Alerta de seguridad informática	2CMV21-0221-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de septiembre de 2021
Última revisión	09 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 las personas que reciben su email de descargar el archivo que viene adjunto y ejecutarlo en su equipo, donde gatillara una infección con malware. Para convencer a la víctima, el mensaje del correo menciona un falso abono que espera ser redimido por el receptor.

Observación

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

IoC Correo Electrónico

Datos del encabezado del correo

Correo electrónico
contacto@commonsense[.]cl

Servidores SMTP
vcct16007.avnam.net

Asunto
Factura de proforma

IoC Archivo

Archivos que se encuentran en la amenaza

Nombre : INV1034391.ISO
SHA256 : ED907DDF528A4DF0B078AC4B1B8949F429B59ECFC96EE4426E90A102AA6F66EF

Nombre : INV1034391.exe
SHA256 : 9710BAC1236CCC3B80610209B7F03732BE51FA32BC2A4814878EC9C2CC027AC7

Imagen del Mensaje

Hola

Acorde a lo conversado:

El día viernes se hizo el abono aplicando la retención correspondiente; por norma según SUNAT tenemos 7 días hábiles para el envío de la constancia, sin embargo, te lo enviaremos a la brevedad posible.

Agradecido por la atención.

Quedamos atentos.

Saludos.

Lic. Iskra Véliz Blacutt.

Ag. Desp. de Aduana Véliz S.R.L.
Teléfono: 4010411.
Móvil personal 76476667.
Cochabamba-Bolivia.

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: 2021.09.09 17:46:28 -03'00'