Alerta de seguridad informática	2CMV21-0234-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de octubre de 2021
Última revisión	14 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 phishing con malware que afecta al ciberespacio nacional. A través de ella, el atacante busca persuadir a las personas que reciben sus mensajes de descargar un archivo adjunto y ejecutarlo en su equipo, donde gatillara la infección con malware. Para convencer a la víctima, el mensaje del correo señala falsamente que se adjuntó orden de compra, siendo realmente un documento malicioso.

Observación

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

IoC Correo Electrónico

Datos del encabezado del correo

Correo electrónico
ventas1@suministrosmorsan.com.mx

Servidor de Correo
[195.33.210.155]

Asunto
Re: Re: Re: Re: Re: Re: Nuevo orden

IoC Archivo

Archivos que se encuentran en la amenaza

Nombre : DBS.cab
SHA256 : A8FD3B40DFDD6ADD285CAA0670B678A6FC7C65CBF1BA487FED174789CCB7793

Nombre : ghfg5776exe
SHA256 : 90BE634820B42505DA42769E83EBC62AB133090C810B64140C551FC4136C5FE7

Nombre : lfsqlrxc.dll
SHA256 : 0605BA2116585EB673DEA3125F0E48DCF90AC52A3E8725DF986EDDFF467A2B47

Imagen del Mensaje

Buen día

Adjunto orden de compra urgente, debido a un pedido especial que nos ingresó.

Agradeceré revisar si pueden entregarnos este viernes 15/octubre.

Quedo a la espera.

atentamente,

Silvia Venturini
Compras

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: 2021.10.14 16:15:55 -03'00'