Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

15-09-2022 | Año 4 | N°167

Boletín de Seguridad Cibernética

Semana del 9 al 14 de septiembre de 2022

La semana en cifras

Parches

65

para vulnerabilidades

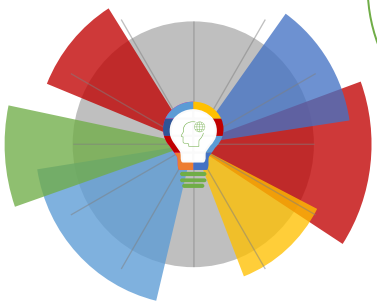
Las mitigaciones son útiles en productos de Microsoft.

IP

4

Informadas

Listado de IP advertidas en múltiples campañas de phishing y de malware.



Se advirtieron

7

URL

Asociadas a sitios fraudulentos y campañas de phishing y malware.

Hash

6

Asociadas a múltiples campañas de phishing con archivos que contienen malware

*Los datos recopilados corresponden a información publicada en diferentes secciones del sitio web https://www.csirt.gob.cl.

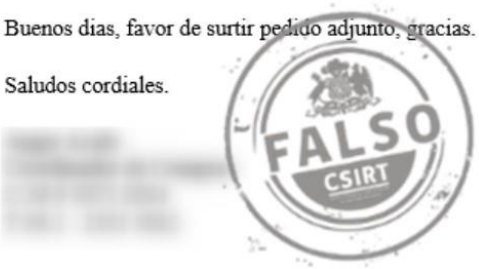
Contenido

Malware

Imagen del Mensaje

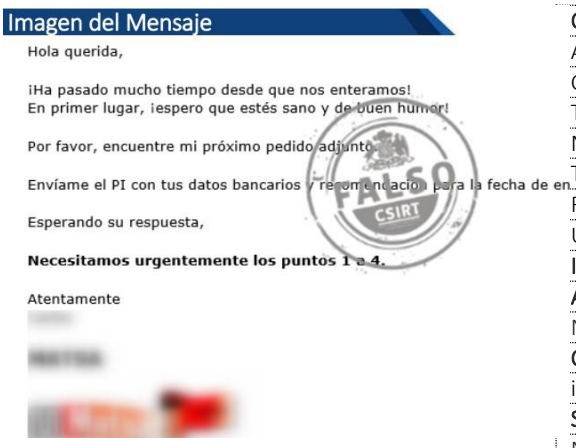
CSIRT alerta ante nueva campaña de phishing que suplanta a cementerio	
Alerta de seguridad cibernética	2CMV22-00343-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de septiembre de 2022
Última revisión	9 de septiembre de 2022
Indicadores de compromiso	
Asunto	
Estado de Saldos Vencidos de Julio y Agosto (SOA)	
Correo de salida	
jefetic@jardineslacolina.com	
SHA256	
Nombre: Doc 02321- Aviso de pago.xlsx SHA256: 187f085ad4f062f5ca8faf70d7b096fd7f274e5aef00808a56d0f557aaf90ee2	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00343-01/	
https://www.csirt.gob.cl/edia/2022/09/2CMV22-00343-PH-01.pdf	

Imagen del Mensaje



CSIRT advierte de campaña de phishing que suplanta a firma chilena con falso pago	
Alerta de seguridad cibernética	2CMV22-00344-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de septiembre de 2022
Última revisión	13 de septiembre de 2022
Indicadores de compromiso	
Asunto	
PEDIDO Nº 5975	
Correo de Salida	
angie.acalo@kupfer.cl	
SHA256	
Nombre: PEDIDO Nº 5975.exe SHA256: 16d20b33c5a1cadda1acc1d383d7c96e9bf57ee847aa9c4ed2561b1171b45306	

Nombre: wAGZF.exe SHA256: 842fa93601b522ff91e2c4805eb568d1cf418d0d45f9cde942491365ea479ab2
Enlaces para revisar el informe:
https://www.csirt.gob.cl/alertas/2cmv22-00344-01/
https://www.csirt.gob.cl/media/2022/09/2CMV22-00344-PH-01.pdf



CSIRT alerta de campaña de phishing que suplanta a Matsa	
Alerta de seguridad cibernética	2CMV22-00345-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de septiembre de 2022
Última revisión	14 de septiembre de 2022
Indicadores de compromiso	
Asunto	
Nuevo pedido	
Correo de Salida	
info@matsa.es	
SHA256	
Nombre: NUEVO PEDIDO-MATSA 13-2022.IMG SHA256: 55b5efd17fc90d33f1934b8f2a42a2e2fccf56007d1ea5090c0a7da72b2a41c2	
Nombre: NUEVO_PE.EXE SHA256: cf7188027fdf9e58695083342a2217ab861354ce960b324f4f59cbd350569a6c	
Nombre: System.dll SHA256: 2e226715419a5882e2e14278940ee8ef0aa648a3ef7af5b3dc252674111962bc	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00345-01/	
https://www.csirt.gob.cl/media/2022/09/2CMV22-00345-PH-01.pdf	

Phishing

Imagen del mensaje

CSIRT alerta ante nueva campaña de phishing que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FPH22-00588-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de septiembre de 2022
Última revisión	9 de septiembre de 2022
Indicadores de compromiso	
URL sitio redirección	
https://asedl.am/Servicio_Cliente/cuenta-ebqv/	
URL sitio falso	
http://prueba.uthh.edu.mx/src/santander.personas/es/	
IP	
[186.64.122.206]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00588-01/	
https://www.csirt.gob.cl/media/2022/09/8FPH22-00588-01-3.pdf	

Imagen del mensaje

SIRT alerta de campaña de phishing que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH22-00589-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de septiembre de 2022
Última revisión	14 de septiembre de 2022
Indicadores de compromiso	
URL sitio redirección	
https://bit[.]ly/3eMz8nj?l=www.bancoripley.cl	
https://julien.dyhost[.]fr/wp-includes/certificates/enviar02.php?l=361929793	
URL sitio falso	
http://web.bancoripley.cl.wollombiorganics[.]com.au/1663159957/login	
IP	
[80.96.234.254]	
[116.0.23.240]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00589-01/	
https://www.csirt.gob.cl/media/2022/09/8FPH22-00589-01.pdf	

CSIRT alerta de campaña de phishing con falso documento de pago	
Alerta de seguridad cibernética	8FPH22-00590-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de septiembre de 2022
Última revisión	14 de septiembre de 2022
Indicadores de compromiso	
URL sitio redirección	
file:///C:/Users/%User%/Downloads/Payroll_____.html	
URL sitio falso	
https://formspree.io/thanks?language=es	
IP	
[80.96.234.254]	
[172.66.40.119]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00590-01/	
https://www.csirt.gob.cl/media/2022/09/8FPH22-00590-01.pdf	

Vulnerabilidades

CSIRT comparte vulnerabilidades del Update Tuesday Microsoft Septiembre 2022	
Alerta de seguridad cibernética	9VSA22-00702-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de septiembre de 2022
Última revisión	13 de septiembre de 2022
CVE	
CVE-2022-26929	CVE-2022-37956
CVE-2022-38013	CVE-2022-37955
CVE-2022-38009	CVE-2022-37954
CVE-2022-38008	CVE-2022-34734
CVE-2022-38007	CVE-2022-34733
CVE-2022-35803	CVE-2022-34732
CVE-2022-38011	CVE-2022-34731
CVE-2022-37959	CVE-2022-34730
CVE-2022-38006	CVE-2022-34729
CVE-2022-37958	CVE-2022-34728
CVE-2022-37964	CVE-2022-34727
CVE-2022-37963	CVE-2022-34726

CVE-2022-37962	CVE-2022-34725
CVE-2022-38010	CVE-2022-34724
CVE-2022-37961	CVE-2022-34723
CVE-2022-38005	CVE-2022-34722
CVE-2022-37957	CVE-2022-34721
CVE-2022-38004	CVE-2022-34720
CVE-2022-35835	CVE-2022-34718
CVE-2022-35834	CVE-2022-34719
CVE-2022-35833	CVE-2022-35841
CVE-2022-35832	CVE-2022-35840
CVE-2022-35831	CVE-2022-35838
CVE-2022-35830	CVE-2022-35837
CVE-2022-35828	CVE-2022-35836
CVE-2022-35823	CVE-2022-38019
CVE-2022-33679	CVE-2022-37969
CVE-2022-33647	CVE-2022-30170
CVE-2022-30200	CVE-2022-26928
CVE-2022-30196	CVE-2022-23960
CVE-2022-34700	CVE-2022-38020
CVE-2022-35805	
Fabricantes	
Microsoft	
Productos afectados	
AV1 Video Extension Azure ARC Microsoft .NET Framework 3.5 AND 4.8 Microsoft Defender for Endpoint for Mac Microsoft Dynamics CRM (on-premises) 9.1 Microsoft Office 2013 Service Pack 1 (64-bit editions) Microsoft Office LTSC 2021 for 32-bit editions Microsoft SharePoint Foundation 2013 Service Pack 1 Microsoft SharePoint Server Subscription Edition Microsoft Visio 2016 (64-bit edition) Microsoft Visual Studio 2022 version 17.2 Raw Image Extension Visual Studio Code Windows 10 Version 21H2 for x64-based Systems Windows 11 for ARM64-based Systems Windows RT 8.1 Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Windows Server 2012 R2 (Server Core installation) Windows Server 2016 (Server Core installation)	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00702-01/	
https://www.csirt.gob.cl/media/2022/08/9VSA22-00693-01.pdf	

Actualidad

Comité Interministerial de Ciberseguridad reinicia sus reuniones

La semana pasada semana se volvió a reunir, por primera vez bajo la administración del Presidente Gabriel Boric, el Comité Interministerial sobre Ciberseguridad, comisión asesora presidencial creada en el año 2015 y que entre sus misiones debe realizar el seguimiento e implementación de la Política Nacional de Ciberseguridad 2018-2022, además de comenzar el trabajo de actualización de la Política para el período 2023-2028.

La reunión se realizó en el Palacio La Moneda, encabezada por el Subsecretario del Interior, Manuel Monsalve y contó con la participación de los subsecretarios de Defensa, Relaciones Exteriores, General de la Presidencia, Justicia, Economía, Energía, Minería, Telecomunicaciones y el director de la Agencia Nacional de Inteligencia

En la reunión fue presentado el abogado y doctor en derecho, Daniel Álvarez Valenzuela, quien presidirá el Comité Interministerial, en su calidad de Coordinador Nacional de Ciberseguridad.

Recomendaciones y buenas prácticas

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet.
- Prestar atención en los detalles de los mensajes o redes sociales.
- Evaluar el bloqueo preventivo de los indicadores de compromisos.
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas.
- Revisar los controles de seguridad de los antispam y sandboxing.
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
- Visualizar los sitios web que se ingresen sean los oficiales.

Muro de la Fama

El siguiente es el listado de personas y organizaciones que han colaborado explícitamente con el CSIRT de Gobierno para mejorar la seguridad informática en instituciones y organismos del Estado, **al informar campañas de phishing, malware y/o sitios fraudulentos.**

El CSIRT de Gobierno destaca en este segmento a quienes reportaron incidentes utilizando canales formales (https://www.csirt.gob.cl o al teléfono **1510** siempre que hayan aportado información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- Daniel Carrasco
- Felipe Cortés
- Romel Rivas
- Rodrigo Torres