Alerta de seguridad informática	2CMV23-00419-01
Clase de alerta	Fraude
Tipo de incidente	Phishing-Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de junio de 2023
Última revisión	19 de junio 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 al Poder Judicial, difundida a través de un email que incluye una falsa notificación.

El malware presente en esta campaña corresponde a un troyano bancario usado como puerta trasera para permitir al atacante acceder a los dispositivos de la víctima y así robar su información personal y bancaria de las sesiones de banca online que abran.

Este programa malicioso posee además requiere de la resolución manual de un Captcha, prueba de desafío-respuesta, para ejecutar el malware en la maquina comprometida.

Indicadores de Compromiso Asociados

Archivos que se encuentran en la amenaza

SHA256

Indicador	Relación
58cfa0e09bc0acc1bc993045633ea70e3cd3797ff55d86045168fee3db2562e1	Archivo_Comprimido_SUYODPONUBVUCHGgypok.zip
49123043ba4257cb61d00a931ea273f724a9cda06ec8eb107ddeab4d664ac883	Resolucion_Archivo_Digital_0417890030DTSMBGJVDGntdlm.exe
0604388f107d1ed9abbb13912e5cdc2f9a2da8d0e528fbb4546c23b2f08c6f15	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~A04468PPSCN.xml
865f12dd2959457978155d2eb83833ea00d0afc06f3aa820866f6a55476ad3e4	ID-Archivo_Attatchment_QQETVKNJJMXKJNTxmldp.zip
84d73fd51c09a001c449100862d48062eee947bc2d632264f820cdf3393789ef	A8F_DOCFBS940708GA4_91317021161ZYYAQLMQCaurko.exe
0604388f107d1ed9abbb13912e5cdc2f9a2da8d0e528fbb4546c23b2f08c6f15	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~A90427QABJC.xml
816266195405aa5c6d9564f0db7fc58dca1c064558f7c96c47f7cbfc3bf68d7d	ID-Archivo_Attatchment_VDIXKIHAVBNFMHLatrzc.zip
5ccb8f4becf4f5c5440d62ebb9c21abf84d5c564eb72ec9d12f27fc824307998	A8F_DOCFBS940708GA4_7339372612YHEYOLYUJJxgelz.exe
0604388f107d1ed9abbb13912e5cdc2f9a2da8d0e528fbb4546c23b2f08c6f15	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~A81876CLSDU.xml

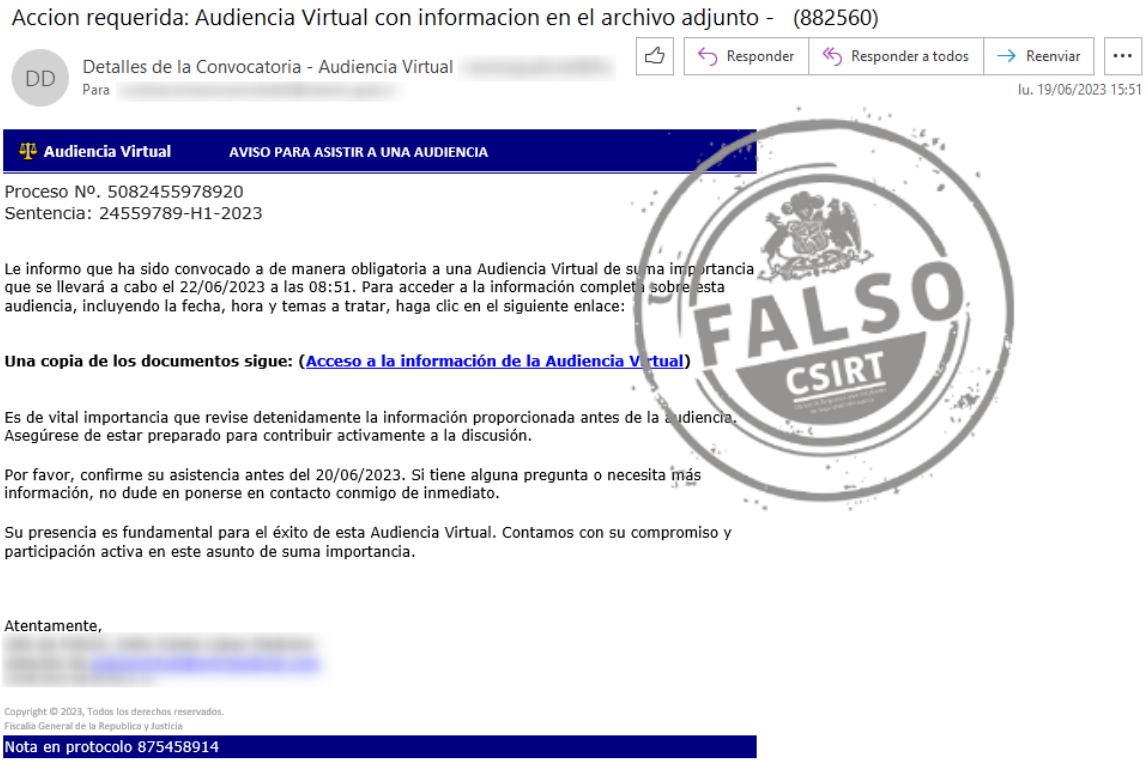
URL-Dominio

Dominio	Relación
https://jccrivelliabogadospublicidad.brazilsouth.cloudapp[.]azure.com/	Descarga del Fichero
http://20.206.121[.]188/	Descarga del Fichero
https://www.dropbox[.]com/s/dl/wdw1uk4rc4iihly/	Directorio del Malware
https://www.dropbox[.]com/s/dl/0thjroopb2nae4x/	Directorio del Malware
https://www.dropbox[.]com/s/dl/zl93ykl0jlz7dcr/	Directorio del Malware
http://ip-api[.]com/json	Whois

MITRE ATT&CK

Descripción	ID
Acceso Inicial (Mediante Phishing)	T1566.002
Descubrimiento (Descubrimiento de información del sistema)	T1082
Descubrimiento (Registro de consultas)	T1012
Persistencia (Carga lateral de DLL)	T1574.002

Imagen del Mensaje



Accion requerida: Audiencia Virtual con informacion en el archivo adjunto - (882560)

DD Detalles de la Convocatoria - Audiencia Virtual
Para

Responder | Responder a todos | Reenviar | ...

lu. 19/06/2023 15:51

Audiencia Virtual AVISO PARA ASISTIR A UNA AUDIENCIA

Proceso Nº. 5082455978920
Sentencia: 24559789-H1-2023

Le informo que ha sido convocado a de manera obligatoria a una Audiencia Virtual de suma importancia que se llevará a cabo el 22/06/2023 a las 08:51. Para acceder a la información completa sobre esta audiencia, incluyendo la fecha, hora y temas a tratar, haga clic en el siguiente enlace:

Una copia de los documentos sigue: (Acceso a la información de la Audiencia Virtual)

Es de vital importancia que revise detenidamente la información proporcionada antes de la audiencia. Asegúrese de estar preparado para contribuir activamente a la discusión.

Por favor, confirme su asistencia antes del 20/06/2023. Si tiene alguna pregunta o necesita más información, no dude en ponerse en contacto conmigo de inmediato.

Su presencia es fundamental para el éxito de esta Audiencia Virtual. Contamos con su compromiso y participación activa en este asunto de suma importancia.

Atentamente,

Copyright © 2023, Todos los derechos reservados.
Fiscalia General de la Republica y Justicia

Nota en protocolo 875458914

FALSO
CSIRT

Convocatoria Aviso de citacion electronica - (119935)

I INTIMO <avisosjudicial[redacted]>
Para [redacted]

Responder | Responder a todos | Reenviar | ...
lu. 19/06/2023 13:39

Advertencia de Citación

Buenos dias Sr(a),

De conformidad con el art. **455, § 1** del Código de Procedimiento Civil se hace presente al **ÍNTIMO**
Su Señoría comparezca, como testigo, en la audiencia que se celebrará
miércoles, 19 de Junio de 2023.

Documento adjunto referente al trámite

Citación Adjunta nº 50824559789200

[redacted]

Resolucion de Archivo Provisional: Accion Legal en curso - (150007)

DI Documentacion Importante <avisosjudicial@[redacted]>
Para [redacted]

Responder | Responder a todos | Reenviar | ...
lu. 19/06/2023 13:40

PODER JUDICIAL

Notificación automática emitida por el sistema de poder judicial.

Sigue la continuación con una copia del caso judicial en PDF.

*Descargue copia en PDF en el Siguiente enlance.

Orden Investigativa Junio 2023/04 - Nº 591004H1-59685

Orden Petición de Ejecución 2023/04 - Ref - 7356-H1-2023

Con el escrito electrónico del 19 de Junio del año en curso y su archivo adjunto, téngase por cumplida la intimación dispuesta (v. proveído de fecha -18-06-2023), pasándose a resolver la presentación de fecha 19 de Junio del corriente año 2023.
Regístrese, notifíquese de oficio y por medios electrónicos (conf. art. 1 acápite 3. «c», resol. Presidencia) y cúmplase con el archivo ordenado.

Suscripto y registrado por el Actuario firmante, , en la fecha indicada en la constancia de la firma digital (Ac. 3.971/20 y modif.).

[redacted]

Atenciosamente
Sistema de Ejecución de Órdenes Judiciales

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.06.20 12:20:32 -04'00'