Alerta de seguridad informática	8FPH20-00308-01
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 Scotiabank.

El atacante busca persuadir a las personas para utilizar un enlace adjunto en el cuerpo del correo.

El mensaje del correo indica que solicita enrolar los dispositivos en dicha banca por internet, debido a una actualización de los servidores de seguridad.

Al seleccionar el enlace, 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 Redirecciones:
hxxps://autocogent404[.]com/
hxxps://alkalthamhome[.]com/scos.php

Urls sitio falso:
hxxps://scotiabankchile-info-chile[.]tk/1600092226/login/personas/index

Sender
@pansel.dpd.go.id

Smtp Host
[103.248.146.11]

Asunto
Usted tiene un plazo máximo de 24 horas después de haber recibido este correo

Otros antecedentes

URL Body SHA-256

1da65ecf52e483bffed96f5db029e9a6be99498ef2817e5c6ad0f970c7524480

Certificado Digital

Fecha Válido	:	11/09/2020
Fecha Término	:	10/12/2020
Emitido	:	Let's Encrypt Authority X3

Datos Alojamiento

IP	:	91.234.99.119
Número de sistema autónomo (AS)	:	AS 48666
Etiqueta del sistema autónomo	:	MAROSNET Telecommunication Company LLC
País	:	Países Bajos
Registrador	:	RIPE NCC

Datos del Dominio

Nombre de dominio	:	scotiabankchile-info-chile[.]tk
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	:	ns01[.]freenom[.]com ns02[.]freenom[.]com ns03[.]freenom[.]com ns04[.]freenom[.]com

Imagen del mensaje

Scotiabank

Hemos actualizado nuestros servidores de seguridad:

FALSO CSIRT

Scotiabank solicita el enrolamiento de su dispositivo registrado en nuestra banca por internet, debido a una actualizacion en nuestros servidores de seguridad.

Esta operacion requiere ser atendida con urgencia para poder ingresar a sus cuentas afiliadas, realizar sus operaciones con total normalidad y comenzar a vivir una nueva experiencia de banca en linea que nuestra plataforma le ofrece.

Enrolar

Usted tiene un plazo maximo de 24 horas despues de haber recibido este correo para completar el proceso de enrolamiento y asi evitar la suspension de su cuenta.

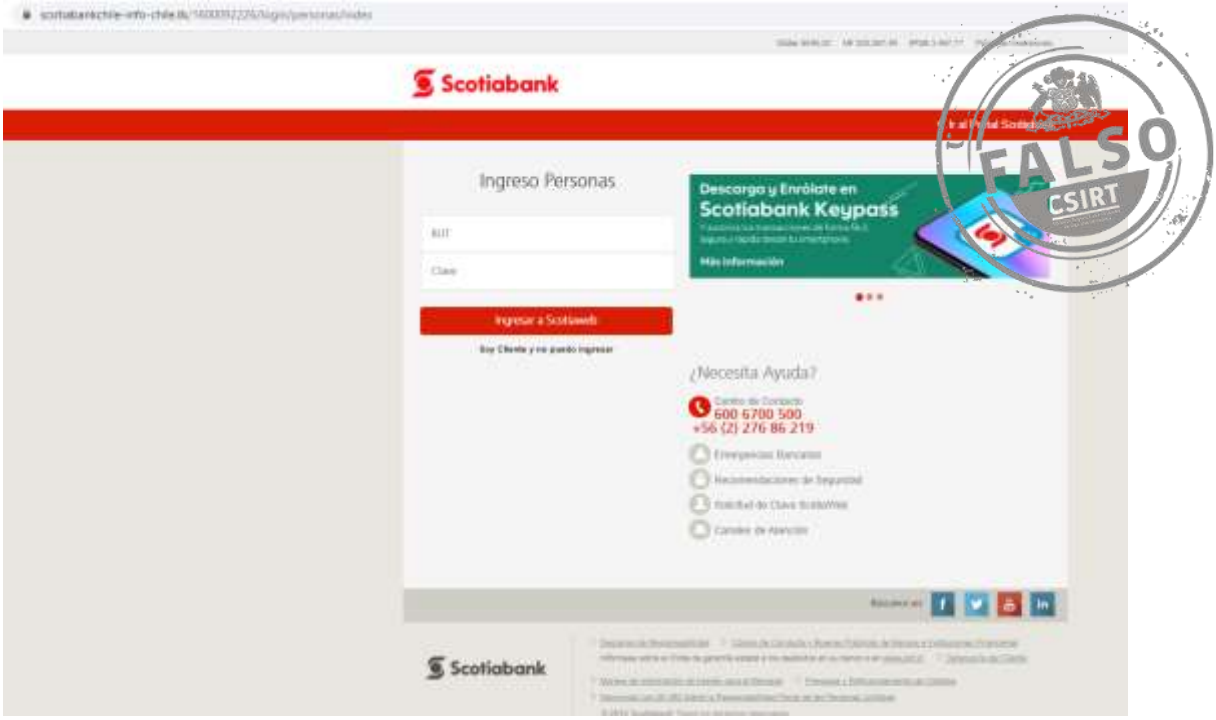
Scotiabank Más información en **Scotiabank.cl**

Porque tu seguridad es lo primero,
te recomendamos seguir estos consejos

Este correo electronico ha sido enviado a correo@correo.cl
Si no deseas seguir recibiendo mensajes de nuestra parte, Haz clic aqui para configurar tus notificaciones

Este correo electronico fue enviado por Scotiabank Chile
Direccion: Casa Matriz S.A. Av. Costanera Sur 2710 Torre A, Parque Titanium, Las Condes ***
2020 Derechos Reservados

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