Alerta
Seguridad Cibernética

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

TLP: BLANCO (la información puede ser distribuida sin restricciones, sujeta a controles de Copyright). JUNIO 2022

Campaña de phishing con sextorsión

El CSIRT de Gobierno informa sobre la detección y notificación de correos electrónicos maliciosos que buscan extorsionar a las personas, amenazándolos con arruinar su reputación si no realizan una transferencia en bitcoin. Es importante recalcar que el mensaje que se envía es falso, el remitente no posee dichas imágenes comprometedoras y el correo es enviado indiscriminadamente a miles de personas.

La sextorsión es una estafa que busca, por lo general, obtener desde la víctima altas sumas de dinero o generar un daño moral o emocional. Es una de las principales amenazas cibernéticas y consiste en un chantaje, amenazando con la difusión de imágenes, videos o mensajes de contenido sexual.

Texto del correo electrónico con la estafa:

Su reputación está en peligro

EW Elena West <info@acehtc.co.kr>
Para srebolledoa@interior.gov.cl

Responder | Responder a todos | Reenviar
miércoles 29-06-2022 7:24

Se han quitado los saltos de línea adicionales de este mensaje.

Hola.

Esta es la última advertencia.

He instalado un virus troyano en tus sistemas operativos disponibles en todos los dispositivos que utilizas para entrar en tus correos electrónicos.
Todos los datos personales han sido copiados en mis servidores.
Tengo acceso a tus mensajeros, redes sociales, correos electrónicos, historial de chat y lista de contactos.

Mi virus me permite infiltrarme en tu sistema. Se trata de un virus multiplataforma con un VNC oculto.
Funciona en iOS, Android, Windows y MacOS.
Está encriptado para que su sistema no pueda detectarlo, borro sus firmas todos los días.

Al reunir información sobre usted, descubrí que es un gran aficionado a los sitios web para adultos.
Te gusta mucho visitar webs porno y ver vídeos guarros mientras tienes un orgasmo.

Ya he hecho una captura de pantalla.
Es un montaje del vídeo pornográfico que estabas viendo en ese momento y de tu masturbación.
Su cara es claramente visible. Este video arruinará su reputación para siempre.

Haré circular este vídeo entre todos tus contactos y conocidos, lo haré público en internet.
Y además publicaré todos tus datos personales (llamadas, correspondencia, historial de visitas, tus fotos y vídeos personales, todos tus secretos serán de dominio público) Pondré todo lo que pude encontrar en tu dispositivo en la Internet pública.

Creo que sabes lo que quiero decir.
Esto va a ser un verdadero desastre para ti.

Podría arruinar tu vida para siempre.

No creo que quieras que eso ocurra.

La solución es la siguiente: me envías 900 dólares estadounidenses (en el equivalente en bitcoin al tipo de cambio en el momento de la transferencia de fondos) y eliminaré inmediatamente toda esta porquería de mis servidores.
Después de eso, nos olvidaremos el uno del otro.

Mi cartera de bitcoin para el pago: bc1qzcggfk7qk8uz0326t3jha4epz88xak34qtrtd5

Si no sabes cómo transferir dinero y qué es Bitcoin. Usa Google.

Le doy 2 días hábiles para transferir el dinero.
El temporizador se puso en marcha automáticamente.
Recibo una notificación cuando se abre este correo electrónico.

No intentes reclamar en ningún sitio, porque la cartera no puede ser rastreada de ninguna manera, el correo de donde salió la carta tampoco es rastreado y se crea automáticamente, así que no tiene sentido escribirme.
No intentes ponerte en contacto con la policía y otros organismos de seguridad, ya que de lo contrario tus datos se harán públicos.

Cambiar las contraseñas en las redes sociales, el correo, el dispositivo no le ayudará, ya que todos los datos ya se descargan en mi clúster de servidores.

Buena suerte y no hagas ninguna tontería.

Para disminuir los riesgos de sextorsión, el CSIRT de Gobierno entrega algunas recomendaciones:

1. No compartas fotografías y videos de contenido sexual con desconocidos. Toda actividad que se realiza en internet permanece de manera indefinida.
2. En caso de perder un dispositivo con imágenes sensibles, recuerda que es factible saber dónde se encuentra, utilizando tecnología de posicionamiento. Además, puedes realizar un borrado a distancia para eliminar los documentos que tengas en él.
3. Revisa continuamente tus dispositivos electrónicos en busca de un malware, ya que podrían espiarte, robarte o grabarte en situaciones comprometedoras. Se recomienda tapar la cámara web de tus dispositivos.
4. Si recibes un correo extorsionándote con imágenes tuyas, ¡ignóralo! No abras correos de personas que conoces y tampoco le respondas.
5. Se recomienda utilizar softwares originales, ya que a través de productos piratas los ciberdelincuentes pueden acceder a tus dispositivos y tomar control.

Indicadores de Compromiso

Correos electrónicos

accounts@virsec.com.au
riken@harasawa.info
auberge@havresurmer.com
mara.cirpanu@kama.or.at
bahrami@tabnak.ir
george.mason@studentemail.in
paldam4@mabesad.mil.id
info@acehtc.co.kr
kyongjun.kim@psg.kr
yabe@asada-unyu.co.jp
maint@rising.com.sg
yoshihito-sato@cls-link.co.jp
seungkyu_woo@amano.co.kr
mirazfeda@azizgroupbd.com
julien@casinadicornia.it

IP

103.28.50.240
221.251.52.189
67.215.8.21
81.19.149.135
94.182.146.22
162.144.199.34
103.89.124.40
183.111.161.97
210.127.211.44
153.128.188.42
103.7.8.209
211.1.227.4
210.181.94.172
182.163.126.123
217.70.183.193

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.06.30 09:45:48 -04'00'