Alerta de seguridad informática	2CMV21-00238-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de octubre de 2021
Última revisión	19 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 phishing con malware. El atacante busca persuadir a las personas para descargar un archivo adjunto, el cual al ser ejecutado gatillará la infección del malware en el equipo. El mensaje del correo informa que se requiere una cotización de los materiales que se envían en el archivo adjunto.

Observación

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

IoC Correo Electrónico

Datos del encabezado del correo

Correo electrónico
gpaliza@budeguer[.]com

Servidor de Correo
[143.110.208.19]

Asunto
Solicitud de Cotización Nº 11536

IoC Archivo

Archivos que se encuentran en la amenaza

Nombre : 64892922.cab
SHA256 : 38E1C5A41DDCC6B3571BE6368F397F6A3B450E2DE30D18189E7D35C0A4A39050

Nombre : rrwq200123.exe
SHA256 : E5EBC473E259EC57E2A831477B449DD07C13198C0DB74CE67732A8FCE59E25AC

Nombre : ylbzgkuxqsi.dll
SHA256 : 23E80D01CF007B17F91366FB1866568F0385FF08767434728F209535D3452FDD

Nombre : 2w7qirwuhiwtme
SHA256 : 7008543C4A44B254EBB0B84F36B96D62866C3B57AD698F3765CA7D5E77831600

IoC Red

www.doeful[.]com/rv9n
www.discountcouponcodes-jp[.]space/rv9n/
www.cjspizza[.]net/rv9n/
www.novaprint[.]pro
www.longhang[.]xyz
www.schwa-bingcorp[.]com

Imagen del Mensaje

Solicitud de Cotización N° 11536

GP Gonzalo Paliza <gpaliza@budeguer.com>
Para

Se han quitado los saltos de línea adicionales de este mensaje.

64892922.cab
241 KB

Buenos días, nos dirigimos a Ud. Con el fin de solicitar la cotización de los siguientes materiales a nombre de Compañía Inversora Industrial S.A:

*Por favor indicar plazo de entrega.

Quedamos a disposición ante cualquier consulta.

Saludos

Gonzalo Paliza

Compras - Grupo Budeguer

Tel: +54 9 381 453 6590 Int. 1133

Cel: +54 9 381 603 9966

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.