Alerta de seguridad informática	2CMV-00039-001
Clase de alerta	Fraude
Tipo de incidente	Phishing - Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Noviembre de 2019
Última revisión	11 de Noviembre 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 detectado una campaña de phishing con malware asociado, a través de un correo electrónico que suplanta al Banco ScotiaBank.

Los estafadores buscan engañar a los usuarios enviando un anuncio que tiene relación con la fusión entre los Bancos BBVA y Scotiabank, advirtiéndoles que producto de este proceso, el usuario debe actualizar sus datos, lo que también es necesario para brindar seguridad a la misma.

A la víctima se le disponibiliza un enlace para realizar la actualización de sus datos. Al seleccionar el hipervínculo, la personas es direccionado a otro sitio hasta descargar el archivo malicioso.

Indicadores de compromisos

Url's:
http://medianews[.]ge/_manager/img/public[.]php
http://medianews[.]ge/_manager/template/actions/c4tOling[.]zip
3.84.132[.]144

Smtp Host
hwsrv-637272.hostwindsdns[.]com [23.254.161.217]

Subject:
Atencion - Nuevas integraciones de BBVA y ScotiaBank

Archivos

Nombre	:	AplicacionSeguridad00139201093109.zip
MD5	:	45bd6120bbcaefd3de1dcac1a6b104f6
Nombre	:	AplicacionSeguridad00139201093109.msi
MD5	:	bfaead2c1e91e6487d6bb9a721b3182a
Nombre	:	c4tOling.zip
MD5	:	5b9d7f3ac548136b6686e011b76770be
Nombre	:	T0S8HTPUS036PVXE6D331IP0XP8F439Y50EWK
MD5	:	ba5619955ea631ecf2d8f3aa82fce704
Nombre	:	W949Z6FZAC9O47WQ28KE2V7LHZ19NB5KUK
MD5	:	c56b5f0201a3b3de53e561fe76912bfd
Nombre	:	ZD1MWY9LAC0WU8D9ZQQU2WKWSBDSLJUCTNWBI
MD5	:	e96e36321a6ab740767568b1279f246b
Nombre	:	sqlite3.dll
MD5	:	744dcc4cbbfbb18fe3878c4e769ec48f

Imagen Phishing de Correo

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