Alerta de seguridad informática	2CMV21-0235-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de octubre de 2021
Última revisión	18 de octubre 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 phishing con malware que afecta al ciberespacio nacional, donde el atacante busca persuadir a las personas para descargar un archivo adjunto y ejecutarlo en su equipo, gatillándose la infección del malware.

Para convencer a la víctima, el mensaje del correo informa que se adjunta la factura y se agradece la confirmación de la recepción.

Observación

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

IoC Correo Electrónico

Datos del encabezado del correo

Correo electrónico
compras@cotripar.com

Servidor de Correo
[server.grupowies.info]

Asunto
FACTURA EMITIDA F001-1481 X SERV MENSUALES 10/18 AL

IoC Archivo

Archivos que se encuentran en la amenaza

Nombre : FACTURA EMITIDA F001-1481 X SERV MENSUALES 1810.ISO
SHA256 : 67D1BFF9AE5FCD660ACC117C1D4F8F23DE4B6C43163B43514D08958FC31A241E

Nombre : FACTURA EMITIDA F001-1481 X SERV MENSUALES 1810.exe
SHA256 : F56AEBD741C745C86FC0B6BAB9E6BD537E9576DB187A78660D48C817089F5EE8

Imagen del Mensaje

Buenos días,

Adjunto factura N° F001-1481 por los servicios mensuales de alquiler de grúa del período 18/10/21 al 31/11/21.

El monto total de la factura asciende a $ 61,162.95 y el vencimiento para el pago correspondiente es el día 31/11/21.

Agradecemos la confirmación de la recepción, así como los datos de la persona encargada de realizar los pagos.

Saludos.

Rogelio Hartwig

Supervisor repuestos

Hernandarias - Alto Paraná - Paraguay

e-mail: compras@cotripar.com

tel: +595-631-2381 / 22182 / 22183

movil: +595-986-300486

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: 2021.10.18 14:34:54 -03'00'