Alerta de seguridad informática	2CMV24-00441-01
Clase de alerta	Fraude
Tipo de incidente	Phishing-Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de enero de 2023
Última revisión	30 de enero 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, difundido en un email que suplanta al Conaset.

Si la víctima interactúa con el fichero malicioso se encuentra con Mekotio, un troyano bancario que destaca por el uso de comandos de base de datos SQL para obtener información del sistema infectado, la que envía a su servidor de comando y control.

Indicadores de Compromiso Asociados

Archivos que se encuentran en la amenaza

SHA256

Indicador	Relación
c1e0f5185a2efc13b4e821ee1a2d445634e87fb380306315c482c05ae26fbd55	conasetnotificacioninfra.zip
17a6f57be6897d2a7456ad9b0f5bc798b951c6c41b2511886706edee16c5c14c	conasetnotificacioninfra.msi
36a9e7f1c95b82ffb99743e0c5c4ce95d83c9a430aac59f84ef3cbfab6145068	l.txt
52f41817669af7ac55b1516894ee705245c3148f2997fa0e6617e9cc6353e41e	aicustact.dll
b55333f085db8ef18ca3ba73a7b3984b3917d95c4f3fa57f939ebfe89c82a03c	rmateoo.dll
0831dbcb3799c9e36ea586582e8ef907dcefeb2045351d6774c7ad0ef02a9af2	SoftwareDetector.dll

URL-Dominio

Dominio	Relación
https://windbender[.]com/conasetinfraccione/?hash={correo}	Descarga del Fichero
https://plataformaepimexicoenganchate[.]org/111xxx/conasetnotificacioninfra.zip	Contenedor Malware
support@litfun.com	Correo de salida
support@alwaysnbs.tv	Correo de salida
support@colbits.com.co	Correo de salida
support@ambaniorganics.com	Correo de salida
support@shop.stadsbrouwerijeindhoven.com	Correo de salida
support@rogersgunsandgrips.com	Correo de salida
104.207.254[.]65	IP de correo de salida

MITRE ATT&CK

Descripción	ID
Acceso Inicial (Mediante Phishing)	T1566.002
Descubrimiento (Consulta del Registro)	T1012
Descubrimiento (Información del Sistema)	T1082
Descubrimiento (Equipos Perimetrales)	T1120
Comando y control (Puerto no estándar)	T1571

Imagen del Mensaje

[redacted]Informe Infracciones 5008032807025758877 - Oportunidad de regularización[redacted]

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

Responder | Responder a todos | Reenviar | ...
lunes 29-01-2024 14:27

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 transito

Estimado Contribuente: [redacted]

Si usted no regulariza las infracciones correspondientes en los proximos 10 dias a partir de la fecha de emison de este comunicado, su vehiculo sera informado como deudor.

Infraciones al dia 24/12/2023 Tiempo '13:17:43'
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.)

FALSO CSIRT

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

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.01.30 13:02:54 -03'00'