Alerta de seguridad informática	2CMV21-0231-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de octubre de 2021
Última revisión	12 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), ha identificado una campaña de malware en la cual el atacante busca persuadir a las personas de descargar un archivo adjunto y ejecutarlo en su equipo, donde gatillará la infección con malware. El mensaje del correo señala falsamente que "se ha procesado un 30% de la factura enviada" para un supuesto pedido, siendo la pretendida factura realmente el programa malicioso.

Observación

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

IoC Correo Electrónico

Datos del encabezado del correo

Correo electrónico
thompson@bradfords.com

Servidor de Correo
[38.103.244.107]

Asunto
Prueba de pago

IoC Archivo

Archivos que se encuentran en la amenaza

Nombre : Nota de pago.zip
SHA256 : BAF44BB98D0A2D4B651A8A1785AE58DAC47692B296F4807614B9894434CBB09F

Nombre : Nota de pago.exe
SHA256 : F67B83F5CFB5D9EEE0B50739AEEE606E79B627AF3409A9730BC7B02CBC45F9B0

IoC Archivo

Trafico a SMTP “@xb-inb.com”

Imagen del Mensaje

Buen día señor

Hoy, procesamos el 30% de la factura enviada para nuestro pedido como archivo adjunto, confirme que recibió esta copia del pago.

El respeto,
Thompson Wood

Bradfords Bemis Company Inc.
300 Mill Street
Buzón 901
Sheboygan Falls, WI 53085-0901 Estados Unidos
Teléfono: +926.469.4621.
Teléfono = + 9221-32466481
Envíe por fax: + 9221-32466428
Teléfono móvil = + 929345-2478830

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: 2021.10.12 11:36:39 -03'00'