Alerta de seguridad cibernética	2CMV20-00065-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de Mayo de 2020
Última revisión	19 de Mayo 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 Carabineros de Chile.
El atacante intenta persuadir a las personas para descargar un archivo adjunto al correo.
El mensaje del correo invita a quien lo recibe a participar de una investigación en curso sin explicar más detalles al respeto, y sugiriendo a la víctima que revise los antecedentes y se contacte con su abogado de existir la necesidad.
Si la persona selecciona el enlace se produce la descarga de un archivo JAR, el cual, al ser descomprimido, permite obtener otro archivo con extensión EXE. Al ser ejecutado, se descarga un malware.

Indicadores de compromisos

Asunto
Invitación final de los Carabineros de Chile.

Conexión IP:
172[.]111[.]188[.]199

Hash

Archivo : PDF.exe
MD5 : a545c585fdb84c6e92484da233292e25

Archivo : YuhOvQLEAEK.exe
MD5 : a545c585fdb84c6e92484da233292e25

Archivo: run.dat
MD5 : 438993a366406c987edd9cb1d13eda9c

Imagen del mensaje

De: Carabineros de Chile <invitations@carabineros.cl>
Para: undisclosed-recipients:
CC:
Asunto: Invitación final de los Carabineros de Chile.
Mensaje | PDF.arj (319 KB)

CARABINEROS DE CHILE
ORDEN Y PATRIA

Cumplidos,

Esperamos que acepte esta carta de buena fe.

Por este aviso, usted está invitado a
Carabineros de Chile sobre una investigación en curso.

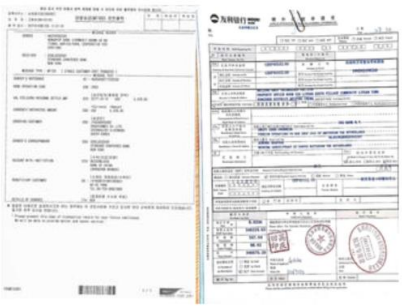
Revise los documentos adjuntos para obtener información y comuníquese con su abogado si es necesario.

Fecha: 3 de mayo de 2020.
Hora: 11:00 a.m.

Gracias,

Mario Rozas

Elías Fernández Albano 165,
Santiago, Región Metropolitana, Chile



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.