

18-11-2022 | Año 4 | N°176



Boletín de Seguridad C i h e r n é t i c a

Semana del 11 al 17 de
noviembre de 2022



La semana en cifras



Parches

44

para vulnerabilidades

Las mitigaciones son útiles en productos de VMware, Microsoft, y Cisco.

IP

16

Informadas

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

Se advirtieron

33

URL

Asociadas a sitios fraudulentos y campañas de phishing y malware.

Hash

19

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.....	2
Sitios fraudulentos	5
Phishing	7
Vulnerabilidades	13
Actualidad.....	16
Recomendaciones y buenas prácticas	19
Muro de la Fama	20

Malware

Imagen del mensaje



CSIRT alerta por campaña de phishing con malware suplantando al Gobierno de Colombia

Alerta de seguridad cibernética	2CMV22-00386-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de noviembre de 2022
Última revisión	10 de noviembre de 2022

Indicadores de compromiso

Asunto

FOTO MULTA COMPARENDO N.º 2022-1404996-02147824-0214

Correo de Salida

system@aravfashion-it.co

SHA256

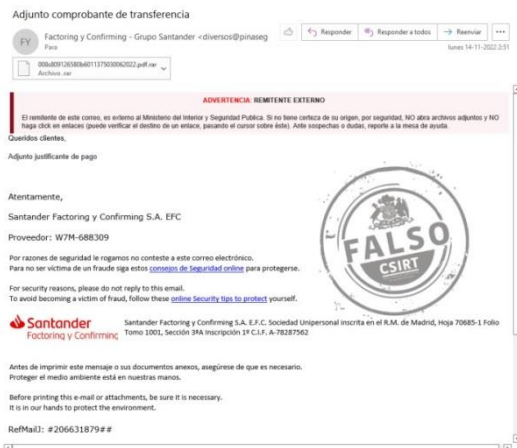
3f3007a39c377bc9950ae5a50e3554bcc7048ee5fe360c6fffe27802c5996cbd
db43da863a30ccb8b9ef22d095d99cc35dcb6b2b00948c9a040b79abb48d4bf
24206ed80e794c58f551f647c94348709113eca7f1bd286aecc4adbb33e95a63
54716a9a3a8fb7cc6be3074ea0472703ec03e1421d553b0dc6b3ebe7b1ec10bb

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/2cmv22-00386-01/>

<https://www.csirt.gob.cl/media/2022/11/2CMV22-00386-01.pdf>

Imagen del mensaje



CSIRT alerta de nueva campaña de phishing con malware que suplanta al Banco Santander

Alerta de seguridad cibernética	2CMV22-00387-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de noviembre de 2022
Última revisión	14 de noviembre de 2022

Indicadores de compromiso

Asunto

Adjunto comprobante de transferencia

Correo de Salida

diversos@pinaseguros.es

SHA256

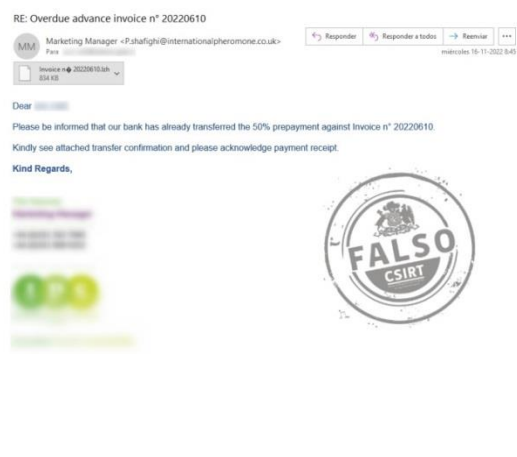
678607d19a7a21422224bce7c253e6f1da0587f516e92b46162b13139e
fa999d
bb6a92b2c43488bf8d0310090aa4036b5e292c9ab5030c8ebdd1864cf0
15f9ba
8dc562cda7217a3a52db898243de3e2ed68b80e62ddcb8619545ed0b4
e7f65a8
cd163c9574c86f211b519830a0bce9c3d74430acc64228215b2d992d9b
39c7fc
343d00b5160de03fee5fee222145b0ac302dc62dff45deb61ea0c4fb804
497ba

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/2cmv22-00387-01/>

<https://www.csirt.gob.cl/media/2022/11/2CMV22-00387-01.pdf>

Imagen del mensaje



CSIRT alerta nueva campaña de phishing que suplanta a International Pheromone Systems

Alerta de seguridad cibernética	2CMV22-00388-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de noviembre de 2022
Última revisión	16 de noviembre de 2022

Indicadores de compromiso

Asunto

RE: Overdue advance invoice n° 20220610

Correo de Salida

saed@prodeksqn.com

SHA256

dfb468fae58c6ee797fb5fd0be45e66fb70faf272b818617b3c2d9c5a153
a8b1

3da539d2f3f68c823e556e637665b03f2501e510c36db2429fe17ad44e903da6
5202e2495a0e7dcf8ac12e7047fa00dfb538a744a208dd961e957d89f00437ac
0df3d05900e7b530f6c2a281d43c47839f2cf2a5d386553c8dc46e463a635a2c
2d0dc6216f613ac7551a7e70a798c22aee8eb9819428b1357e2b8c73bef905ad
3da539d2f3f68c823e556e637665b03f2501e510c36db2429fe17ad44e903da6
798af20db39280f90a1d35f2ac2c1d62124d1f5218a2a0fa29d87a13340bd3e4

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/2cmv22-00388-01/>

<https://www.csirt.gob.cl/media/2022/11/2CMV22-00388-01.pdf>

Imagen del mensaje



SIRT alerta ante campaña de phishing con malware, que suplanta a Visal

Alerta de seguridad cibernética	2CMV22-00389-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de noviembre de 2022
Última revisión	17 de noviembre de 2022

Indicadores de compromiso

Asunto
Pago
Correo de Salida
hp0.wx16.mxox.live
SHA256
4d68da161b1af8576c9369c6eec16c3d03a5e8e64ca174bf7f8973ce9307e7dc ca7434f2057c0acfdcd70e9cd0681aa277114b919574210e74f241c5b3821dd7 e49a4116f04876e54b060724fbfc883e81c0b454274586d3fc14c4c5f03308dc

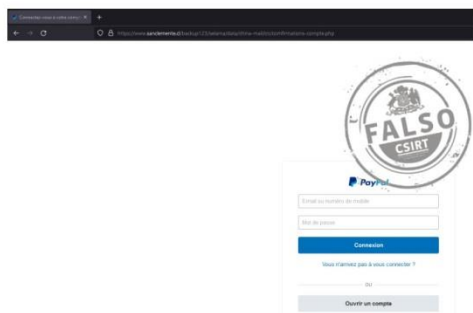
Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/2cmv22-00389-01/>

<https://www.csirt.gob.cl/media/2022/11/2CMV22-00389-01.pdf>

Sitios fraudulentos

Imagen del sitio



CSIRT alerta de página fraudulenta que suplanta login de PayPal	
Alerta de seguridad cibernética	8FFR22-01135-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de noviembre de 2022
Última revisión	10 de noviembre de 2022
Indicadores de compromiso	
URL sitio falso	https://www.sanclemente[.]cl/backup123/selama/data/china-mail/cn/comfirmations-compte.php
IP	[190.121.17.234]
Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8ffr22-01135-01/
	https://www.csirt.gob.cl/media/2022/11/8FFR22-01135-01.pdf

Imagen del sitio



CSIRT alerta de sitio fraudulento que suplanta banco DCU de EE.UU.	
Alerta de seguridad cibernética	8FFR22-01136-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de noviembre de 2022
Última revisión	16 de noviembre de 2022
Indicadores de compromiso	
URL sitio falso	https://educacioncolaborativa[.]cl/wp-includes/dcu.org.htm
IP	[131.72.236.23]
Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8ffr22-01136-01/
	https://www.csirt.gob.cl/media/2022/11/8FFR22-01136-01.pdf

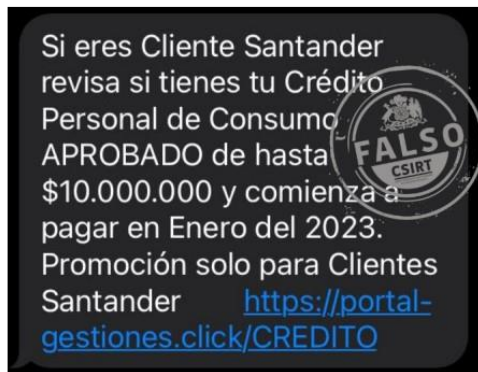
Imagen del sitio



CSIRT alerta de nueva página fraudulenta que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR22-01137-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de noviembre de 2022
Última revisión	17 de noviembre de 2022
Indicadores de compromiso	
URL sitio falso	
http://santandermovil-personas.drlisandroromagnoli[.]com	
http://santandermovil-personas.drlisandroromagnoli[.]com/1668697001/portada/personas/home.asp	
http://santandermovil-personas.drlisandroromagnoli[.]com/1668697001/LoginJSFGenerico	
IP	
[186.64.119.165]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01137-01/	
https://www.csirt.gob.cl/media/2022/11/8FFR22-01137-01.pdf	

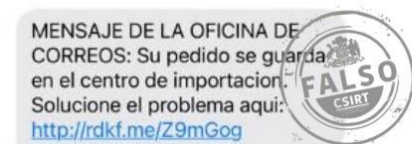
Phishing

Imagen del mensaje



CSIRT alerta de campaña de phishing que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FPH22-00640-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de noviembre de 2022
Última revisión	9 de noviembre de 2022
Indicadores de compromiso	
URL redirección	https://portal-gestiones[.]click/inicio/gestor
URL sitio falso	https://portal-gestiones[.]click/inicio/gestor
IP	[172.67.178.246]
Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8fph22-00640-01/
	https://www.csirt.gob.cl/media/2022/11/8FPH22-00640-01.pdf

Imagen del mensaje



CSIRT alerta de campaña de phishing con falso mensaje de «la oficina de correos»	
Alerta de seguridad cibernética	8FPH22-00641-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de noviembre de 2022
Última revisión	9 de noviembre de 2022
Indicadores de compromiso	
URL sitio redirección	http://rdkf[.]me/Z9mGog
URL sitio falso	https://lukygift[.]live/ips_cl/?cep=5TAaChbLAV6Fr2QTrMOz4YiZwHW0iKYS6-FLfbCIB_vx-4tcl43VqVIBFidyKx1BfS9urhD2HqrvDcDyufSo9NFuPiEHyCwvdpWrC83TU9_1K3FVu0AdTosB4gyfS3JtyuKsDiM_Py-oKVuYcuYlhjAP7zIOrHLh0pTW783I9Y_HmZAlfujkW2s-B5Dh-cbJeCXXQPMmWofA1yg4OsgAHLQJlx4cmBSLBRxWRB-Rd-3w3-hBRwmiHBXbcEiY4hJlktbjQCMz4-cYjSfNLbWwQsLMQKMgwt8yPNqU8RY8L9kGdLCXYNvzubIMq-SCg6NZYitbodGLK3rbSiQQu2narKLQT-SS8geOM4fTWtsE-uQkMmyB010ACjPlyxf-g&Iptoken=16f668db044c332068f8
URL sitio falso	https://www.securepagenow[.]com/?gra=6a7b5176&transaction_id=636c4b89ece13a0343f4040b&info1=1127_19-&info2=19-
IP	[5.199.173.123]
Enlaces para revisar el informe:	

<https://www.csirt.gob.cl/alertas/8fph22-00641-01/>
<https://www.csirt.gob.cl/media/2022/11/8FPH22-00641-01.pdf>

Imagen del mensaje



CSIRT alerta de campaña de phishing que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FPH22-00642-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de noviembre de 2022
Última revisión	10 de noviembre de 2022
Indicadores de compromiso	
URL redirección	https://grandbwis[.]com/activacion/cuenta-rgqo/
URL sitio falso	https://fu3rzasolu[.]site/1668084774/imagenes/_personas/home/default.asp
IP	[47.87.240.144]
Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8fph22-00642-01/
	https://www.csirt.gob.cl/media/2022/11/8FPH22-00642-01.pdf

Imagen del mensaje

Si eres Cliente Santander revisa si tienes tu Crédito Personal de Consumo APROBADO de hasta \$10.000.000 y comienza a pagar en Enero del 2023. Promoción solo para Clientes Santander <https://portal-gestiones.click/CREDITO>



CSIRT alerta de nueva campaña de phishing por SMS que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FPH22-00643-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de noviembre de 2022
Última revisión	10 de noviembre de 2022
Indicadores de compromiso	
URL redirección	http://rdkf[.]me/Z9mGog
URL sitio falso	https://lukygift[.]live/ips_cl/?cep=5TAaChbLAV6Fr2QTrMOz4YiZwHW0ikY56-FLfbCIB_vx-4tcl43VqVIBFidyKx1BfS9urhD2HqrvDcDyufSo9NFuPiEHyCwmdpWrc83TU9_1K3FVU0AdTOsB4gyfS3JtyuKsDiM_Py-oKVuYcuYlHjAP7zI0rHLh0pTWWh783l9Y_HmZAlfujkW2s-B5Dh-cbJeCXQQPmmWofA1yg4OsgAHLQJlx4cmBSLBRxWRb-Rd-3w3-hBRwmiHBXBcEY4hJlktbjQCMz4-cyJsfNLbWwQsLMQKMgwt8yPNqU8RY8L9kGdLCXYNvzubIMq-SCg6NZYitbodGkK3rbSiQQu2narKLQT-SS8geOM4fTWtsE-uQkMmyB010ACjPlyxf-g&lptoken=16f668db044c332068f8
URL sitio falso	https://www.securepagenow[.]com/?gra=6a7b5176&transaction_id=636c4b89ece13a0343f4040b&info1=1127_19-&info2=19-
IP	[172.67.178.246]

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8fph22-00643-01/>

<https://www.csirt.gob.cl/media/2022/11/8FPH22-00643-01.pdf>

Imagen del mensaje



CSIRT alerta de nueva campaña de phishing que suplanta al BancoEstado

Alerta de seguridad cibernética	8FPH22-00644-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de noviembre de 2022
Última revisión	14 de noviembre de 2022

Indicadores de compromiso

URL redirección

[https://nmhpatito\[.\]info/Solicitud_Aprobada/cuenta-bini/](https://nmhpatito[.]info/Solicitud_Aprobada/cuenta-bini/)

URL sitio falso

[https://vircomarthe\[.\]buzz/1668436192/imagenes/_personas/home/default.asp](https://vircomarthe[.]buzz/1668436192/imagenes/_personas/home/default.asp)

IP

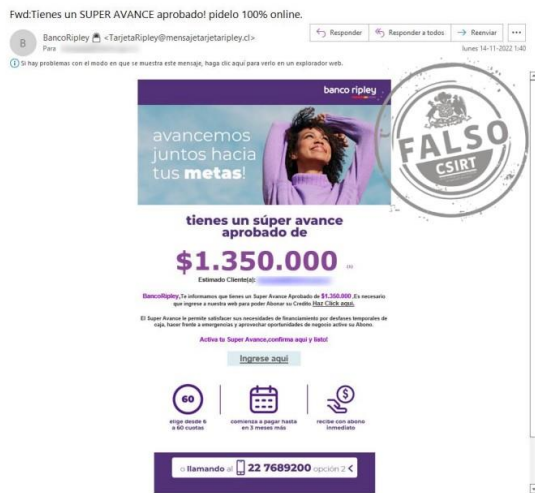
[47.87.146.254]

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8fph22-00644-01/>

<https://www.csirt.gob.cl/media/2022/11/8FPH22-00644-01.pdf>

Imagen del mensaje



CSIRT alerta de nueva campaña de phishing que suplanta al Banco Ripley

Alerta de seguridad cibernética	8FPH22-00645-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de noviembre de 2022
Última revisión	14 de noviembre de 2022

Indicadores de compromiso

URL redirección

[https://bit\[.\]ly/3G9NNEN?l=www.bancoripley.cl](https://bit[.]ly/3G9NNEN?l=www.bancoripley.cl)

URL sitio falso

[https://web.bancoripley\[.\]cl.madhurmatka.live/1668436962/login](https://web.bancoripley[.]cl.madhurmatka.live/1668436962/login)

IP

[47.87.146.254]

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8fph22-00645-01/>

<https://www.csirt.gob.cl/media/2022/11/8FPH22-00645-01.pdf>

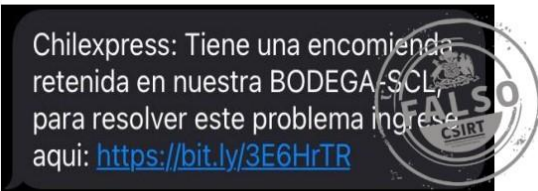
Imagen del mensaje



CSIRT alerta de campaña de phishing por SMS (smishing) que suplanta a Chilexpress

Alerta de seguridad cibernética	8FPH22-00646-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de noviembre de 2022
Última revisión	14 de noviembre de 2022
Indicadores de compromiso	
URL redirección	https://nostracontrical[.]com/promociones/cuenta-lvpc/
URL sitio falso	https://carterplush[.]com/1668437915/portada/personas/home.asp
URL redirección	https://nostracontrical[.]com/promociones/cuenta-lvpc/
IP	[190.107.176.120]
Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8fph22-00646-01/
	https://www.csirt.gob.cl/media/2022/11/8FPH22-00646-01.pdf

Imagen del mensaje



CSIRT alerta de campaña de phishing por SMS (smishing) que suplanta a Chilexpress

Alerta de seguridad cibernética	8FPH22-00647-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de noviembre de 2022
Última revisión	14 de noviembre de 2022
Indicadores de compromiso	
URL redirección	https://bit[.]ly/3E6HrTR
URL sitio falso	https://r.chilexpress-sclb[.]live/r/k4o3ksn
URL redirección	https://envios.chilexpress-sclb[.]live/Contingencia/Of7f904ced195adb8b4f2fcbda525464
URL sitio falso	https://envios.chilexpress-sclb[.]live/chilexpress/payment/id/40fa73c9d0083043c6/transbankPaymentProceso/Ti9BfHx8Ti9BPTFINTU1Zjc3NDliNDQzNmFjZmE4ZTQxMGlyZDk2MTI0PWFInzRlODUyZGJmMmMyN2M2NmY4NTg0ZWwEONWE2ODIm
IP	[23.227.202.26]
Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8fph22-00647-01/

<https://www.csirt.gob.cl/media/2022/11/8FPH22-00647-01.pdf>

Imagen del mensaje



CSIRT alerta de nueva campaña de phishing que suplanta al BancoEstado

Alerta de seguridad cibernética	8FPH22-00648-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de noviembre de 2022
Última revisión	15 de noviembre de 2022

Indicadores de compromiso

URL redirección	https://nmhpatito[.]info/Solicitud_Aprobada/cuenta-bini/
URL sitio falso	https://notipatico[.]site/1668524693/imagenes/_personas/home/default.asp
IP	[47.87.240.144]
Enlaces para revisar el informe:	https://www.csirt.gob.cl/alertas/8fph22-00648-01/ https://www.csirt.gob.cl/media/2022/11/8FPH22-00648-01.pdf

Imagen del mensaje



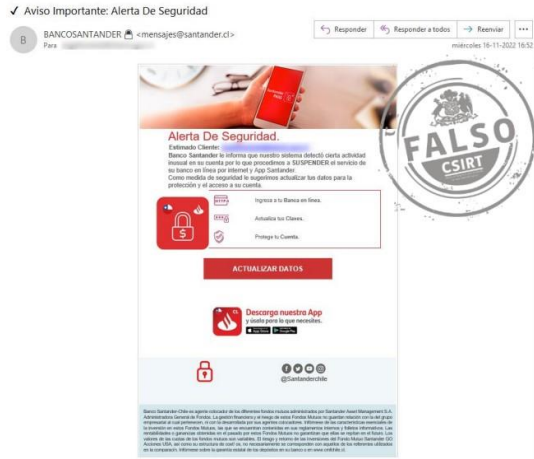
CSIRT alerta de nueva campaña de phishing que suplanta al BancoEstado

Alerta de seguridad cibernética	8FPH22-00649-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de noviembre de 2022
Última revisión	16 de noviembre de 2022

Indicadores de compromiso

URL redirección	https://nhmwcotitostado.info/activacion/cuenta-ulen/
URL sitio falso	https://nwmonline.site/1668625089/imagenes/_personas/home/default.asp
IP	[47.87.240.144]
Enlaces para revisar el informe:	https://www.csirt.gob.cl/alertas/8fph22-00649-01/ https://www.csirt.gob.cl/media/2022/11/8FPH22-00649-01.pdf

Imagen del mensaje



CSIRT alerta de nueva campaña de phishing que suplanta al Banco Santander

Alerta de seguridad cibernética	8FPH22-00650-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de noviembre de 2022
Última revisión	16 de noviembre de 2022

Indicadores de compromiso

URL redirección	https://nostracontral[.]com/promociones/cuenta-chzw/
URL sitio falso	https://hannaplus[.]com/1668628647/portada/personas/home.asp
IP	[162.241.60.25]

Enlaces para revisar el informe:

- <https://www.csirt.gob.cl/alertas/8fph22-00650-01/>
- <https://www.csirt.gob.cl/media/2022/11/8FPH22-00650-01.pdf>

Imagen del mensaje



CSIRT alerta de nueva campaña de phishing que suplanta al BancoEstado

Alerta de seguridad cibernética	8FPH22-00651-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de noviembre de 2022
Última revisión	17 de noviembre de 2022

Indicadores de compromiso

URL redirección	https://nhmwcotitostado[.]info/activacion/cuenta-ulen/
URL sitio falso	https://nwmonline.site/1668693567/imagenes/_personas/home/default.asp
IP	[47.87.240.144]

Enlaces para revisar el informe:

- <https://www.csirt.gob.cl/alertas/8fph22-00651-01/>
- <https://www.csirt.gob.cl/media/2022/11/8FPH22-00651-01.pdf>

Vulnerabilidades



INFORME DE Vulnerabilidad

9VSA22-00743-01
CSIRT comparte vulnerabilidades que son resueltas por Xcode 14.1 de Apple

PARA REGISTRAR | 1510
UN INCIDENTE | www.csirt.gob.cl

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT comparte información sobre vulnerabilidades parchadas por Xcode 14.1 de Apple	
Alerta de seguridad cibernética	9VSA22-00743-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de noviembre de 2022
Última revisión	9 de noviembre de 2022
CVE	
CVE-2022-29187	
CVE-2022-39253	
CVE-2022-39260	
CVE-2022-42797	
Fabricante	
Apple	
Productos afectados	
macOS Monterey 12.5 y posterior	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00743-01/	
https://www.csirt.gob.cl/media/2022/11/9VSA22-00743-01.pdf	



INFORME DE Vulnerabilidad

9VSA22-00744-01
CSIRT comparte vulnerabilidades comunicadas por Cisco para varios productos

PARA REGISTRAR | 1510
UN INCIDENTE | www.csirt.gob.cl

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT comparte vulnerabilidades comunicadas por Cisco		
Alerta de seguridad cibernética	9VSA22-00744-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Crítico	
TLP	Blanco	
Fecha de lanzamiento original	15 de noviembre de 2022	
Última revisión	15 de noviembre de 2022	
CVE		
CVE-2022-20947	CVE-2022-20928	CVE-2022-20838
CVE-2022-20946	CVE-2022-20950	CVE-2022-20839
CVE-2022-20924	CVE-2022-20922	CVE-2022-20840
CVE-2022-20927	CVE-2022-20943	CVE-2022-20843
CVE-2022-20745	CVE-2022-20941	CVE-2022-20872
CVE-2022-20854	CVE-2022-20940	CVE-2022-20905
CVE-2022-20918	CVE-2022-20831	CVE-2022-20932
CVE-2022-20826	CVE-2022-20832	CVE-2022-20935
CVE-2022-20949	CVE-2022-20833	CVE-2022-20936
CVE-2022-20925	CVE-2022-20834	CVE-2022-20713
CVE-2022-20926	CVE-2022-20835	CVE-2022-20938
CVE-2022-20934	CVE-2022-20836	
Fabricantes		

Cisco
Productos afectados
Cisco Firepower Threat Defense Software
Cisco Firepower Threat Defense Software
Cisco Firepower Management Center Software
Cisco Firepower Software for ASA Firepower Module
Cisco Adaptive Security Appliance Software
Cisco NGIPS Software
Cisco Secure Firewall 3100 Series
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00744-01/
https://www.csirt.gob.cl/media/2022/11/9VSA22-00744-01.pdf



CSIRT comparte vulnerabilidades en Citrix Gateway y Citrix ADC	
Alerta de seguridad cibernética	9VSA22-00745-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	15 de noviembre de 2022
Última revisión	15 de noviembre de 2022
CVE	
CVE-2022-27510	
CVE-2022-27513	
CVE-2022-27516	
Fabricantes	
Citrix	
Productos afectados	
Citrix Gateway	
Citrix ADC	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00745-01/	
https://www.csirt.gob.cl/media/2022/11/9VSA22-00745-01.pdf	



CSIRT alerta de nuevas vulnerabilidades en BIG-IP y BIG-IQ de F5	
Alerta de seguridad cibernética	9VSA22-00746-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	17 de noviembre de 2022
Última revisión	17 de noviembre de 2022
CVE	
CVE-2022-41622 CVE-2022-41800	
Fabricantes	
F5	
Productos afectados	
BIG-IP 13.x, 14.x, 15.x, 16.x, y 17.x BIG-IQ Centralized Management versiones 7.x y 8.x.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00746-01/	
https://www.csirt.gob.cl/media/2022/11/9VSA22-00746-01.pdf	

Actualidad

CSIRT de Gobierno participa en conversatorio sobre Digitalización y Ciberseguridad en Personas Mayores

El incremento de la población de adultos mayores y el aumento del uso de Internet y la tecnología, ha demostrado la importancia de educar y acercar la ciberseguridad tanto a este grupo etario como a toda la población.

Como parte de su misión y para contribuir en la concientización en temas de digitalización, la Caja de Compensación Los Héroes organizó el miércoles 9 de noviembre un conversatorio titulado “Digitalización y Ciberseguridad en Personas Mayores”, actividad en la que participó Ingrid Inda, jefa de la División de Redes y Seguridad Informática y del CSIRT del Ministerio del Interior, Pelayo Covarrubias, Presidente de la Fundación País Digital y Director de Proyectos Corporativos de la Universidad del Desarrollo, y Marcelo Wong, jefe del Centro Nacional de Ciberseguridad de la PDI.



Al evento también fueron invitados grupos de adultos mayores beneficiarios de Los Héroes, siendo precisamente el sector de la población cuyo uso de internet motivó la investigación de la caja de compensación y la UDD.

El evento se inició con las palabras de Alejandro Muñoz, Gerente General de la Caja de Compensación los Héroes, quien enfatizó que “este conversatorio aborda un tema muy interesante como es la digitalización y ciberseguridad en personas mayores. Un tema que nos toca directamente, ya que poco antes de la pandemia, teníamos disponible nuestra cuenta de prepago, siendo la primera caja hoy en día en emitir una cuenta con provisión de fondos. Y la experiencia fue muy exitosa, logrando que adultos mayores que jamás habían tenido contacto con un medio de pago digital, comenzaran este camino”.

Ver más: <https://www.csirt.gob.cl/noticias/conversatorio-los-heroes/>

Ciberconsejos para evitar estafas en personas mayores

De acuerdo al estudio «Radiografía Digital en Personas Mayores», un tercio de las personas mayores encuestadas han sido víctima de estafas digitales, principalmente, con tarjetas y cuentas bancarias. Existen distintas técnicas para cometer las estafas, entre ellas, phishing, smishing y vishing, y en todos estos casos el delincuente busca obtener robar dinero u obtener información de la víctima suplantando la identidad de una institución o una persona.



ESTUDIO "RADIOGRAFÍA DIGITAL EN PERSONAS MAYORES"

De acuerdo a este estudio, 1 de cada 3 personas mayores ha sido víctima de estafas digitales, principalmente, con tarjetas y cuentas bancarias.

Fuente: Estudio Radiografía Digital en Personas Mayores* elaborado por VTR y Critería.



TIPOS DE ESTAFAS

- **Phishing:** Correo electrónico que suplanta la identidad de una institución o persona.
- **Smishing:** Estafa que circula por mensajes de texto (SMS) o WhatsApp.
- **Vishing:** Fraude que se realiza vía telefónica, suplantando la identidad de un tercero de confianza.



¿CÓMO RECONOCER UN MENSAJE MALICIOSO?

- El nombre del destinatario está mal escrito o el correo no es de la institución.
- El mensaje es de carácter urgente, solicitando dinero o informando de una situación irregular con tu cuenta bancaria.
- Tiene faltas de ortografía.



RECOMENDACIONES SI RECIBES UN PHISHING O SMISHING:

- 1 **NUNCA** descargues archivos adjuntos. Pueden tener un programa malicioso.
- 2 **EVITA** ingresar a los enlaces que se adjuntan en el correo. En caso de hacerlo, nunca ingreses tus datos personales.
- 3 **PUEDES** reportar al CSIRT de Gobierno al 1510 o a soc@interior.gob.cl



OTROS CONSEJOS:

- 1 **EVITA** anotar las contraseñas. Si lo haces, nunca las dejes en lugares visibles.
- 2 **SIEMPRE** cierra la sesión de la página del banco, correo o app.
- 3 **CONFIRMA** lo que recibes
- 4 **USA** contraseñas diferentes.
- 5 **NUNCA** entregues información personal o transfieras dinero a desconocidos.

Ver más: <https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-personas-mayores/>

Ciberdiccionario Volumen 23

En la vigesimotercera entrada del Ciberdiccionario, les hablamos de NFT, ataques a la cadena de suministro, fintechs y trabajo híbrido.



Ciber diccionario

NFT: Sigla en inglés de "ficha no fungible", activos digitales inscritos en un blockchain y que en teoría son únicos y no pueden ser replicados (de ahí lo de "no fungible"). Asociados principalmente a imágenes, se han vuelto un producto popular para la inversión especulativa en los últimos años.



Ciber diccionario

Trabajo híbrido: Modalidad de trabajo impulsada por la pandemia, que combina instancias de teletrabajo con trabajo presencial. Requiere de coordinación para que los empleados puedan seguir trabajando en equipo sin importar si están en casa o en la oficina.



Ciber diccionario

Ataque a la cadena de suministro: Se trata de una amenaza en la que los actores maliciosos infectan a un proveedor tecnológico con el objetivo de comprometer, a través de éste, a sus clientes y usuarios. Esto, al introducir código malicioso en el software del proveedor, y aprovechar la confianza que tienen en éste sus clientes.



Ciber diccionario

Fintech (o Fintec): A punto de ser reguladas en Chile (apenas se promulgue la ley que las define), son empresas que entregan productos y servicios financieros por vías tecnológicas, compañías que ahora serán supervisadas por la Comisión para el Mercado Financiero (CMF).



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.

- Sebastián Fuentes
- Roberto Alvarado
- Rose Fuentes
- Pablo Abarca
- Leonel Contreras
- Angelo Olivares
- Rosa Concha
- Sebastián Hernández
- Ana Castro
- Pablo Ascencio
- Héctor Hidalgo

