Alerta de seguridad informática	2CMV24-00449-01
Clase de alerta	Fraude
Tipo de incidente	Phishing-Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de marzo de 2024
Última revisión	04 de marzo 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 suplantando con una falsa acción de demanda.

Este troyano bancario llamado grandoreiro dirigido a los países de Latinoamérica, este programa malicioso es usado como puerta trasera para permitir al atacante acceder a los dispositivos de la víctima y así robar su información personal y bancaria en las sesiones de banca online que abran.

Este malware posee una técnica de CAPTCHA, en particular, requiere la realización manual de la prueba de desafío-respuesta para ejecutar el malware en la maquina comprometida, lo que significa que el implante no se ejecuta al menos que la víctima resuelva este CAPTCHA.

Indicadores de Compromiso Asociados

Archivos que se encuentran en la amenaza

SHA256

Indicador	Relación
571c694a88a7187135e203990af43edcab1234406d3ffe964b60b0aa26b4060b	1020-TFWAC-4702509150918285.zip
a74b87754eb9a6a7e6b19da79eb02192b6e1a802fe58d037065a33ac7171f57d	6645 Detalles-5931LSOP FC-RGXR78118123 Ref-DP-UHTT9388.exe
f2d850025dd7b65c44d979ec74a3f5a77e1c15b4070812be5656887cee95dc59	_____ _____ _____5942FMJI4480GTFA.xml
013dbfa17653c4fc89a20f7c988bdfb6b5c3367a0c6a8e3a87e189e164e53460	pRcRVZUG.xml

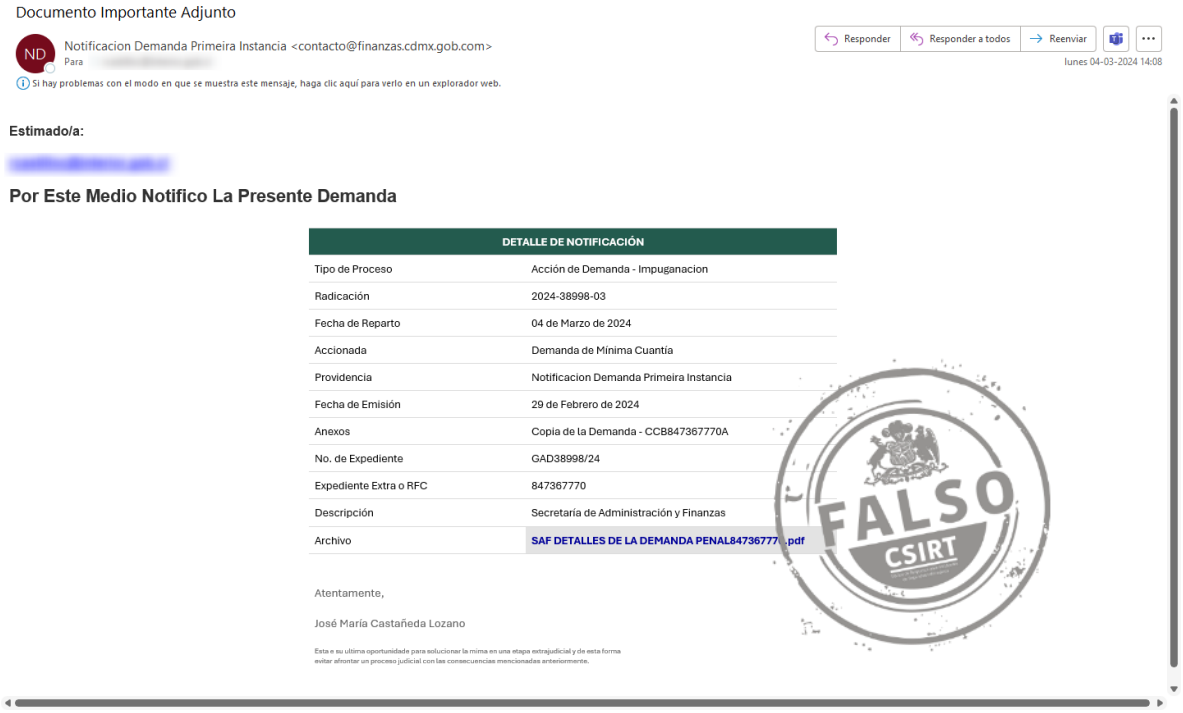
URL-Dominio

Dominio	Relación
https://ijfacdigitasmitty.swedencentral.cloudapp[.]azure.com/?finanzas.busqueda?q=Secretar%C3%ADa+de+Administraci%C3%B3n+y+Finanzas?30337974_3097_705331937556-157889157889770732479410588494105884	Descarga del Fichero
https://www.dropbox[.]com/scl/fi/8xvft27zvs4k1u3lhvdi3/4988-TFWAC-6807205622474888.zip?rlkey=w86llc6ks6ir69k4sojnnbyxl&dl=1	Redirección de directorio
https://uc4a4d5347b517a418e5ce058c49.dl.dropboxusercontent[.]com/cd/0/get/COcN3jlLD1RVwb3YUwmP-jCtwYOJCQzfcQon2q7wsiSp7PZXnNSSJZY5gdLQlSBg-wYSkh3J4M90J2pBog04-nt5EZ8ncxABITlOIIa9hCgauTarAXZtVHCLLSkH3mZLeTyH4bjWHFV5u2SIkSBBdaha/file?dl=1#	Contenedor de malware
http://15.229.46.181:40187/pRcRVZUG.xml	Payload
15.229.46[.]181:40187	C2
http://ip-api.com/json	Whois
root@nm1.clidilfrtd[.]com	Correo de salida
root@nm3.clidilfrtd[.]com	Correo de salida
root@nm4.clidilfrtd[.]com	Correo de salida
root@nm6.clidilfrtd[.]com	Correo de salida
root@nm7.clidilfrtd[.]com	Correo de salida
root@nm9.clidilfrtd[.]com	Correo de salida

MITRE ATT&CK

Descripción	ID
Acceso Inicial (Mediante Phishing)	T1566.002
Ejecución por el usuario (Archivo malicioso)	T1204.002
Enmascaramiento (Renombrar las Utilidades del Sistema)	T1036.003
Credenciales no garantizadas (Credenciales en archivos)	T1552.001
Descubrimiento (Consulta del Registro)	T1012
Descubrimiento (Detección de la configuración de red del sistema)	T1016
Comando y control (Puerto no estándar)	T1571

Imagen del mensaje



Documento Importante Adjunto

ND Notificacion Demanda Primeira Instancia <contacto@finanzas.cdmx.gob.com>
Para [redacted]

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

Responder | Responder a todos | Reenviar

lunes 04-03-2024 14:08

Estimado/a:

[redacted]

Por Este Medio Notifico La Presente Demanda

DETALLE DE NOTIFICACIÓN	
Tipo de Proceso	Acción de Demanda - Impuganacion
Radicación	2024-38998-03
Fecha de Reparto	04 de Marzo de 2024
Accionada	Demanda de Mínima Cuantía
Providencia	Notificacion Demanda Primeira Instancia
Fecha de Emisión	29 de Febrero de 2024
Anexos	Copia de la Demanda - CCB847367770A
No. de Expediente	GAD38998/24
Expediente Extra o RFC	847367770
Descripción	Secretaría de Administración y Finanzas
Archivo	SAF DETALLES DE LA DEMANDA PENAL84736777[redacted].pdf

Atentamente,

José María Castañeda Lozano

Esta e su ultima oportunidade para solucionar la mima en una etapa extrajudicial y de esta forma evitar afrontar un proceso judicial con las consecuencias mencionadas anteriormente.

FALSO
CSIRT

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.03.04 16:38:33 -03'00'