suplantada.

REJECT

Le indica al servidor que rechace el correo, evitando que llegue al destinatario. Al igual que los anteriores, se enviaría notificación a la entidad suplantada. Sin embargo, para evitar ser descubiertos, los atacantes hacen uso de dominios propios, ya sean comprados o proporcionados en hostings gratuitos. Con esta táctica se aseguran de evadir los protocolos de seguridad implementados en los servidores de correo, tales como SPF, DKIM y DMARC, siendo el usuario final el encargado de evaluar si el correo es o no legítimo. En caso de que el usuario no esté bien formado, puede caer en la trampa sin percatarse de tal ataque.

Es por ello por lo que la **formación del usuario es fundamental** y debe estar contemplada en el plan operativo anual de la organización.

Para ello, **IaaS365** dispone de un **SERVICIO PARA EL DISEÑO DE UN PLAN DE FORMACIÓN Y CONCIENCIACIÓN**, con el apoyo de una plataforma cloud y encontrándose dicho servicio alineado con el cumplimiento de la cláusula 7.2 y 7.3 de la ISO/IEC 27001. Con este servicio cumplirá los objetivos de:

- Reducir las vulnerabilidades de los usuarios a través de procesos periódicos de formación y concienciación.
- Entrenamiento de usuarios frente a ataques simulados y controlados de seguridad.
- Asegurar los conocimientos y comportamientos de los trabajadores de la organización.
- Disponer de un plan de formación y concienciación que permita evidenciar su cumplimiento.

De esta forma, a través de diversos módulos educativos y simulaciones phishing/ransomware el usuario irá adquiriendo la formación necesaria para **reducir el riesgo de ser víctima de un ciberataque real**, con la repercusión y consecuencias que puede conllevar a la organización.

Si estás interesado, puedes consultar nuestro **SERVICIO PARA EL DISEÑO DE UN PLAN DE FORMACIÓN Y CONCIENCIACIÓN** y te asesoraremos para establecer el plan formativo que mejor se adapte a tus necesidades.