Alerta de seguridad informática	2CMV21-00215-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de agosto de 2021
Última revisión	19 de agosto 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 de Gobierno) ha identificado una campaña de malware que suplanta a TNT. Con ella, el atacante busca persuadir a las personas de descargar el archivo adjunto y ejecutarlo en el equipo, donde gatillara la infección con malware. El mensaje del correo indica falsamente que se envió un pedido a través de TNT y que este se encuentra programado para su entrega el 24 de agosto.

Observación

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

IoC Correo Electrónico

Datos del encabezado del correo

Servidores SMTP
cp2.loft-dev.live

Correo Electrónico
[postmaster@loft-dev.live]

Asunto
Factura TNT: 07633976

IoC Archivo

Archivos que se encuentran en la amenaza

Nombre : Factura TNT 07633976.zip
SHA256 : 2D23F05BA32B12E837AA34DD9CD41EABBEF0063579BD316A042EC79C82251F66

Nombre : Factura TNT 07633976.exe
SHA256 : 969FF1FB205201B293B0859D5955EFC6109549AAC06F5ED99566AB562FA1B39D

Imagen del mensaje

Estimado cliente,

Se ha organizado un envío para usted a través de TNT.

El envío está programado para su entrega el 24 de agosto de 2020 y tiene el número de envío TNT: 213596003.

DESCRIPCIÓN GENERAL DE LOS DETALLES DEL ENVÍO: (Ver adjunto)

Pieces : 1
Weight : 0.5 KG
Referencia de envío: Factura # 10623-24
Descripción: documento
Descargue el archivo adjunto para obtener la factura y los detalles completos del

envío.

Este mensaje y cualquier archivo adjunto son confidenciales y pueden tener privilegios o estar protegidos de cualquier otro modo contra la divulgación.
Si usted no es el destinatario previsto, por favor llame por teléfono o envíe un correo electrónico al remitente y elimine este mensaje y cualquier archivo adjunto de su sistema.
Si usted no es el destinatario previsto, no debe copiar este mensaje o archivo adjunto ni revelar el contenido a ninguna otra persona.
Por favor, considere el impacto ambiental antes de imprimir este documento y sus anexos.
Imprima en blanco y negro y a doble cara siempre que sea posible.

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: 2021.08.20 10:30:38 -04'00'