Alerta de seguridad informática	2CMV20-00121-01
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 Tarpulin.

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

El mensaje del correo indica que envía una solicitud de cotización y una factura por los pedidos realizados.

El atacante adjunta dos archivos .GZ comprimidos, los que supuestamente son la cotización y la factura, pero contienen un archivo .src 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
[128.199.79.199]

Sender
mail@portaer.xyz

Asunto
Orden de compra

IoC Archivo Adjunto

Archivos que se encontraban adjunto en el correo

Nombre: IMG-20181024-WA0005_pdf.gz
SHA256: 69648D3959A59C225107CCFAE22AF07745841655B04DFBD61173E91FB580BC80

Nombre: KAKLEBI EUROPRODUCT_pdf.scr
SHA256: FC956A2B7D33E3DE5063028A0852B2FB1E86EAA91BCF469B157032852F281211

Imagen del mensaje

Para undisclosed-recipients:

Mensaje | IMG-20181024-WA0005_pdf.gz (2 MB) | KAKLEBI EUROPRODUCT_pdf.gz (2 MB)

Hola,

Espero que estés bien.

Se adjunta una nueva solicitud de cotización.
También envíeme una factura por los pedidos adjuntos.

BR

Gonzalo Aránguiz
Jefe de Proyectos Industrial

Central +56223477600
Directo +56223477633
Celular +56983608547

garanguiz@tarpulin.cl
www.tarpulin.cl
Gladys Marín Millie 6290, Estación Central, Santiago
TARPULIN® GL events Group
www.gl-events.cl - www.gl-events.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.