

Alerta de seguridad informática	8FPH22-00637-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de noviembre de 2022
Última revisión	08 de noviembre de 2022

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del CSIRT de Gobierno. 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 se hace pasar como proveniente de Copec, anunciando un supuesto Subsidio del Gobierno. Para ganar este falso premio, los ciberdelincuentes indican a la víctima que debe a compartir esta falsa promoción con sus contactos. De esta forma, el ciberdelincuente expande su ataque, abarcando más usuarios para ser afectados. Finalmente, la víctima es dirigida a sitios no confiables para realizar descarga de aplicativos maliciosos.

Observación

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

Indicadores de compromiso

Texto del Mensaje

Subsidio del Gobierno Copec 88 Aniversario!

URL sitio falso:

<http://classificationcriterion.cn/empresascopec/tb.php?wy=mh1667900210206>

https://8yue22.cn/PkkfZcpa/empresascopec/?_t=1667908737331#1667908740560

Otros antecedentes

Certificado Digital

Fecha Valido	14 Sept 2022
Fecha Término	13 Dec 2022
Emitido	Let's Encrypt E1

Datos Alojamiento y Dominio

IP	[104.21.77.105]
Número de sistema autónomo (AS) IP	13335
Emitido Etiqueta del sistema autónomo IP	CLOUDFLARENET
Registrador IP	ARIN
País IP	US
Dominio	8yue22.cn
Registrador Dominio	N/A

Imagen del mensaje

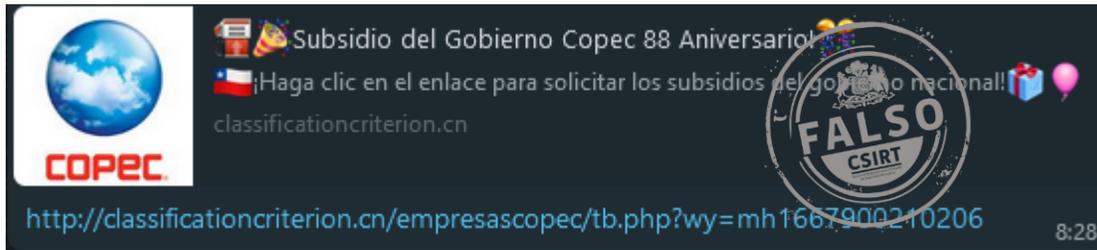
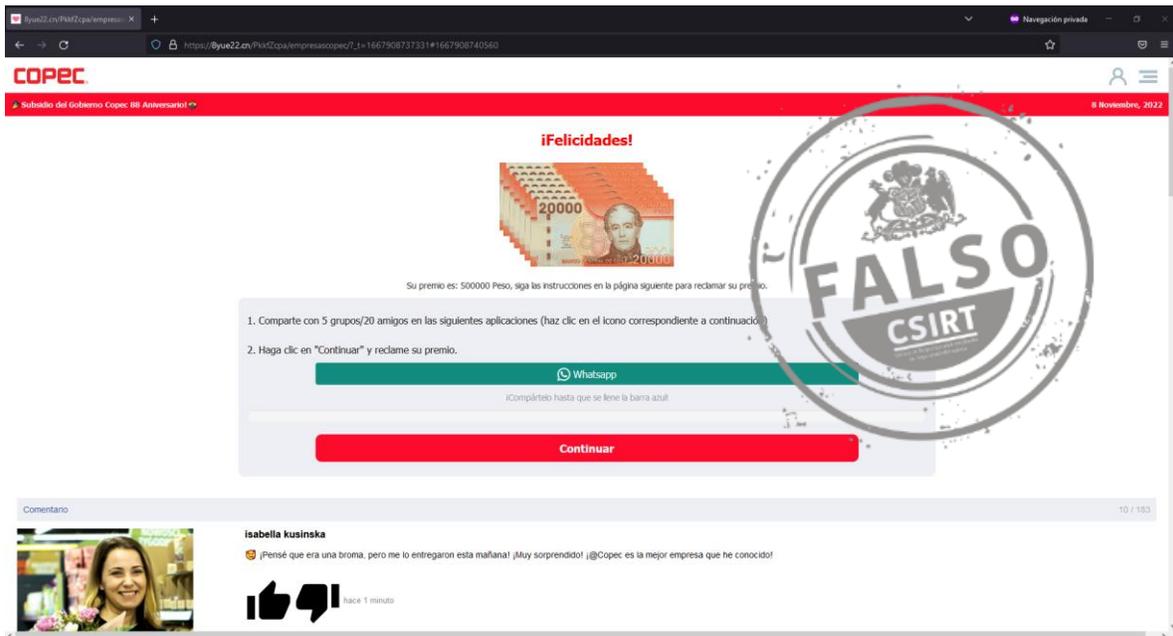


Imagen del sitio



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.

