Alerta de seguridad cibernética	2CMV20-00064-01
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 que la víctima abra un archivo adjunto en el cuerpo del correo.
El mensaje consiste en una invitación para una investigación en curso enviada por el Director de la Policía de Investigaciones. El correo utiliza el nombre de Carabineros de Chile, así como los símbolos de Bomberos y la Policía de Investigaciones, PDI.
Al seleccionar 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, descarga un malware.

Indicadores de compromisos

Asunto
Carta de invitación

DNS
atiku2[.]duckdns[.]org

Conexión IP:
185[.]165[.]153[.]28

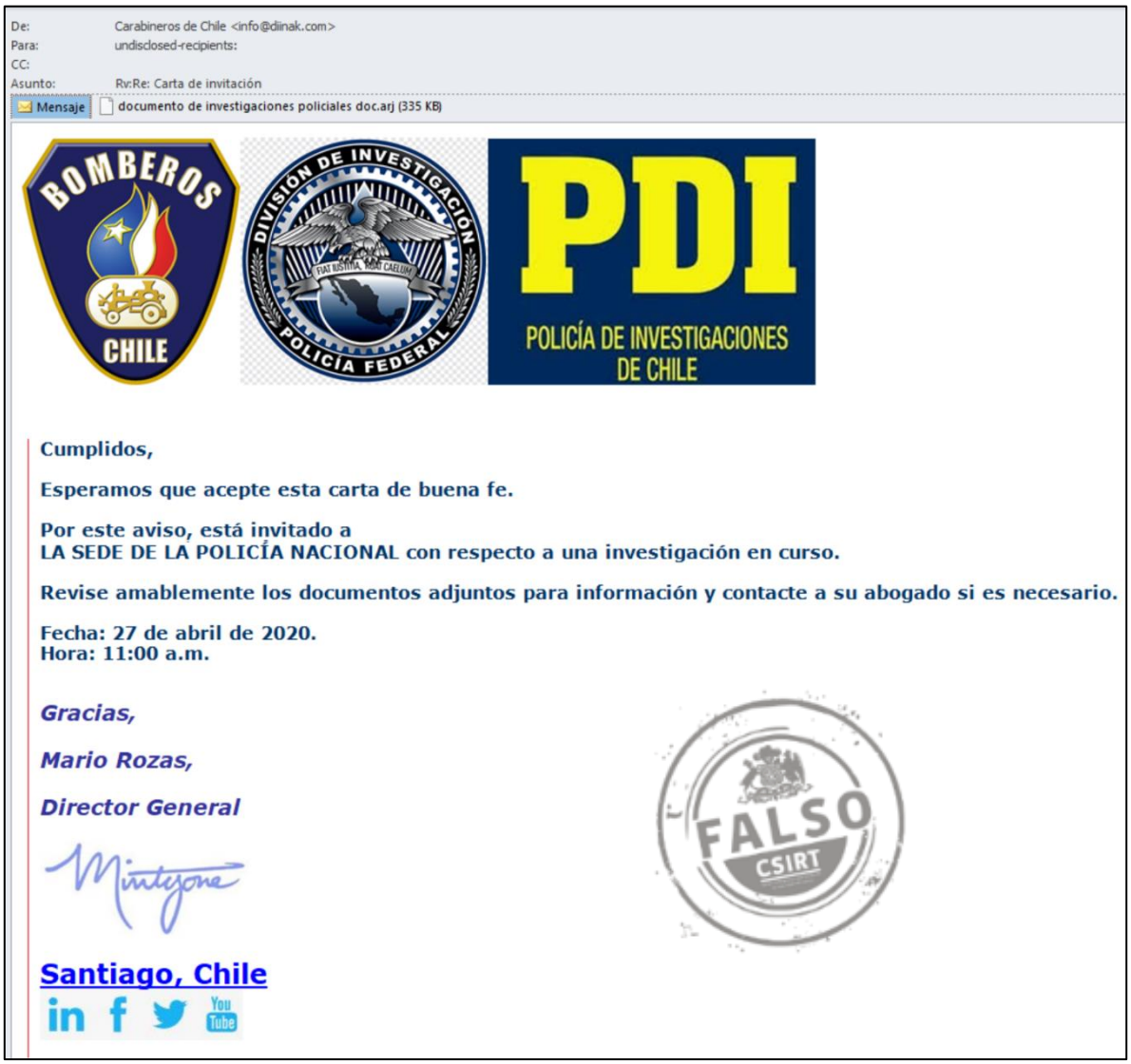
Hash

Archivo : documento de investigaciones policiales doc.exe
MD5 : 3d04bc54174218f4cc83d97a32e7ee73

Archivo : goNcIKPXKGrGKW.exe
MD5 : 3d04bc54174218f4cc83d97a32e7ee73

Archivo: MSBuild.exe
MD5 : 6c6762e46a8281edd32f9cfd81181406

Imagen del mensaje



De: Carabineros de Chile <info@diinak.com>
Para: undisclosed-recipients:
CC:
Asunto: Rv:Re: Carta de invitación
Mensaje documento de investigaciones policiales doc.arj (335 KB)

BOMBEROS CHILE

DIVISIÓN DE INVESTIGACIÓN POLICÍA FEDERAL

PDI
POLICÍA DE INVESTIGACIONES DE CHILE

Cumplidos,

Esperamos que acepte esta carta de buena fe.

Por este aviso, está invitado a
LA SEDE DE LA POLICÍA NACIONAL con respecto a una investigación en curso.

Revise amablemente los documentos adjuntos para información y contacte a su abogado si es necesario.

Fecha: 27 de abril de 2020.
Hora: 11:00 a.m.

Gracias,

Mario Rozas,

Director General

FALSO CSIRT

Santiago, 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.

CSIRT Gobierno de Chile Firmado digitalmente por CSIRT Gobierno de Chile Fecha: 2020.05.19 19:22:28 -04'00'