Alerta de seguridad informática	2CMV22-00309-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de Agosto de 2022
Última revisión	9 de Agosto de 2022

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 phishing con malware. El mensaje es enviado supuestamente de la empresa Heinz-Glas. En esta campaña, los delincuentes indican falsamente a la víctima que se adjunta nuevo pedido. Al descargarlo y ejecutarlo (abrir el archivo) se realizará la infección del equipo por parre de un programa malicioso (malware) tipo troyano.

Observación

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

IoC Correo Electrónico

Datos del encabezado del correo

Asunto
Nueva solicitud

Correo de salida
Teresa.Novillo@heinz-glas[.]com

IoC Archivo

Archivos que se encuentran en la amenaza

Nombre: Nuevo pedido adjunto.zip
SHA256: 1eb8d76fd884aa3574449f0e7f3d7551e670f0f181252d669b717e29c35db3c5

Nombre: Nuevo pedido adjunto.exe
SHA256: a5587070de0961536ff5d59569a7733fd58f74953a69bfd46e3c38cabb95d378

Imagen del mensaje

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: 2022.08.09 09:08:57 -04'00'