BACSIRT
Vamos Buenos Aires | Centro de Ciberseguridad
Agencia de Sistemas

+54 (011) 4323-9362
www.ba-csirt.gob.ar
ciberseguridad@ba-csirt.gob.ar

CAMPAÑA SEXTORSIÓN:

UNA NUEVA OLA DE PHISHING

Vamos Buenos Aires | Centro de Ciberseguridad
Agencia de Sistemas

+54 (011) 4323-9362
www.ba-csirt.gob.ar
ciberseguridad@ba-csirt.gob.ar

CAMPAÑA FRAUDULENTA - PHISHING

Se recibe un correo electrónico sospechoso como posible caso de phishing (correo fraudulento, una de las técnicas de la "Ingeniería Social"), con la particularidad de que el mensaje llega supuestamente enviado desde la propia cuenta del usuario o a nombre del usuario (minombre@micorreo.com.ar), lo que lleva a suponer que el atacante tiene de alguna forma acceso a la cuenta.

En algunos casos, el cuerpo del correo electrónico está compuesto por un mensaje intimidatorio donde se le hace creer al usuario que su dispositivo ha sido infectado con un malware (virus informático) y, por lo tanto, el atacante dice poseer información confidencial y/o privada del usuario.

El objetivo final del correo puede ser realizar una estafa, donde se solicita un pago en bitcoins (criptomoneda) a la potencial víctima (extorsión) o simplemente enviar mensajes (SPAM) utilizando las vulnerabilidades presentes en la configuración del servidor de correo.

De: e@_____.com.ar
Para: ____e@_____.com.ar
→ Mismo destinatario y remitente
Enviados: Miércoles, 26 de Septiembre 2018 5:45:08
Asunto: Correspondencia urgente!

¡Hola!

Engaño

Puede que no me conozca y probablemente esté preguntándose por qué está recibiendo este correo electrónico, ¿correcto?
En este momento pirateé tu cuenta (e@_____.com.ar). ¡Tengo pleno acceso a tu dispositivo! Te envio un correo electrónico desde tu cuenta !
De hecho, coloqué un malware en el sitio web de videos para adultos (material pornográfico) y usted sabe qué, usted visitó este sitio web para divertirse (ya sabe a qué me refiero).
Mientras estabas viendo clips de video,
su navegador de Internet comenzó a funcionar como un RDP (escritorio remoto) que tiene un registrador de teclas que me proporcionó acceso a su pantalla y también a su cámara web.
Inmediatamente después, mi programa de software reunió todos sus contactos desde su Messenger, redes sociales y correo electrónico.

¿Qué hice?
Hice un video de doble pantalla. La primera parte muestra el video que estabas viendo (tienes un buen gusto ya veces extraño), y la segunda parte muestra la grabación de tu cámara web.
¿Exactamente qué deberías hacer?

Bueno, creo que $250 es un precio justo para nuestro pequeño secreto. Realizará el pago con Bitcoin (si no lo sabe, busque "cómo comprar bitcoin" en Google).
Dirección de BTC: 139XY4ZjWYqHMJvGCySuzXq7o6tGccKKrJ
(Es muy sensible, así que cópielo y péguelo)

Nota:
Tienes 2 días para hacer el pago.
(Tengo un píxel específico en este mensaje de correo electrónico, y en este momento sé que ha leído este mensaje de correo electrónico).

Si no obtengo los BitCoins, definitivamente enviaré su grabación de video a todos sus contactos, incluidos familiares, compañeros de trabajo, etc.

Sin embargo, si pagas, destruiré el video inmediatamente.
Esta es la oferta no negociable, así que no pierda mi tiempo personal y el suyo respondiendo a este mensaje de correo electrónico.

Extorsión

La próxima vez, ¡ten cuidado!
¡Adiós!

Ejemplo de correo recibido en el BA-CSIRT.

EL PHISHING ES UNA PRÁCTICA DE INGENIERÍA SOCIAL QUE TIENE COMO OBJETIVO APROPIARSE DE DATOS PERSONALES AJENOS PARA USARLOS EN BENEFICIO PROPIO.

+54 (011) 4323-9362
www.ba-csirt.gob.ar
ciberseguridad@ba-csirt.gob.ar

La técnica mediante la cual el atacante logra falsificar el remitente se llama email spoofing (suplantación de identidad en correos electrónicos) donde los datos de los mensajes son modificados para que parezcan haber sido enviados por otra persona.

La suplantación de identidad es posible debido a que el protocolo SMTP (Simple Mail Transfer Protocol) no incluye un mecanismo de autenticación, por lo que, si no se establecen las precauciones adecuadas al configurar los servicios de correo electrónico, será posible enviar correos falsificados que a simple vista parecieran provenir de una dirección o un dominio legítimo, pero que en realidad no corresponden con el emisor.

Detrás de estas campañas fraudulentas existe un propósito económico. En este caso, a cambio de eliminar la información confidencial supuestamente obtenida por el atacante, se solicita un pago en BTC (bitcoin) durante el plazo de 48hs.

Al revisar los movimientos de la billetera virtual (del ejemplo sería: 139XY4ZjWYqHMJvGCySuzXq7o6tGccKKrJ) se detectó que algunas víctimas han caído en el engaño y han realizado el pago solicitado, ya que se registran movimientos de transacciones en los últimos días; incluso en algunos sitios puede verse reportada la billetera como parte de una campaña de fraude.

LO QUE HABITUALMENTE BUSCAN SON:

- Datos y claves bancarias.
- Datos de tarjetas de crédito.
- Información personal y privada.

Resumen		Actas	
Dirección	139XY4ZjWYqHMJvGCySuzXq7o6tGccKKrJ	Número de transacciones	5
Hash 160	178d11ad30fd5f5a25667cb1e23290647c549c56	Total recibido	0.13293496 BTC
		Saldo final	0.13293496 BTC

Ejemplo del movimiento de la billetera virtual.

Address	*139XY4ZjWYqHMJvGCySuzXq7o6tGccKKrJ*
Report Count	59
Latest Report	Thu, 27 Sep 18 17:23:16 +0000 (1 hour ago)

Cantidad de cuentas que pagaron la extorsión

Después de revisar el modo de operación de la campaña de extorsión, corroboramos que se trata de una campaña de Ingeniería Social mediante la cual se busca engañar a los usuarios para que realicen un pago.

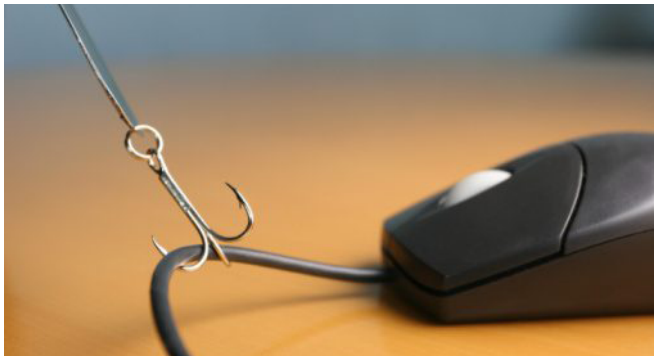
+54 (011) 4323-9362
www.ba-csirt.gob.ar
ciberseguridad@ba-csirt.gob.ar

A MODO PREVENTIVO SUGERIMOS

- No responder los correos de este estilo y entender que se trata de un engaño y, por supuesto, tampoco se debe pagar a los atacantes.
- Hacer caso omiso de este tipo de mensajes y aplicar las buenas prácticas en el uso del correo electrónico junto a otras recomendaciones, como cambiar las contraseñas de manera regular, utilizar soluciones de seguridad en los equipos, así como habilitar las opciones de doble autenticación disponibles en los diferentes servicios de Internet.
- Cambiar las contraseñas de todas las cuentas online que disponga y nunca vuelva a utilizar aquellas que fueron comprometidas.
- Si bien se trata de una práctica útil para muchas personas, guardar las contraseñas en los navegadores no es una medida segura de tratar su información personal. En caso de contar con sus credenciales de inicio de sesión guardadas en cualquiera de los navegadores (Mozilla Firefox, Google Chrome, Internet Explorer, etc.), sugerimos borrar todas las claves que hayan sido almacenadas.
- Si trabaja en alguna organización y cree que podría haber revelado información confidencial sobre la misma, infórmelo a las personas apropiadas, incluidos los administradores de red, para que estén alerta ante cualquier actividad sospechosa o inusual.
- Si cree que sus cuentas financieras pueden verse comprometidas, comuníquese de inmediato con las instituciones correspondientes indicando cuáles son las cuentas que puedan haber sido vulneradas y preste especial atención a cualquier movimiento inexplicable que pudiera aparecer en alguna de ellas.
- Esté atento a cualquier otra señale de robo de identidad que pudiera aparecer.

UTILIZAR CONTRASEÑAS SEGURAS CONSTITUYE LA PRIMERA LÍNEA DE DEFENSA PARA LA PROTECCIÓN DE NUESTRA INFORMACIÓN.

PARA MÁS INFORMACIÓN LEÉ NUESTRO BOLETÍN N° 3 ACERCA DE PHISHING, Y NUESTRO MATERIAL DIDÁCTICO DE CÓMO CREAR CONTRASEÑAS ROBUSTAS Y SEGURAS.



La palabra *phishing* deriva del verbo en inglés *fish* que significa “pescar”.