Alerta de seguridad informática	8FPH22-00518-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de mayo de 2022
Última revisión	2 de mayo 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 correo electrónico que proviene, supuestamente, del BancoEstado. En esta campaña, los delincuentes indican falsamente a la víctima que se inhabilitaron las cuentas y el acceso a la banca, debido a un problema por supuestos fraudes informáticos. Para esto, el atacante dispone de un enlace para verificar los datos. Al ingresar, la persona es dirigida a un sitio falso, semejante al Banco Estado, donde se expone al robo de su usuario y contraseña (credenciales).

Observación

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

Indicadores de compromiso

URL redirección:
hXXps://gestionvalpa[.]net/activacion/cuenta-afsn/

Sitio falso:
hXXps://kendranew[.]com/pagina/imagenes/comun2008/banca-en-linea-personas.html

Asunto:
✓ ALERTA: AVISO DE SEGURIDAD

Correo de salida:
apache@21129.bodis[.]com

SMTP Host:
[190.114.253.236]

Otros antecedentes

Certificado Digital

Fecha Válido	:	05-04-2022
Fecha Término	:	05-07-2022
Emitido	:	cPanel, Inc. Certification Authority

Datos Alojamiento y Dominio

IP	:	[138.128.170.234]
Número de sistema autónomo (AS) IP	:	33182
Etiqueta del sistema autónomo IP	:	DIMENOC
Registrador IP	:	ARIN
País IP	:	US
Dominio	:	kendranew[.]com
Registrador Dominio	:	Arsys Internet, S.L. dba NICLINE.COM

Imagen del mensaje

✓ ALERTA: AVISO DE SEGURIDAD.

B BancoEstado <Bancoestado@plusconsulting.cl>
Sáb 30-04-2022 0:23
Para: Usted

BancoEstado

Estimado(a),

Le comunicamos por motivos de su seguridad y salvaguardar a nuestros usuarios **BancoEstado Inhabilito De Manera Temporal** las cuentas y el acceso a la banca por internet debido a estos ultimos acontecimientos a nuestro sistema que surgieron mediante el fraude informatico comunmente llamado **Phishing**.

Por lo que nuestra entidad bancaria por seguridad extrema pedimos a nuestros clientes procedan a la verificacion de sus datos para poder brindarles un mayor respaldo de seguridad.

Realizado este proceso su cuenta sera habilitado para el uso correcto y asi poder evitar inconvenientes con el acceso a la banca en linea y App BancoEstado.

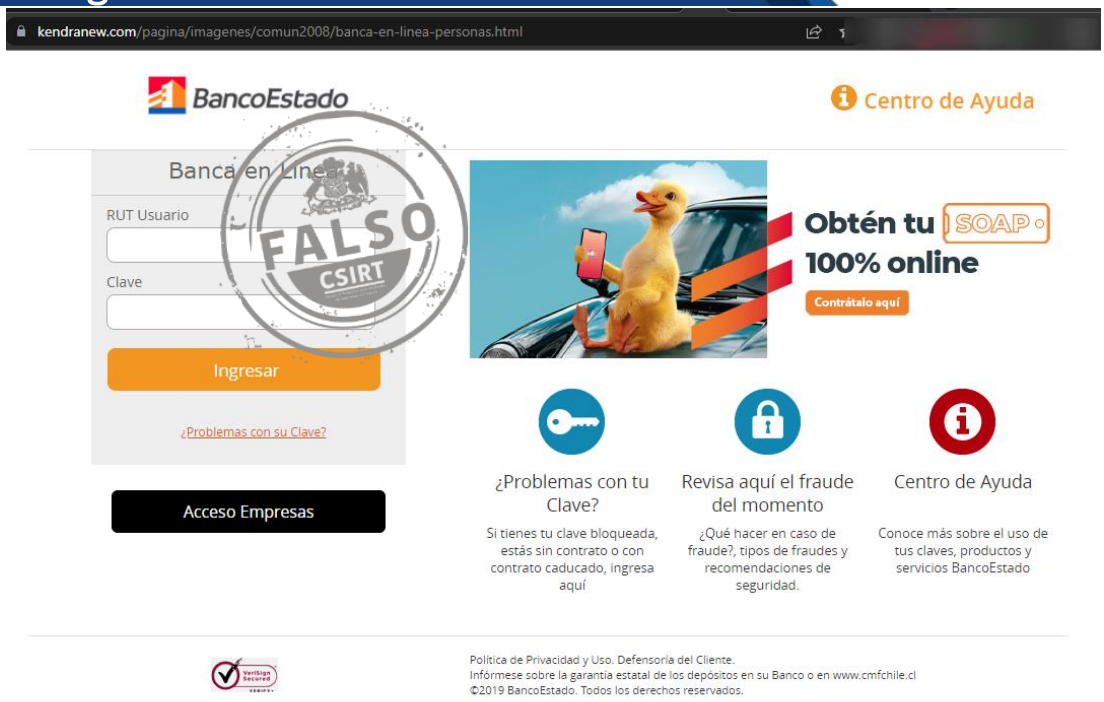
De no proceder con este pedido de seguridad podra acercarse a nuestra sucursal mas cercana.

Verificar Mis Datos

www.bancoestado.cl

Atentamente, BancoEstado.

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: 2022.05.02 10:30:19 -04'00'