Alerta de seguridad informática	2CMV23-00415-01
Clase de alerta	Fraude
Tipo de incidente	Phishing-Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de mayo de 2023
Última revisión	25 de mayo de 2023

PARA EL CORRECTO USO Y DIVULGACIÓN DE ESTE DOCUMENTO LEER ACÁ

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT de Gobierno) ha identificado una nueva campaña de phishing con malware suplantando a Conaset con un email sobre una falsa multa.

Si la víctima interactúa con el fichero malicioso se encuentra con el malware conocido como Mekotio, un troyano bancario que apunta principalmente a Brasil, Chile, México, España, Perú y Portugal, y cuya característica más notable es el uso de una base de datos SQL como servidor de C2.

Indicadores de Compromiso Asociados

Archivos que se encuentran en la amenaza

SHA256

Indicador	Relación
00b8b72c1353a2a6646e20bdddad58318dab20ade02151ce3864ff04c912a2cc	InfraccioneNuevaCS.zip
c8c6ff192502979e1a1983919bd3cadfb8e0c7409f02476c540a6802397222f6	InfraccioneNuevaCS.msi
14cef33c97ba660caca4bb0552caa4e68bfa3f117111a10b8d3a3addab7b06b5	ordencompra20052023.zip
c8c6ff192502979e1a1983919bd3cadfb8e0c7409f02476c540a6802397222f6	ordencompra20052023.msi
c09d0790e550694350b94ca6b077c54f983c135fab8990df5a754628041509l2	737f93fd.dll
e1cba56f20dbad484273f58df3d672b4b07f36d237e4cb16dcedd9fba0a720a1	SOEUVGVPII.Xxv
a5a770b8d64d757f8894e551ace0627dbe60c3b4e5032d2ccb8ca56f0d0ee352	oje.p.ahk
de87c8713fac002b0b0a0f9b02c4e3ebcccf65282a22f5ab5912a9da00f35c2a	oje.p.exe

URL-Dominio

Dominio	Relación
https://psdasyogapathy[.]org/images/conaset/	Descarga del Fichero
https://montao.com.pe/adslink/	Contenedor de Malware
50.116.72[.]199	IP
89.116.255[.]59:9999	IP

MITRE ATT&CK

Descripción	ID
Acceso Inicial (Mediante Phishing)	T1566.002
Colección (Datos del sistema local)	T1005
Acceso a Credenciales (Credenciales en Archivos)	T1081
Evasión de Defensa (Modificación de registro)	T1112
Evasión de Defensa (Evasión de Virtualización/Sandboxing)	T1497
Descubrimiento (Consulta del Registro)	T1012

Imagen del Mensaje

Informe Infracciones 629360429857856802978 2 - Oportunidad de regularización

CN CONASET - Notificacion <support@followthetrolley.com>
Para [redacted]

Responder | Responder a todos | Reenviar

ju. 25/05/2023 12:14

Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.

CONASET - Notificacion

Informe Online sobre multas y sanciones de tránsito

Estimado Contribuente: [redacted]

Si han transcurrido 10 días desde que se comunicó la infracción, se lo notificaremos a través de los tribunales.

Infraciones al dia 10/04/2023 Tiempo '15:27:39'
Siga los archivos adjuntos a continuación para ver los detalles de la infracción de tránsito

Infracciones	Acceso	Detalle
Estacionemtno no permitido - Girar en lugar prohibido	Ir a Trámite en línea	Más información

(Para acceder al documento electronico recuerde que la version de este documento es unicamente para PC no funciona en dispositivos moviles.)

Para consultar tu sanción, accede a Más información arriba o Accede a Trámite online y regulariza tu situación ante las autoridades.

El proprietario del vehiculo queda notificado por este medio

La informacion contenida en el sistema es generada y respostada por los organismos de transito

Comisión nacional de Seguridad de Tránsito

FALSO
CSIRT

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.05.25 21:03:22 -04'00'