Alerta de seguridad cibernética	8FPH20-00276-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de Julio de 2020
Última revisión	31 de Julio 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), advierte sobre una campaña de phishing que se está difundiendo a través de un correo electrónico que supuestamente proviene del Banco Estado.

El atacante intenta persuadir a las personas para utilizar un enlace adjunto en el cuerpo del correo.

El mensaje del correo invita al receptor a revisar si cuenta con un crédito de capital de trabajo con garantía Estatal (FOGAPE), información que puede ser consultada en el enlace adjunto del correo.

Al seleccionar el botón para ingresar al Banco Estado, la persona es dirigida a un sitio falso del banco, donde se expone al robo de sus credenciales.

Observación

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

Indicadores de compromiso

Urls Redirecciones:

Urls sitio falso:
hxxp://bancoestado-cl-creditos[.]tk

Sender
www-data@gmail[.]com

Smtp Host
[103.248.146.11]

Asunto
Credito para Capital de Trabajo FOGAPE COVID-19 - Conoce sus Historias

Otros antecedentes

URL Body SHA-256

5be55e893cfbf1a7db90de57e6f32f1c1d8151ef535f4afb95144f05d27e30bb

Datos Alojamiento

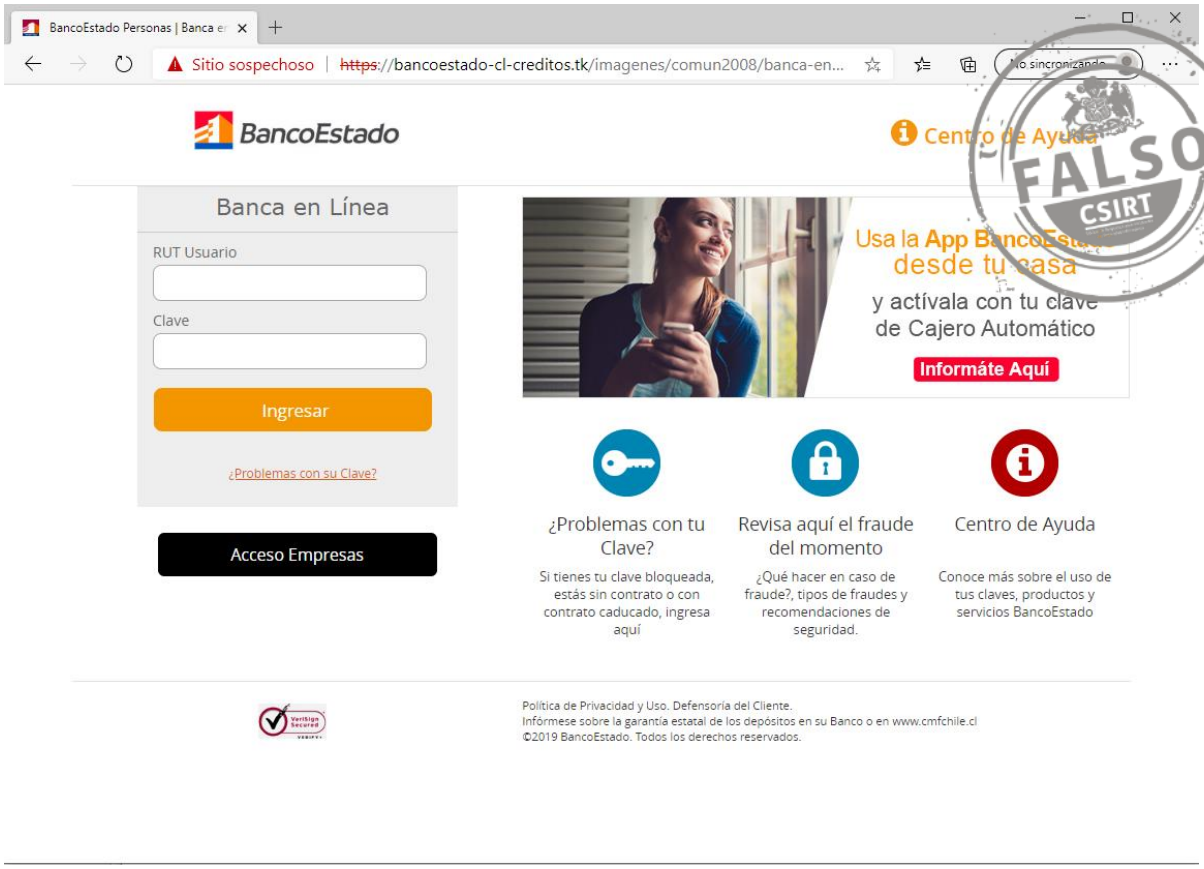
IP	:	178.159.36.76
Número de sistema autónomo (AS)	:	AS 48666
Etiqueta del sistema autónomo	:	MAROSNET Telecommunication Company LLC
País	:	Rusia
Registrador	:	RIPE NCC

Datos del Dominio

Nombre de dominio	:	bancoestado-cl-creditos.tk
Estado del dominio	:	clientTransferProhibited
Creado	:	
Expira	:	
Información del registrador	:	
ID IANA	:	
Correo electrónico	:	
Servidores de nombres	:	ns01.freenom.com ns02.freenom.com ns03.freenom.com ns04.freenom.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.