Alerta de Seguridad Informática (8FPH-00018-001)

Nivel de Riesgo: Alto

Tipo: Phishing-Malware

Fecha de lanzamiento Original: 09 de Mayo de 2019 | Última revisión 09 de Mayo 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 (CSIRT), ha identificado una campaña de Phishing-Malware través de un correo electrónico que busca engañar a las personas que lo reciben, haciéndoles creer que deben presentarse a la Corte Suprema para comparecer en un día específico, por un supuesto caso que afecta a una empresa ficticia asociada a la persona.

El documento adjuntando realiza una vinculación a una URL maliciosa utilizando la vulnerabilidad CVE-2017-0199.

Indicadores de compromisos

Url's: (Payload delivery)

http[:]//avanscure[.]ml/2/123.doc

Archivos adjuntos

3fb7051945e875a7f5bc694c69ca9de37338075e91596ca8e2e32deebe238b75

Smtp Host

sales.axa.co.id [117.54.124.44]

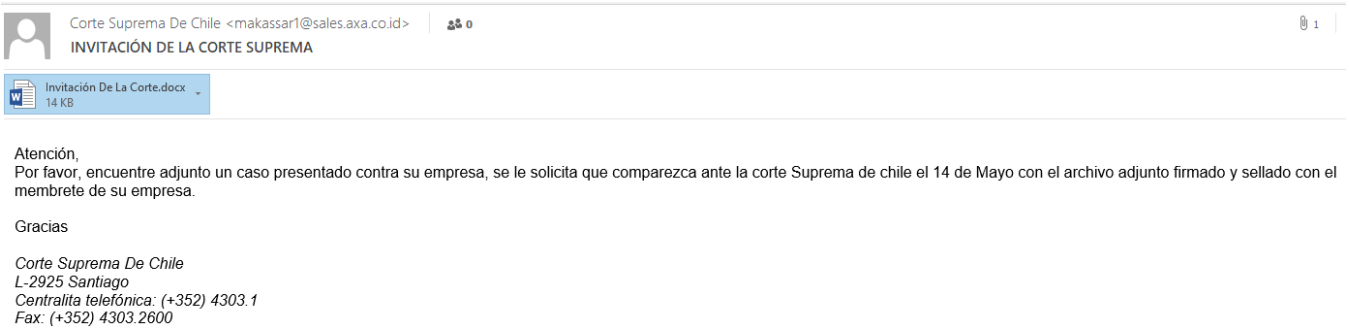
From:

Corte Suprema De Chile <makassar1@sales.axa.co.id>

Subject:

INVITACIÓN DE LA CORTE SUPREMA

Imagen


Corte Suprema De Chile <makassar1@sales.axa.co.id> 0 1
INVITACIÓN DE LA CORTE SUPREMA
Invitación De La Corte.docx
14 KB

Atención,
Por favor, encuentre adjunto un caso presentado contra su empresa, se le solicita que comparezca ante la corte Suprema de chile el 14 de Mayo con el archivo adjunto firmado y sellado con el membrete de su empresa.

Gracias

Corte Suprema De Chile
L-2925 Santiago
Centralita telefónica: (+352) 4303.1
Fax: (+352) 4303.2600

Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java, entre 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
https://www. linkedin.com/company/csirt-gob
@CSIRTGOB