Alerta de seguridad informática	2CMV21-00159-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Marzo de 2021
Última revisión	29 de Marzo 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), ha identificado una campaña de malware. El atacante busca persuadir a las personas de descargar el archivo adjunto contenido en el email y ejecutarlo.

El mensaje del correo indica que contiene los costos de una orden de compra. El atacante adjunta un archivo con extensión .DOC para ser descargado, el que al ser ejecutado gatilla la infección del equipo.

Observación

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

IoC Correo Electrónico

Datos del encabezado del correo

Servidores Smtp
[185.82.126.149]

Correo Electrónico
inf0@agbadogun.site

Asunto
Re: Solicitud de costo de orden de compra

IoC Archivo Adjunto

Archivos que se encuentran en la amenaza

Nombre : PO33273-CSFM.doc
SHA256 : 87A90A46CEE92BC5DD281628F12B2431FC418F3EAB21AFB6BDE86D59D470CA5B

IoC Comunicación de Red

URL

http://cfsmarthome[.]net/0/

https://u.teknik[.]io/mG0i6.jpg

Imagen del mensaje

Buenos días,

Espero que estés bien,

Por favor, puede proporcionar sus costos con respecto a la orden de compra 33273,

Muchas gracias,

Maria Yaundé
Departamento de cuentas
Fezeco Trading L.L.C

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: 2021.03.30 18:35:58 -03'00'