Alerta de seguridad informática	8FPH22-00465-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de enero de 2022
Última revisión	18 de enero 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) ha identificado una campaña de phishing vía WhatsApp, indicando que supuestamente Supermercados Tottus tiene un concurso en el que está regalando más de dos mil premios.

El atacante disponibiliza un vínculo para que la víctima participe en la promoción. Al ingresar al enlace, es direccionado a un sitio semejante al del Supermercado, dónde se le invita a completar una encuesta y participar en el sorteo. Al concluir las preguntas, al usuario se le solicita compartir esta campaña entre sus amistades en WhatsApp. De esta forma el atacante obtiene sus credenciales, redirecciona a sitios falsos y además propaga a través de sus contactos la estafa.

Observación

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

Indicadores de compromiso

Urls sitio falso:

https://superfluouscritic[.]top/m2I0Y0OC/tustot/?_t=1642529381207#1642529383319

Otros antecedentes

Certificado Digital

Fecha Válido	:	04-06-2021
Fecha Término	:	04-06-2022
Emitido	:	Cloudflare Inc ECC CA-3

Datos Alojamiento

IP	:	[104.21.45.96:]
Número de sistema autónomo (AS)	:	13335
Etiqueta del sistema autónomo	:	CLOUDFLARENET
País	:	US
Registrador	:	ARIN

Datos del Dominio

Nombre de dominio	:	superfluouscritic[.]top
Creado	:	31-05-2021
Expira	:	31-05-2022
Información del registrador	:	Alibaba.com Singapore
ID IANA	:	3775
Correo electrónico	:	abuse@list.alibaba-inc.com
Servidores de nombres	:	dora.ns.cloudflare.com lakas.ns.cloudflare.com

Imagen del mensaje

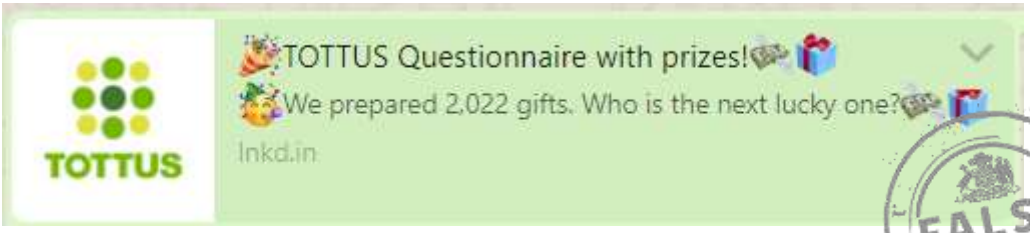

Imagen del sitio

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.