Alerta de seguridad cibernética	8FPH20-00265-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Julio de 2020
Última revisión	09 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 Scotiabank.

El atacante intenta persuadir a las personas para utilizar un vínculo en el cuerpo del correo.

El mensaje del correo solicita el enrolamiento del dispositivo registrado en la banca por internet, por temas de seguridad.

Al seleccionar el enlace, la persona es dirigida a un sitio falso del banco, 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:
hxxp://elec-brico[.]fr/home[.]php

Urls sitio falso:
hxxps://www.bellndeal.com/www.scotiabank.cl/nuevo/scotiabank/portal/Pre-login/www.scotiabank.cl/RK8WX2/login/YOANU/personas//

Sender
www-data[@]gmail[.]com

Smtp Host
[103.248.146.11]

Asunto
Hemos actualizado nuestros servidores de seguridad

Otros antecedentes

URL Body SHA-256

349cb94dd6f46cda4bdca1152a872a55dfc359acbe6f18b742f751dc4752086f

Certificado Digital

Fecha Valido	:	25-06-2020
Fecha Termino	:	23-09-2020
Emitido	:	Let's Encrypt Authority X3

Datos Alojamiento

IP	:	46.4.227.96
Número de sistema autónomo (AS)	:	AS 24940
Etiqueta del sistema autónomo	:	Hetzner Online GmbH
País	:	Alemania
Registrador	:	RIPE NCC

Datos del Dominio

Nombre de dominio	:	BELLNDEAL[.]COM
Estado del dominio	:	clientTransferProhibited
Creado	:	19-07-2019
Expira	:	19-07-2020
Información del registrador	:	PDR Ltd. d/b/a PublicDomainRegistry.com
ID IANA	:	303
Correo electrónico	:	abuse-contact@publicdomainregistry.com
Servidores de nombres	:	NS20.HOSTBREAK.COM NS21.HOSTBREAK.COM

Imagen del mensaje

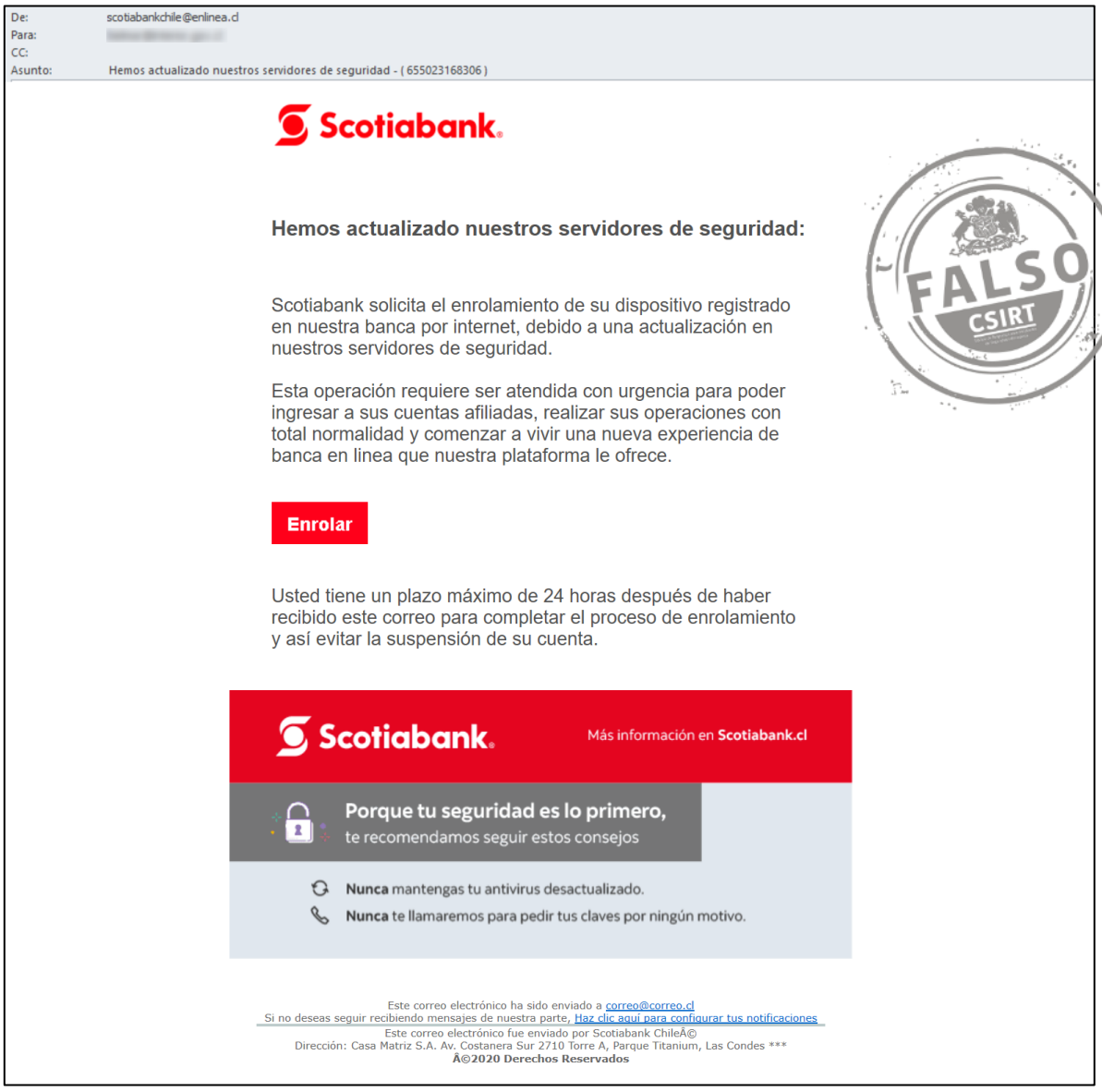
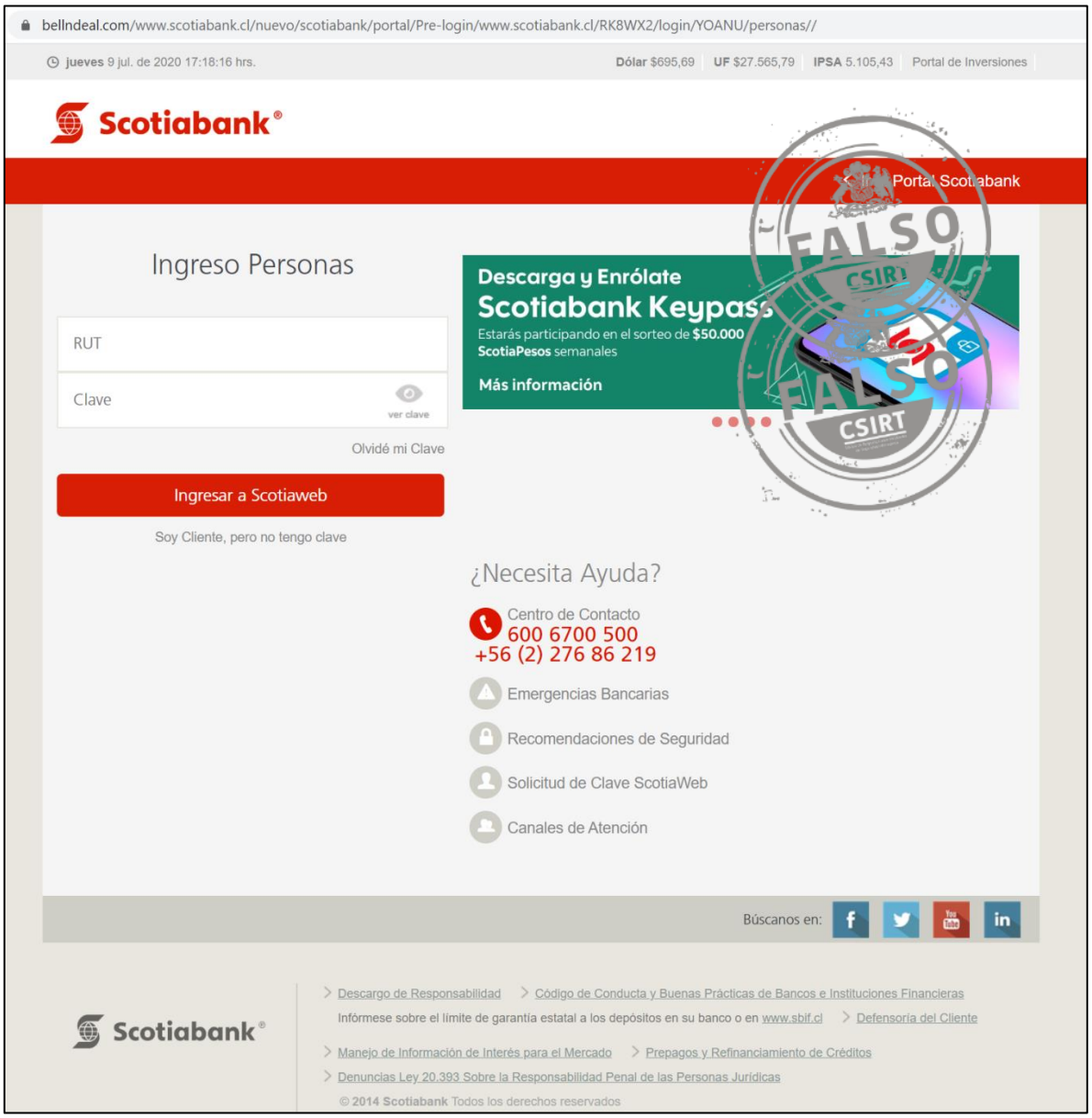


Imagen del sitio



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.