

Alerta de Seguridad Cibernética

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT
Ministerio del Interior y Seguridad Pública
Subsecretaría del Interior



Alerta de seguridad informática	2CMV23-00420-01
Clase de alerta	Fraude
Tipo de incidente	Phishing-Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de junio de 2023
Última revisión	27 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, difundida a través de emails con información de ventas.

El malware incluido en estos correos electrónicos maliciosos es Agent Tesla, programa que sustrae información confidencial y la envía a los atacantes. Para lograrlo, busca las credenciales que se almacenan en diferentes programas como navegadores, clientes de correo electrónico, clientes FTP/SCP, bases de datos, herramientas de administración remota, VPN y mensajería instantánea. Además, este malware es capaz de robar datos que se encuentren en el portapapeles, grabar las pulsaciones del teclado (función de keylogger) y realizar capturas de pantalla.

Agent Tesla envía toda la información sustraída a los atacantes por medio de correo electrónico, Telegram o los sube a un sitio web o servidor de FTP.

CONTACTO Y REDES SOCIALES CSIRT

 <https://www.csirt.gob.cl>
 Teléfonos: 1510 | + (562) 24863850 | Correo: soc-csirt@interior.gob.cl
 @csirtgob
 <https://www.linkedin.com/company/csirt-gob>

Alerta de Seguridad Cibernética

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT
Ministerio del Interior y Seguridad Pública
Subsecretaría del Interior



Indicadores de Compromiso Asociados

Archivos que se encuentran en la amenaza

SHA256

Indicador	Relación
4fd825574f5084d155dc6deacedb51ba422cc3904b651af71b7298a9e8ab202f	Pedido P20230620-N enviado_pdf.uue
371de82eccda3f11d11e98a6265274bb708b2350ad47c77b4319da1d51764f64b	Pedido P20230620-N enviado_pdf.exe

URL-Dominio

Dominio	Relación
40.79.189[.]59	IP
209.197.3[.]8	IP
http://api.ipify[.]org/	Whois

MITRE ATT&CK

Descripción	ID
Acceso Inicial (Mediante Phishing)	T1566.002
Colección (Datos del sistema local)	T1005
Colección (Colección de correos)	T1114
Credenciales de acceso	T1081

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>
 Teléfonos: 1510 | + (562) 24863850 | Correo: soc-csirt@interior.gob.cl
 @csirtgob
 <https://www.linkedin.com/company/csirt-gob>

Imagen del Mensaje

Re: Pedido P20230620-N enviado



Jessika Gomez <djaramillo@umcoecuador.com>
Para [Redacted]

   Responder  Responder a todos  Reenviar 

ju. 22/06/2023 16:33

 Haga clic aquí para descargar imágenes. Para ayudarle a proteger su confidencialidad, Outlook ha impedido la descarga automática de algunas imágenes en este mensaje.

 Pedido P20230620-N enviado_pdf.uue
727 KB

Hola pibacache

Ordene P20230620-N (SFI SFI1812ML470C-LF) * 2000PCS Por favor verifique
Ordene P20230620-O (SFI SFI1812ML470C-LF) * 2000PCS por favor verifique

Gracias

=====

[Blurred contact information]



CONTACTO Y REDES SOCIALES CSIRT

 <https://www.csirt.gob.cl>
 Teléfonos: 1510 | + (562) 24863850 | Correo: soc-csirt@interior.gob.cl
 @csirtgob
 <https://www.linkedin.com/company/csirt-gob>