Alerta de seguridad cibernética	8FPH20-00162-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Abril de 2020
Última revisión	08 de Abril de 2020

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los IoC mencionados, previa evaluación de impacto en servicios productivos; una vez que sus plataformas de monitoreo no detecten actividad maliciosa, se debe evaluar la posibilidad de liberar del bloqueo a los IoC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

Estos casos de phishing no involucran directamente a las entidades ni al sistema bancario, sino que son técnicas de fraude indirecto, en las que en infraestructura externa a éstas se arma el mencionado phishing, para construir el engaño. Las entidades, en general, al tomar conocimiento de estos portales maliciosos articulan, dentro de sus potestades y marco legal vigente, las acciones necesarias para poder desarticularlos, pero ciertamente los usuarios también estamos llamados a estar atentos a estos intentos de engaño.

RESUMEN

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, ha identificado una campaña de phishing a través de un correo electrónico en inglés.

El mensaje informa que un atacante supuestamente logró obtener acceso a la pantalla y cámara web de quien recibe el correo, y con un software logra reunir todos los contactos de Messenger, Facebook y la cuenta de la persona.

En el mensaje se le indica al receptor del correo que fue grabado mientras visitaba un sitio con pornografía. Luego, el atacante señala que con un software que descargó en el equipo de la víctima pudo grabarla utilizando la cámara web. Bajo la amenaza de exponer el video grabado a sus contactos, como amigos, familiares y colegas, el atacante demanda el pago de $2.000 dólares, el cual no es negociable y el que debe ser cancelado en Bitcoins dentro de 24 horas. De acuerdo a lo que indica el atacante, el correo posee un pixel de rastreo con el cual ya sabe que ha leído mensaje. El mensaje de extorsión finaliza desafiando a la víctima, indicándole que si desea tener evidencia del video solo debe responder “Yes" y le serán enviadas copias de la grabación a 5 de sus contactos.

OBSERVACIÓN

Solicitamos tener en consideración las señales de compromiso en su conjunto.

INDICADORES DE COMPROMISO

Smtp Host
40[.]92[.]42[.]16
40[.]92[.]40[.]74
40[.]92[.]40[.]51
40[.]92[.]40[.]67
40[.]92[.]23[.]90
40[.]92[.]20[.]38
40[.]92[.]19[.]61
40[.]92[.]23[.]47
40[.]92[.]19[.]59
40[.]92[.]19[.]19

Sender
wkjoseyax[@]outlook[.]com
gixtabbfu[@]outlook[.]com
pujdanielatli[@]outlook[.]com
kogtieboldzuq[@]outlook[.]com
pzyfrederickaqdy[@]outlook[.]com
rlleanorzjj[@]outlook[.]com
ympsayeryu[@]outlook[.]com
refidalinaxai[@]outlook[.]com
xxfeliclegx[@]outlook[.]com
czmkrystalleun[@]outlook[.]com

IMAGEN DEL MENSAJE

Alisa Kroncke <wkjosevax@outlook.com>

Your password is [redacted] I know a lot more things about you than that.

How?

I placed a malware on the porn website and guess what, you visited this web site to have fun (you know what I mean). While you were watching the video, your web browser acted as an RDP (Remote Desktop) and a keylogger, which provided me access to your display screen and webcam. Right after that, my software gathered all your contacts from your Messenger, Facebook account, and email account.

What exactly did I do?

I made a split-screen video. The first part recorded the video you were viewing (you'e got an exceptional taste haha), and the next part recorded your webcam (Yep! It's you \ doing nasty things!).

What should you do?

Well, I believe, $2000 is a fair price for our little secret. You'll make the payment via Bitcoin to the below address (if you don't know this, search "how to buy Bitcoin" in Google).

Bitcoin Address:
[redacted]
(It is cAsE sensitive, so copy and paste it)

Important:

You have 24 hours to make the payment. (I have a unique pixel within this email message, and right now I know that you have read this email). If I don't get the payment, I will send your video to all of your contacts, including relatives, coworkers, and so forth. Nonetheless, if I do get paid, I will erase the video immediately. If you want evidence, reply with "Yes!" and I will send your video recording to your five friends. This is a non-negotiable offer, so don't waste my time and yours by replying to this email.

Alisa Kroncke

FALSO CSIRT

RECOMENDACIONES

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet
- Prestar atención en los detalles de los mensajes o redes sociales
- Evaluar el bloqueo preventivo de los indicadores de compromisos.
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas.
- Revisar los controles de seguridad de los AntiSpam y SandBoxing.
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
- Visualizar los sitios web que se ingresen sean los oficiales.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.04.08 17:49:26 -04'00'