Alerta de seguridad informática	2CMV-00038-001
Clase de alerta	Fraude
Tipo de incidente	Phishing - Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Noviembre de 2019
Última revisión	06 de Noviembre 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 detectado una campaña de phishing con malware asociado, a través de un correo electrónico suplantando al Ministerio de Justicia y Derechos Humanos.

Los estafadores buscan engañar a los usuarios advirtiéndoles que existe un proceso criminal en su nombre y que tienen un plazo de 48 horas para recurrir en su defensa. A la potencial víctima se le ofrece la posibilidad de descargar desde un enlace en el correo, una copia del proceso judicial. Al seleccionar el hipervínculo, la víctima es direccionada automáticamente hasta página donde se descarga el archivo malicioso.

Indicadores de compromisos

Url's:

http://medianews[.]ge/_manager/img/public[.]php
http[:]//18[.]209[.]163[.]113/cont/puma[.]php
http[:]//www[.]mckenzie[.]com[.]br/bkp/fonts/_notes/p0reXacnelt0[.]zip

Sender

www-data@[103.3.60.67]
www-data@[172.104.23.84]
www-data@[97.107.135.6]
www-data@[172.105.115.130]
www-data@[172.104.6.250]
www-data@[139.162.43.238]
www-data@[172.104.212.190]
www-data@[45.33.30.117]
www-data@[45.79.17.145]
www-data@[45.79.37.95]
www-data@[172.105.222.144]

Smtp Host

li828-67[.]members[.]linode[.]com	[103.3.60.67]
li1842-84[.]members[.]linode[.]com	[172.104.23.84]
li65-6[.]members[.]linode[.]com	[97.107.135.6]
li2008-130[.]members[.]linode[.]com	[172.105.115.130]
li1742-250[.]members[.]linode[.]com	[172.104.6.250]
li1456-238[.]members[.]linode[.]com	[139.162.43.238]
li1922-190[.]members[.]linode[.]com	[172.104.212.190]
li1047-117[.]members[.]linode[.]com	[45.33.30.117]
li1116-145[.]members[.]linode[.]com	[45.79.17.145]
li1136-95[.]members[.]linode[.]com	[45.79.37.95]
li1876-144[.]members[.]linode[.]com	[172.105.222.144]

Subject:

Informamos que hoy se ha abierto un proceso criminal en su nombre.

Archivos

Nombre : 00PROCESO070083204256129_.zip
MD5 : ea917166e0a28f8ce63773e709b6723f

Nombre : CAENDELH9123243051.msi
MD5 : 691f542935f7c8ae675c88e4021eef83

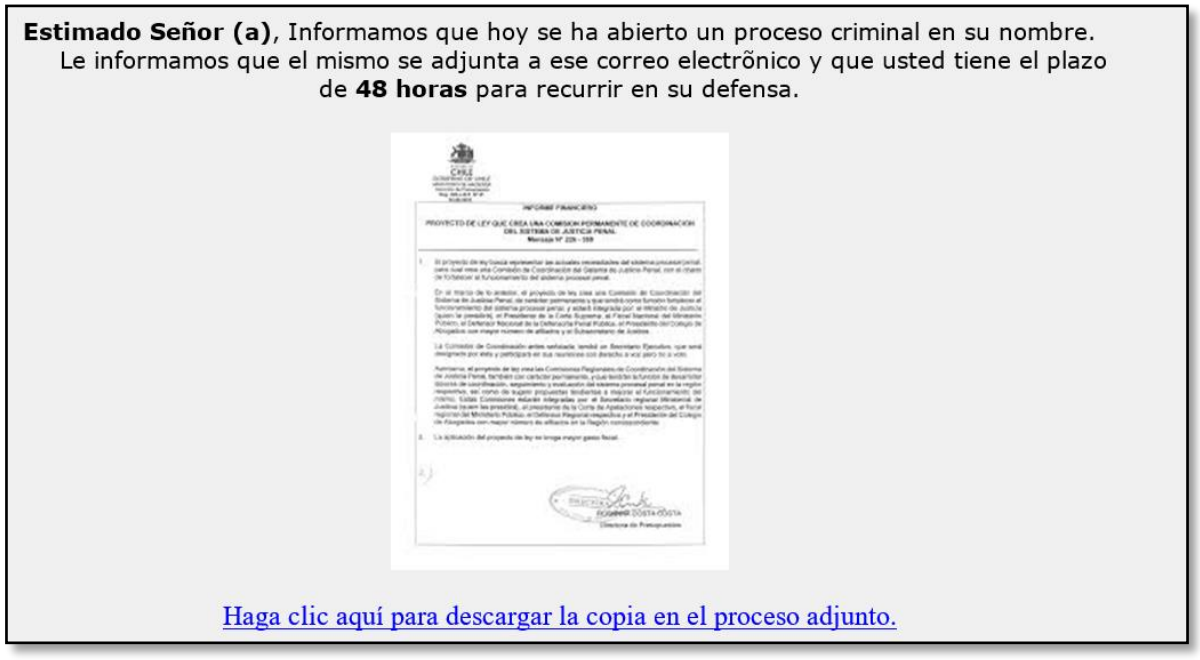
Nombre : p0reXacnelt0.zip
MD5 : ad28459e8ce3419b2a83a4923c2288c6

Nombre : Q2Y9JO0ELC7VXV6G2AVQHECVFFDFJ49IOC
MD5 : b0d0e310cf0f1c6adc65057d0217196d

Nombre : TOB1PM9H0FLX4KVTYQ5ODV4NCYS91H7K963MC
MD5 : 26d838856d2867ef7d286ed649b55878

Nombre : JUKEQPXB8ZY54D2CLKJC9VWRZUTMEA37LKKI
MD5 : c56b5f0201a3b3de53e561fe76912bfd

Imagen Phising de Correo



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

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.11.06 10:13:35 -03'00'