Ministerio del Interior y Seguridad Pública

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

FRAUDE A TRAVÉS DE EMAILS CORPORATIVOS

Una lucrativa tendencia en estafas digitales

I.- INTRODUCCCIÓN

Business Email Compromise (BEC) es una técnica de estafa cibernética utilizada por delincuentes para obtener acceso a informacón confidencial de una compañia o dinero. A menudo, un BEC involucra adicionalmente un ataque de ransomware. Los perpetradores se centran principalmente en objetivos financieros, y diseñan inteligentemente sus acciones, averi-guando con antelación datos de sus víctimas, por ejemplo, como los puntos debiles de una organización o información sobre los canales pagadores o responsables de pagos.

Una de las características de los ataques BEC es que puede realizarse de diferentes formas. Si bien la principal manera en que se realiza este tipo de estafa es comprometiendo la cuenta de correo electrónico de un empleado en la organización objetivo, también son métodos del BEC el spear phishing y el denominado fraude al CEO, siendo este último el mecanismo preferido por los delincuentes.

La ejecución del BEC se ha ido sofisticando al punto de que los delin-cuentes hoy no sólo utilizan correos electrónicos fiables, sino que tam-bién adicionan programas maliciosos como los malware.

No es sólo una cuestión del tamaño de la empresa

Al usar la técnica de BEC, los autores actúan de manera extremadamente profesional. Ya no sólo vemos a un perpetrador individual técnicamente inteligente que quiere ganar de dinero. Más bien, y especialmente en el caso del BEC, notamos a atacantes que eligen el área de la ciberdelincuencia principalmente por razones económicas ya que la consideran extremadamente lucrativa.

¿Qué es lo que más cuenta al responder a un ataque BEC? ¡La velocidad!

Existen mecanismos especiales de protección que defienden a las empresas de un caso tan grave como este. Sin embargo, un firewall o un antivirus no están entre ellos. Estas formas especiales de ataque requieren mecanismos de defensa específicos, que en este caso deben además actuar con especial rapidez.

Especialmente, las empresas que no están muy familiarizadas con la implementación de mecanismos de seguridad de este tipo deberían considerar el uso de Servicios de Seguridad gestionados, que cuenten con la capacidad y los conocimientos para luchar contra ataques de software de rescate y phishing.

II.– BUSINESS EMAL COMPROMISE (BEC)

El compromiso del correo electrónico empresarial (del inglés Business Email Compromise, BEC), también conocido como compromiso de la cuenta de correo electrónico (Email Account Compromise, EAC), es uno de los delitos en línea más perjudiciales desde el punto de vista financiero. Aprovecha el hecho de que muchos de nosotros dependemos del correo electrónico para realizar negocios, tanto personales como profesionales.

En una estafa de BEC, los delincuentes envían un mensaje de correo electrónico que parece provenir de una fuente conocida que realiza una solicitud legítima, como en estos ejemplos:

- Un proveedor con el que su empresa trata regularmente envía una factura con una dirección actualizada.
- El director ejecutivo de una empresa le pide a su asistente que compre docenas de tarjetas de regalo para enviar a los empleados. Pide los números de serie para poder enviarlos por correo electrónico de inmediato.
- Un comprador de una propiedad recibe un mensaje del banco con instrucciones sobre cómo transferir su pago inicial.

Las versiones de estos escenarios les sucedieron a víctimas reales. Todos los mensajes eran falsos. Y en cada caso, se enviaron miles, o incluso cientos de miles de pesos a los delincuentes.

Business Email Compromise (BEC)

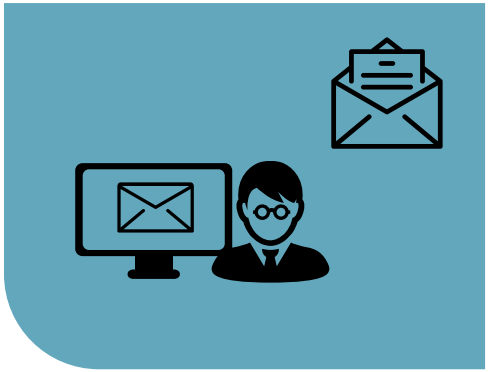
1. Identificar el objetivo

Los ciberdelincuentes recopilan infromación sobre las empresas para perfilar a los ejecutivos y empleados.

2. Ingeniería social

Los malhechores contactan personas en la empresa, haciendose pasar por superiores o clientes. Si alguien cae, el proceso continùa.

3. Intercambio de datos



Un segundo correo el supuesto CEO se vuekve más concreto. Pide una transferencia bancaría.

4. Transferencia

El empleado transfiere el dinero sin saberlo a la cuenta del cibercriminal.

Cómo los delincuentes llevan a cabo estafas BEC

Los ciberdelincuente siguen, en general, un mismo patron de pasos y actividades para lograr la estafa y finalmente robar tanto dinero como puedan de la institución víctima:

1.- Identificar el objetivo:
En esta fase, los ciberdelincuentes recopilan información sobre las empresas para perfilar a sus ejecutivos y empleados. En esto ayudan las páginas de transparencia, en el caso de las instituciones públicas, donde de manera muy simple se pueden identificar los nombres de las personas y sus cargos funcionales, entre otros datos.

2.- Ingeniería Social:
En esta etapa, los perpetradores contactan a miembros de la organización mediante técnicas de ingeniería social, entre las que se puede mencionar el spear phishing, y llamadas telefónicas típicamente enfocadas en personas identificadas en los departamentos de finanzas.

Los ciberdelincuentes usan en su comunicación una combinación de persuación y presión, con términos como "esto es urgente" o apelando a alguna situación contextual que requiere de una respuesta rápidamente, y de esta forma, explotan la naturaleza humana.
Esta proceso de persuación y engaño podría ocurrir tanto en unos pocos días como también a lo largo de semanas.

3.- Intercambio de información
Una vez que se ha logrado convencer a la víctima, esta es conducida a realizar una transacción legítima, recibiendo las instrucciones y documentaciones debidamente adulteradas para cumplir con los procesos identificados con antelación por los delincuentes.

4.- Transferencia
Finalmente, los fondos son tranferidos a una cuenta bancaria controlada por los ciberdelincuentes. Cabe destacar que esto no es necesariamente el final de un ataque BEC, ya que el engaño podría continuar si los ciberdelincuentes detectan la más minima posibilidad de volver a realizar otra transacción, perpetuando así su estafa.

Hay que tener presente que los ciberdelincuentes van eliminado las evidencias de su delito, para reducir al máximo la posibilidad de que actores intermedios puedan detectar que está en curso una acción fraudulenta. Por ejemplo, van borrando tanto los correos enviados como las respuestas recibidas.

UN CIBERDELIENCUENTE PODRÍA

1.- **Falsificar una cuenta de correo electrónico o un sitio web.**
Leves variaciones en direcciones legítimas (juan.perez@ejemplo.com vs. juan.perez@ejemplo.cl) engañan a las víctimas haciéndoles creer que cuentas falsas son auténticas.

2.- **Enviar correos electrónicos de spear phishing**.
Esta técnica busca que los mensajes parezcan provenir de un remitente confiable para engañar a las víctimas y que revelen información confidencial. Esa información permite a los delincuentes acceder a las cuentas de la empresa, calendarios y datos que les brindan los detalles necesarios para llevar a cabo los esquemas BEC.

3.- **Usar malware.**
Estos software maliciosos puede infiltrarse en las redes de la empresa y obtener acceso a hilos de correo electrónico legítimos sobre facturación y facturas. Esa información se utiliza para programar solicitudes o enviar mensajes para que los contadores o los funcionarios financieros no cuestionen las solicitudes de pago. El malware también permite a los delincuentes obtener acceso no detectado a los datos de la víctima, incluidas las contraseñas y la información de la cuenta financiera.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CÓMO INFORMAR

Si usted, su institución o su empresa son víctimas de una estafa BEC, es importante actuar rápidamente:

1.– Comuníquese con su institución financiera de inmediato y solicite que se comuniquen con la institución a la que se envió la transferencia.

2.– A continuación, comuníquese con la Policía de Investigaciones para denunciar el crimen.

3.– Si es una institución pública o una entidad privada regulada, notifique al CSIRT de Gobierno

III.– CÓMO PROTEGERSE

Tenga cuidado con la información que comparte en línea o en las redes sociales. Al compartir abiertamente datos como nombres de mascotas, escuelas a las que asistió, enlaces a miembros de la familia y su cumpleaños, puede brindarle a un estafador toda la información que necesita para adivinar su contraseña o responder a sus preguntas de seguridad.

No haga clic en ningún elemento de un correo electrónico o mensaje de texto no solicitado pidiéndole que actualice o verifique la información de alguna cuenta. Busque el número de teléfono de la empresa por sus propios medios (no utilice el que le proporciona un posible estafador) y llame a la institución para preguntar si la solicitud es legítima.

Examine cuidadosamente la dirección de correo electrónico, la URL y la ortografía utilizada en cualquier correspondencia. Los estafadores usan pequeñas diferencias para engañarlo y ganarse su confianza.

Tenga cuidado con lo que descarga. Nunca abra un archivo adjunto de correo electrónico de alguien que no conoce y tenga cuidado con los archivos adjuntos de correo electrónico que le reenvían.

Revise y fortalezca la Política de Contraseñas de su organización y la suya propia, considerando, por ejemplo, elevar el largo de las contraseñas mínimas.

Configure la autenticación de dos factores (o de múltiples factores) en cualquier cuenta que lo permita y nunca la desactive.

Verifique las solicitudes de pago y compra en persona si es posible o llamando a la persona a cargo para asegurarse de que sean legítimas. Debe verificar cualquier cambio en el número de cuenta o en los procedimientos de pago directamente con la persona que realiza la solicitud.

Ante la hipótesis probable de que el vector de entrada por medio del cual fueron capturadas las credenciales de los usuarios fue algún tipo de spear phishing , se sugirie reforzar con una campaña interna de concientización sobre este tipo de incidentes. Se sugiere utilizar material que ya ha generado con este fin el CSIRT de Gobierno, y que este tipo de campañas internas se mantenga en el tiempo.

Link de "Protocolos Ante Incidentes"
https://www.csirt.gob.cl/media/2020/03/Protocolo-incidentes-Spearphishing.pdf

Link de "Ciberataques Dirigidos"
https://www.csirt.gob.cl/media/2020/05/Suplantaci%C3%B3n-de-imagen.pdf

Se recomienda, asímismo, revisar el protocolo de transferencias o pagos de la organización, para que en caso de que superen ciertos montos sea obligatorio obtener una segunda o tercera confirmación por canales de comunicación distintos al correo electrónico. Esto es equivalente a establecer un segundo factor de verificación para transacciones financieras.

Las alertas de sesiones sospechosas son muy valiosas y debieran asegurarse de que lleguen a todas las personas pertinentes (es importante habilitar esta configuración en O365). Se debe revisar si es posible mejorar los criterios por los cuales se considera sospechosa una sesión y establecer un procedimiento escrito de respuesta ante dicha situación.

Se sugiere evaluar establecer algún tipo de control de sesiones por geolocalización, confinando las sesiones a solamente Chile, por ejemplo. Si algún funcionario viaja al extranjero y necesita acceso a su cuenta de email, debiera hacerlo mediante una sesión VPN primero y luego acceder de manera nacional al correo electrónico.

Incluso si el incidente finalmente no logra robar el dinero de la empresa, de todas maneras hay acciones delictivas que deben ser consideradas por su unidad jurídica y llevadas a la justicia, tales como robo y suplantación de identidad. Para esto, cuentan con la disponibilidad del apoyo jurídico del CSIRT de Gobierno, cuyo contacto es legalcsirt@interior.gob.cl.

Finalmente, es importante rescatar el máximo de evidencia que sean posible, para apoyar la denuncia:

- Correos enviados y recibidos Imagenes
- Coordinaciones con el ejecutivo bancario
- Documentos adulterados

Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

FRAUDE A TRAVÉS DE EMAILS CORPORATIVOS

Una lucrativa tendencia en estafas digitales

Director: Carlos Landeros Cartes

Jefa de contenidos y edición: Katherina Canales Madrid

Colaboradores equipo CSIRT:

Hernán Espinoza

Ramón Rivera

Diseño y diagramación: Jaime Millán

CSIRT
https://www.csirt.gob.cl/

Teatinos 92 piso 6
Santiago, Chile