Alerta de seguridad informática	8FPH21-00352-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de enero de 2021
Última revisión	13 de enero de 2021

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 correo electrónico que supuestamente proviene del Banco Scotiabank.

El atacante busca persuadir a las personas para utilizar un enlace adjunto.

El mensaje del correo indica que se aprobó la solicitud de avance en efectivo.

Al seleccionar el enlace para ver el detalle del avance, 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 sitio falso:
http[:]//scotiapersonal-cl.computekstr[.]com/45fdf968ef42f346ebfe7245a3d03372/login/personas

Asunto
Préstamo aprobado

Smtp Host:
[92.223.65.46]

Otros antecedentes

URL Body SHA-256

65adcb045aefb4d0028a6af36ec9d42bbd4dae9aff2cf85810bb4a6f44d4b25c

Certificado Digital

Fecha Válida	:	No aplica
Fecha Término	:	No aplica
Emitido	:	No aplica

Datos Alojamiento

IP	:	107.189.160.195
Número de sistema autónomo (AS)	:	53755
Etiqueta del sistema autónomo	:	Input Output Flood LLC
País	:	US
Registrador	:	AS

Datos del Dominio

Nombre de dominio	:	scotiapersonal-cl.computekstr[.]com
Creado	:	09-05-2020
Expira	:	09-05-2021
Información del registrador	:	PDR Ltd
Correo electrónico	:	miracleinfotech@ymail.com
Servidores de nombres	:	ns3.aapkahost.com ns4.aapkahost.com

Imagen del mensaje

Scotiabank.

SE APROBO SU PRESTAMO PERSONAL,

[redacted] Banco Scotiabank le informa que su solicitud de "AVANCE EN EFECTIVO SCOTIABANK", se ha aprobado con el numero de contrato CTK-CL-429-156797308-3-44 el dia 11/01/2021 / 19:51:53, el cual te permite :

- Tener dinero de inmediato en tu Cuenta Corriente o en efectivo para lo que necesites.
- Tener liquidez en tu cuenta bancaria para asumir deudas o pagos importantes que estimes convenientes.

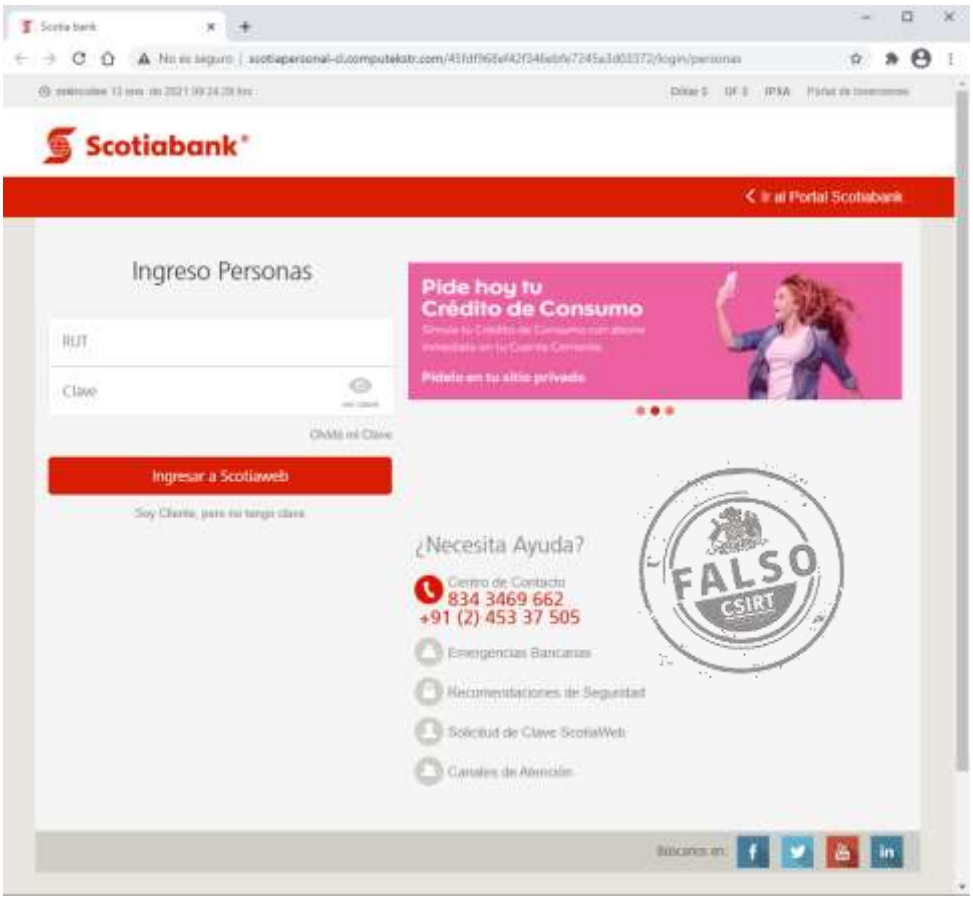
A continuacion le brindamos una seccion en nuestra plataforma virtual donde podra ver los detalles del contrato, recuerde que tiene un plazo de 2 dias para finalizar este proceso de manera virtual pasada esta fecha tendra que realizarlo de manera presencial.

DETALLES AVANCE EN EFECTIVO

Has recibido este correo porque figura como el E-mail de tu cuenta Scotiabank. Para modificarlo contactate con tu ejecutiva o visita una de nuestras sucursales.

2020, S.A.C.I Scotiabank Chile,Todos los 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.