Alerta de Seguridad Informática (2CMV-00023-001)

Nivel de Riesgo: Alto

Tipo: Phishing - Malware

Fecha de lanzamiento original: 25 de Julio de 2019 | Última revisión 25 de Julio 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 con Malware asociado, a través de un correo electrónico que supuestamente proviene del Ministerio de Justicia y Derechos Humanos

Los delincuentes buscan engañar a los usuarios advirtiéndoles de la falsa apertura de un proceso criminal en su contra, teniendo un plazo de 48 horas para recurrir en su defensa. Para facilitar el trámite, se adjunta en el correo una copia del proceso, un archivo en formato ZIP que al ser ejecutado desencadena la infección del malware que tiene la capacidad de recopilar información sin el consentimiento del usuario, dejando además, puertas traseras con la posibilidad de infectar con otros malware según sea el propositito del atacante.

Indicadores de compromisos

Url's:

- https[:]//fv1-2.failiem[.]lv/down[.]php
- http[:]//descargadoc[.]com/downs/?descargar
- https[:]//files[.]fm/pa/Joshua-bueno/2019-07-24_qg2z6ey6/docs_download[.]zip
- https[:]//files[.]fm/down[.]php
- http[:]//m.berel[.]com[.]mx/modules/node/tf4/AhOjtVSg2KJ06E0IE5K2444KCI0CA8F8DNLBAF[.]txt
- http[:]//www.autoitscript[.]com/autoit3/0

Smtp Host

[185.206.215.245]
[185.206.215.242]
[185.206.215.248]
[185.206.215.240]
[185.206.215.246]
[185.206.215.247]
[185.206.215.241]
[185.206.214.164]
[185.206.214.162]
[185.206.214.163]
[185.206.214.168]
[185.206.214.166]
[185.206.214.167]
[185.206.214.169]

From: (Original)

- root@zomro[.]com
- root@cp.zomro[.]com

Subject:

Aviso (Justicia)

Archivos adjuntos

Archivo : docs_download.zip
MD5 : 5769bc87b01321a1e7a171b7578efb26
SHA-256 : cd0acd78be8e691f6d19bcb0f2035b50b1ee4ae8d9e1ab457d4e69c4360ebb58

Archivo : docs_download.cmd
MD5 : 42bf6025dad19af52259d0a5c9d267aa
SHA-256 : dd99b1a8b816c2ad0e4de5b8d5b1913a68d9738d8b4309748417e81547a5104e

Archivo : uMoBgfiElUCx1.vbs
MD5 : 67f50514c9c3aa8ba89b535bcf81d347
SHA-256 : ea98aa87ce19d9ff538f994abeace9f7a10f24e7ebff3209eefc207560901955

Archivo : tf4[1].btc.zip
MD5 : 3d0699c5485021647033d0c0cf12cb45
SHA-256 : f0ac4b8bf50f57771295081e92846ecfe47e0ee175a38c85e3f88286f0d7260c

Archivo : RARDOJH221TW6CCV0HRUHC2J1RZ5JUL
MD5 : 6c314ba03b2813b90a1f306476c0d408
SHA-256 : 51c7055699e382abfd9e681ddf97fe16943288649d6c9cac05af870a1968646e

Archivo : WQJUH7I7Z06TQKC48WJ5WUBI5FKYEB9A
MD5 : a39c2c135e953e230c589ac81150e59b
SHA-256 : 74450668d4f71dcf686fb962e8c0a65e48ab272cf2967efa19ac728610bc305a

Archivo : JXfnQNj9436013.exe
MD5 : b06e67f9767e5023892d9698703ad098
SHA-256 : 8498900e57a490404e7ec4d8159bee29aed5852ae88bd484141780eaadb727bb

Imagen Phising de Correo

msg229@minjusticia.gob.cl

AVISO (JUSTICIA)

Ministerio de Justicia y Derechos Humanos

Gobierno de Chile

Estimado Señor (a), Informamos que hoy se ha abierto un proceso criminal en su nombre. Le informamos que el mismo se adjunta a ese correo electrõnico y que usted tiene el plazo de **48 horas** para recurrir en su defensa.

Haga clic aquí para descargar la copia en el proceso adjunto.

Ministerio de Justicia y Derechos Humanos | 2019
Morandé 107, Santiago - Teléfonos (56-2) 26743100

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

Contactos

https://www.csirt.gob.cl
+ (562) 24863850
@CSIRTGOB
https://www.linkedin.com/company/csirt-gob

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.07.25 13:03:29 -04'00'