Alerta de seguridad informática	2CMV21-00219-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de septiembre de 2021
Última revisión	03 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. En ella, el atacante busca persuadir a los receptores de descargar el archivo adjunto y ser ejecutarlo en el equipo, donde gatillará una infección con malware. Para convencer a la víctima de hacer clic en el archivo, el mensaje del correo señala falsamente que se requiere una supuesta cotización urgente.

Observación

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

IoC Correo Electrónico

Datos del encabezado del correo

Servidores SMTP
bizcloud-mtk0.cardenas[.]bar

Asunto
Solicitud de cotización

IoC Archivo

Archivos que se encuentran en la amenaza

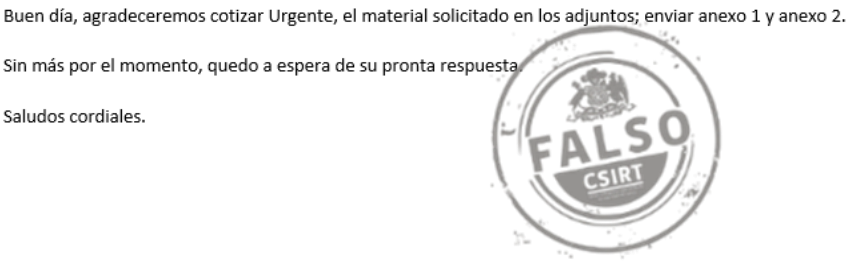
Nombre : 30707475486_019_00003_00000223.cab
SHA256 : FEF392F98572CB50481B1A5613927743A2BD4C5E3B0F13844E52908564638A97

Nombre : bth09123.exe
SHA256 : 9828BFE3D475FCC606327F7F3340CE2BDABE44A5A5866903DAA21EE931F0FD42

IoC Red

http://bulverderoofing[.]com/lt0h
https://img.neko[.]airforce/files/gzzztn

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: 2021.09.03 11:55:01 -04'00'