Alerta de seguridad informática	2CMV21-0226-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de octubre de 2021
Última revisión	01 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 malware que amenaza el ciberespacio nacional. En ella, el atacante busca persuadir a las personas para descargar el archivo adjunto y ser ejecutado en el equipo, donde gatillara la infección del malware. El mensaje del correo indica falsamente que se adjunta una factura pendiente de pago.

Observación

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

IoC Correo Electrónico

Datos del encabezado del correo

Correo electrónico
intemo.reymsa@gmail.com

Servidores SMTP
[138.197.163.80]

Asunto
Facturas Pendientes

IoC Archivo

Archivos que se encuentran en la amenaza

Nombre : 01102021FP.cab
SHA256 : 7D2CF7D6F460E143C8E55CE0F4EA1F4F5C8D20374A7DB6BB25493FEE1C8DFF7A

Nombre : fvbgr12345.exe
SHA256 : 7249D67D49A862E577120D3125E33566C61241969B4F48D701DE97A5FE0ABC04

Imagen del mensaje

Buen día

Adjunto envió facturas pendientes de pago, en caso de haber realizado el pago correspondiente agradecería enviar el comprobante de pago, o en su defecto fecha programada para pago.

Quedo a sus órdenes para cualquier duda o comentario.

Un saludo.

Gabriela Crespo
Administration

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 10:35:24 -03'00'