

Alerta de seguridad cibernética	8FPH20-00226-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de Mayo de 2020
Última revisión	19 de Mayo 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 loC 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 loC 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 de utilizar un enlace en el cuerpo del correo.

El mensaje del correo informa que se realizó una mantención en los servicios de Caja Vecina, ServiEstado y su aplicación móvil, donde se detectó una inconsistencia en la cuenta. Por ese motivo se realizó el bloqueo de la cuenta.

Al seleccionar el enlace para activar la cuenta es dirigido a un sitio falso del banco, donde se expone al robo de sus credenciales y de su tarjeta de coordenadas.

Observación

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

Indicadores de compromiso

Urls Redirecciones:

Urls sitio falso:

hxxp://rakitys[.]info/natu/imagenes/comun2008/banca-en-linea-personas.html

Smtip Host

[186.64.121.8]

[45.7.231.109]

Sender

apache@universal[.]io

apache@panfila[.]net

Asunto

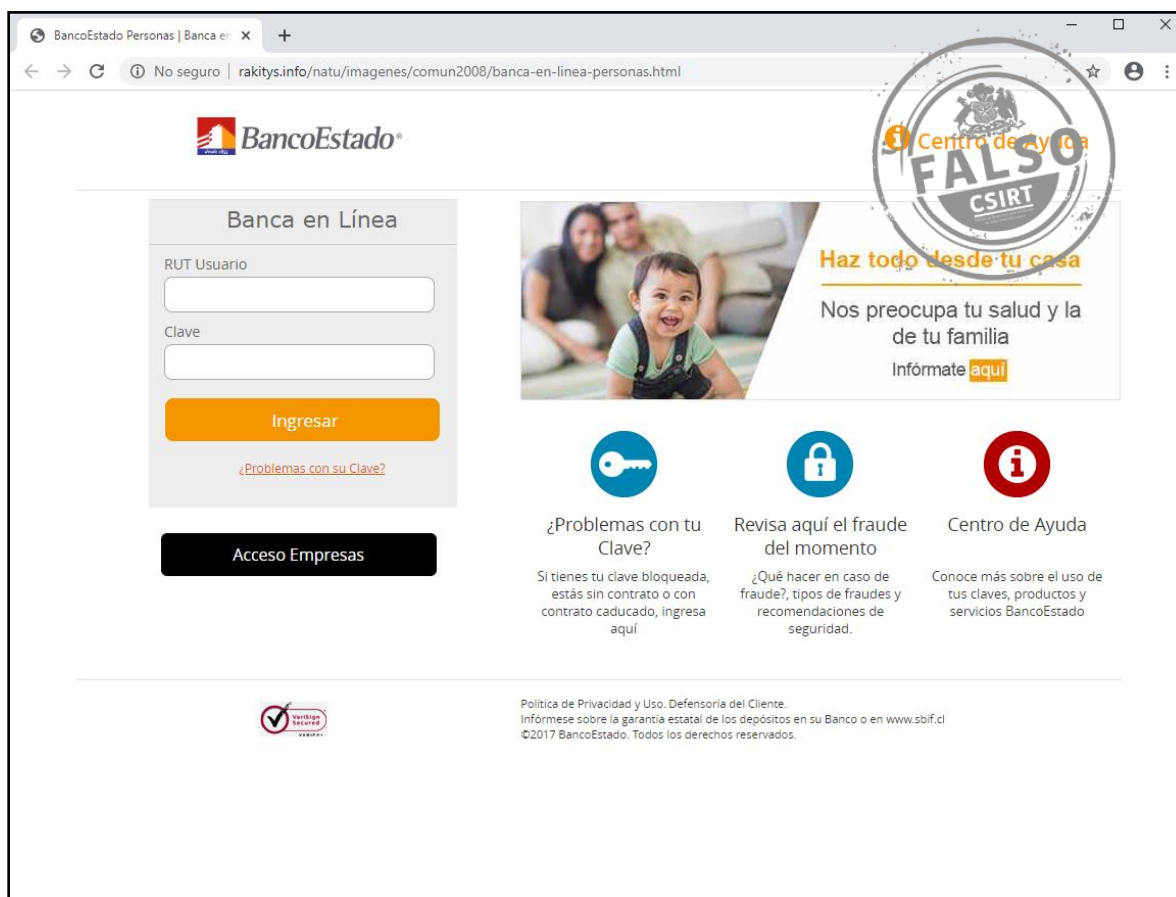
Aviso Importante: Cuenta Bloqueado

Cuenta Bloqueada

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.