Alerta de seguridad informática	2CMV21-00214-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de agosto de 2021
Última revisión	19 de agosto 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 las personas para descargar el archivo adjunto y ejecutarlo en el equipo, donde gatillará la infección con malware. El mensaje del correo indica falsamente que se pagó el 30% de una supuesta factura.

Observación

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

IoC Correo Electrónico

Datos del encabezado del correo

Servidores SMTP
ns1.omnis.com

Correo Electrónico
[isabel.alvarev@bci.com]

Asunto
Transferencia

IoC Archivo

Archivos que se encuentran en la amenaza

Nombre : TRANSFERECIA VPC 51,874.00 USD.zip
SHA256 : 5D3245861842E4B8DE436C0423072FB3CEA02F991F611B52637E7634B2CF8F66

Nombre : TRANSFERECIA VPC 51,874.00 USD.exe
SHA256 : BE63B5F1E9EEB9CB151ECEB866B338626026F606A2656F3545651C94078821CC

Imagen del mensaje

Buenos días Señor,

Hoy procesamos como adjunto el pago del 30% de la factura enviada en relación con nuestro pedido, por favor confirme la recepción de esta copia de pago.

Respecto,
Isabel Álvarez
Bemis Company Inc.
300 Mill Street
P. O. Box 901
Sheboygan Falls, WI 53085-0901 Estados Unidos
Teléfono: +926.469.4621.
Teléfono = + 9221-32466481
Fax: + 9221-32466428
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: 2021.08.20 10:13:58 -04'00'