Alerta de seguridad informática	2CMV24-00442-01
Clase de alerta	Fraude
Tipo de incidente	Phishing-Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de enero de 2023
Última revisión	31 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, difundida en un correo electrónico haciéndose pasar por una supuesta firma "Asesoría e Inversiones" con un falso aviso del vencimiento de una factura electrónica.

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 y enviarla a su servidor de comando y control.

Indicadores de Compromiso Asociados

Archivos que se encuentran en la amenaza

SHA256

Indicador	Relación
c98da79639217f83596fe9959fcc15d907255e098b972dc00535858710204cd8	FactAsesoriasInversiones.zip
ac2e3c0663c9ce6f5791afbddbb0614d8417efd230b08a0d68f84b923999c0e7	FactAsesoriasInversiones.msi
d955856d80c8127ccd38b7a04be1b48984078e9e6416e3c1846b772956dda003	qvfphzy.dll
52f41817669af7ac55b1516894ee705245c3148f2997fa0e6617e9cc6353e41e	aicustact.dll
0831dbcb3799c9e36ea586582e8ef907dcefeb2045351d6774c7ad0ef02a9af2	SoftwareDetector.dll

URL-Dominio

Dominio	Relación
https://sunsericorp[.]com/facturaAsesoriasInversiones/?hash={correo}	Descarga del Fichero
https://sumitathemes[.]com/verdacted/FactAsesoriasInversiones.zip?13753358	Contenedor Malware
support@colbits.com.co	Correo de salida
support@alwaysnbs.tv	Correo de salida
support@rogersgunsandgrips.com	Correo de salida
104.207.254[.]65	IP de correo de salida
66.228.42.147:8089	C2

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

Factura electrónica Nº27388 (Vencimiento 20/2/2024) de Asesorias e Inversiones

AE Asesorias e Inversiones <support@rogersgunsandgrips.com>
Para [redacted]

Responder | Responder a todos | Reenviar | ...

martes 30-01-2024 21:54

Asesorias e Inversiones

Estimado(a) [redacted]
Junto con saludarte, este correo es para indicarte que con fecha 20/2/2024 se ha emitido un nuevo documento electrónico #27338 por un total de $442.899.

FACTURA	TOTAL
27338	$442.899

Descargar Factura

(.zip) (Para acceder al documento electronico recuerde que la version de este documento es unicamente para PC, no funciona en dispositivos moviles.)

FALSO CSIRT

Esta notificación ha sido generada automáticamente cumpliendo los más altos estándares de seguridad con certificaciones AWS y certificación ISO 27001.

Asesorias e Inversiones 1999 - 2024

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.01.31 16:56:47 -03'00'