Alerta de seguridad informática	8FPH20-00307-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Septiembre de 2020
Última revisión	15 de Septiembre 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 que ha dispuesto un plan de medidas especiales para enfrentar esta contingencia nacional, por lo que la persona cuenta con un crédito pre-aprobado.

Al seleccionar el enlace para acceder al crédito es dirigido 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 Redirecciones:
hxxps://login.ujdi[.]xyz/cliente/

Urls sitio falso:
hxxps://p0rtal-personas-serviestado[.]cf/comun2019/banca-en-linea-personas-session-1600090870-optimized-1600090870.html

Sender
jlc@server.latiendecita.es

Smtp Host
[185.104.152.200]

Asunto
Tiene un Crédito de Consumo Preaprobado con abono inmediato a su CuentaRUT, Chequera Electrónica o Cuenta Corriente para Contingencia Familiar COVID19

Otros antecedentes

URL Body SHA-256

d5a89e26beae0bc03ad18a0b0d1d3d75f87c32047879d25da11970cb5c4662a3

Certificado Digital

Fecha Válido	:	08/09/2020
Fecha Término	:	08/12/2020
Emitido	:	cPanel, Inc. Certification Authority

Datos Alojamiento

IP	:	154.16.118.172
Número de sistema autónomo (AS)	:	AS 45839
Etiqueta del sistema autónomo	:	Shinjiru Technology Sdn Bhd
País	:	Malasia
Registrador	:	APNIC

Datos del Dominio

Nombre de dominio	:	p0rtal-personas-serviestado[.]cf
Estado del dominio	:	active
Creado	:	No encontrado
Expira	:	No encontrado
Información del registrador	:	No encontrado
ID IANA	:	No encontrado
Correo electrónico	:	No encontrado
Servidores de nombres	:	A.NS.CF b.NS.CF C.NS.CF D.NS.CF

Imagen del mensaje

BancoEstado ha dispuesto un Plan de Medidas especiales, para enfrentar esta Contingencia Nacional apoyando a los Chilenos.

Ahora Tiene un Credito de Consumo
Preaprobado con cupo de:

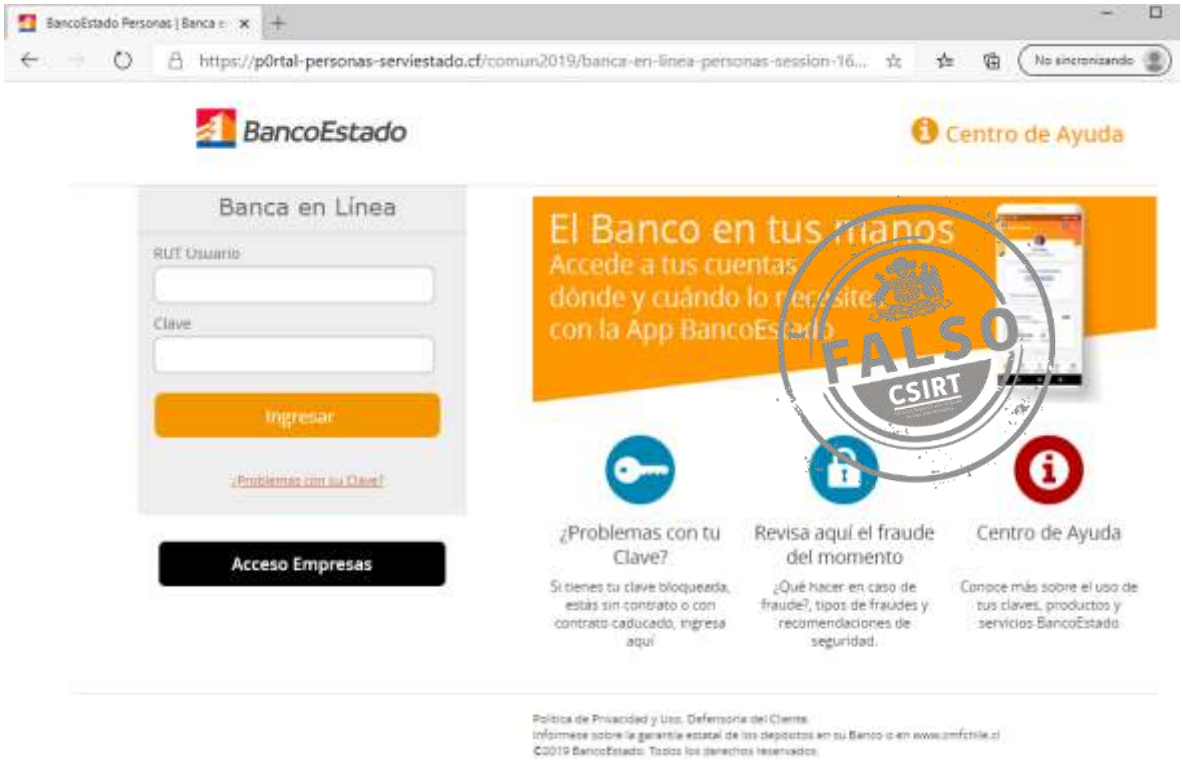
$2.500.000

Participa por 3 meses de gracia con garantia Estatal y alternativas para postergacion de creditos personal y consumo, Pidelo Aqui.
https://www.bancoestado.cl/

En BancoEstado nos preocupa tu salud y la de tu familia,
Trabajando dia a dia para orientarte, ahora realiza tus transacciones bancarias de forma online, sera rapido, comodo y no necesitara ir a sucursal BancoEstado.

Aplica terminos y condiciones BancoEstado. Oferta valida desde el 10 de Agosto al 31 de Octubre del 2020.
Sujeto a evaluacion comercial.

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: 2020.09.15 16:53:03 -03'00'