Alerta de seguridad informática	8FPH21-00438-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de octubre de 2021
Última revisión	26 de octubre de 2021

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 busca persuadir a las personas para utilizar un enlace adjunto en el cuerpo del correo.

El mensaje invita a activar el bono IFE Universal que se encuentra pendiente por cobrar. Para convencer a la víctima, en el correo se asegura que el enlace es personalizado y sincronizado con el RUT del cliente. Al ingresar al enlace, las personas son dirigidas a un sitio falso, donde se expone al robo de datos confidenciales.

Observación

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

Indicadores de compromiso

Urls redirección:
https://bit[.]ly/3gUlIlZ

Urls sitio falso:
https://www-personas-banco-estado-web[.]cf/promos-feriadas?235695623ffiof26jqbc

Asunto:
Active su Bono IFE Universal | Para ayuda Familiar en Banca en Linea con abono inmediato en su Cuenta RUT Referencia Bono IFE # 77899014

Correo electrónico
li923-9.members.linode.com

SMTP Host
[45.56.73.9]

Otros antecedentes

Certificado Digital

Fecha Valido	:	06-10-2021
Fecha Término	:	04-01-2022
Emitido	:	R3

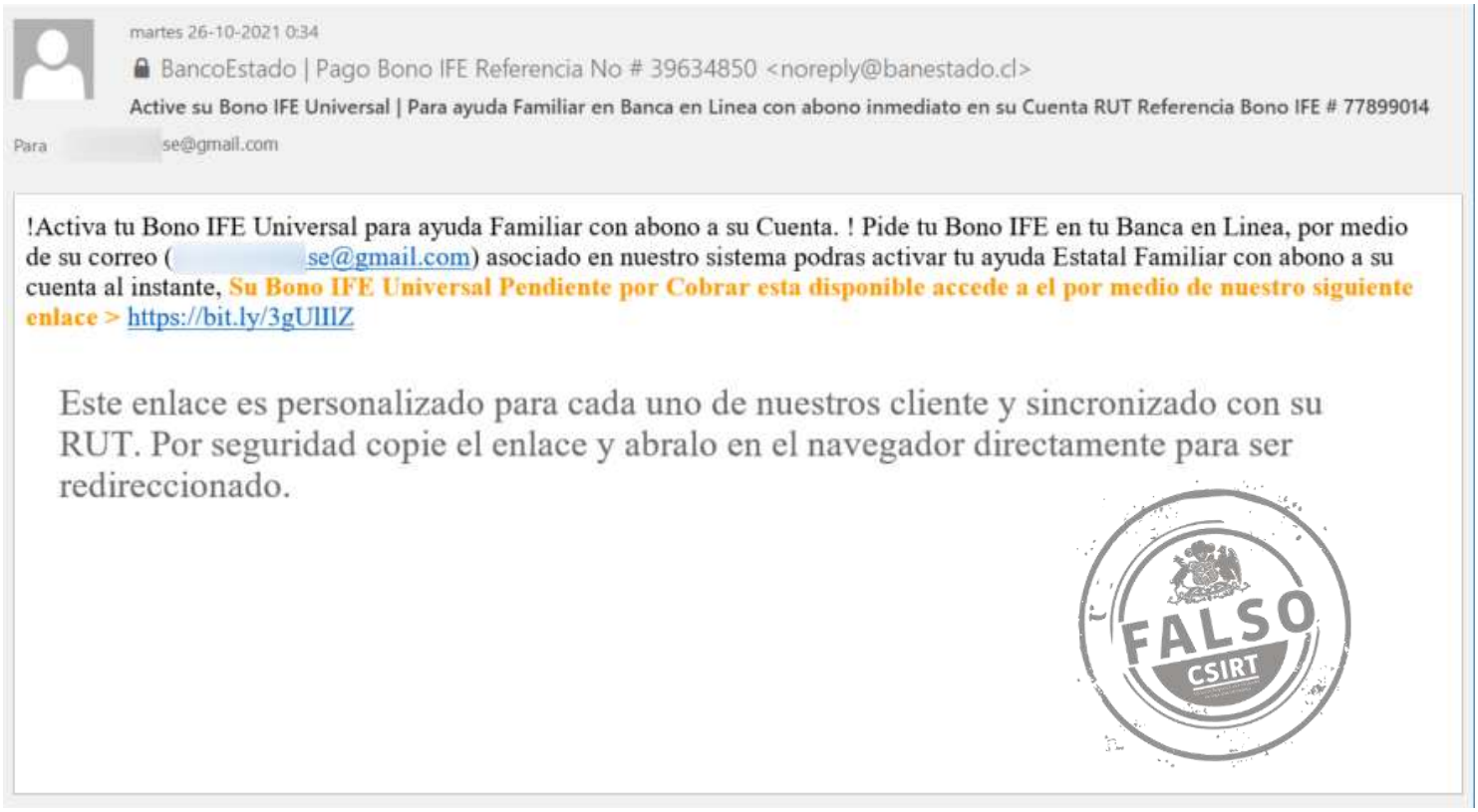
Datos Alojamiento

IP	:	[204.12.234.154]
Número de sistema autónomo (AS)	:	32097
Etiqueta del sistema autónomo	:	WII
País	:	US
Registrador	:	ARIN

Datos del Dominio

Nombre de dominio	:	www-personas-banco-estado-web[.]cf
Creado	:	NO APLICA
Expira	:	NO APLICA
Información del registrador	:	NO APLICA
ID IANA	:	NO APLICA
Correo electrónico	:	NO APLICA
Servidores de nombres	:	ns1.serverdns.bid ns2.serverdns.bid

Imagen del mensaje



martes 26-10-2021 0:34

BancoEstado | Pago Bono IFE Referencia No # 39634850 <noreply@banestado.cl>

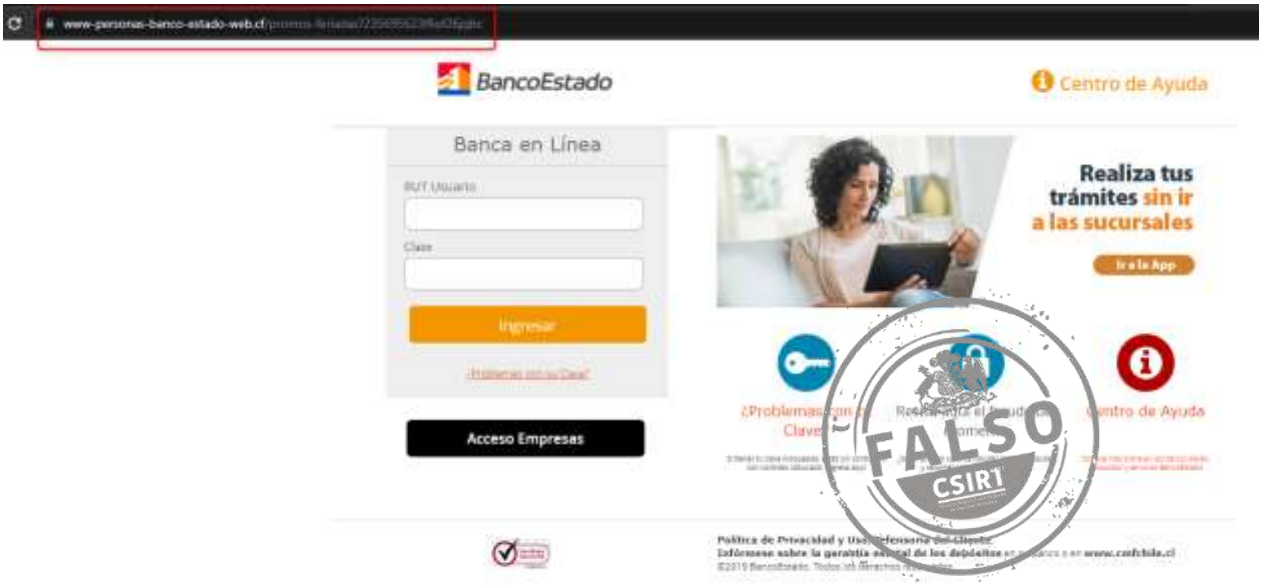
Active su Bono IFE Universal | Para ayuda Familiar en Banca en Linea con abono inmediato en su Cuenta RUT Referencia Bono IFE # 77899014

Para se@gmail.com

!Activa tu Bono IFE Universal para ayuda Familiar con abono a su Cuenta. ! Pide tu Bono IFE en tu Banca en Linea, por medio de su correo (se@gmail.com) asociado en nuestro sistema podras activar tu ayuda Estatal Familiar con abono a su cuenta al instante, **Su Bono IFE Universal Pendiente por Cobrar esta disponible accede a el por medio de nuestro siguiente enlace >** https://bit.ly/3gUlIlZ

Este enlace es personalizado para cada uno de nuestros cliente y sincronizado con su RUT. Por seguridad copie el enlace y abralo en el navegador directamente para ser redireccionado.

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: 2021.10.26 11:47:53 -03'00'