Alerta de seguridad cibernética	8FPH22-00540-01
Clase de alerta	Fraude
Tipo de incidente	Phishing WhatsApp
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de junio de 2022
Última revisión	10 de junio de 2022

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 de Gobierno) ha identificado una campaña de phishing vía mensaje WhatsApp, que proviene supuestamente de la marca de cerveza Corona, promocionando un falso concurso para el Día del Padre. En esta campaña, los delincuentes invitan a las personas a completar una encuesta para participar en el sorteo. Para esto, adjuntan en el mensaje un enlace que direcciona hacia un sitio similar al de cerveza Corona.

Al terminar de responder las preguntas, direcciona hacia proceso de verificación y se le solicita a la víctima participar en un juego donde deberá seleccionar entre distintas opciones para obtener el premio y, además, debe compartir la campaña entre sus amistades en WhatsApp. De esta forma, el delincuente expande su ataque abarcando más usuarios para ser afectados y, posteriormente, la víctima es dirigida a sitios de baja reputación para descargar extensiones, registrarse a sitios falsos de criptomonedas o de publicidad, entre otros.

Observación

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

Indicadores de compromiso

Texto Mensaje:
Concurso día del Padre https://wp20.[ru]/s146782024/

URL sitio redirección:
https://wp20[.]ru/s146782024/

URL sitio falso:
https://tinyurl5[.]ru/s146782024/#1654868122674

Otros antecedentes

Certificado Digital

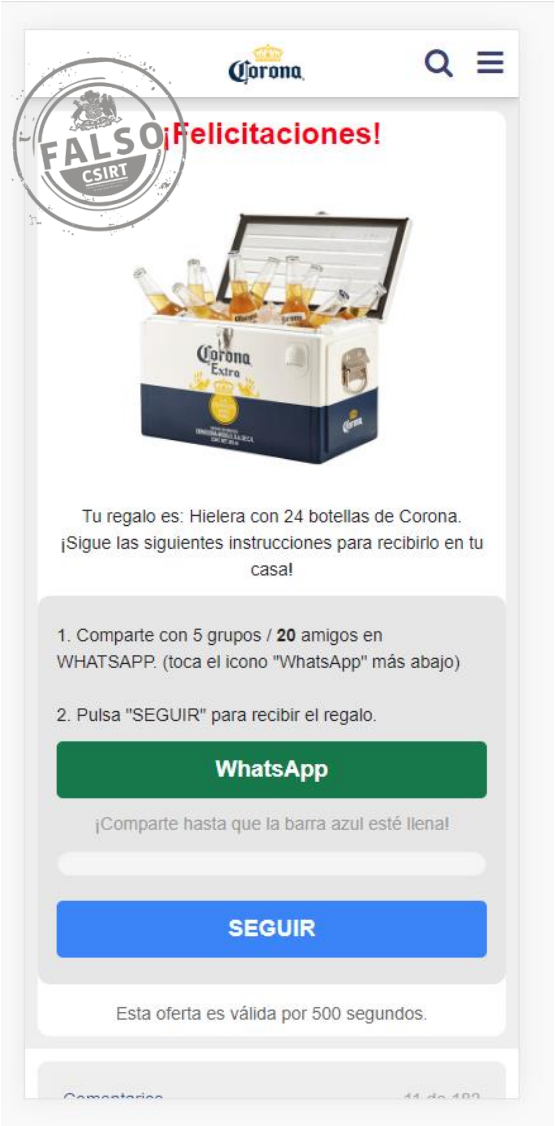
Fecha Válido	:	04-06-2022
Fecha Termino	:	02-09-2022
Emitido	:	Let's Encrypt E1

Datos Alojamiento y Dominio

IP	:	[172.67.195.165]
Número de sistema autónomo (AS) IP	:	13335
Etiqueta del sistema autónomo IP	:	CLOUDFLARENET
Registrador IP	:	ARIN
País IP	:	US
Dominio	:	tinyurl5[.]ru
Registrador Dominio	:	R01-RU

Imagen del mensaje

Imagen del sitio



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: 2022.06.10 12:37:24 -04'00'