Alerta de seguridad informática	2CMV23-00416-01
Clase de alerta	Fraude
Tipo de incidente	Phishing-Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de mayo de 2023
Última revisión	31 de mayo 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, que se difunde a través de un email malicioso que alude a un falso pago supuestamente devuelto a la víctima.

En el email se adjunta un archivo .rar, dentro del cual se encuentra un ejecutable de Windows, el cual despliega dos malware, Agent Tesla y Guloader.

El primer malware actúa como un troyano de acceso remoto (RAT) esta destinado principalmente a sustraer información del equipo infectado, y además despliega técnicas para ser una amenaza persistente.

Mientras tanto, Guloader tiene como objetivo final robar información confidencial y llevar a cabo acciones que generen acceso a los ciberdelincuentes.

Indicadores de Compromiso Asociados

Archivos que se encuentran en la amenaza

SHA256

Indicador	Relación
7c8967960ad84f41435692215c414f6b21f804a6679b4754be52e866cd9bfec8	Transferencia 8074360002017047.rar
8ba3f2678bd2622e665539d20ba61643782d2e99ee0f9cd703221fae5d49e2c0	Transferencia 8074360002017047.exe
f004c568d305cd95edbd704166fcd2849d395b595dff814bcc2012693527ac37	System.dll
9c22043cc1b16fcbcbd6cc8d4784207794 37a04626f82c4ba4345add0a025caa	Crypteroniaceae.Vin
d76f82f670ae983c553ecac05ca77958e9c761e05f3e0e6d741372d34348a340	Ragworm.Bat
30612f5a43f9cb99f90f87fa6b63bf0f886f6acf2ef0ddddc2663437e9ec0261	DefenderCSP.dll

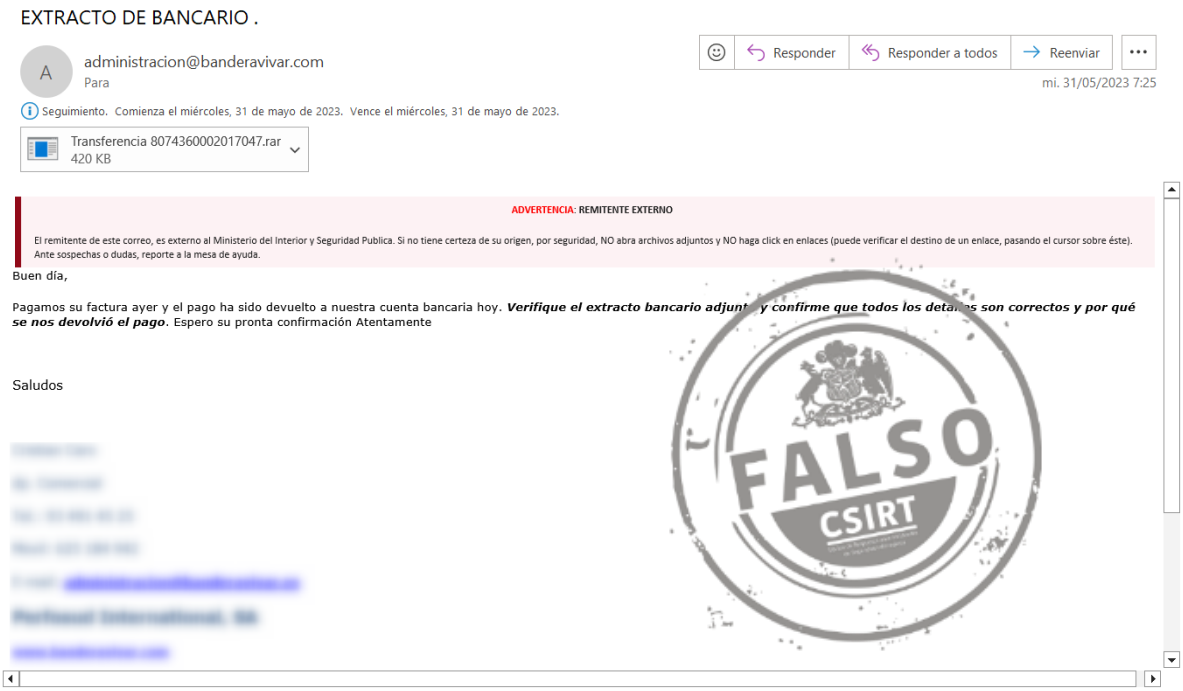
URL-Dominio

Dominio	Relación
23.72.32[.]173	IP

MITRE ATT&CK

Descripción	ID
Acceso Inicial (Mediante Phishing)	T1566.002
Ejecución (Intérprete de comandos y secuencias de comandos)	T1059
Escalación de Privilegios (Manipulación de tokens de acceso)	T1134
Evasión de Defensa (Modificación de Registros)	T1112
Descubrimiento (Consulta de Registros)	T1012
Colección (Captura de Video)	T1125

Imagen del Mensaje



CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.05.31 15:58:17 -04'00'