Alerta de Seguridad Informática (2CMV-00022-001)

Nivel de Riesgo: Alto

Tipo: Phishing - Malware

Fecha de lanzamiento original: 24 de Julio de 2019 | Última revisión 24 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 del Gobierno de Chile (CSIRT), ha identificado una campaña de Phishing con Malware, indicando que existe una copia de pago pendiente en un documento adjunto. El atacante persuade a la víctima para que descargue el documento que presuntamente proviene de Itau Corpbanca. El documento es un archivo ZIP, el que al ser ejecutado desencadena la infección.

Indicadores de compromisos

Smtp Host

- ns18[.]onlinebiz[.]pt [185.80.220.139]

From: (Falso)

- Itaú Corpbanca no_reply@eurobank.com

Subject:

- Notificación de pago

URL

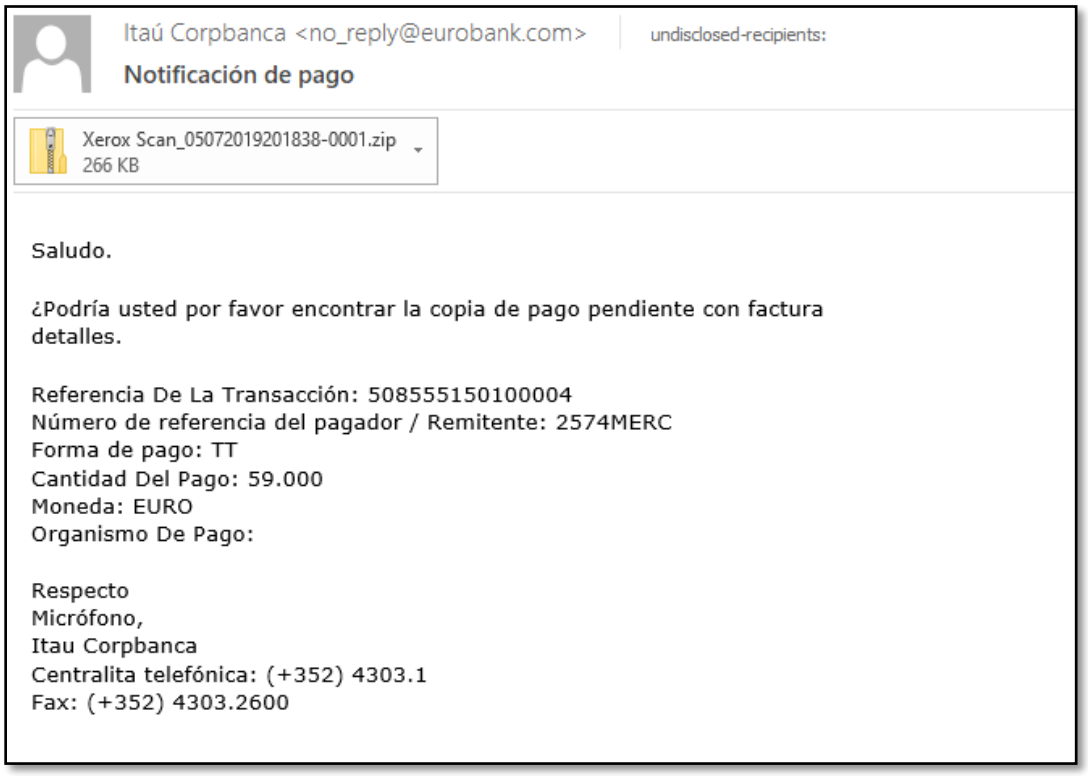
- http[:]//vman21[.]com/ab17/ab17[.]exe
- http[:]//vman21[.]com/ab17/gate[.]php
- http[:]//vman21[.]com/ab15/gate[.]php
- http[:]//vman21[.]com/ab26/ab26[.]exe

Archivo

Nombre : xerox scan_05072019201838-0001[.]zip
MD5 : 9848d2cf5fce84606c2a238a79c59fb8
SHA256 : 09f21e0a6c2f140e4e723f468368e4dd83a31056b12369cc4dc49ca4b36a18d8

Nombre : Xerox Scan_05072019201838-0001[.]bat
MD5 : 8a17e68b97e00a4b22679abeb32b062b
SHA256 : 4a657f440c049465a610220fdcb57f5d5aa3f3a9a4bc874914e357abbd0dec52

Imagen



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

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.07.24 15:15:38 -04'00'