Alerta de Seguridad Informática (8FPH-00012-001)

Nivel de Riesgo: Alto

PHISHING

Fecha de lanzamiento Original: 26 de abril de 2019 | Última revisión 26 de abril de 2019

RESUMEN

El equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de Phishing con Malware asociado. Actualmente CSIRT está monitoreando el incidente, ya que el cuerpo del Phishing contiene un mensaje para obtener el permiso de circulación 2019 y solicita verificar si existen multas pendientes.

Si bien el proceso de renovación del permiso de circulación ocurrió en marzo de 2019, cabe tener presente que hay una segunda fase en agosto de 2019, razón por la cual sigue vigente esta estrategia de phishing.

A continuación, se adjuntan indicadores de compromisos:

IoC

Urls involucradas :

https[:]//bit[.]ly/2UxeaJn
https[:]//drive[.]google[.]com/uc?export=download&id=1yHf4sI67uARwJttgm9T0iMb63vahvfQe
https[:]//technodrive[.]cl/wp-content/plugins/acf-options-page/acf-page.png
http[:]//www.ingenieriaelectricidad[.]cl/css/style.png

Sender Original : www-data@multa-id3.ddns.me

Received : multa-id1.ddns.me [139.99.75.59]
multa-id2.ddns.me [139.99.72.151]
multa-id3.ddns.me [139.99.78.62]
multa-id4.ddns.me [139.99.223.245]
multa-id5.ddns.me [139.99.221.132]

From : TrÃ¡nsito 2019 Gob.799344
TrÃ¡nsito y transporte319153
TrÃ¡nsito 2019 Gob.461933
TrÃ¡nsito y transporte854130

Subject : #Registrada un Multa Folio: 886591
#Registrada un Multa Folio: 845557
Infraccion Registrada Folio: 78302
Infraccion Registrada Folio: 922900

Archivos Involucrados.

SHA-256 : bb8e4f3e171f65c8b76922615f5426b107a9756945b30b32ccddf16df09a4c55
Path : Infraccion-Grave_PDF.cmd

MD5 : C3528E8D2E21EBD37AF7301D13B576A6
Path : 42.vbs

SHA-256 : 2543b34e40cbd8f26b779d00265aa5756009999ce732d1c989865285240d38ca
Path : acf-page.png (Type Doc)

SHA256 : d77b02726243b7d040f783c757629f878b02bc28d405c4c68b2bf7da6af44cb6
Path : style.png

SHA-256 : 0e6999e1a0109bfd8c55d32e19a1a43ea7eac2e7daaad29cdf051d4d8d9be548
Path : C:\Windows\Installer\MSI9216.tmp

SHA-256 : 2543b34e40cbd8f26b779d00265aa5756009999ce732d1c989865285240d38ca
Path : C:\Windows\Installer\24547aa.msi

SHA-256 : a99d2c6fd1667942a085f01784bd599762182fce8a8f866fa12ac93f52ae2ed1
Path : C:\Windows\Installer\MSI85C3.tmp

SHA-256 : a1cfd2e5721a56c0c0af52086f73c090574f6652d55493b7012ccc13350b7c9e
Path : C:\Config.Msi\24547ad.rbs

SHA-256 : 2781b73fc4d1da0cfeecb3a01215f12bfbff23c763e16830bf1397b33e989587
Path : C:\Windows\Installer\MSI915A.tmp

MITIGACIONES.

Bloquear Urls involucradas
Bloquear Sender Original
Bloquear Subject
Actualizar las tecnologías de detección de amenazas
Revisar los controles de los AntiSpam y SandBoxing
Realizar concientización permanente para los usuarios sobre este tipo de amenazas

IMAGEN DE CORREO

TrÃjnsito y transporte854130 <transito.2019@multa-id2.ddns.me>
Infracción Registrada Folio: 922900

FISCALIZACIÓN TRANSPORTES

Para obtener el permiso de circulación 2019, debe saber si su vehículo posee multas registradas. Aquí encontrara la única información válida respecto al tema, para mayor informacion sobre su multa de transito no pagada, descargue el detalle en el siguiente elance:

Multa ID:	
INFRACCIÓN:	INFRACCION: TRANSITAR SIN DISPOSITIVO ELECTRONICO POR AUTOPISTA CONCESIONADA
FECHA INFRACCIÓN:	23-03-2019
FECHA SENTENCIA:	23-04-2019

No se pude mostrar la imagen vinculada. Puede que se haya movido, cambiado de nombre o eliminado el archivo. Compruebe que el vínculo señal...

Vea Aqui Su Infraccion

Servicio de Registro Civil e Identificación - Teléfono: 600 370 2000
Política de Privacidad
Términos y Condiciones