Ministerio del Interior y Seguridad Pública

CIBERATAQUES DIRIGIDOS

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

ATAQUE AL **CEO** • ATAQUE **SPEAR PHISHING** • ATAQUE **SUPLANTACIÓN DE LA IMAGEN PÚBLICA**

Suplantar la identidad de forma pública o dentro de las organizaciones es bastante recurrente por parte de los cibercriminales. Y las consecuencias de estos ataques son difíciles de cuantificar, muchas veces porque las personas afectadas se enteran –si logran detectarla- muy tarde de la estafa o porque se rehúsan a compartir públicamente que fueron víctimas.

Ataques dirigidos: suplantación de identidad en las organizaciones

Los ciberataques dirigidos, aunque no son masivos, si se han vuelto cada vez más frecuentes y por lo general apuntan a una persona relevante para una organización.
Uno de esos tipos de ataques dirigidos es el denominado ataque al CEO. En este tipo de ataque el cibercriminal se aprovecha de un error en un mando medio de la organización que gira sobre esta persona, para explotar la confianza o costumbres y así obtener réditos, por lo general, económicos.

Para exponerlo de otra manera más sencilla, un ataque de este tipo puede iniciar con un correo electrónico como cualquier otro, proveniente del presidente, gerente general o de finanzas de una compañía para quien administra las finanzas. En su contenido se puede leer un mensaje breve, directo y con una instrucción urgente. “Oye, necesito que realices una transferencia de X millones a X cuenta lo antes posible. Tiene que estar lista antes de que termine el día. Gracias”. Si el mensaje es convincente, el receptor lo tomará como legítimo y procederá a cumplir la tarea sin cuestionamientos.

Este tipo de ataque depende en gran medida de la ingeniería social. En él se busca imitar la dirección del correo electrónico de una persona relevante en la organización y se envía una solicitud convincente. Las pérdidas económicas pueden llegar a ser cuantiosas.

Un correo corporativo comprometido es uno de las amenazas cibernéticas más complejas y costosas que puede enfrentar una institución.

Es muy frecuente que los ataques cibernéticos busquen, ya no solo diseminar phishing para robar dineros, sino penetrar en una organización. Ese tipo de ataque se conoce como spearphishing, y el objetivo es obtener credenciales de ingreso, información confidencial o esparcir malware en una entidad determinada.

El spear phishing es más difícil de detectar ya que el atacante realizó una investigación previa sobre la víctima. De esta forma el mensaje no le parecerá extraño a la víctima, y como en ataque al CEO, se hará pasar por un conocido o una persona con autoridad. El remitente crea una casilla de correo la cual puede contener el nombre de la persona que está suplantando o la organización para engañar a la víctima. La forma de reconocer este tipo de phishing es fijándose en la casilla del remitente y si el contenido del correo es realmente válido.

Suplantación de la imagen pública

Muy similar al uso de la imagen a una persona relevante en una organización es la suplantación de una persona influyente en el ciberespacio.
El uso de la imagen de personas, marcas o instituciones es muy recurrente entre los cibercriminales. Este les permite sembrar noticias falsas en sitios web, correos de phishing y redes sociales.

En este caso, la ingeniería social funciona de una manera distinta. El atacante busca explotar la imagen exitosa de una figura para persuadir a otras de imitarlo. Es en ese momento en que crea la historia de cómo esa figura pública logró cierto estatus económico y, a partir de ello, arma una trama que, si es lo suficientemente persuasiva, es capaz de hacer que las personas para realizar depósitos en bitcoins en cuentas difíciles o imposible de rastrear. En este caso, la imagen de una persona pública juega un rol fundamental como gancho, pues sugiere a las demás personas que el tema que trata un correo, un post en red social o una noticia en un sitio web, puede ser legítima.

Es difícil contener la producción de esta información falsa y el abuso de las imágenes, especialmente de ciertas personalidades del espectáculo, políticos o empresarios. La vida de estas personas está demasiado expuesta y en primer término son los propios afectados los que están llamados a denunciar el uso de su imagen.

El rol de CSIRT es advertir fraudes, tal como se hace con respecto a las decenas de campañas de phishing y centenares de sitios fraudulentos que mensualmente se comunican en nuestro sitio web y redes sociales, pero sobre todo, tenemos que educar a la ciudadanía sobre los riesgos cibernéticos existentes, sobre cómo van mutando y como los cibercriminales se van adaptando a la realidad del país, para que así las personas tengan la capacidad de identificar cuando están frente a un fraude y de esa manera eviten ser sean víctimas de los ciberataques.

Una criptomoneda es un tipo de moneda digital que está basado en código informático. Funcionan de forma autónoma y difieren significativamente de las monedas tradicionales. Son valores especulativos

La utilidad de las Bitcoin para los ciberdelitos es muy alta. En primer lugar, las criptomonedas proporcionan una forma sencilla para que los delincuentes exijan el pago. En segundo lugar, facilitan las metodologías de "delincuencia como servicio" entre los delincuentes. En tercer lugar, proporcionan un método para blanquear el producto de los delitos informáticos dado la falta de trazabilidad de las operaciones toda vez que no operan intermediarios.

La calificación de los delitos cibernéticos es algo que se escapa del rol del CSIRT. Esto pertenece a la Fiscalía, entidad que puede iniciar una persecución penal previa denuncia en esa entidad o en la PDI. Pero cuando somos contactados por ésta u otras situaciones de estafa, nosotros ayudamos a orientar a las personas sobre los pasos que debe seguir para mitigar el impacto de un ataque cibernético, y entregamos recomendaciones para evitar que vuelvan a ser víctimas de los cibercriminales.

Algunas recomendaciones que podemos compartir sobre estos ataques de suplantación son:

- Revisar el correo del remitente. La mayoría de las veces, los atacantes usan una pequeña variante del correo para parecer creíbles, sin embargo también puede pasar que la cuenta haya sido comprometida por un hackeo.

- Ser escéptico frente a los correos. Al recibir un email de una persona con autoridad sobre un tema especialmente delicado, se recomienda confirmar la información llamando a la persona o al CEO de la empresa.

- Nunca responder correos que tengan una apariencia sospechosa.

- Como este tipo de ataques está dirigido a organizaciones y están basados en técnicas de ingeniería social, una buena manera de prevenir es educando a los colaboradores, explicando la forma en que operan estos delitos y cómo reconocerlos.

- Establecer protocolos de pagos y/o transferencias para evitar caer en este tipo de estafas.

- Dudar cuando se solicite el pago en criptomonedas, recordar en la utilidad que prestan para aprovechar los réditos de los ciberdelitos.

- No confiar en las invitaciones a invertir en criptomonedas, hoy día son altamente especulativas no alcanzando aun el grado de madurez y estabilidad en el mercado.

- No descargar archivos o ir a enlaces de dudosa procedencia, ya que se pueden contener malware.

- Mantener actualizados los softwares para prevenir posibles infecciones, además de instalar y configurar filtros antispam.

- Asegurarse de que la organización utilice contraseñas robustas y limitar las cuentas con privilegios.

- Nunca se debe compartir información personal (fecha de nacimiento, rut o número de cuenta bancaria, contraseñas, etc.).

- Limitar la información que se comparte en redes sociales, especialmente para los CEOs. Los atacantes suelen aprovecharse de la ausencia de estos en su entorno de trabajo para perpetrar los ataques.

- Recurrir siempre a fuentes reconocidas para informarse

- Verificar el autor de la promociones o noticias

- No guiarse solo por el titular de una noticia antes de compartir. Podríamos estar difundiendo noticias falsas. Es importante leer toda la noticia para saber de qué se trata.