En los últimos meses se ha visto un aumento considerable en los intentos de phishing utilizando correos electrónicos donde se adjuntan supuestas facturas por cobrar, ya sea como archivos ZIP adjuntos, archivos PDF o HTML adjuntos, o con URLs que apuntan a la supuesta descarga, que en realidad se trata de malware.

Esta técnica de phishing se ha visto en distintos países de Latinoamérica, y últimamente un crecimiento exponencial en México. Aunque parecen ser obra de hackers brasileños, se ha logrado detectar intentos de ataques incluso desde el mismo país, indicando que son piratas informáticos mexicanos los que están dentro de las campañas.

> *«Los hackers mexicanos aprovechan la ingenuidad de los usuarios desprevenidos en el país, colocando la mayor información posible dentro del correo electrónico para que parezca legítimo, con un texto coherente, que no proviene de una traducción del inglés u otro idioma, colocando direcciones reales y sitios web legítimos, lo que también da a entender que los hackers lograron comprometer los correos electrónicos empresariales desde los que envían los correos de phishing»,* dijo Igor Stepanenko, investigador de Masterhacks.

En la siguiente imagen se puede ver un correo electrónico falso de los que podrían verse como más creíble, pues proviene de un dominio coherente y de México, el texto es claro y cuenta con datos de la empresa, al entrar al dominio, se puede observar una página web real. Pero si se descarga el archivo HTML adjunto, se abrirá una página web falsa donde se descargará el malware.

Esto podría ser un ejemplo de un correo electrónico empresarial comprometido, desde el que envían los correos electrónicos de phishing.

De igual forma, se detectan muchos correos electrónicos provenientes de otros países,

especialmente Brasil, que no cuentan con la coherencia suficiente para hacerse pasar por un correo electrónico legítimo, sin embargo, existen muchas personas desprevenidas que han caído en la trampa, aún simplemente leyendo el siguiente cuerpo de mensaje:

> *«Se emitió una Factura Electrónica número 856835151 realizada el 05/25/2023 a las 10:58:43»*

Lo anterior provienen de un dominio con terminación .com.br, proveniente de Brasil, además de un enlace a la descarga de la supuesta factura.

> *«En México es muy común que la gente no se detenga a analizar un correo electrónico, que por el simple hecho de creer que se les pagará dinero tal vez por error, descarguen los archivos adjuntos y los ejecuten, y peor cuando no existe una cultura de ciberseguridad, pues muchas personas navegan en Internet sin contar con un antivirus actualizado que pueda proteger al usuario de dichas amenazas. Sin embargo, estos correos electrónicos han llegado a empresas que sí esperan facturas para recibir o enviar pagos, y por lo mismo, no lo piensan dos veces para abrirlo y ver de qué se trata, algo preocupante pues de igual forma, se trate o no de una empresa, muchas veces no se cuenta con la capacitación requerida en materia de seguridad cibernética»,* agregó Stepanenko.

Aunque muchos de estos correos electrónicos pueden tomarse como falsos, por el hecho de tener un texto que no se entiende, que utiliza palabras que no son comunes en México, llama mucho la atención aquellos que parecen legítimos y son capaces de engañar a los usuarios, pues provienen de hackers mexicanos.

> *Buenos dias.*
> *Se anexa el CFDI No Pagada del servicio con fecha 15/05/2023*

> *Favor de revisar lo antes posible.*
> *Gracias !*

Este correo, recibido en un correo electrónico empresarial, podría pasar como legítimo, pues comenzando por el título *«Reciba su Facturación. No Pagada (Segundo Aviso)»*, llama la atención del responsable, por ejemplo, del área de finanzas. Posteriormente, el cuerpo del mensaje está escrito de una forma que se entiende en México, con términos utilizados para la facturación en México, como *«CFDI»*. El remitente, Daniel Fuentes, lleva un nombre común en México, y utiliza un correo electrónico *«facturaenlinea@network.org»* que no parece falso.

Con estos detalles, un empleado puede creer que se trata de un correo legítimo y descargar el archivo HTML (considerando que no cuente con los conocimientos necesarios para distinguir entre un archivo PDF y un HTML) para poder descargar su supuesta factura, para posteriormente instalar algún tipo de malware como troyano, gusano o en el peor de los casos, ransomware.

Cómo evitar ser víctima de phishing

Para evitar caer en estas trampas y ser víctimas de cualquier tipo de ataque cibernético referente a correos electrónicos de phishing, puedes considerar seguir los siguientes consejos:

- Prestar atención al remitente y cuerpo del mensaje: Si el remitente es desconocido y no se espera una factura o cualquier otro documento de dicho remitente, lo más seguro es que se trate de un fraude. Si revisando el cuerpo del correo, siguen habiendo detalles inesperados, lo mejor es no descargar ningún archivo adjunto y comunicarse al teléfono de la empresa, en caso de venir en el correo electrónico.
- Contar con un software antivirus actualizado: Si por alguna razón llegas a descargar un archivo falso que contenga malware, el antivirus podría ayudarte a bloquear la amenaza si es que ya se encuentra en su base de datos.

- Revisar la coherencia del texto: Si no conoces el remitente y aún así decides abrir el correo electrónico, es mejor revisar la coherencia del texto, que sea legible, que no parezca una mala traducción, y verificar el tipo de dominio del remitente.

Este tipo de ataques de phishing se ha extendido en todo el mundo, por lo que es necesario tener extrema precaución y capacidad de análisis para poder minimizar los riesgos.

Si tienes alguna duda o comentario, déjalo aquí abajo!