Alerta de seguridad informática	2CMV24-00444-01
Clase de alerta	Fraude
Tipo de incidente	Phishing-Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de febrero de 2024
Última revisión	13 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 como un archivo adjunto que se hace pasar como una factura.

Si la víctima interactúa con el fichero malicioso se encuentra con Formbook, un malware del tipo infostealer que sustrae información sensible del dispositivo de la víctima. Dentro de la información sustraída por este programa malicioso se encuentran credenciales de acceso y capturas de pantalla. Esta información es enviada a un servidor controlado por los ciberdelincuentes.

Indicadores de Compromiso Asociados

Archivos que se encuentran en la amenaza

SHA256

Indicador	Relación
e64a5a0e34ecb51c2c40cb84016354e096b7c5bc34f5a841d685e94844644ad6	Factura de proforma jpg.exe.xz
220977b28fc847b8a2d7c65d3d19a3859e3e62dc5e19edaf4909965516a91694	Factura de proforma jpg.exe
522cad95d3fa6ebb3274709b8d09bbb1ca37389d0a924cd29e934a75aa04c6c9	DB1
11eec98226b37a2a84c990ed445db42fa3558354b523d76d1919791b82ce7cb9	LK3logim.jpeg
1662d01a2d47b875a34fc7a8cd92e78cb2ba7f34023c7fd2639cbb10b8d94361	LK3logrf.ini
220977b28fc847b8a2d7c65d3d19a3859e3e62dc5e19edaf4909965516a91694	skype.exe

URL-Dominio

Dominio	Relación
http://www.longfangyun[.]com/kmge/	C2
103.196.103[.]176:80	IP
199.34.228[.]73:80	IP

MITRE ATT&CK

Descripción	ID
Acceso Inicial (Mediante Phishing)	T1566.002
Ejecución (Ejecución del usuario)	T1204.002
Ejecución (Intérprete de comandos y scripts)	T1059.003
Evasión de Defensas (Modificación de registros)	T1112
Acceso a credenciales (Credenciales en archivos)	T1552.001
Descubrimiento (Consulta del registro)	T1012
Descubrimiento (Información del sistema)	T1082
Descubrimiento (Detección remota de sistemas)	T1018
Colección (Datos del sistema local)	T1005
Comando y control (Protocolo de la capa de aplicación)	T1071

Imagen del Mensaje

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.02.13 11:59:18 -03'00'