CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE CIBERSEGURIDAD

Año 5 | N.º 255

semana del 17 al 23 de mayo de 2024

LA SEMANA EN CIFRAS

IP INFORMADAS

4

IP advertidas en múltiples campañas de phishing y de fraude.

URL ADVERTIDAS

4

URL asociadas a sitios fraudulentos y campañas de phishing y malware

PARCHES COMPARTIDOS

50

Las mitigaciones son útiles en productos de Adobe, Ivanti, D-Link y Apache Flink.

HASH REPORTADOS

6

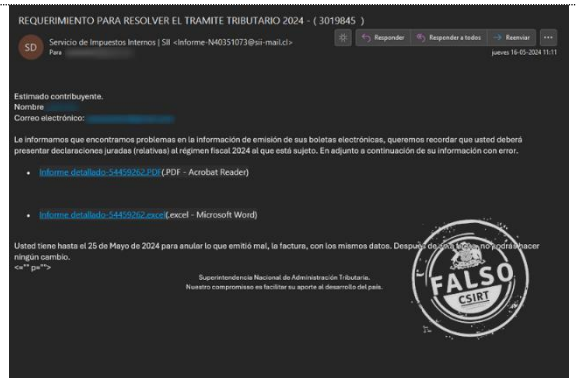
Hashes asociados a múltiples campañas de phishing con archivos que contienen malware.

CONTENIDO

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

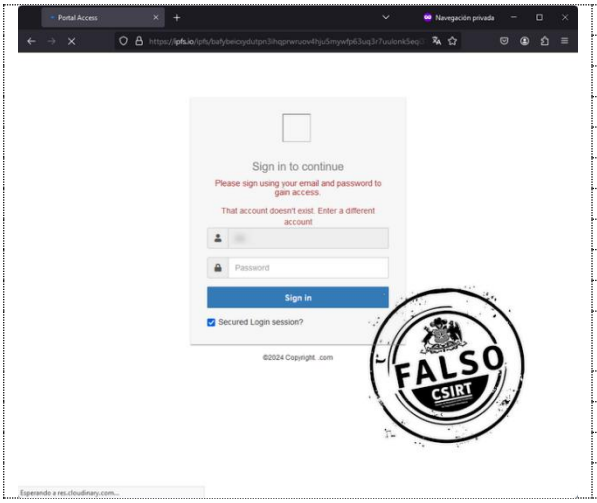
1. Malware

Ministerio Público (Fiscalia de Chile) - Suplantación con malware	
Código de alerta	CMV24-00462
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de mayo de 2024
Última revisión	17 de mayo de 2024
Indicadores de compromiso	
Asunto	
Citacion a fiscalia	
SHA256	
aa7d80daa488e8627316e1e24bef1a713ae4f86e4a6304c6784b6187ad0433d9 f98cb51b72234756df112ccfa9a412c20b313c26ef459b042a99a090a0ced8d8	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/cmv24-00462/	



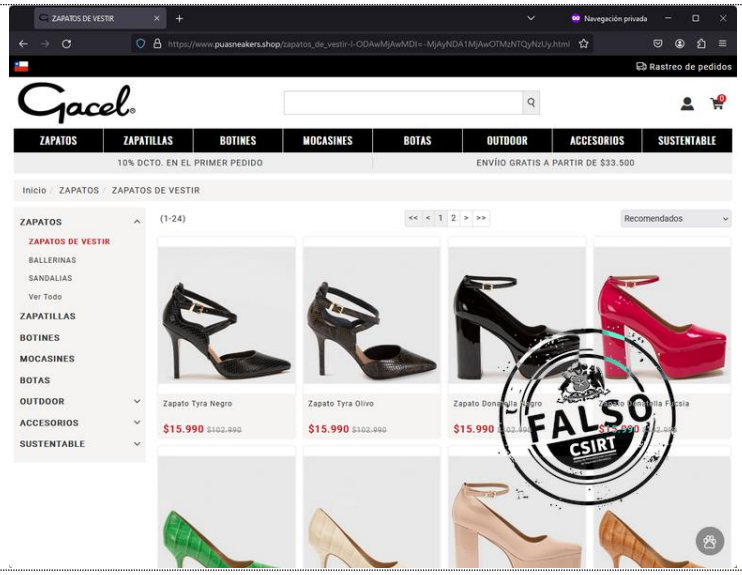
Servicio de Impuestos Internos - Suplantación con malware	
Código de alerta	CMV24-00463
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de mayo de 2024
Última revisión	22 de mayo de 2024
Indicadores de compromiso	
Asunto	
REQUERIMIENTO PARA RESOLVER EL TRAMITE TRIBUTARIO 2024 – (3019845)	
Correo de salida	
Informe-N40351073@sii-mail.cl	
SHA256	
7e643c188a1ee3b0251b7dfcab000b7c48fd840eff35189e8a45901852e3910a d12f56009bcdf27276235380343948f1f909cf17c1490c5c91ec2c2a8cffc699 e28e34fbdaff077669586dcdb4e10f0ba2ca6c9973ed4d372a5c3ec3b8ad20e7 e87329c39e9647d1f4bd64400a2988f9c83b3547845c998ae6bfbcb361d6240c	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/cmv24-00463/	

2. Phishing

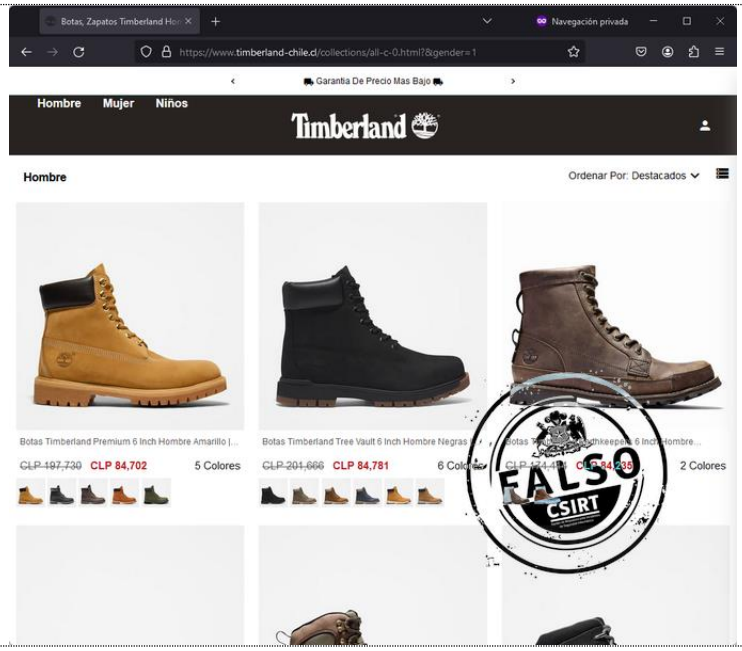


BancoEstado - Phishing	
Alerta de seguridad cibernética	FPH24-00959
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de mayo de 2024
Última revisión	20 de mayo de 2024
Indicadores de compromiso	
URL del sitio falso	
https://ipfs.io/ipfs/bafybeicxydutpn3ihqprwruov4hju5mywfp63uq3r7uulonk5eqi37xnha/bar050824.html#{Correoelectronico}	
Dirección IP sitio falso	
[209.94.90.1]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/fph24-00959/	

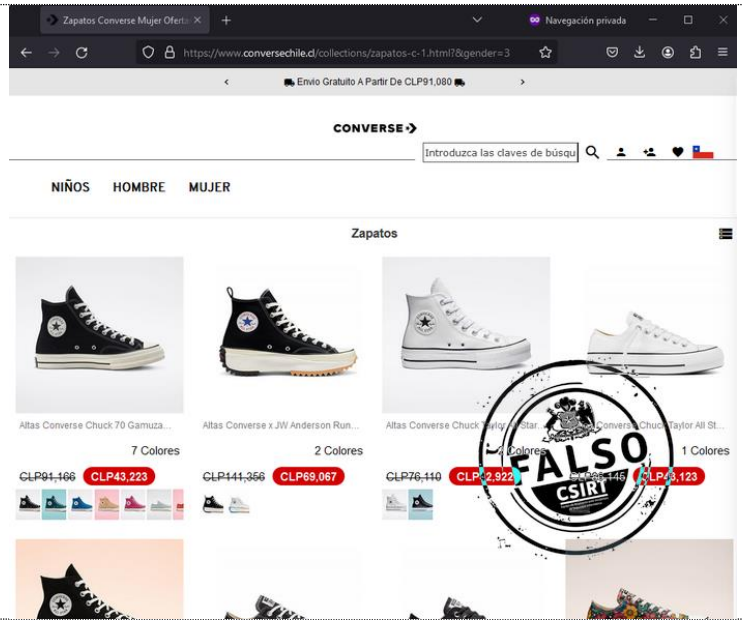
3. Sitios fraudulentos



Gacel - Falsificación	
Código de alerta	FFR24-01685
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de mayo de 2024
Última revisión	20 de mayo de 2024
Indicadores de compromiso	
URL del sitio falso	
https://www.puasneakers.shop	
Dirección IP sitio falso	
[23.252.71.140]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr24-01685/	



Timberland - Falsificación	
Código de alerta	FFR24-01686
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de mayo de 2024
Última revisión	20 de mayo de 2024
Indicadores de compromiso	
URL del sitio falso	
https://www.timberland-chile.cl	
Dirección IP sitio falso	
[172.67.148.127]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr24-01686/	



Converse - Falsificación	
Código de alerta	FFR24-01687
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de mayo de 2024
Última revisión	22 de mayo de 2024
Indicadores de compromiso	
URL del sitio falso	
https://www.conversechile.cl	
Dirección IP sitio falso	
[196.196.206.102]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr24-01687/	

4. Vulnerabilidades

Adobe

Detalles e informe en https://csirt.gob.cl/alertas

Adobe Acrobat y otros - Vulnerabilidades			
Código de alerta	VSA24-01018		
Clase de alerta	Vulnerabilidad		
Tipo de incidente	Sistema y/o Software Abierto		
Nivel de riesgo	Alto		
TLP	Blanco		
Fecha de lanzamiento original	17 de mayo de 2024		
Última revisión	17 de mayo de 2024		
CVE y puntaje CVSS al momento de la publicación			
CVE-2024-30284	7.8	CVE-2024-30309	5.5
CVE-2024-30310	7.8	CVE-2024-30275	7.8
CVE-2024-34094	7.8	CVE-2024-30281	5.5
CVE-2024-34095	7.8	CVE-2024-30282	7.8
CVE-2024-34096	7.8	CVE-2024-30293	7.8
CVE-2024-34097	7.8	CVE-2024-30294	7.8
CVE-2024-34098	7.8	CVE-2024-30298	5.5
CVE-2024-34099	7.8	CVE-2024-30295	7.8
CVE-2024-34100	7.8	CVE-2024-30296	7.8
CVE-2024-30311	5.5	CVE-2024-30297	7.8
CVE-2024-30312	5.5	CVE-2024-30283	5.5
CVE-2024-34101	5.3	CVE-2024-30286	5.5
CVE-2024-20791	7.8	CVE-2024-30287	5.5
CVE-2024-20792	7.8	CVE-2024-30288	7.8
CVE-2024-20793	5.5	CVE-2024-30289	7.8
CVE-2024-30274	7.8	CVE-2024-30290	7.8
CVE-2024-30307	7.8	CVE-2024-30291	7.8
CVE-2024-30308	5.5	CVE-2024-30292	7.8
Fabricante			
Adobe			
Productos afectados			
Adobe Acrobat 24.002.20736 y anteriores 20.005.30574 y anteriores Adobe Illustrator 28.4 y anteriores 27.9.3 y anteriores Adobe Substance 3D Painter 9.1.2 y anteriores Adobe Aero: 0.23.4 y anteriores Adobe Substance 3D Designer 13.1.1 y anteriores Adobe Animate 23.0.5 y anteriores 24.0.2 y anteriores Adobe FrameMaker 2020 Release Update 5 y anteriores 2022 Release Update 3 y anteriores Adobe Dreamweaver: 21.3 y anteriores			
Enlaces para revisar el informe:			
https://csirt.gob.cl/alertas/vsa24-01018/			

Apache Flink - Vulnerabilidades	
Código de alerta	VSA24-01019
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de mayo de 2024
Última revisión	23 de mayo de 2024

CVE, CVSS y EPSS al momento de la publicación

CVE-2020-17519	7.5	97.08%

Fabricante

Apache Software Foundation

Productos afectados

Apache Flink
1.11.0
1.11.1
1.11.2

Enlaces para revisar el informe:

https://csirt.gob.cl/alertas/vsa24-01019

Ivanti - Vulnerabilidades	
Código de alerta	VSA24-01020
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de mayo de 2024
Última revisión	23 de mayo de 2024

CVE y CVSS al momento de la publicación

CVE-2024-29822	9.6
CVE-2024-29823	9.6
CVE-2024-29824	9.6
CVE-2024-29825	9.6
CVE-2024-29826	9.6
CVE-2024-29827	9.6
CVE-2024-29828	8.4
CVE-2024-29829	8.4
CVE-2024-29830	8.4
CVE-2024-29846	8.4
CVE-2024-29848	7.2

Fabricante

Ivanti

Productos afectados

Ivanti Endpoint Manager (EPM)
2022 SU5 y anteriores
Ivanti Avalanche
6.4.3.602

Enlaces para revisar el informe:

https://csirt.gob.cl/alertas/vsa24-01020

ivanti

Detalles e informe en https://csirt.gob.cl/alertas

Ivanti - Vulnerabilidades	
Código de alerta	VSA24-01020
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de mayo de 2024
Última revisión	23 de mayo de 2024

CVE y CVSS al momento de la publicación

CVE-2024-29822	9.6
CVE-2024-29823	9.6
CVE-2024-29824	9.6
CVE-2024-29825	9.6
CVE-2024-29826	9.6
CVE-2024-29827	9.6
CVE-2024-29828	8.4
CVE-2024-29829	8.4
CVE-2024-29830	8.4
CVE-2024-29846	8.4
CVE-2024-29848	7.2

Fabricante

Ivanti

Productos afectados

Ivanti Endpoint Manager (EPM)
2022 SU5 y anteriores
Ivanti Avalanche
6.4.3.602

Enlaces para revisar el informe:

https://csirt.gob.cl/alertas/vsa24-01020

D-Link®

Detalles e informe en https://csirt.gob.cl/alertas

D-Link DIR-600 (routers) - Vulnerabilidades	
Código de alerta	VSA24-01021
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de mayo de 2024
Última revisión	23 de mayo de 2024

CVE al momento de la publicación

CVE-2014-100005
CVE-2021-40655

Fabricante

D-Link

Productos afectados

D-Link DIR-600 (routers)
firmware anterior a 2.17b02
D-LINK-DIR-605 B2
firmware 2.01MT

Enlaces para revisar el informe:

https://csirt.gob.cl/alertas/vsa24-01021

5. 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 que los sitios web a los que se ingrese sean los oficiales.

6. 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.

- Adrián Muñoz
- Pablo cornejo
- Alejandro Cuzmar
- Pablo Cornejo
- José
- Raul Ciudad De la Cruz
- Francisco Melipin
- Sergio Mateluna Durán
- Jenny Garrido Escobar
- Oscar Alejandro Guarda Ríos
- Melissa Silva Sandoval

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.05.24 16:56:40 -04'00'