Alerta de seguridad informática	2CMV23-00438-01
Clase de alerta	Fraude
Tipo de incidente	Phishing-Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de diciembre de 2023
Última revisión	20 de diciembre 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 contenido en un email que se hace pasar por proveniente de una "Defensoría Pública".

El malware corresponde al troyano bancario Grandoreiro, usado como puerta trasera para permitir al atacante acceder a los dispositivos de la víctima y así robar su información personal y bancaria ingresada en sesiones de banca online.

Este malware requiere la realización manual de la prueba de desafío-respuesta para ejecutar el malware en la maquina comprometida, lo que significa que la implantación 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
cf1dc1c23e8470735195101f8d0bbaef6e9b1550326d14c54bd9d8c9127ee59c	ConsultPagZDFKMQXVtlvhipmbetpeegdfYNSU.zip
92bca8063250dcb09c12e00648e20acc8cd75eee2a7f1f83ab7755d0024049cd	HojaDCalculProfessziufRQCLmstryjfhltjltljoZYSA.exe
f5774d9f5e519d068c6d8bbf6cafaf0d46c51cd76c5364bdffc86ba74fd472ab	_____ _____ _____ _____8962132579 05.xml

URL-Dominio

Dominio	Relación
https://espangmtes.westus2.cloudapp.azure[.]com/?25236754_966-108935108935=817902817902	Descarga del Fichero
https://www.dropbox[.]com/scl/fi/j3m0poowjfq9zp9glmsal/ConsultPagZDFKMQXVtlvhipmbetpeegdfYNSU.zip?rlkey=2tjq03gyi6fe4jddmo8loiarr&dl=0	Directorio del Malware
http://15.229.5[.]172:24163/KvMXecvipA.xml	Archivo DLL
http://15.229.5[.]172:4917/	Configuración Malware
http://ip-api.com/json	Whois
15.229.5[.]172	IP

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 (Descubrimiento de programas)	T1518
Descubrimiento (Descubrimiento de la información del sistema)	T1082
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

Acciones requeridas tras el Veredicto de Archivamiento - 606072

CA Convocatoria a Revision <info@gob.bo>
Para [redacted]

Responder | Responder a todos | Reenviar | ...
jueves 16-11-2023 10:17

Mensaje enviado con importancia Alta.

Estimado/a:

[redacted]

Me dirijo a usted como Laura Ramírez, **Analista de Procesos en el Área de Selección de Personal de la Defensoría Pública.** Adjunto encontrará el Veredicto de Archivado Temporal.

Veredicto de Archivado Temporal: 665179.xls (8116 KB)

Cualquier pregunta que surja tras revisar el Veredicto, por favor, hágamela saber.

El no cumplimiento de las obligaciones en el plazo establecido acarreará intereses y recargos según el ***Artículo 60[illegible] del Código Fiscal.***

Agradezco su atención,

13:16:48 - 16/11/2023

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.01.08 15:12:56 -03'00'