Alerta de Seguridad Informática (2CMV-00019-001)

Nivel de Riesgo: Alto

Tipo: Phishing - Malware

Fecha de lanzamiento original: 15 de Julio de 2019 | Última revisión 15 de Julio 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 con Malware asociado, a través de un correo electrónico donde los delincuentes buscan engañar a los usuarios insinuando, en el título del correo, que existe una transferencia al exterior y que el Banco BBVA Continental S.A. ha enviado un documento donde puede confirmar la recepción del pago.

Al seleccionar el documento adjunto, se desencadena la descarga de archivos maliciosos que, en realidad, son troyanos tipo RAT que tienen la capacidad de recopilar información sin el consentimiento del usuario, dejando puertas traseras con la posibilidad de infectar con otros malware según sea el propositito del atacante. Estos troyanos tiene una arquitectura de cliente y de servidor.

Indicadores de compromisos

Url's:

191.101.151.15:1414
191.101.151.15:1990

Smtp Host

mailout02[.]t-online[.]de [194.25.134.17]
fwd06.aul[.]t-online[.]de [172.20.26.150]

From: (Original)

ds-technik-scur@t-online[.]de

Subject:

TRANSFERENCIA AL EXTERIOR

Archivos adjuntos

Archivo : Digitalization_15_07_2019.pdf
MD5 : c9f19ee093adde0aed6a60cf542ee0ea
SHA-256 : 4adcfed2024f27c297d29ac1b49dfd3e9c666f2c3fbd0d9e2b8ff908da617ff4

Imagen

BBVA CONTINENTAL S.A <ds-technik-scur@t-online.de>

TRANSFERENCIA AL EXTERIOR

Digitalization_15_07_2019.pdf
294 KB

ATTN:

Encuentra el comprobante de pago transferido a tu cuenta bancaria.

Por favor en contacto con su banco local para confirmar la recepción del pago adjunto.

Un Saludos!

BBVA

Juan Daniel Fernández Fernández
Banca de Empresas e Instituciones - Gestor Interno
Tel +595 21 417 6106 – juandaniel.fernandez.contractor@bbva.com
Mcal. López esq. Torreani Viera, 4° Piso, Asunción - Paraguay

Antes de imprimir este mensaje, por favor comprueba que es necesario hacerlo. Before you print this message please consider if it is really necessary

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

Contactos

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