Alerta de seguridad informática	2CMV20-00120-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Diciembre de 2020
Última revisión	17 de Diciembre de 2020

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 a través de un correo electrónico que utiliza el nombre de la compañía SIAN WHILESSALE.

El atacante busca persuadir a las personas para descargar el archivo adjunto y ser ejecutado.

El mensaje del correo indica que se realizó el nuevo pedido No. S77u/1220 y debe descargar la factura adjunta en el correo.

El atacante adjunta un archivo .ZIP que supuestamente es la factura, el cual contiene un archivo .exe 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:

Servidor Smtp
[198.46.81.48]

Sender
hakam@sevenarrow-jo.com

Asunto
Proforma Invoice & Shipping Schedule

IoC Archivo Adjunto

Archivos que se encontraban adjunto en el correo:

Nombre: Proforma Invoice.Pdf.rar
SHA256: 3A3E74C5B52D1CF2308A276952F92C2954A7F6AD064D18334EF0129DD4DD4829

Nombre: Q7QE40EiLEt9UeN.exe
SHA256: E6633B5015CAD9D0A683B91202358E01F0E568E1A5F333F0FFBC5B4E3E8B1FB8

IoC Urls

Comunicación de red:

Url's

http://azzmtool.com/kin/kin1/fre.php

Imagen del mensaje

Mensaje Proforma Invoice.Pdf.rar (386 KB)

Good Morning

Thank you very much for placing new order No.S77u/1220

Please kindly find attached Proforma invoice No. FC-091218 for your reference.

Many thanks,

Emma

Emma Ellen

Sales Manager

T: +44 (0)1306 621060 **D:** +44 (0)1306 621252 M: +447590 426856 www.sianwholesale.com

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.