Edición No. 16 – marzo 2022

Seguridad Informática en el sector Salud

¡Porque la seguridad es de todos!

SUPLANTACIÓN Y SUS MECANISMOS

Email Spoofing:

Es la suplantación de identidad en correos electrónicos, técnica que utilizan los atacantes para ocultar la verdadera dirección del remitente en un correo malicioso y sustituirla por una legítima, suplantando la identidad de una empresa o un usuario al utilizar un dominio auténtico. Los atacantes suelen utilizar este mecanismo para hacer que los correos tengan una apariencia más creíble. Para entender un poco cómo funciona el email Spoofing es importante entender los mecanismos involucrados en las comunicaciones.

Comunicaciones en el envío de correos electrónicos

Los sistemas que gestionan el envío y recepción de correos utilizan tres protocolos, *SMTP* para el envío, *IMAP o POP* para la recepción. El SMTP se basa en transacciones entre remitente y receptor, emitiendo secuencias de comandos y suministrando los datos necesarios ordenados mediante un protocolo de control de transmisión de conexión (TCP). Estas transacciones cuenta con tres secuencias de comando/respuesta: *La dirección de retorno o emisor* (MAIL), la dirección del destinatario (RCPT) y *el contenido del mensaje* (DATA). Estos datos generalmente son completados de manera automática por el servidor de proveedor de correo, en donde los usuarios cuentan con autenticación previa, y no exige ningún tipo de verificación de identidad en su uso. Algunos proveedores de correo como Gmail u Outlook que no permiten suplantar la identidad de correos dentro de su dominio, la mayoría de direcciones existentes pueden llegar a ser víctimas de este ataque. Por ejemplo, en la imagen 1 vemos Spoofing de correo en el cual se utiliza un dominio @usps.com suplantando la identidad de un servicio.

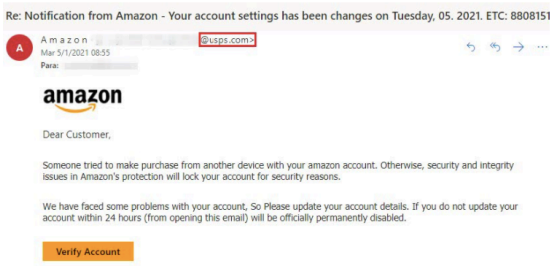

Imagen 1.

Algunos de los ataques y amenazas que con mayor frecuencia se distribuyen o utilizan el email Spoofing son:

- **Ransomware y botnets**

En el año 2020 se registró una gran actividad de botnets y en el que los ataques de ***Ransomware*** fueron protagonistas afectando a varios sectores, entre ellos el de la salud. Estos ataques buscan que la víctima descargue y ejecute un archivo que infectará el equipo, bien para cifrar una parte o toda la información que contiene y luego pedir un rescate monetario para la supuesta liberación de los archivos, o bien convertir al equipo en "zombie", pudiendo ser controlado por otro equipo para enviar spam, alojar malware, entre otras cosas más. Por ejemplo en la imagen 2 Archivo adjunto que contiene malware

Imagen 2.

Edición No. 16 – marzo 2022

Seguridad Informática en el sector Salud

¡Porque la seguridad es de todos!

- **Phishing**

En este tipo de ataque se busca convencer a la víctima para que ingrese a un enlace adjunto que buscará robar información, los atacantes suplantan la identidad de reconocidas compañías o bancos que ofrecen servicios en línea, alegando algún inconveniente o movimiento sospechoso en una cuenta a nombre de la víctima, para luego indicarle que acceda a un sitio que simula ser el oficial de la compañía y que inicie sesión. De esta manera, se entregan credenciales y el atacante obtiene el acceso a la cuenta, por ejemplo, en la imagen 3 Notificación que llegó a un usuario de MercadoPago indicando que alguien comprometió su cuenta

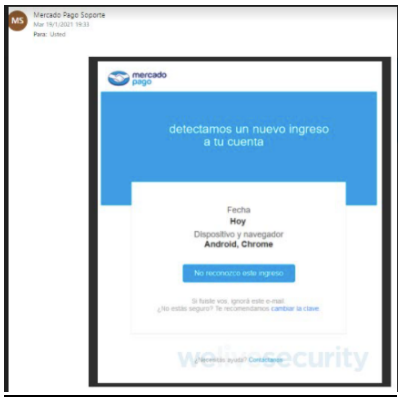

Imagen 3.

- **Spam**

La distribución de publicidad no deseada o contenido malicioso mediante envíos masivos constituyen un ataque que tiene tantos años de antigüedad como la propia Internet. Sin embargo, los mecanismos de ataque van evolucionando y los cibercriminales se adaptan y combinan el spam con distintas oportunidades, como fueron las campañas masivas a nivel global de correos que incluían una antigua contraseña en el asunto.

Fuente: welivesecurity

Libro recomendado: Datanomics

Llevas meses aceptando nuevas políticas de privacidad sin leerlas. Subes fotografías a Instagram, publicas tus gustos y tendencias políticas en Twitter, compartes los recuerdos de tus vacaciones en Facebook y charlas por WhatsApp. Te bajas aplicaciones por doquier en el móvil y consultas temas a diario en Google. Y todo eso lo haces sin pagar ni un centavo. Un poco raro, **¿no te parece?** ***¿Te has parado a pensar qué ganan esas empresas si te ofrecen el servicio sin ningún costo?*** Que si el producto es gratis, quizá se deba a que el producto eres tú.

Datanomics te mostrará, con datos, informes y hechos comprobados lo que las empresas de tecnología hacen, realmente, con tus datos personales y cómo le sacan rentabilidad mientras tú, sin darle importancia, se los regalas. La autora realiza una acertada radiografía sobre cómo se recaba y se usa nuestra información personal, y de cuáles han sido las consecuencias indeseadas de estos usos.

De cómo hemos sido capaces de pasar de una economía productiva a una economía del dato, y cómo, para mantenerla, la sociedad que conocemos ha pasado a creer religiosamente que los datos son la solución y no el problema. Ya lo decía Tim Cook: *«El potencial de la tecnología se basa en la fe que la gente tiene en ella.»* Una fe que se asienta en el desconocimiento total y en la desinformación. Si quieres abrir los ojos antes de que sea demasiado tarde, éste es tu libro.