

Alerta de Seguridad Cibernética

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT
Ministerio del Interior y Seguridad Pública
Subsecretaría del Interior



Alerta de seguridad informática	2CMV24-00455-01
Clase de alerta	Fraude
Tipo de incidente	Phishing-Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de febrero de 2024
Última revisión	15 de febrero de 2024





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, contenido en una falsa factura.

El malware corresponde al troyano bancario Grandoreiro, dirigido a los países de Latinoamérica. Es usado como puerta trasera para permitir al atacante acceder a los dispositivos de la víctima y así robar su información personal y financiera en las sesiones de banca online que abran.

CONTACTO Y REDES SOCIALES CSIRT

 <https://www.csirt.gob.cl>
 Teléfonos: 1510 | + (562) 24863850 | Correo: soc-csirt@interior.gob.cl
 @csirtgob
 <https://www.linkedin.com/company/csirt-gob>

Indicadores de Compromiso Asociados

Archivos que se encuentran en la amenaza

SHA256

Indicador	Relación
bd62e3f190f376ece6e9c3c92f24fd366230bcb059d3c010e6699b4e5b90a27d8347a377b7041c6e2f85506cc57e1cf3b343817435f6dcefef9892a3ac3a411	FC-SAT0251706897350138.zip 5302 Factura SAT - RFC Emisor-8856VFPF - Serie-DORM99781391 Ref-AHOK5520.exe
f2d850025dd7b65c44d979ec74a3f5a77e1c15b4070812be5656887cee95dc59	6236OPLZ9308UYLG.xml

URL-Dominio

Dominio	Relación
https://edrfacdigitsservconsulospl.westus3.cloudapp.azure[.]com/?docs/xml/WCA161006TN9/15540f02-d006-4e3b-b2de-6873baff3b2a	Descarga del Fichero
https://www.dropbox[.]com/scl/fi/zrh7teb6n5rkkazv6ap6/FC-SAT0251706897350138.zip?rlkey=4e6gas0wul37n18p5frzmwgm&dl=1	Directorio del Malware
https://ucb3350fbd464fe7d3ee4744f6d.dl.dropboxusercontent[.]com/cd/0/get/CNVBSYNyoQmzOd6mA9WDT11QrBJQD24EGybWVmx3tFTyc9qxFmBjYkcT1rwnV-sr3fKdkOXDeDGYUfBrbVGzK2ztsg5jn1UzqnL31pbNVJl9q1MuP0ekT5ooJokyd6n9stqKbhE-LHZya_YyeaSWO/file?dl=1#	Directorio Malware
http://18.231.53.141:40626/iOvNGsPS1xAiG1vvKZ.txt	Fichero comprobación
http://18.230.211[.]48:30657/RVTBoFMeBv.xml	Archivo ZIP
http://ip-api[.]com/json	Whois
18.230.211[.]48:4318	IP
18.230.211[.]48:30657	IP
root@zx16.vycancs.com	Correo de salida
root@zx15.vycancs.com	Correo de salida
root@zx14.vycancs.com	Correo de salida

MITRE ATT&CK

Descripción	ID
Acceso Inicial (Mediante Phishing)	T1566.002
Ejecución (Ejecución del usuario)	T1204.002
Acceso a credenciales (Credenciales en archivos)	T1552.001
Descubrimiento (Descubrimiento de información del sistema)	T1082
Descubrimiento (Consulta de registro)	T1012
Descubrimiento (Descubrimiento de software)	T1518
Descubrimiento (Detección de la configuración de red del sistema)	T1016
Comando y control (Puerto no estándar)	T1571

CONTACTO Y REDES SOCIALES CSIRT

Alerta de Seguridad Cibernética

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT
Ministerio del Interior y Seguridad Pública
Subsecretaría del Interior

Imagen del Mensaje

Ha recibido un(a) Factura Electronica - Documento Importante Adjunto



SAT <gruposat@sat.gob.com>

Para

Responder Responder a todos Reenviar

jueves 15-02-2024 9:13

Estimado Cliente:

Usted está recibiendo un comprobante fiscal digital (Factura Electrónica) de

De acuerdo a la reglamentación del Servicio de Administración Tributaria (SAT)

[Ver Factura PDF](#)

[Ver Factura XML](#)

Atentamente,

SAT - Servicio de Administración Tributaria
Información de Contacto



- Ingresa al Portal del SAT, opción Otros trámites y servicios, Aclaración, asistencia y orientación electrónica; Aclara tu requerimiento de obligaciones omitidas o carta invitación.
- Da clic en el botón INICIAR e ingresa tu RFC y Contraseña.

- Localiza la opción Servicios por Internet: Aclaraciones, opción Solicitud y elige el trámite Requerimiento Control de Oblig y describe brevemente el motivo de tu aclaración.

Fundamento legal: Artículos 33, fracciones I, III y IV incisos b y c, así como el último párrafo de esta fracción y 63 del Código Fiscal de la Federación.

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>
Teléfonos: 1510 | + (562) 24863850 | Correo: soc-csirt@interior.gob.cl
@csirtgob
<https://www.linkedin.com/company/csirt-gob>