Alerta de seguridad cibernética	8FPH20-00259-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Julio de 2020
Última revisión	01 de Julio 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, el que le permite tener acceso un crédito. La información asociada a este supuesto beneficio, se encontraría en el enlace adjunto.

Al seleccionar el enlace para revisar el crédito, la víctima es dirigida 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
hxxps://acumensurgical[.]com/catalog/enviar.php?l=1963615076

Urls sitio falso:
hxxps://www.spalvosspektras[.]lt/Creditos/www.bancosecurity.cl/

Sender
gprint@host.freedominternational[.]net

Smtp Host
[67.205.103.117]

Asunto
Credito Aprobado.

Otros antecedentes

URL Body SHA-256

05523d0a2e007b7fff9bc68ba6deebced6dc124f3da1a2b1bd14a67205e97c0c

Certificado Digital

Fecha Valido	:	28-05-2020
Fecha Termino	:	26-08-2020
Emitido	:	Let's Encrypt Authority X3

Datos Alojamiento

IP	:	93.115.31.106
Número de sistema autónomo (AS)	:	16125
Etiqueta del sistema autónomo	:	UAB Cherry Servers
País	:	Lituania
Registrador	:	RIPE NCC

Datos del Dominio

Nombre de dominio	:	spalvosspektras[.lt
Estado del dominio	:	Registered
Creado	:	19-11-2019
Expira	:	20-11-2019
Información del registrador	:	UAB "Virtuali erdvė"
ID IANA	:	1636
Correo electrónico	:	info@kasa.lt
Servidores de nombres	:	ns1.tera.lt ns2.tera.lt ns3.tera.lt ns4.tera.lt

Imagen del mensaje

BANCO security

OPERA SEGURO Siempre

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 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

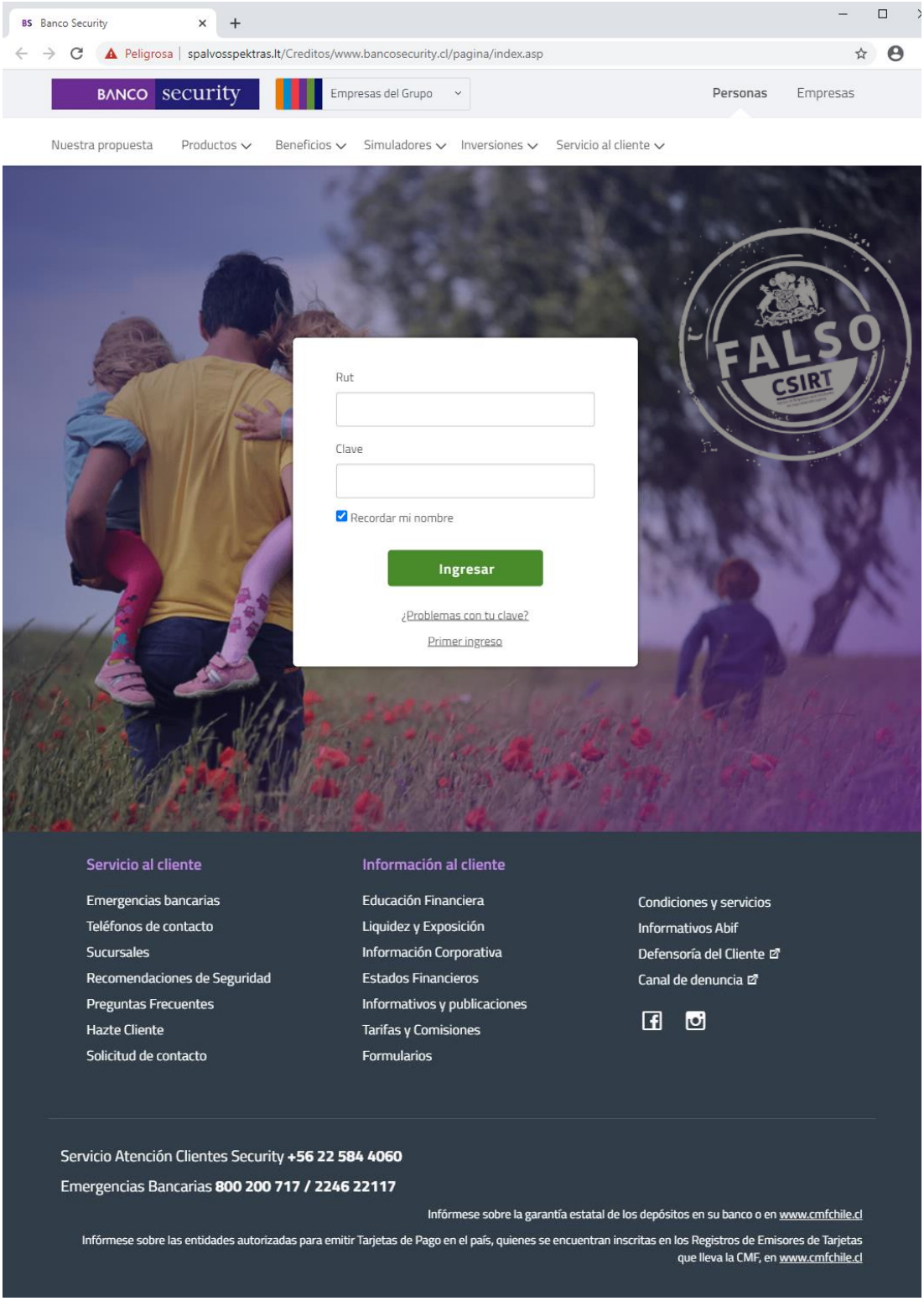
https://www.bancosecurity.cl/opera-seguro

Lamentamos las molestias que esta situacion pueda ocasionar.

Si no deseas continuar recibiendo correos de BancoSecurity, por favor haz click aqui

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.