Alerta de Seguridad Informática (2CMV-00018-001)

Nivel de Riesgo: Alto

Tipo: Phishing - Malware

Fecha de lanzamiento original: 15 de Julio de 2019 | Última revisión 15 de Julio de 2019

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 del Gobierno de Chile (CSIRT), ha identificado una campaña de Phishing con Malware asociado, a través de un correo electrónico donde los delincuentes buscan engañar a los usuarios insinuando en el título del correo que se trataría de una copia de factura, de la empresa Hellmann Worldwide S.A.

Al seleccionar la imagen adjunta, se desencadena la descarga de archivos maliciosos que tienen la capacidad de recopilar información sin el consentimiento del usuario, dejando puertas traseras con la posibilidad de infectar con otros malware según sea el propositito del atacante.

Indicadores de compromisos

Url's:

https[:]//www[.]mediafire[.]com/file/zmqwkf303k9wg12/COPIAS_DE_FACTURAS_REMITADAS[.]7z

Smtp Host

srv205[.]artexsaigon[.]com[.]vn [210.211.117.205]

From: (Original)

bachthao@artexsaigon.com.vn
imex@artexsaigon.com.vn

Subject:

COPIAS DE FACTURAS REMITADAS
FACTURA PARA NUEVO PAGO

Archivos adjuntos

Archivo : COPIAS DE FACTURAS REMITADAS.exe
MD5 : 7f9b3d1b03cc7f49788ec5610c711bf4
SHA-256 : 4f7d10102d35976b1b10a7a03002bd0d98cfc25ea20c7d90dc7080d06930a759

Imagen

Pilar Rodriguez <bachthao@artexsaigon.com.vn> | undisclosed-recipients:

COPIAS DE FACTURAS REMITADAS

Buen día,
Espero que el email te encuentre bien.
Copia de la factura de pago y el recibo TT suministrados para su revisión y confirmación.

Saludos
Pilar rodriguez
Director contable
Hellmann Worldwide S.A.
Av.de Aragón, 334-1º Pl-Pg. Las mercedes
Madrid españa 28022

Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras)
- 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

Contactos

https://www.csirt.gob.cl
+ (562) 24863850
@CSIRTGOB
https://www.linkedin.com/company/csirt-gob