Alerta de seguridad cibernética	8FPH20-00257-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Junio de 2020
Última revisión	27 de Junio 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 Security.

El atacante intenta persuadir a la víctima para utilizar un enlace en el cuerpo del correo.

El mensaje del correo informa que el banco se ha adherido al programa del gobierno denominado Línea Covid-19 y se aprobó un crédito. Para obtener más información puede acceder a n enlace.

Al seleccionar el enlace para supuestamente evitar la suspensión es dirigido a un sitio falso de Banco Security, 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://bit[.]ly/31r5lYL?l=www[.]bancosecurity[.]cl

Urls sitio falso:
hxxps://innovativeiteration[.]com/www[.]bancosecurity[.]cl/pagina/index[.]asp

Sender
uk17books[@]host[.]freedominternational[.]net
gprint[@]host[.]freedominternational[.]net

Smtp Host
[67.205.103.117]

Asunto
Credito Aprobado.

Otros antecedentes

URL Body SHA-256

332dd04ae9deb819b7345e6f9d455c1b29b7f828cbb7d2a96afda1a9f3a6b48f

Certificado Digital

Fecha Valido	:	18-06-2020
Fecha Termino	:	16-09-2020
Emitido	:	Let's Encrypt Authority X3

Datos Alojamiento

IP	:	111.118.215.77
Número de sistema autónomo (AS)	:	AS 394695
Etiqueta del sistema autónomo	:	PDR
País	:	India
Registrador	:	APNIC

Datos del Dominio

Nombre de dominio	:	innovativeiteration[.]com
Estado del dominio	:	clientDeleteProhibited clientRenewProhibited clientTransferProhibited clientUpdateProhibited
Creado	:	19 de enero del 2016
Expira	:	19 de enero del 2021
Información del registrador	:	GoDaddy.com, LLC
ID IANA	:	146
Correo electrónico	:	abuse@godaddy.com
Servidores de nombres	:	NS1.MD-IN-22.WEBHOSTBOX.NET NS2.MD-IN-22.WEBHOSTBOX.NET

Imagen del mensaje

De: BancoSecurity.cl <noreply@publimailer.com>
Para:
CC:
Asunto: Fwd:Credito Aprobado.

Estimado(a) :

BancoSecurity, en su permanente interes por apoyar a sus clientes, ha adherido al programa del gobierno denominado Linea Covid-19.

Su credito fue aprobado por el comite del banco por el Plazo de 24 a 48 meses y 6 meses de gracia.para sus necesidades financieras.**Asi no tendras que salir de casa.**

Revisa tu credito por este E-mail. Aqui

Si tienes consultas o deseas mas informacion,ingresa aqui:

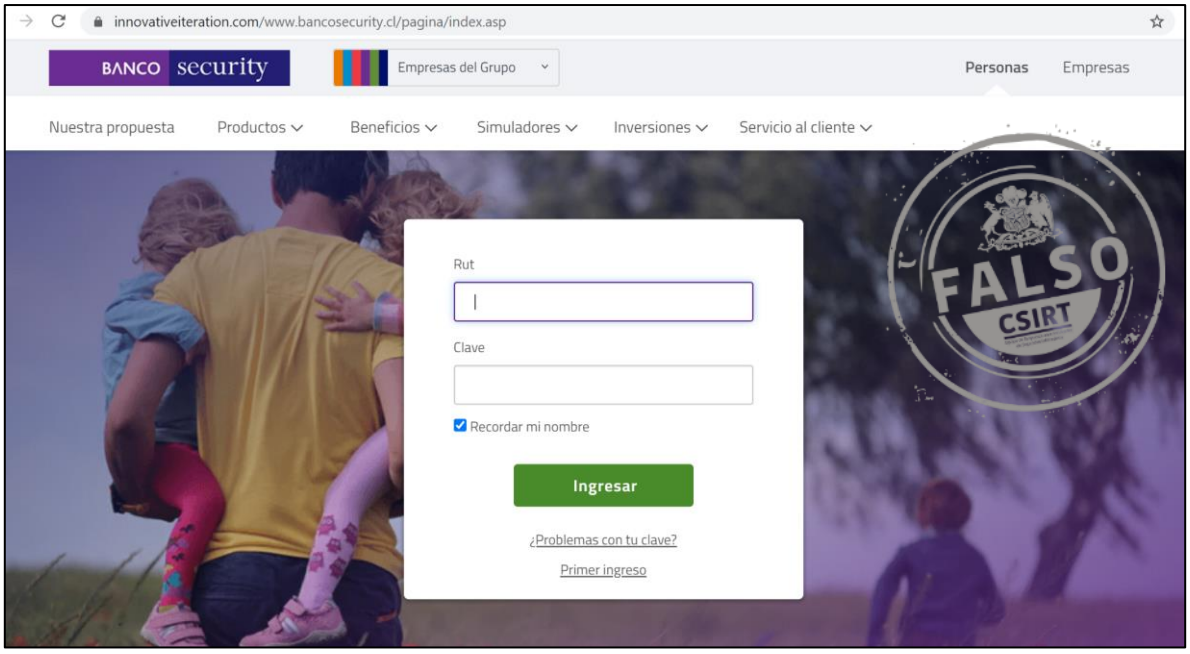
www.bancosecurity.cl

https://www.bancosecurity.cl/opera-seguro

Lamentamos las molestias que esta situacion pueda ocasionar.

FALSO CSIRT

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: 2020.06.27 17:22:57 -04'00'