Alerta de seguridad informática	8FPH20-00120-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Febrero de 2020
Última revisión	25 de Febrero 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), ha identificado una campaña de phishing a través de un correo electrónico supuestamente proveniente del Banco Scotiabank. El atacante envía mensaje de diversos contenidos, por ejemplo:

- Existe una operación irregular y que debe verificar
- Que la cuenta se encuentra suspendida por no realizar el pago de los impuestos
- Que se ha realizado un descuento de $321.00 pesos de su cuenta automáticamente
- Que se ha bloqueado su cuenta por realizar una operación sospechosa

De esa forma intenta persuadir al usuario que seleccione el enlace, al hacerlo, la víctima es dirigida a un sitio semejante al del banco donde se expone al robo de sus credenciales.

Observación
Solicitamos tener en consideración las señales de compromiso en su conjunto.

Indicadores de compromisos

Urls Redirecciones:
https://htmanagementvb[.]com/43b46f05c3d4d89799c76a63a0420ba9
http://ipscrp[.]com/d00cb7d560960357c0780c953179b6fd
http://ieee-icus[.]com/e73caeab4c54898306b359feb954dc0e

Urls sitio falso:
https://www3[.]scotia[.]chileweb[.]cl[.]0c3[.]live/login/personas/

Sender
scotiabanksoporte@nangoldinphotography[.]com

Smtp Host
[164.68.107.60]
[45.148.120.33]
[45.148.120.129]
[45.148.120.130]
[45.148.120.131]
[45.148.120.137]
[45.148.120.136]
[45.148.120.139]
[45.148.120.140]

Asunto
Verificar Operación
Deuda cancelada
Operación Sospechosa
Detalle de Operación
Descuento solucionado
Cuenta Bloqueada
Suspensión por Fraude
Transferencia Dudosa
Movimiento Ilegal
Aprobar Transacción
Deuda Pendiente
Retención por deuda

Imagen del correo

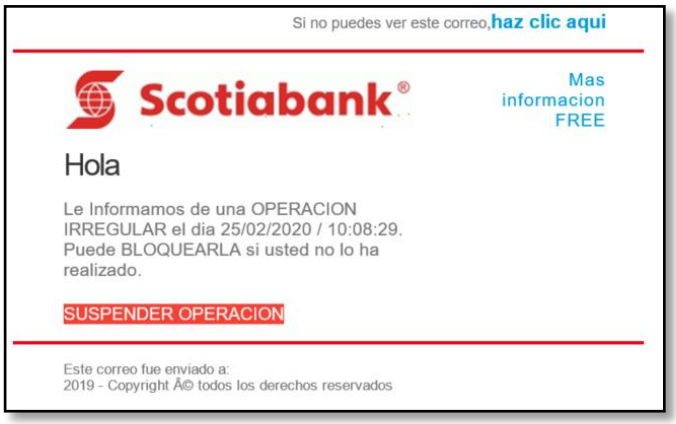
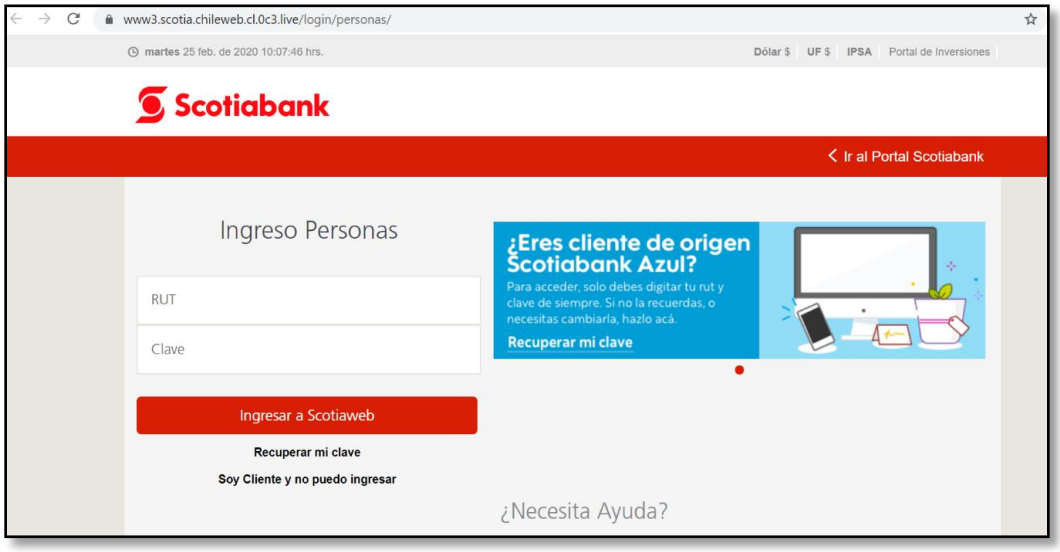


Imagen sitio web



Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- 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 que sean los oficiales.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.02.25 16:06:04 -03'00'