Alerta de seguridad informática	8FPH22-00634-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de noviembre de 2022
Última revisión	05 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 dice provenir de Soprole. Para realizar su engaño, asegura que el usuario tiene un problema con un envío, invitándolo a presionar un link y contestar una encuesta.

De ingresar al enlace y responder las preguntas, se llama además a la víctima a compartir la URL con sus contactos. De esta forma, el ciberdelincuente expande su ataque. Finalmente, la víctima es dirigida a más sitios maliciosos.

Observación

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

Indicadores de compromiso

Texto del Mensaje

Mensaje de la Oficina de Correos

URL sitio falso:

http://retrievalconverse.cn/soprole/tb.php?ju=gt1667573409024
https://upceshop.cn/o4hfodFS/soprole/?_t=1667671047609#1667671050703

Otros antecedentes

Certificado Digital

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

Datos Alojamiento y Dominio

IP	[172.67.182.117]
Número de sistema autónomo (AS) IP	13335
Emitido Etiqueta del sistema autónomo IP	CLOUDFLARENET
Registrador IP	ARIN
País IP	US
Dominio	upceshop.cn
Registrador Dominio	N/A

Imagen del mensaje

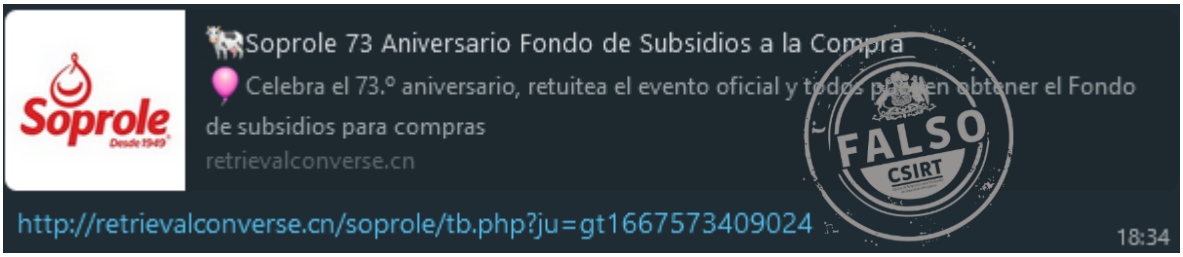
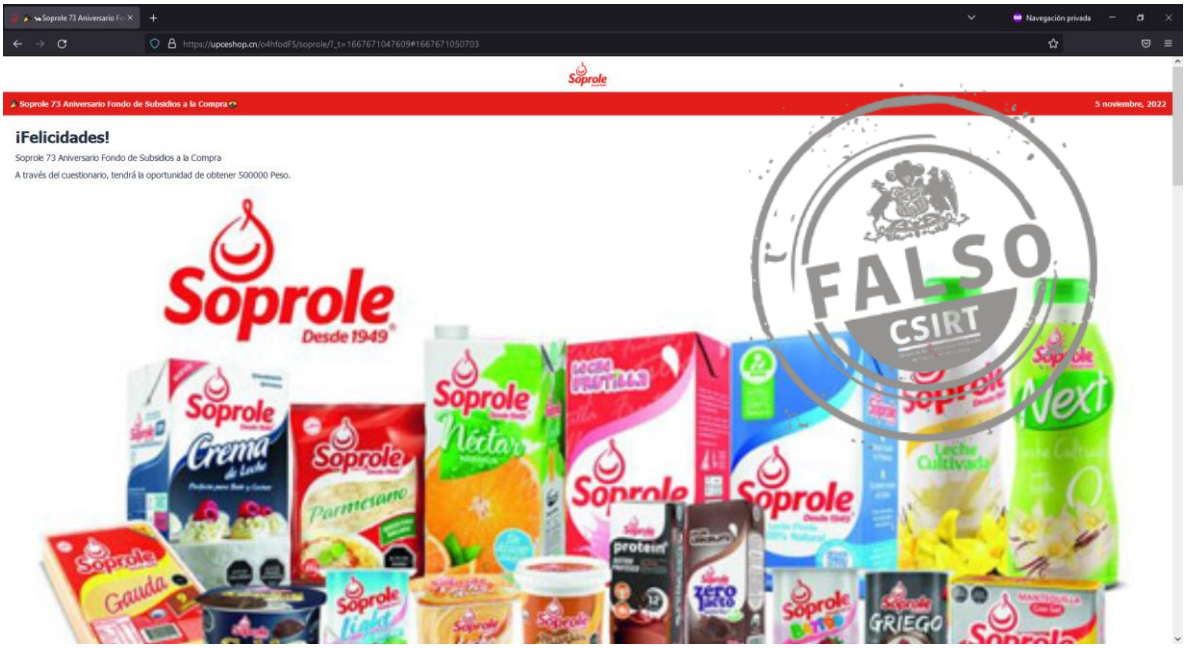


Imagen del sitio



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.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.11.07 09:22:01 -03'00'