Alerta de seguridad informática	2CMV21-00220-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de septiembre de 2021
Última revisión	09 de septiembre 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 nueva campaña de malware. Con ella, el atacante busca persuadir a las personas de descargar un archivo adjunto y ejecutarlo en su equipo. De hacerlo, gatillará la infección de su equipo con malware. Para convencer al destinatario de ejecutar el archivo malicioso, el mensaje del correo señala falsamente que se requiere realizar el pago de un supuesto pedido, para hacer lo cual llaman a hacer clic en un enlace.

Observación

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

IoC Correo Electrónico

Datos del encabezado del correo

Correo electrónico
ysantiago@tifs[.]com

Servidores SMTP
195.33.210.155

Asunto
Factura de proforma

IoC Archivo

Archivos que se encuentran en la amenaza

Nombre : Factura proforma adjunta.zip
SHA256 : 652BC4540760E11A3C230517E8063C55587AA29D3FA132EE9B4D050F0FA77A92

Nombre : Factura proforma adjunta.exe
SHA256 : BDBFB1EB22E055C50DAA28F2F6C0CF8DC03F5FF5EBC229289FCC7739EEFAD60B

Imagen del Mensaje

Hola.

Queremos realizar el pago de este pedido.
Confirme los datos bancarios en la factura proforma para que podamos realizar el pago ahora.
Responde lo antes posible
Saludos.

Gerente de ventas,
Santiago, Yoryiana,
Sistema de fluidos TI,

TI Fluid Systems

Dirección: Mike Allen S / N Parque Industrial Reynosa, 88788 Reynosa Tamaulipas, México.
Teléfono: +52899921 7978
Dirección de correo electrónico: ysantiago@tifs.com

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: 2021.09.09 12:22:52 -03'00'