Alerta de seguridad informática	2CMV21-0239-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de octubre de 2021
Última revisión	25 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 el archivo adjunto y ser ejecutado en el equipo, donde gatillará la infección del malware. El mensaje del correo informa que se adjuntan, supuestamente, los documentos de envío originales según lo consignado por el cliente.

Observación

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

IoC Correo Electrónico

Datos del encabezado del correo

Correo electrónico
@exprecohn.com

Servidor de Correo
[hwsrv-913001.hostwindsdns.com - 142.11.216.88]

Asunto
Su confirmación / notificación de envío de DHL Express

IoC Archivo

Archivos que se encuentran en la amenaza

Nombre : Dhl_WX678.img
SHA256 : 682C6CEECD131B1D921137C402CBD0FDFE3921CBB07342082D379FC0D463C8AC

Nombre : rrwq200123.exe
SHA256 : 3B8333C95F03BCEFC683AC075A6F3629DE98D38B3766498323E95F6C73CA6BEB

IoC Red

http://kbfvzoboss.bid/alien/fre.php
http://alphastand.trade/alien/fre.php
http://alphastand.win/alien/fre.php
http://alphastand.top/alien/fre.php
http://63.250.40.204/~wpdemo/file.php?search=8376882

Imagen del Mensaje

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: 2021.10.25 16:14:33 -03'00'