Alerta de seguridad informática	8FPH20-00325-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Noviembre de 2020
Última revisión	09 de Noviembre 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 busca persuadir a las personas para utilizar un enlace adjunto en el cuerpo del correo.

El mensaje del correo indica al usuario que su clave de internet caducó y ofrece una alternativa para recuperarla a través de un enlace malicioso.

Al seleccionar el enlace para recuperar la clave, la persona es dirigida a un sitio falso donde se expone al robo de sus credenciales.

Observación

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

Indicadores de compromiso

Urls Redirección:
http[:]//mariap.webd[.]pl/_personas/centro-de-ayuda/

Urls sitio falso:
http[:]//asedl[.]am/Suppor/pagina/imagenes/comun2008/banca-en-linea-personas.html

Smtp Host
[45.7.231.17]

Sender:
apache@titan[.]com

Asunto
Informacion de seguridad de cuenta bloqueada.

Otros antecedentes

URL Body SHA-256

338a24e2206d3b76f8a9c7364991fbada0908b7432c66a294645e7cc5f937d5d

Certificado Digital

Fecha Valido	:	No aplica
Fecha Término	:	No aplica
Emitido	:	No aplica

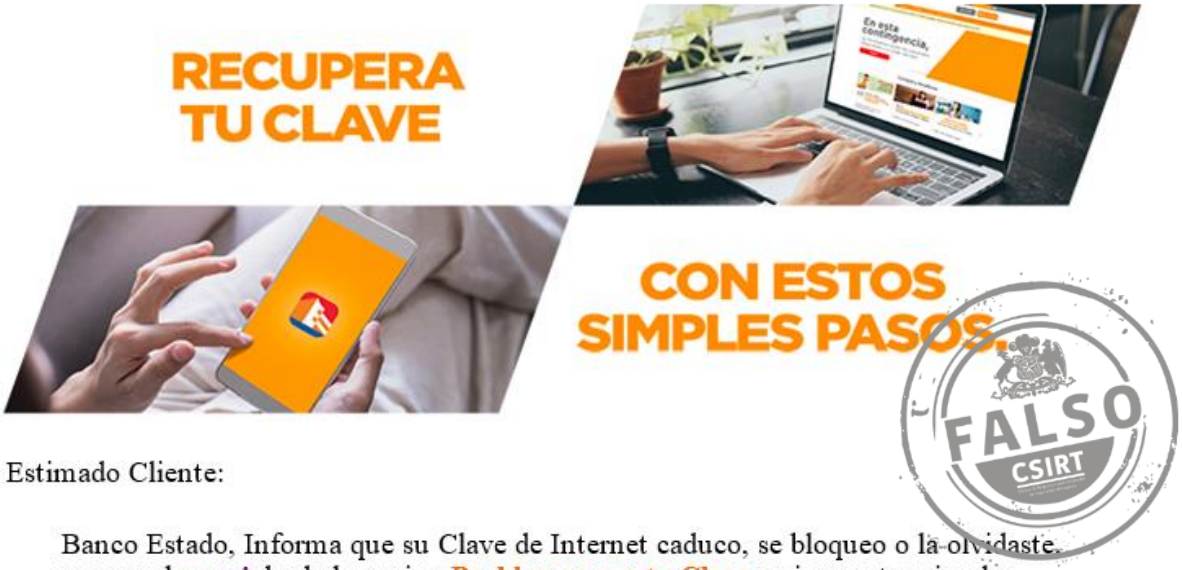
Datos Alojamiento

IP	:	192.254.225.27
Número de sistema autónomo (AS)	:	46606
Etiqueta del sistema autónomo	:	Unified Layer
País	:	US
Registrador	:	ARIN

Datos del Dominio

Nombre de dominio	:	asedl[.]am
Creado	:	2009-11-27
Expira	:	2020-11-27
Información del registrador	:	ucom (Ucom LLC)
ID IANA	:	
Correo electrónico	:	sure.baboyan.asedl.am
Servidores de nombres	:	ns6193.hostgator.com ns6194.hostgator.com

Imagen del mensaje



Estimado Cliente:

Banco Estado, Informa que su Clave de Internet caduco, se bloqueo o la olvidaste, recuperala **aqui** desde la opcion **Problemas con tu Clave** y sigue estos simples pasos:

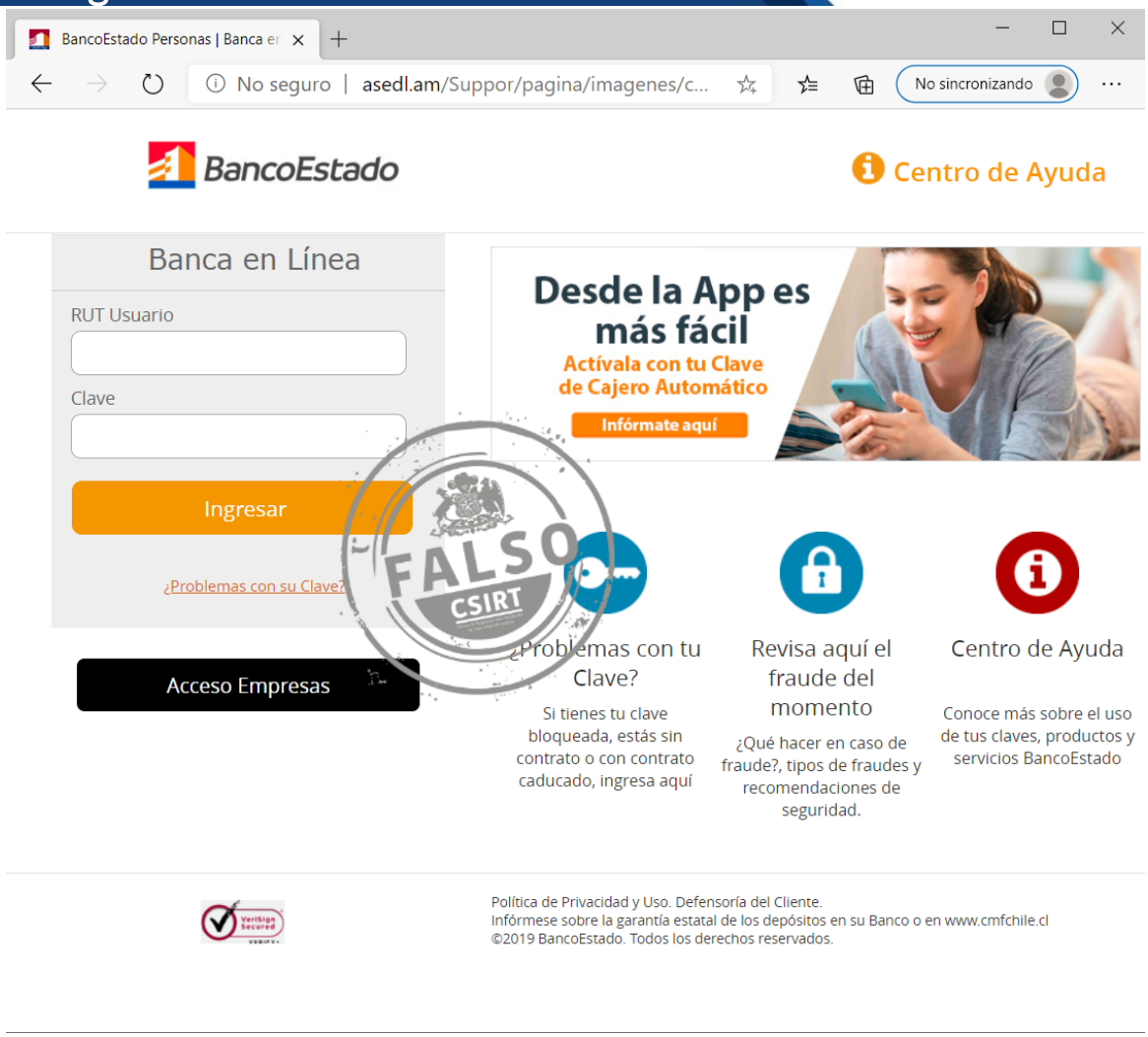
- **Selecciona la opcion que corresponde a tu tipo de Cuenta.**
- **Ingresa tu RUT y sigue el proceso Banca en Linea.**
- **Confirma tu nueva Clave con tu Tarjeta Clave de Transferencias o BE Pass.**

Solicitud Clave de Ingreso

BancoEstado

Nota: Si al recibir este mensaje ya solucionó su situación, agradecemos no considerarlo.

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.