Alerta de seguridad informática	2CMV21-0229-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de octubre de 2021
Última revisión	05 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 campaña de malware. En ella, el atacante busca persuadir a las personas de descargar el archivo que viene adjunto y que este sea ejecutado en el equipo, donde gatillara una infección con malware. El mensaje del correo indica falsamente que se adjunta una cotización.

Observación

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

IoC Correo Electrónico

Datos del encabezado del correo

Correo electrónico
cjavier.benito@grupoantolin.com

Servidor de Correo
bizcloud-mtk0.ciceroinc.com

Asunto
REQUISICIÓN N° 0002-0002017065

IoC Archivo

Archivos que se encuentran en la amenaza

Nombre : N° 0002.rar
SHA256 : D51EC30DA8DE0B7487119F9501A6710EA582C5B7A21E023A37F1E356BE77CEEB

Nombre : N° 0002.exe
SHA256 : 44DC661DCA92EFFF41CC571F43370D5BA77280EF8D4386B6DD902334C864F2F6

Nombre : N° 0001.7z
SHA256 :8BD2DEBCDB3C6E54B4042D937478B1CABD8AA00824687F35B1DE14990FCF0B43

Nombre : N° 0001.exe
SHA256 : 184F46651603FCCCCBBA6AB8283A1551C8B41213E1B2522493E4B309E5FFCF56

Imagen del Mensaje

Buenos dias,

Aquí se adjunta nuestra nueva solicitud de cotización para su atención.

Considere sus mejores precios y tiempo de entrega.

Agradeceré su amable respuesta.

Gracias

Saludos
Carlos Javier

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: 2021.10.05 15:11:03 -03'00'