Alerta de seguridad informática	**8FPH-00053-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Phishing**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**05 de Agosto de 2019**
Última revisión	**05 de Agosto de 2019**

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 que intenta engañar a los usuarios del Banco Scotibank, solicitando con urgencia sincronizar su dispositivo para ingresar a la cuenta de ScotiaWeb y así optar a los beneficios que tiene como afiliado. El correo también advierte de un plazo máximo de 48 horas para realizar el procedimiento, de lo contrario la cuenta será bloqueada. Si el usuario ingresa al enlace se expone a que el atacante rober sus credenciales desde un sitio semejante al del Banco.

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto

Indicadores de compromisos

Url's:

http[:]//scotiablakclpersonasxibancenlinea[.]peredureurythmy[.]com/8U4AH4/login/S1APE/personas

http[:]//www[.]systemawindsor[.]com/80c7ae983e1fbd5865d967a41181d4ce

Smtp Host

vovego.com (96.9.222.153)

From:

root@localhost

Subject:

Urgente: Cuenta Bloqueada.

Imagen Phishing Correo

Estimado Cliente:

Scotiabank solicita sincronizar con urgencia su Dispositivo registrado en nuesta banca por internet, esta operacion requiere ser atendida para poder ingresar a sus cuentas afiliadas a ScotiaWeb y empezar a gozar de los beneficios que nuestra plataforma le ofrece.

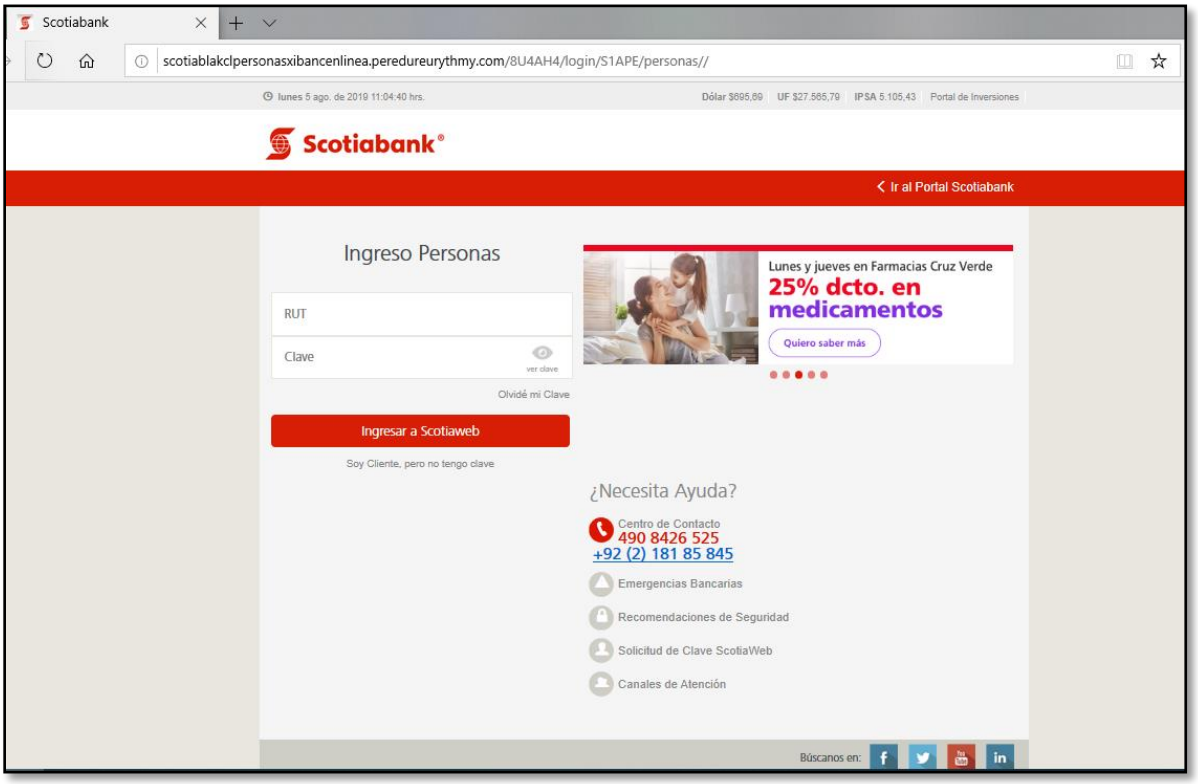
ScotiaPass	Estado de Dispotivo	No Sincronizado

Sincronizar Dispositivo

Recuerde que solo tiene 48 horas despues de recibir este email para realizar dicho proceso, de lo contrario su cuenta sera bloqueada y tendra que acercarse a la sucursal mas cercana para solicitar una nueva tarjeta.

2019. S.A.C.I Scotiabank Chile. Todos los Derechos Reservados

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