Alerta de Seguridad Informática (8FPH-00021-001)

Nivel de Riesgo: Alto

Tipo: Phishing

Fecha de lanzamiento original: 23 de Mayo de 2019 | Última revisión 23 de Mayo 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.

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 Scotiabank. El correo trata de persuadir a los clientes del Banco para que sincronicen con urgencia un dispositivo asociado al banco por internet, operación necesaria para obtener los beneficios que ofrece la plataforma vía web, tratando así de convencer al cliente de ingresar a los link maliciosos del sitio en cuestión.

Indicadores de compromisos

Url's:

http[:]//mobiledigishop[.]com

http[:]//consejeroenlared[.]com

Smtp Host

mta186.qbi04zpo[.]org
104[.]217[.]128[.]133

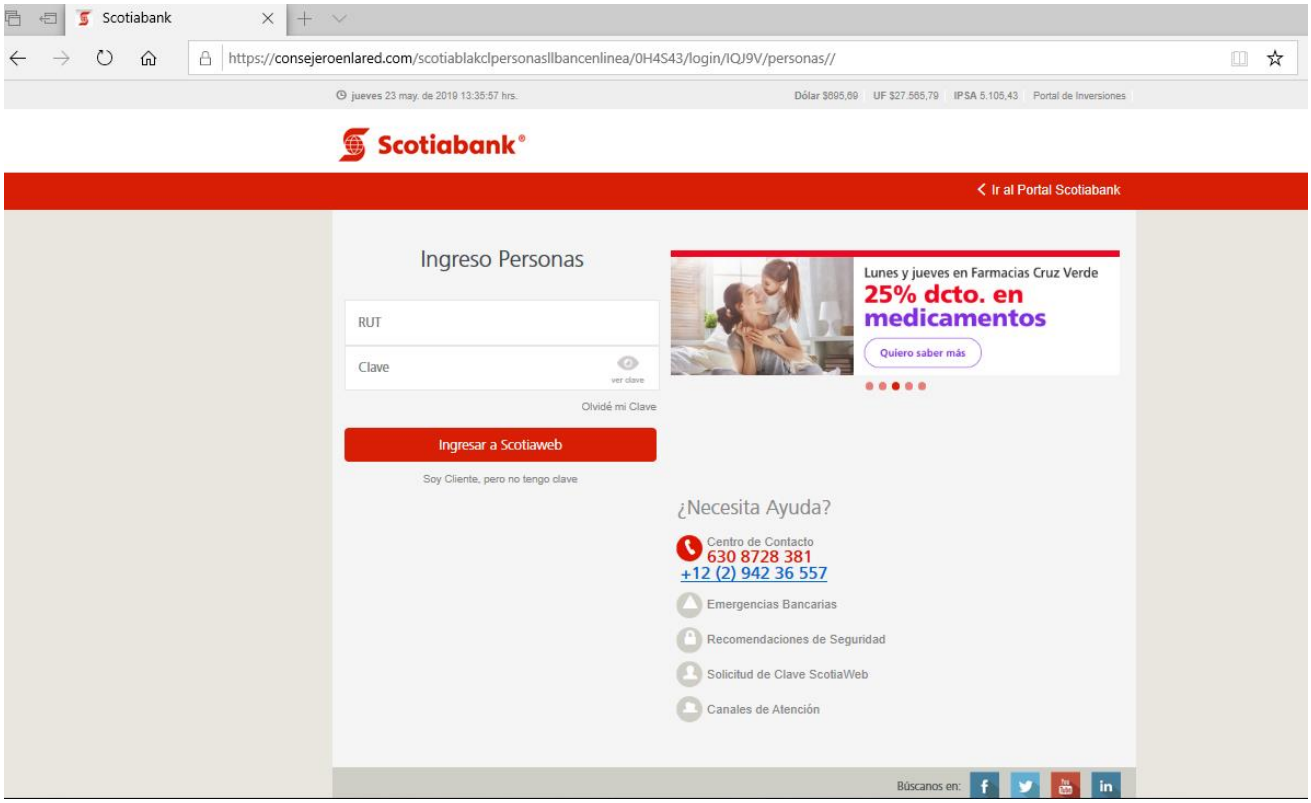
From:

root@vps.server[.]com

Subject:

Alerta: Sincronizacion de dispositivo pendiente.
Por su seguridad requerimos enrolar y validar su ScotiaPass

Imagen



Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java, entre 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

Contactos

https://www.csirt.gob.cl
+ (562) 24863850
@CSIRTGOB
https://www.linkedin.com/company/csirt-gob