| | |
|---|---|
| Alerta de seguridad informática | 2CMV21-00153-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Malware |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 12 de Marzo de 2021 |
| Última revisión | 12 de Marzo de 2021 |

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 malware supuestamente proveniente de Banco Santander. El atacante busca persuadir a las personas para descargar el archivo adjunto y ser ejecutado.

El mensaje del correo indica que se adjunta una copia del pago que se realizó a su cuenta bancaria. El atacante adjunta un archivo comprimido con extensión ISO, que contiene un archivo EXE que al ser ejecutado gatilla la infección del equipo.

## Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto.

# IoC Correo Electrónico

Datos del encabezado del correo

Servidorres Smtp
108.175.14.66

Correos Electrónicos
santander@venex.com.ar

Asunto
Copia de transferencia de pago

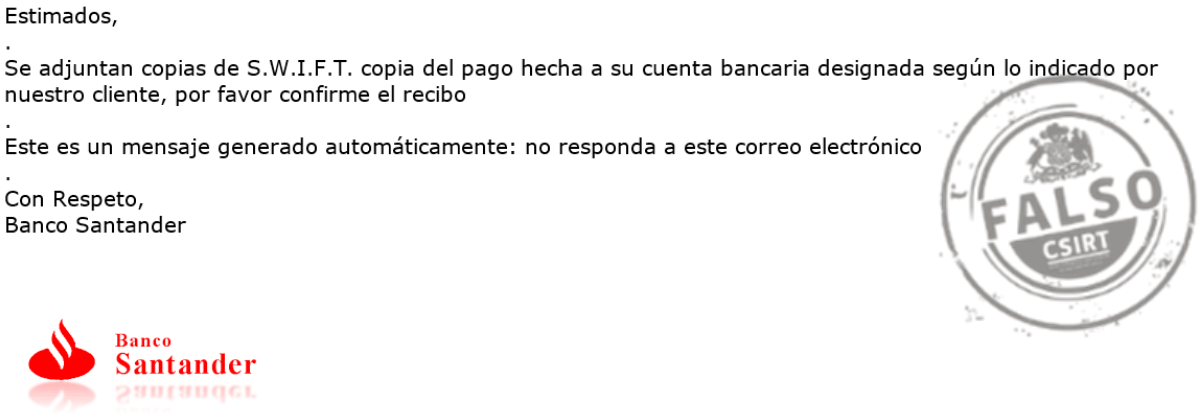
# IoC Archivo Adjunto

Archivos que se encuentran en la amenaza

Nombre : Copia de pago 11_03_21.iso
SHA256 : D7B0B24695FEDABD57E8311EF54CA3A18B38A417508E2D2117707B371373EBB3

Nombre : Copia de pago 11_03_21.exe
SHA256 : 67124B34E5007609FA92B69DD26DB1A1925D0C64E34A5795929DE89DA54D4F20

# Imagen del mensaje


Estimados,
.
Se adjuntan copias de S.W.I.F.T. copia del pago hecha a su cuenta bancaria designada según lo indicado por nuestro cliente, por favor confirme el recibo
.
Este es un mensaje generado automáticamente: no responda a este correo electrónico
.
Con Respeto,
Banco Santander

# Recomendaciones

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet.
- Prestar atención en los detalles de los mensajes o redes sociales.
- 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 sean los oficiales.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.03.12 11:08:53 -03'00'