Alerta de seguridad informática	2CMV23-00422-01
Clase de alerta	Fraude
Tipo de incidente	Phishing-Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de junio de 2023
Última revisión	29 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 a Falabella con una falsa orden de compra.

Si la víctima interactúa con el fichero malicioso se encuentra con Formbook, un malware del tipo infostealer, esto es, programas que sustraen información sensible del dispositivo de la víctima como credenciales de acceso y capturas de pantalla, entre otros. 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
653025b16f9404285563b3e17df27b665689d0e8d85a021c90e111ad07c96136	PEDIDO T338.bz
3a338ce32d49e5b279311019e01551483c6a90c0d013be2336a65bb2fd15b10b	PEDIDO T338.exe
ea474ba40224d8899c19d1dacf9fb88d39ab65eba3cbddb0fa41c4da05c5b663	qcnyliem.dll

URL-Dominio

Dominio	Relación
www.gudusisamfbank[.]africa/a04y/	C2
154.64.247[.]44	IP
64.190.63[.]111	IP
64.190.62[.]22	IP

MITRE ATT&CK

Descripción	ID
Acceso Inicial (Mediante Phishing)	T1566.002
Ejecución (Ejecución del usuario)	T1204.002
Ejecución (Shell de comandos de Windows)	T1059.003
Descubrimiento (Información del sistema)	T1082

Imagen del Mensaje

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.06.29 17:21:25 -04'00'