Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

17-12-2021 | Año 3 | N°128

Boletín de Seguridad Cibernética

Semana del 10 al 16 de diciembre de 2021

La semana en cifras

Hash

137

SHA

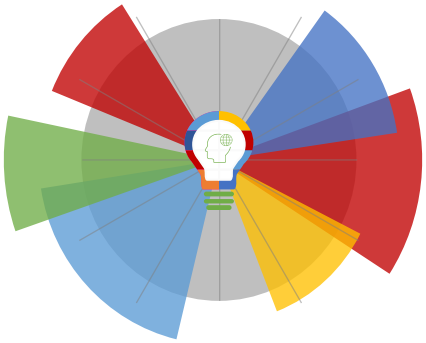
Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron

54

URL

Asociadas a sitios fraudulentos y campañas de phishing y malware.



Parches

101

para vulnerabilidades

Las mitigaciones son útiles en productos Apache, Google, Microsoft y Apple.

IP

95

Informadas

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

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

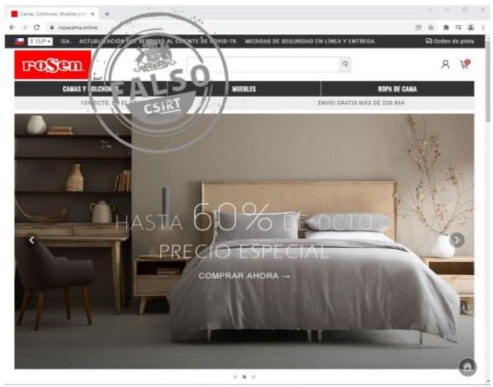
Contenido

Sitios fraudulentos 2
Phishing 8
Malware 10
Vulnerabilidades 12
IoC Malware 15
IoC Ataques de Fuerza Bruta 21
Noticias 22
Actualidad 24
Recomendaciones y buenas prácticas 25
Muro de la Fama 26

Sitios fraudulentos

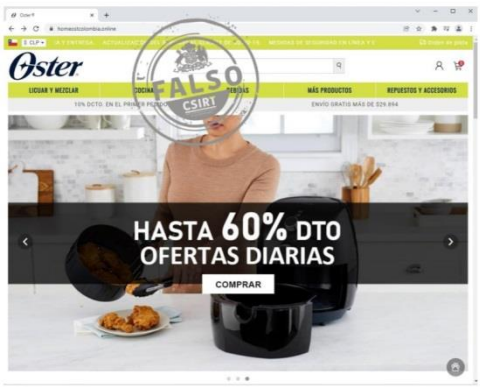
Imagen del sitio

Así lucen algunos de los sitios fraudulentos.



CSIRT alerta 13 sitios fraudulentos que suplantan a varias conocidas tiendas online	
Alerta de seguridad cibernética	8FFR21-01029-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de diciembre de 2021
Última revisión	10 de diciembre de 2021
Indicadores de compromiso	
URL sitio falso	
https://www.vicoloutlet[.]shop https://www.lippoutlet[.]website https://www.calzeoutlet[.]online https://www.myroupadormir[.]shop https://www.amphoutlet[.]online https://www.stradivonline[.]shop https://www.jokchaussures[.]online https://www.velecoutlet[.]online https://www.nafnarobes[.]online https://www.romarebajas[.]online https://www.cnonropacama[.]shop https://www.mereloutlet[.]online https://ropacama[.]online	
IP	
[5.255.62.156] [5.255.62.157] [5.255.62.154] [5.255.62.140] [5.255.62.139] [5.255.62.138]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01029-01/	
https://www.csirt.gob.cl/media/2021/12/8FFR21-01029-01.pdf	

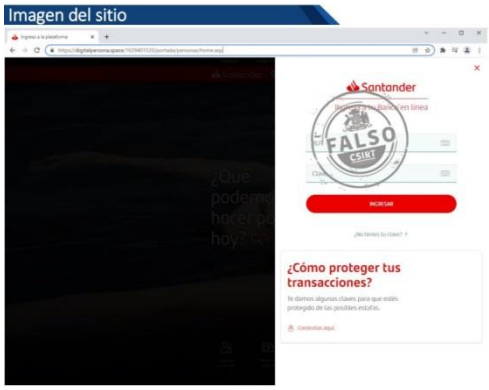
Imagen del sitio



CSIRT alerta de páginas fraudulentas que suplantan a 28 marcas de vestuario y decoración	
Alerta de seguridad cibernética	8FFR21-01030-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de diciembre de 2021
Última revisión	10 de diciembre de 2021
Indicadores de compromiso	
URL sitio falso	
https://www.brunosale[.]online https://www.esalbotas[.]online https://www.monoprixv[.]online https://www.tezenisaldi[.]store https://www.azaleiacl[.]online https://www.skizapatillas[.]shop https://www.lcosoldes[.]online https://www.masduoutlet[.]online https://www.roupaspringfield[.]online https://www.deitecl[.]com https://www.costeoutlet[.]shop https://www.cannsabanas[.]online https://www.ovsshop[.]online https://www.tezenisonline[.]store https://www.okaidshop[.]online https://www.dogsmall[.]shop https://www.szapatosk[.]online https://www.doitechile[.]shop https://www.coajanuary[.]shop https://www.womanroupas[.]website https://www.certeflout[.]online https://www.calzesoldes[.]online https://www.hakaoutlet[.]shop https://www.vetementsvente[.]online https://www.bramhaco[.]com https://www.bershoutlet[.]online https://www.homeostcolombia[.]online https://www.bimbobagshop[.]online	
IP	
[185.212.172.121] [185.212.172.125] [185.212.172.126] [185.212.172.118] [185.212.172.116] [185.212.172.115] [185.212.172.114]	

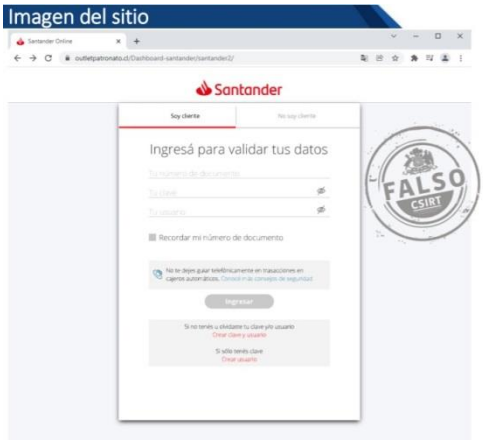
[185.212.172.113] [185.212.172.112] [185.212.172.111] [185.212.172.110] [185.212.172.109] [185.212.172.107] [185.212.172.105] [185.212.172.103] [185.212.172.102] [185.212.172.101] [185.212.172.99] [185.212.172.98]
Enlaces para revisar el informe:
https://www.csirt.gob.cl/alertas/8ffr21-01030-01/
https://www.csirt.gob.cl/media/2021/12/8FFR21-01030-01.pdf

Imagen del sitio



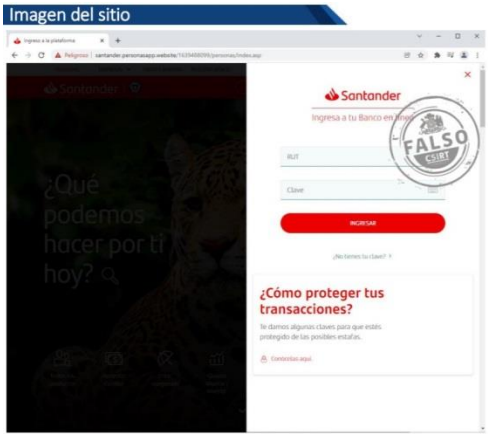
CSIRT advierte suplantación del sitio web del Banco Santander	
Alerta de seguridad cibernética	8FFR21-01031-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de diciembre de 2021
Última revisión	13 de diciembre de 2021
Indicadores de compromiso	
URL sitio falso	
https://digitalpersona[.]space/1639401520/portada/personas/home.asp	
IP	
[51.255.26.63]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01031-01/	
https://www.csirt.gob.cl/media/2021/12/8FFR21-01031-01.pdf	

Imagen del sitio



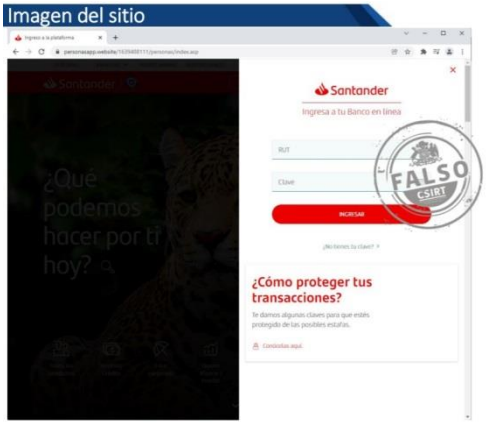
CSIRT informa página falsa del Banco Santander	
Alerta de seguridad cibernética	8FFR21-01032-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de diciembre de 2021
Última revisión	13 de diciembre de 2021
Indicadores de compromiso	
URL sitio falso	
https://outletpatronato[.]cl/Dashboard-santander/santander2/	
IP	
[186.64.117.125]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01032-01/	
https://www.csirt.gob.cl/media/2021/12/8FFR21-01032-01.pdf	

Imagen del sitio



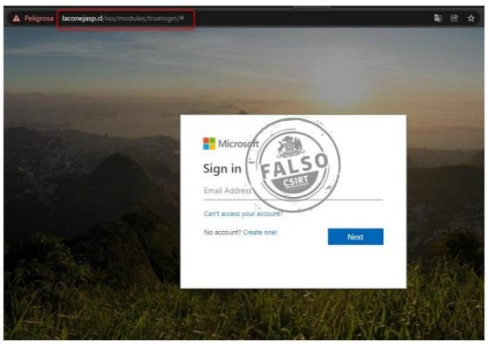
CSIRT informa sitio falso del Banco Santander	
Alerta de seguridad cibernética	8FFR21-01033-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de diciembre de 2021
Última revisión	14 de diciembre de 2021
Indicadores de compromiso	
URL sitio falso	
https://santander.personasapp[.]website/1639488099/personas/index.asp	
IP	
[198.54.116.174]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01033-01/	
https://www.csirt.gob.cl/media/2021/12/8FFR21-01033-01.pdf	

Imagen del sitio



CSIRT advierte sitio web fraudulento del Banco Santander	
Alerta de seguridad cibernética	8FFR21-01034-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de diciembre de 2021
Última revisión	14 de diciembre de 2021
Indicadores de compromiso	
URL sitio falso	
https://personasapp[.]website/1639488111/personas/index.asp	
IP	
[198.54.116.174]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01034-01/	
https://www.csirt.gob.cl/media/2021/12/8FFR21-01034-01.pdf	

Imagen del sitio



CSIRT alerta sitio web que suplanta a Microsoft	
Alerta de seguridad cibernética	8FFR21-01035-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de diciembre de 2021
Última revisión	15 de diciembre de 2021
Indicadores de compromiso	
URL sitio falso	
hXXps://laconejasp[.]cl/xxx/modules/truelogin/#	
IP	
[50.87.148.157]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01035-01/	
https://www.csirt.gob.cl/media/2021/12/8FFR21-01035-01.pdf	

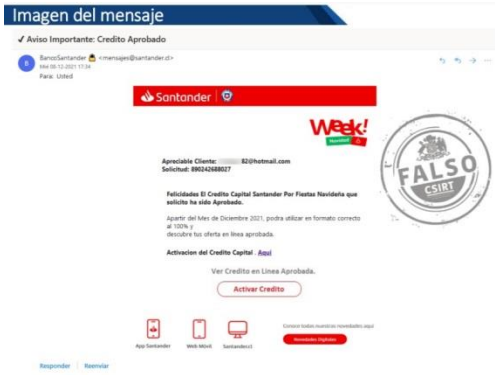
Imagen del sitio

CSIRT advierte sitio web que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR21-01036-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de diciembre de 2021
Última revisión	16 de diciembre de 2021
Indicadores de compromiso	
URL sitio falso	
https://personaschile[.]website/1639658356/personas/index.asp	
IP	
[162.0.229.159]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01036-01/	
https://www.csirt.gob.cl/media/2021/12/8FFR21-01036-01.pdf	

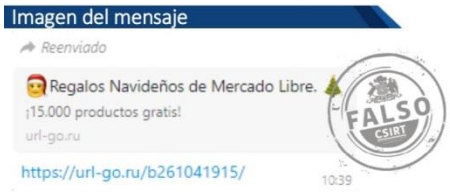
Imagen del sitio

CSIRT informa suplantación de página web del Banco Santander	
Alerta de seguridad cibernética	8FFR21-01037-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de diciembre de 2021
Última revisión	16 de diciembre de 2021
Indicadores de compromiso	
URL sitio falso	
hXXps://midtownlokal[.]com/vin/santander.co.uk.html	
IP	
[172.67.171.187]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01037-01/	
https://www.csirt.gob.cl/media/2021/12/8FFR21-01037-01.pdf	

Phishing



CSIRT alerta campaña de phishing con falso crédito navideño aprobado	
Alerta de seguridad cibernética	8FPH21-00450-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de diciembre de 2021
Última revisión	10 de diciembre de 2021
Indicadores de compromiso	
URL redirección	
hXXp://yashevents.co[.]in/ganador/promo-nqfs/	
URL sitio falso	
hXXp://katka-masopustova[.]cz/solutions/pagina/login.asp	
IP	
[46.101.52.30]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00450-01/	
https://www.csirt.gob.cl/media/2021/12/8FPH21-00450-01.pdf	



CSIRT advierte phishing con falsos regalos navideños de Mercado Libre	
Alerta de seguridad cibernética	8FPH21-00451-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de diciembre de 2021
Última revisión	14 de diciembre de 2021
Indicadores de compromiso	
URL sitio falso	
https://url-go[.]ru/b261041915/#1639489602478	
IP	
[172.67.204.75]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00451-01/	
https://www.csirt.gob.cl/media/2021/12/8FPH21-00451-01.pdf	

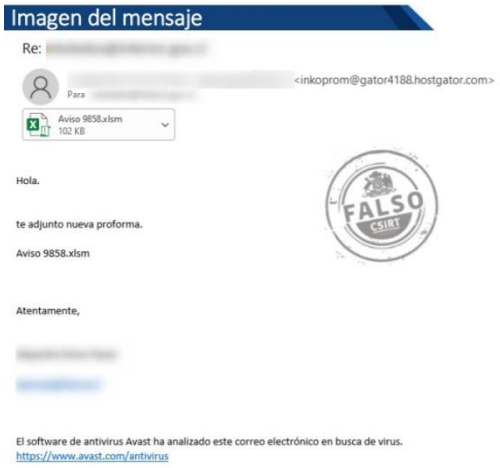
Imagen del mensaje

CSIRT advierte phishing con un supuesto crédito aprobado del Banco Estado	
Alerta de seguridad cibernética	8FPH21-00452-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de diciembre de 2021
Última revisión	14 de diciembre de 2021
Indicadores de compromiso	
URL redirección	
https://antoinedl[.]com/activacion/cuenta-qghl/	
URL sitio falso	
http://resilit[.]co/Cliente/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[173.201.176.153]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00452-01/	
https://www.csirt.gob.cl/media/2021/12/8FPH21-00452-01.pdf	

Imagen del sitio

CSIRT advierte phishing de falso regalo por parte del Supermercado Líder	
Alerta de seguridad cibernética	8FPH21-00453-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de diciembre de 2021
Última revisión	14 de diciembre de 2021
Indicadores de compromiso	
URL sitio falso	
https://studiocustomers[.]com/	
IP	
[172.67.74.50]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00453-01/	
https://www.csirt.gob.cl/media/2021/12/8FPH21-00453-01.pdf	

Malware



CSIRT informa campaña de malware Emotet	
Alerta de seguridad cibernética	2CMV21-00259-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de diciembre de 2021
Última revisión	13 de diciembre de 2021

Indicadores de compromiso

SHA256

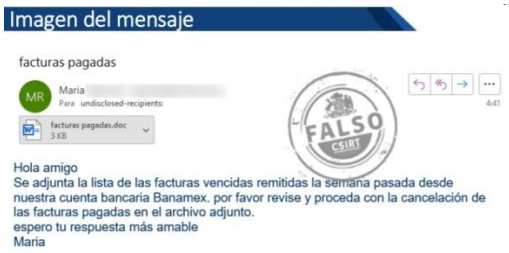
fd26a94765cceb90cee033ac4a4f2a69d919525c40aa2aac30680f27df1c35ba
1357816A7FC1F42F32D31D5F44A9F87CA42E9AC40E759CD970F386661FC7062F

IoC red

209[.]239.112.82:8080
116[.]124.128.206:8080
45[.]63.5.129:443
128[.]199.192.135:8080
51[.]178.61.60:443
168[.]197.250.14:80
177[.]72.80.14:7080
51[.]210.242.234:8080
142[.]4.219.173:8080
78[.]47.204.80:443
78[.]46.73.125:443
37[.]44.244.177:8080
37[.]59.209.141:8080
104[.]131.62.48:8080
190[.]90.233.66:443
185[.]148.168.220:8080
185[.]148.168.15:8080
62[.]171.178.147:8080
191[.]252.103.16:80
54[.]38.242.185:443
85[.]214.67.203:8080
217[.]182.143.207:443
159[.]69.237.188:443
210[.]57.209.142:8080
54[.]37.228.122:443
207[.]148.81.119:8080
195[.]77.239.39:8080
66[.]42.57.149:443
195[.]154.146.35:443

Enlaces para revisar el informe:

https://www.csirt.gob.cl/alertas/2cmv21-00259-01/
https://www.csirt.gob.cl/media/2021/12/2CMV21-00259-01.pdf



CSIRT informa campaña de phishing con malware con supuestas facturas vencidas	
Alerta de seguridad cibernética	2CMV21-00261-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de diciembre de 2021
Última revisión	14 de diciembre de 2021
Indicadores de compromiso	
SHA256	
071f6a846ef55f40bd430507bec2649deaf832ce64d51a092a955a1b0dc236a9 524F4BEE46FC825847C3CA6FF14B3D457E3A3D3629AB3B9489B6716C275976A8	
IoC red	
http://kbfvzoboss[.]bid/alien/fre.php http://alphastand[.]trade/alien/fre.php http://alphastand[.]win/alien/fre.php http://alphastand[.]top/alien/fre.php http://archbal[.]sbs/ebraznmsd/enebz.exe http://secure01-redirect[.]net/gb29/fre.php	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv21-00261-01/	
https://www.csirt.gob.cl/media/2021/12/2CMV21-00261-01.pdf	

Vulnerabilidades

CSIRT alerta de vulnerabilidad grave en Apache Log4j 2	
Alerta de seguridad cibernética	9VSA21-00531-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de diciembre de 2021
Última revisión	10 de diciembre de 2021
CVE	
CVE-2021-44228	
Fabricante	
Apache	
Productos afectados	
Apache Log4j 2 versiones 2.0 a 2.14.1.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00531-01/	
https://www.csirt.gob.cl/media/2021/12/9VSA21-00531-01-1.pdf	

CSIRT alerta de vulnerabilidades en Google Chrome	
Alerta de seguridad cibernética	9VSA21-00532-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de diciembre de 2021
Última revisión	14 de diciembre de 2021
CVE	
CVE-2021-4098 CVE-2021-4099 CVE-2021-4100 CVE-2021-4101 CVE-2021-4102	
Fabricante	
Google	
Productos afectados	
Google Chrome, versiones anteriores a la 96.0.4664.110.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00532-01/	
https://www.csirt.gob.cl/media/2021/12/9VSA21-00532-01.pdf	

CSIRT alerta de vulnerabilidades informadas en el Update Tuesday de Microsoft para diciembre	
Alerta de seguridad cibernética	9VSA21-00533-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de diciembre de 2021
Última revisión	14 de diciembre de 2021

CVE

CVE-2021-43905 - CVE-2021-43899 - CVE-2021-42310
CVE-2021-43233 - CVE-2021-43217 - CVE-2021-43215
CVE-2021-43907 - CVE-2021-43892 - CVE-2021-43908
CVE-2021-43896 - CVE-2021-43893 - CVE-2021-43877
CVE-2021-43891 - CVE-2021-43889 - CVE-2021-43888
CVE-2021-43883 - CVE-2021-41365 - CVE-2021-42315
CVE-2021-42314 - CVE-2021-42313 - CVE-2021-42312
CVE-2021-42311 - CVE-2021-43882 - CVE-2021-43880
CVE-2021-43875 - CVE-2021-43256 - CVE-2021-43255
CVE-2021-43248 - CVE-2021-43247 - CVE-2021-43246
CVE-2021-43245 - CVE-2021-43244 - CVE-2021-43243
CVE-2021-43240 - CVE-2021-43239 - CVE-2021-43238
CVE-2021-43237 - CVE-2021-43236 - CVE-2021-43235
CVE-2021-43234 - CVE-2021-43232 - CVE-2021-43231
CVE-2021-43230 - CVE-2021-43229 - CVE-2021-43228
CVE-2021-43227 - CVE-2021-43226 - CVE-2021-43225
CVE-2021-43224 - CVE-2021-43223 - CVE-2021-43222
CVE-2021-43216 - CVE-2021-43214 - CVE-2021-42320
CVE-2021-42295 - CVE-2021-42293 - CVE-2021-41360
CVE-2021-43890 - CVE-2021-42294 - CVE-2021-41333
CVE-2021-40453 - CVE-2021-40452 - CVE-2021-40441
CVE-2021-43242 - CVE-2021-42309 - CVE-2021-43207
CVE-2021-43219

Fabricante

Microsoft

Productos afectados

App Installer
ASP.NET Core 6.0
Bot Framework SDK for .NET Framework
HEVC Video Extensions
Microsoft 4K Wireless Display Adapter
Microsoft BizTalk ESB Toolkit 2.3
Microsoft Defender for IoT
Microsoft Office 2013 Service Pack 1 (64-bit editions)
Microsoft Office LTSC 2021 for 32-bit editions
Microsoft Office Web Apps Server 2013 Service Pack 1
Microsoft SharePoint Foundation 2013 Service Pack 1

Microsoft SharePoint Server Subscription Edition
Office app
PowerShell 7.2
Raw Image Extension
Visual Studio Code
Visual Studio Code WSL Extension
VP9 Video Extensions
Windows 10 Version 21H2 for x64-based Systems
Windows 11 for ARM64-based Systems
Windows Server 2012 R2 (Server Core installation)
Windows Server 2016 (Server Core installation)
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00533-01/
https://www.csirt.gob.cl/media/2021/12/9VSA21-00533-01-1.pdf

CSIRT alerta ante vulnerabilidades en productos Apple	
Alerta de seguridad cibernética	9VSA21-00534-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de diciembre de 2021
Última revisión	14 de diciembre de 2021
CVE	
CVE-2021-30995 - CVE-2021-30954 - CVE-2021-30953 CVE-2021-30984 - CVE-2021-30952 - CVE-2021-30951 CVE-2021-30936 - CVE-2021-30934 - CVE-2021-30964 CVE-2021-30767 - CVE-2021-30947 - CVE-2021-30946 CVE-2021-30968 - CVE-2021-30955 - CVE-2021-30960 CVE-2021-30993 - CVE-2021-30949 - CVE-2021-30980 CVE-2021-30927 - CVE-2021-30937 - CVE-2021-30916 CVE-2021-30939 - CVE-2021-30945 - CVE-2021-30958 CVE-2021-30957 - CVE-2021-30942 - CVE-2021-30926 CVE-2021-30966	
Fabricante	
Apple	
Productos afectados	
iOS 15.2, iPadOS 15.2: iPhone 6s y posteriores, iPad Pro (todos), iPad Air 2 y posteriores, iPad quinta generación y posteriores, iPad mini 4 y posteriores y el iPod touch (séptima generación). macOS Monterey 12.1 tvOS 15.2 (Apple TV 4K y Apple TV HD) watchOS 8.3 (Apple Watch Series 3 y posteriores).	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00534-01/	
https://www.csirt.gob.cl/media/2021/12/9VSA21-00534-01.pdf	

IoC Malware

A continuación, se comparten los Indicadores de Compromisos que fueron detectados durante la semana pasada por el Equipo del CSIRT.
CSIRT recomienda a los administradores y usuarios bloquear los hash publicados en este informe, y mantener un permanente monitoreo sobre el resto de los Indicadores de Compromiso.

HASH	Tipo Malware	Documento web
d83a6855de90f0b74ce3fb412d5352f61128803ace715fff7402138da1ff3468	W32/Kryptik.EQRK!tr	2CMV21-00257-01
9a5ae66f1966774052fc559f2bdfeb42d5e0fd78d659867ed83500c9a3638664	W32/Kryptik.EQRK!tr	2CMV21-00257-01
b037cb6416f8833008a624a80ceb9dc7eb1d3364c57dc7f3a173cff9aac8bc6e	MSIL/GenKryptik.FOPG!tr	2CMV21-00257-01
6bcf9a1d16ef260ca69194251864a1a3b3cf1a78023e20edf2becbb8056f6c1f	MSOffice/CVE_2018_0798	2CMV21-00257-01
71831142b54cc9f5a84b2d17f38daba406ca4ae6ef8702c53d221093c74199ae	Malicious_Behavior.SB	2CMV21-00257-01
981874fe98ed1a2d6435dd2936788aa34416bce7a8de85ae76f0c9ea0abe52ff	MSIL/GenKryptik.FOPG!tr	2CMV21-00257-01
c099d123a8cb3789c6d67f6024e43b108efe07a3c71019832bd55a6a7b22c09a	Riskware/POC_Iframe_CID	2CMV21-00257-01
71831142b54cc9f5a84b2d17f38daba406ca4ae6ef8702c53d221093c74199ae	MSIL/GenKryptik.FOPG!tr	2CMV21-00257-01
8f9e7454dece68ce5af892a7b3603d1c4744841548fcd6ab16e5becf07cfed56	MSIL/GenKryptik.FOPG!tr	2CMV21-00257-01
9efefcb5718fc4a9e45f947ceece6af2454ea4bc7cdc18f427412a335b691ffd	W32/Kryptik.EQRK!tr	2CMV21-00257-01
a7b7b09ad1b216536d85bb7f55f62852ada71f3d0818464e319eee7e8eb2ad2e	MSIL/Kryptik.ADRI!tr	2CMV21-00257-01
c34c5d0575dfe2e39c9e49184dbe26353206193c1f593f0463b082484e6d8738	MSIL/Kryptik.ADRI!tr	2CMV21-00257-01
d3c391224e44ac3cf7c7ba502d0c47316c5e2fc2be6b2da4172900728853f708	MSIL/Kryptik.ADRI!tr	2CMV21-00257-01
2484fb64f74b2c49b5ea851f2f609c9084d0d8aa0b04670d3ecc13fbbe93d62f	MSExcel/CVE_2017_11882	2CMV21-00257-01
6ff96b788c7f56e168ec5d7b81d0e6f2334cfbe764859ee8c9a49a4dbc3c3c78	MSIL/Kryptik.ADRI!tr	2CMV21-00257-01
910b1e687bf0031c11e812c4c0802e9ca6381621a082fbc39aa87c0d5cdb5da0	MSOffice/Agent.GV!tr	2CMV21-00257-01
05c2d3ad069c667d1e9e82a29809c7d31d2e8c060922eb5daec6f3193650d46c	MSIL/Kryptik.ADRI!tr	2CMV21-00257-01
e5d147726f83fec9eb89817a2546d466ef46e1097e95a1ac90c70145bfda2e16	W32/Injector.EQRT!tr	2CMV21-00257-01
4d78612257ceedbc8f6f936d268394fde6e5b655bdf4700be0808d3965c12cc5	Malicious_Behavior.SB	2CMV21-00258-01
6397254ef2bd8192630ab3e7875953bbf935cfecc9e9c8d3cd1d355c9cf59eee	MSIL/GenKryptik.FOSS!tr	2CMV21-00258-01
8d641e6838772e3c8abb29ac45acd00d80b6ff6dd8ca3c777b7e618ee9d3e9df	W32/Netsky.R@mm	2CMV21-00258-01
5f1d1c3d5d7851b7943f79b037240bc6d375cec9c13eb30c1de3e1025aae7c41	Malicious_Behavior.SB	2CMV21-00258-01
1aed792d29e5f829fa7b1de54f698d8e4ee4e77f0baa9e7362dd46b686fc581b	MSOffice/Agent.GV!tr	2CMV21-00258-01
9cfca15e6abc547bf958ee65ce0d3093d20b989985f883f63790016b67f206c8	MSOffice/CVE_2017_11882	2CMV21-00258-01
5b8584126ece868308877be0859df6e192aa60f465c6f4589754f47e45e23183	W32/Delf.DCB!tr	2CMV21-00258-01
c53df9212791555290f7f9a486af114a9091c017a01f919ac0391fb8fd2574de	MSIL/Kryptik.ADRI!tr	2CMV21-00258-01
36fd445f7215f55090523b5b0a604c8a1b1a6629ae87ffed83d9b2bc33d4b4bf	MSIL/Kryptik.ADRI!tr	2CMV21-00258-01
581cc3b056bd984285daeec21b1fd1886d5a50fa8bc99c686a62c841b762ae07	MSIL/Kryptik.ADRI!tr	2CMV21-00258-01
28fa5ae5f98493476cc678ddd20e60adf994246590ea498a9675aa246eec922c	MSIL/Kryptik.ADRI!tr	2CMV21-00258-01
20f38fb8736e46246cb99181ab0f28e4919e0d73a82135c56b29b4a655913654	HTML/Script.INF!tr	2CMV21-00258-01
cdbbd12f250b87938ef4de6ac54b60b5a19058d0bf619ca71877c40cb85a4c8d	HTML/Script.INF!tr	2CMV21-00258-01
9ac117adb94bf928a375b82992f301620d8c1f875345ad9184d5a4009c9891e5	HTML/Script.INF!tr	2CMV21-00258-01
8f47db836fe44c82478d1d558e3ebb7ea6f18841c30a8c6a6a733fce8bd246ed	HTML/Script.INF!tr	2CMV21-00258-01
f2400069e7140bbcc8e86fb49aa81a4920330cf91b515fa0db5e5e64371c0432	FSA/RISK_HIGH	2CMV21-00258-01
89db5ada297bab1bbf1eae6bd09f117a7b1523091b2dea4d39d0af69f1556cfa	MSOffice/CVE_2018_0798!tr	2CMV21-00258-01
1419671c7d3afacc61b8efbcf507da94beaf22e4950939a77fefc1ef22bc29fb	Malicious_Behavior.SB	2CMV21-00258-01

57572309c6230b4a28d8ceb8adcb7e2acf688077ac02026524065ce579276621	MSOffice/CVE_2017_11882	2CMV21-00258-01
df0b9713e18faef8c8f15599cda51a02bc40c9e9a71c57721726227f3b37af94	MSOffice/CVE_2018_0798!tr	2CMV21-00258-01
09cb02282dd302ca4b5bb7b8a2b62f38bd5ec558e0704880eff8b6e5ba8d8d18	MSOffice/CVE_2018_0798!tr	2CMV21-00258-01
f955df810b77345797cb5e437c7224c8bbcfa9f038254d3feca17a510c96073e	MSIL/Kryptik.GZW!tr	2CMV21-00258-01
9cf256892fd468ebb1c711a46ccba76a2e24713b80a256c04c6a80cb0de76a6c	MSIL/Kryptik.GZW!tr	2CMV21-00258-01
961efc90a3e1b9d7d5dfc45e46cb69708a9388065215c68ec56e5cbc16e60a69	MSIL/Kryptik.GZW!tr	2CMV21-00260-01
c5dbe61b435f9e00338c371c08cbc8f47cb6019c3525584bcccdafa17d1537fc	MSIL/Kryptik.GZW!tr	2CMV21-00260-01
c8b4b7e65134120d0d68dbdfb6bbff5557251b6022cb63456831973fc1f45258	MSIL/Kryptik.GZW!tr	2CMV21-00260-01
1c3b1dc48d4c0304cfde7a7a3fc9890180757408319 44d2656600830d67f19aa	MSIL/GenKryptik.FOSS!tr	2CMV21-00260-01
09ed2d0833a281d7e3ccdee8eacdf649399d54fbc8bf269ca9761ebd12b88a85	MSIL/Kryptik.GZW!tr	2CMV21-00260-01
071f6a846ef55f40bd430507bec2649deaf832ce64d51a092a955a1b0dc236a9	RTF/Abnormal.F!tr	2CMV21-00260-01
2a2cc6fb30a8f2d6bf85817d195b548b133db0a59bb25134c7961d3fb3e30e9e	W32/Injector.EQTC!tr	2CMV21-00260-01
5ecf2095c32ac496cdcfa5b2f3dc33020a35bc8bfb34987b4887c9f4c0ce398e	FSA/RISK_HIGH	2CMV21-00260-01
563b344948369495099d74506d91e051b891d71e4157754d863e80f80e014893	MSIL/Injector.VRI!tr	2CMV21-00260-01
ded7f9a705e0e6e85a1394393f3e0a419626cd99b56829ae0ca59f5978c2242f	MSIL/GenKryptik.FOSS!tr	2CMV21-00260-01
9c4882250a3e4dc76a7690d61bb007e4356f9953f2b4ecedeb5e70c92409d6a9	MSOffice/CVE_2017_11882.DMP	2CMV21-00260-01
5f1d1c3d5d7851b7943f79b037240bc6d375cec9c13eb30c1de3e1025aae7c41	Malicious_Behavior.SB	2CMV21-00260-01
7401473364009ddf9fc3e562a66ad96d7a9c742016ec5c89b09591f56f5df216	MSIL/Kryptik.ADRI!tr	2CMV21-00260-01
a9c87b61af7d6267183083e9fc7a84cd14a4e68835d3c75ad9b439b0b7977fcd	MSIL/GenKryptik.FOSS!tr	2CMV21-00260-01
159080c8fbff25a457c9d23306ad80e4ababa32cfa2a73b38337fbee749f2b17	MSIL/Kryptik.ADRI!tr	2CMV21-00260-01
60bf38351075022fb10f8f9a954e27e7164f6983ec36ad444679ab0747fc9df1	MSOffice/Agent.GV!tr	2CMV21-00260-01
2bef232f30824c32c750360bd2eb96a912734a75b909272cba70309dcbd39051	MSIL/GenKryptik.FOSS!tr	2CMV21-00260-01
02be2acc2bc4878da5f573a27400a480122da8ae3d68182fd009e379d490352a	MSIL/GenKryptik.FOSS!tr	2CMV21-00260-01
badf68d8c7fab2ba3094cebc4d2a59c076c3e444851f4e8a661ff8bbe01ecfdc	PossibleThreat.ZDS	2CMV21-00260-01
c53df9212791555290f7f9a486af114a9091c017a01f919ac0391fb8fd2574de	MSIL/Kryptik.ADRI!tr	2CMV21-00260-01
6397254ef2bd8192630ab3e7875953bbf935cfecc9e9c8d3cd1d355c9cf59eee	MSIL/GenKryptik.FOSS!tr	2CMV21-00260-01
36fd445f7215f55090523b5b0a604c8a1b1a6629ae87ffed83d9b2bc33d4b4bf	MSIL/Kryptik.ADRI!tr	2CMV21-00260-01
bc22ccd8dee2929533e83404e5281db532818b510a343279098d398ecda87d4e	MSIL/GenKryptik.FOSS!tr	2CMV21-00260-01
581cc3b056bd984285daeec21b1fd1886d5a50fa8bc99c686a62c841b762ae07	MSIL/Kryptik.ADRI!tr	2CMV21-00260-01
28fa5ae5f98493476cc678ddd20e60adf994246590ea498a9675aa246eec922c	MSIL/Kryptik.ADRI!tr	2CMV21-00260-01
aa52d9c063592963d44c2b4c08fe63913c692e5cd535f573561ba1c01d818b3a	MSOffice/Agent.GV!tr	2CMV21-00260-01
9199c001fe31056cec82bb1464b3bf952986b895149bb71ed3cb195dd92a4b1c	JS/Phish.6DAB!tr	2CMV21-00260-01
530799139eb9d987c89df0969a39361ee62bde2b6da92da645f875cb2eb6c925	JS/Phish.6DAB!tr	2CMV21-00260-01
c83556b6a023a7f462e6bd45e30d4ee1598565e5575575b138ea628bf26875b4	JS/Phish.6DAB!tr	2CMV21-00260-01
e8deda35086241df398a8b721a8bda9084c9bc549d0deb112ab9a698de886aab	JS/Phish.6DAB!tr	2CMV21-00260-01
f4f2d6f1466e3cd8967e95587c713efd7a2cca56a59a47757425998e0a4ab820	JS/Phish.6DAB!tr	2CMV21-00260-01
578698115397779ba54edaa544686507acfc404136fd4717ff5b2e93b7efa465	JS/Phish.6DAB!tr	2CMV21-00260-01
61d817389079da60461ae89f9f39644de9156e302ad042924c27c6d51d94b738	JS/Phish.6DAB!tr	2CMV21-00260-01
03ce9b418177cf1d5d407e23e711d7bcd272ce90cc3e167feef1ec4cec13eb98	JS/Phish.6DAB!tr	2CMV21-00260-01
763fcf2740f70fe9ea7933d4385f2f45d1aa0256a2414e74274d2e693c81df76	JS/Phish.6DAB!tr	2CMV21-00260-01
41465d6eb5a30c995867d0e0dbd00daa59a90a4e06f69f6d46a4569ec0f45747	JS/Phish.6DAB!tr	2CMV21-00260-01
3e0ba3bd3d54aece7f53ab6c62c330042d741ca40f99f32ed79511e7c066add2	JS/Phish.6DAB!tr	2CMV21-00260-01
8c7fabc295be11ad8fd784667f438fe363727e35ef79697f0142d120d097162d	JS/Phish.6DAB!tr	2CMV21-00260-01
1f6099652723c4d7168ea8862c4f87b2fb2afc2a0ab258ae5707a8644d284fed	JS/Phish.6DAB!tr	2CMV21-00260-01

1fad86a6dfe93cf5b1fa65d3b91e42db252820c7db8ccb0d9a587ec0b45816af	JS/Phish.6DAB!tr	2CMV21-00260-01
15f808f2faa3864454ae147d172c7556e427f22dd7f7e03bb2d68a4b0b0aca9c	JS/Phish.6DAB!tr	2CMV21-00260-01
754b645510132e17d7f143deee16063a1cac90d9bd415a9fb552ef353119b0ed	JS/Phish.6DAB!tr	2CMV21-00260-01
bce673d075ffbf676f7b60581ebdd2ed454c485e41f284b92b81bdd702a36e86	JS/Phish.6DAB!tr	2CMV21-00260-01
95b5de5da0b3557b8172a47c6f9a041bc62fada468bae4771fb74b8eef1d1db8	JS/Phish.6DAB!tr	2CMV21-00260-01
d78d9df95c4d5ff9652ef8f8661b066054083f858de213f383aebcaefecda82d	JS/Phish.6DAB!tr	2CMV21-00260-01
72d38742bfc7676e292a5a1064156786cc8f51fc03c7ad84f3dfbe4ac2c2ac38	JS/Phish.6DAB!tr	2CMV21-00260-01
551ff4c4da91c545b354eeb6df1250dba9b99ad1f7126997a601768e27a3bd55	JS/Phish.6DAB!tr	2CMV21-00260-01
07dbe5634f36fe59b96129b5beb344c6a8a906a64cbed102b18292d0962f484f	JS/Phish.6DAB!tr	2CMV21-00260-01
81a0ab49a197c97bc66c32d392bd588bdf561d10288e1e8af4b8f601a5c5125f	JS/Phish.6DAB!tr	2CMV21-00260-01
f71f5abe13fdeedb19f272ffabcca318a7de55ad347373e62d65c46713ee70bc	JS/Phish.6DAB!tr	2CMV21-00260-01
787488a730a0b2b5b66917fec82c034b890d14f9030f8b2d7f5d4b399a76a186	JS/Phish.6DAB!tr	2CMV21-00260-01
151a855b8320e7e5918abd8c09074e7689569237d47f1a29cce8091457b636f8	JS/Phish.6DAB!tr	2CMV21-00260-01
6cd551733485b7af6a2e09aacb2de6062ec571d7ed507ab6a8368bc4ca3cd8a3	JS/Phish.6DAB!tr	2CMV21-00260-01
5cb0aced6c4c238e77b198076e53e9b9705852db6919a8361144ab12ddde0787	JS/Phish.6DAB!tr	2CMV21-00260-01
0ef5132cbb87acff0793397d6bd39e78a849db7c126cd6d02d39af400bacb4a6	JS/Phish.6DAB!tr	2CMV21-00260-01
711fb0cf9d880470be7037f4dfd30eb8bedce3327380bed0cfe419581577b04f	JS/Phish.6DAB!tr	2CMV21-00260-01
d1f4443c37371adcf5983160fbbcf8c6079f5aa516753b95b6452b5c0cc72128	MSIL/GenKryptik.FOSS!tr	2CMV21-00260-01
22bf512a38e371b7fe797e1d539a3bce0079bd76f58abfeeaa6be698df43ff4a	Malware_Generic.P0	2CMV21-00260-01
5b8584126ece868308877be0859df6e192aa60f465c6f4589754f47e45e23183	W32/Delf.DCB!tr	2CMV21-00260-01
4d78612257ceedbc8f6f936d268394fde6e5b655bdf4700be0808d3965c12cc5	Malicious_Behavior.SB	2CMV21-00260-01
8d641e6838772e3c8abb29ac45acd00d80b6ff6dd8ca3c777b7e618ee9d3e9df	W32/Netsky.R@mm	2CMV21-00260-01
5a3453c7deeb9d93fa1e10eb1c07fdfb8e89612bc336ade1e6b51f612bdcfd67	W32/Injector.EQPQ!tr	2CMV21-00262-01
b680a3dae6dc4be696b00d0ac81c1a7e92140a5c707ac281daf1e57cf982ef44	MSIL/GenKryptik.FOTN!tr	2CMV21-00262-01
a2a6e9e20be0c2faf8206f084fb1badb04a4c11d6dd47defe64a42f3e203e102	PossibleThreat.ZDS	2CMV21-00262-01
d9a3f7d170e6f1f7849e2afdf8a8e9d0e3d16c6be4ae6c01e74599106a4666b1	MSOffice/CVE_2017_11882	2CMV21-00262-01
a6e8bbf4b3ec7b44f670d49a9266b436e627a9d1694c3a538362c62a13f7c8c6	PossibleThreat.ZDS	2CMV21-00262-01
61a61e463cb388e62c0cb01469605ad088405ad9df866bc4a3dc3dc4f56e7b1e	HTML/Agent.BRV!tr	2CMV21-00262-01
dbfa1c4b3cb64148353c357fa81db631a5e1601cb55162d768801abc2559d9fa	MSIL/GenKryptik.FOTN!tr	2CMV21-00262-01
5b9a5a47cc830bbbe4dc19e01c7849dd507f23ba7cb58ea6651f41303c06d556	FSA/RISK_HIGH	2CMV21-00262-01
9c19464dba638f619a8f12453cb0f03f418aa2f4da69144c8672c3d4f78d3143	JS/Phishing.2100!tr	2CMV21-00262-01
c90047524c263f981bc16f205e841459673cbfe1f6ddc6cd34311e4d7311bece	MSOffice/Agent.GV!tr	2CMV21-00262-01
1d7cd8896af1ba4aa060ed9ddc474ccb3ca0280cbe55fcf7de73f3b400a55e5f	PossibleThreat.ZDS	2CMV21-00262-01
45f9438361c30aaa7fa985414e8b704252af774577948fe510b7971a304ed95e	FSA/RISK_HIGH	2CMV21-00262-01
35206f807170142d3de297e9e3e9cf24d917aca6520c6ae0ff39160c1435cb36	MSIL/GenKryptik.FODQ!tr	2CMV21-00262-01
319fa413c15b8fa70f9b21b0262b56da4c0f4fb4b2b544a2d69bbd6b9fc02aa8	MSIL/GenKryptik.FODQ!tr	2CMV21-00262-01
d2439a1119456ad673996aead51b535b0c6f0ebcd32009386b34d8a624ab6c26	MSIL/GenKryptik.FODQ!tr	2CMV21-00262-01
0f334c6b31f5b74651ef3ab62d81ff79854b1a507d267a5e962f62596dae0bd8	MSIL/GenKryptik.FODQ!tr	2CMV21-00262-01
3bb73ca9c1fd2ee82d1229c8f279da6af2f3073a39f3b9554cca4440cd85ba7e	FSA/RISK_HIGH	2CMV21-00262-01
2378132353236da81daa44ed6ad3ede1aa5499e78d71a202a40d69885f613209	HTML/Phishing.FA66!tr	2CMV21-00262-01
74cf6c9becf89216ffd1663de93c8004c99390e55652317428d039e68af286d1	HTML/Phishing.FA66!tr	2CMV21-00262-01
3f6172f20ca6c6d6147bb254edac4c328624b8d58275892bb399ea8d4323e260	Malware_Generic.P0	2CMV21-00262-01
efb7989ec057b34ac70c18311fb9a1fef2e138ac6002c6dde8f11db5aecd9946	MSIL/GenKryptik.FOTN!tr	2CMV21-00262-01
e033a7008a9372145a6b95208a9483fe53356f377bba80f84d2d17ca6949301d	JS/Phish.8C3C!tr	2CMV21-00262-01

79eb77d134682da6529d798231b4cf49e79619b3a6d98761d203b6e1c9eb2e04	MSIL/GenKryptik.FOVV!tr	2CMV21-00262-01
a8e4f11fd027c166196d22e73cfbd9805b7ff4755f8e2fef3efc088b7b045c72	MSExcel/CVE_2017_11882	2CMV21-00262-01
9a2ce03b2d41147f020791d5e9ca7b959b783d0d76754e28d29fc2a73f673fbf	MSIL/GenKryptik.FODQ!tr	2CMV21-00262-01
5cbad8c20578556056d155303d843fc66fb2263be62afee85912cecececee70a96	MSIL/GenKryptik.FODQ!tr	2CMV21-00262-01
aba2eb67f79087c5e7cc125933d59e7d2b44fee3ea8a50fb6f5b4520b0c196ea	MSOffice/Agent.GV!tr	2CMV21-00262-01
1ca7ef5f502df55094507ec87cf0ced46534ab14ee569b2a9f5b86e58be2f43a	PossibleThreat.ZDS	2CMV21-00262-01
4ed10c2a7083769911b1de3cc49a0cc6e11ab124d0e3f0682bccdf2810d09a42	PossibleThreat.PALLASNET.H	2CMV21-00262-01
712a53babdd05b3bfc60705aee1b48946fb9da37f15c4e18463414d9c35283c6	MSIL/Injector.VRI!tr	2CMV21-00262-01
1dc5e1ebd133ce483936a5f19864a3c79dcd770437d72941e4c7bec1db10715e	PossibleThreat.PALLASNET.H	2CMV21-00262-01

Direcciones IP de servidor SMTP donde es enviado el correo malicioso. Recomendamos establecer cuarentena preventiva para estos indicadores de compromiso, previa evaluación del impacto en los servicios productivos. Una vez que sus plataformas de monitoreo no detecten actividad maliciosa, puede evaluar la posibilidad de liberar el bloqueo. Es importante considerar que podrían aparecer direcciones de IP de servicios Cloud reconocidos o amenazas mitigadas.

IP	Etiqueta de sistema autónomo	ASN	Documento web
157.245.141.184	DIGITALOCEAN-ASN	AS 14061	2CMV21-00257-01
216.117.136.131	AITNET	AS 10843	2CMV21-00257-01
128.199.88.216	DIGITALOCEAN-ASN	AS 14061	2CMV21-00257-01
134.209.174.50	DIGITALOCEAN-ASN	AS 14061	2CMV21-00257-01
185.222.57.186	RootLayer Web Services Ltd.	AS 51447	2CMV21-00257-01
185.222.57.237	RootLayer Web Services Ltd.	AS 51447	2CMV21-00257-01
212.192.241.11	Delis LLC	AS 211252	2CMV21-00257-01
45.137.22.78	RootLayer Web Services Ltd.	AS 51449	2CMV21-00257-01
45.137.22.93	RootLayer Web Services Ltd.	AS 51450	2CMV21-00257-01
45.137.22.78	RootLayer Web Services Ltd.	AS 51447	2CMV21-00258-01
144.126.208.154	DIGITALOCEAN-ASN	AS 14061	2CMV21-00258-01
185.222.57.198	RootLayer Web Services Ltd.	AS 51447	2CMV21-00258-01
173.231.242.4	IMH-IAD	AS 54641	2CMV21-00258-01
85.209.91.33	Zomro B.V.	AS 204601	2CMV21-00258-01
185.222.58.137	RootLayer Web Services Ltd.	AS 51447	2CMV21-00258-01
190.210.132.6	NSS S.A	AS 16814	2CMV21-00258-01
2.58.149.150	AS-SERVERION	AS 399471	2CMV21-00258-01
185.222.58.105	RootLayer Web Services Ltd.	AS 51447	2CMV21-00258-01
180.214.238.171	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP	AS 135905	2CMV21-00260-01
109.71.42.89	Almouroltec Servicos De Informatica E Internet Lda	AS 24768	2CMV21-00260-01
45.137.22.93	RootLayer Web Services Ltd.	AS 51447	2CMV21-00260-01
62.197.136.27	Des Capital B.V.	AS 213035	2CMV21-00260-01
162.248.49.179	PRIVATESYSTEMS	AS 63410	2CMV21-00260-01
2.56.57.118	AS-SERVERION	AS 399471	2CMV21-00260-01

185.222.57.163	RootLayer Web Services Ltd.	AS 51447	2CMV21-00260-01
185.222.57.237	RootLayer Web Services Ltd.	AS 51447	2CMV21-00260-01
136.144.41.186	Delis LLC	AS 211252	2CMV21-00260-01
147.182.247.91	DIGITALOCEAN-ASN	AS 14061	2CMV21-00260-01
85.202.169.234	Des Capital B.V.	AS 213035	2CMV21-00260-01
190.210.196.89	NSS S.A.	AS 16814	2CMV21-00260-01
159.203.174.203	DIGITALOCEAN-ASN	AS 14061	2CMV21-00262-01
212.193.30.24	Delis LLC	AS 211252	2CMV21-00262-01
85.202.169.166	Des Capital B.V.	AS 213035	2CMV21-00262-01
165.227.101.188	DIGITALOCEAN-ASN	AS 14061	2CMV21-00262-01
212.192.241.126	Delis LLC	AS 211252	2CMV21-00262-01
159.223.138.109	DIGITALOCEAN-ASN	AS 14061	2CMV21-00262-01
138.68.148.116	DIGITALOCEAN-ASN	AS 14061	2CMV21-00262-01
185.222.57.186	RootLayer Web Services Ltd.	AS 51447	2CMV21-00262-01
45.137.22.123	RootLayer Web Services Ltd.	AS 51447	2CMV21-00262-01
138.197.153.100	DIGITALOCEAN-ASN	AS 14061	2CMV21-00262-01
147.182.255.15	DIGITALOCEAN-ASN	AS 14061	2CMV21-00262-01
193.56.29.135	Web Hosted Group Ltd	AS 210228	2CMV21-00262-01
104.168.254.177	HOSTWINDS	AS 54290	2CMV21-00262-01
92.204.134.95	GO-DADDY-COM-LLC	AS 388108	2CMV21-00262-01

Nombres de archivo: Corresponden a aquellos documentos que vienen adjuntos en las campañas de phishing con malware. El CSIRT de Gobierno recomienda que cada institución analice las extensiones de los archivos y evalúe cuáles serán bloqueadas o permitidas. Asimismo se deben ejecutar de forma permanente las actualizaciones de los módulos de antivirus de los antispam y de las estaciones de trabajo.

Nombres de archivos con malware	Documento web
DEPARTAMENTO_INTERNACIONAL_DE_MOLOTERÃ⍰A	2CMV21-00257-01
PAGO - 30503.cab	2CMV21-00257-01
factura 071221_PDF.GZ	2CMV21-00257-01
NAM-PRODUCTS_LIST#20220017689322.7Z	2CMV21-00257-01
PI NO. RRPL112021-2022.xlsx	2CMV21-00257-01
PO PJM2021PO283.r00	2CMV21-00257-01
Building Plan 9028AWT.uue	2CMV21-00257-01
DHL DOC 74653898.xlsx.bz	2CMV21-00258-01
PROFORMA INVOICES 0073524252.LZH	2CMV21-00258-01
msg29041.zip	2CMV21-00258-01
PAYMENT SLIP USD56,000.iso	2CMV21-00258-01
SECURED QUOTATION FOR 674993 ORDER .xlsx	2CMV21-00258-01
PO-200345.xlsx	2CMV21-00258-01
bancaria SWift pdf.exe.xz	2CMV21-00258-01
AMENDED ORDER.zip	2CMV21-00258-01

REQUIREMENTS.zip	2CMV21-00258-01
SHIPPING DOCUMENT.zip	2CMV21-00258-01
DOCUMENTO-PDF284837.html	2CMV21-00258-01
DOCUMENTO-PDF284837.htm	2CMV21-00258-01
DOCUMENTO-PDF723843.html	2CMV21-00258-01
DOCUMENTO-PDF723843.htm	2CMV21-00258-01
Image009.r09	2CMV21-00258-01
Payment Advice - Advice Ref[GLVC18304421].xlsx	2CMV21-00258-01
Ñ‚Ó©Ð»ÐµÐ¼Ð½Ñ–Ò£ Ð´Ó™Ð»ÐµÐ»Ñ–.PDF.zip	2CMV21-00258-01
RQ455677.xlsx	2CMV21-00258-01
Eastern Poly - NEW PO#4501607801.xlsx	2CMV21-00258-01
TT SWIFT COPY.zip	2CMV21-00258-01
AY21USDKI02 DN.zip	2CMV21-00260-01
facturas pagadas.doc	2CMV21-00260-01
NEW ORDER_pdf.img	2CMV21-00260-01
301086.r13	2CMV21-00260-01
Product-7036192.img	2CMV21-00260-01
PO - Drawings And Specifications Sheet^.IMG	2CMV21-00260-01
SWIFT-AWD-0801486XXB21.doc	2CMV21-00260-01
TT CHG-154421150899_pdf.gz	2CMV21-00260-01
BID FA-0002040.doc	2CMV21-00260-01
PO (PO202101129 & PO202101130).rar	2CMV21-00260-01
VOLGOIL LLC SOFT CORPORATE OFFER VESSEL TO TANK.7z	2CMV21-00260-01
PO 235080.gz	2CMV21-00260-01
PRUEBA DE PAGO # 216974 #,pdf.iso	2CMV21-00260-01
Draft BL.xlsx	2CMV21-00260-01
FILE.html	2CMV21-00260-01
Muestras de Ã³rdenes de compra.Pdf.zip	2CMV21-00260-01
PI S30C-921111218111.GZ	2CMV21-00260-01
AMENDED OFFER.zip	2CMV21-00262-01
bank details.rar	2CMV21-00262-01
BANK SLIP.zip	2CMV21-00262-01
BL-SHIPPING DOCUMENTS.zip	2CMV21-00262-01
Dhl.html	2CMV21-00262-01
DHL-AWB 1228282098-12132021.IMG	2CMV21-00262-01
EDC Purchase Order.gz	2CMV21-00262-01
IMG_1125602_0255.zip	2CMV21-00262-01
NEW _ORDER#.rar	2CMV21-00262-01
ORDER CONFIRMATION 0012721918.xlsx	2CMV21-00262-01
Order_110921.r13	2CMV21-00262-01
OVERDUE(SOA).xlsx	2CMV21-00262-01
Payment Advice PDF GLV211429671.7Z	2CMV21-00262-01
Payment Slip.ace(-248KB)	2CMV21-00262-01
pedido.zip	2CMV21-00262-01

PI 43447.xlsx	2CMV21-00262-01
PO NUMAFA dec534244516876562,pdf.iso	2CMV21-00262-01
PO SPLACK DEC2021764534523,pdf.iso	2CMV21-00262-01
print_01.rar	2CMV21-00262-01
shipment docu..rar	2CMV21-00262-01
SHO211216_xlsx .html	2CMV21-00262-01
Statement as at DEC 2021.xlsx	2CMV21-00262-01
Urgent December Rfq #34567745.PDF.arj	2CMV21-00262-01

IoC Ataques de Fuerza Bruta

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una serie de intentos de acceso a servidores de correos del sector público y privado. Estos ataques de fuerza bruta intentan vulnerar la autenticación del protocolo para transferencia simple de correos (SMTP), con el fin de suplantar un remitente original y así depositar correos con contenido o enlaces maliciosos en las bandejas de entrada de sus potenciales víctimas.

IP	Etiqueta de sistema autónomo	Documento web
212.70.149.57	SS-Net	4IIA21-00046-01
212.70.149.89	SS-Net	4IIA21-00046-01
87.246.7.246	SS-Net	4IIA21-00046-01
103.61.100.202	Cify IT Services Pvt Ltd	4IIA21-00046-01
2.56.56.225	AS-SERVERION	4IIA21-00046-01
37.0.10.95	Delis LLC	4IIA21-00046-01
93.62.72.229	Fastweb	4IIA21-00046-01
212.70.149.89	SS-Net	4IIA21-00047-01
212.70.149.57	SS-Net	4IIA21-00047-01
87.246.7.246	SS-Net	4IIA21-00047-01
107.182.128.11	AS-SERVERION	4IIA21-00047-01
98.143.104.200	295CA-TOR-ASN	4IIA21-00047-01
43.224.128.22	Northeast Dataa Network Pvt Ltd	4IIA21-00047-01
59.125.122.90	Data Communication Business Group	4IIA21-00047-01

Noticias

Alerta de Seguridad Cibernética | Vulnerabilidad severa en Apache Log4J 2

El CSIRT de Gobierno, advierte de una vulnerabilidad severa que afecta a múltiples versiones (2.0 a 2.14.1) de la utilidad Apache Log4j 2. Conoce los fabricantes que se vieron afectados en sus productos.

Log4j 2 es una biblioteca de registro de Java de código abierto desarrollada por Apache Foundation y se utiliza en diversas aplicaciones web y servicios en la nube. De acuerdo a lo informado, la vulnerabilidad permite la ejecución remota de código (RCE) no autenticado en sistemas con Log4j 2.0-beta9 hasta 2.14.1.

La vulnerabilidad fue registrada como CVE-2021-44228 y denominada Log4Shell, y ya cuenta con la última versión disponible (2.16.0), la cual modifica la conducta por defecto que permitía explotar esta vulnerabilidad.

El CSIRT de Gobierno recomienda realizar esta actualización lo antes posible. El informe con su respectiva mitigación lo pueden encontrar en el siguiente enlace: https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00531-01/.

Es importante enfatizar que esta es una mitigación temporal, a la espera de un parche definitivo por parte de los desarrolladores. Por su parte, los proveedores que integran esta biblioteca entregaron en sus sitios web una evaluación de sus productos afectados. Estos son:

Apache Solr
Apache Struts
Atlassian
BMC
Cisco
Citrix
Debian
Docker
F-Secure
Fortinet
RedHat
Solarwinds
VMware

Detección de 41 sitios fraudulentos por parte del CSIRT llega a Las Últimas Noticias, EMOL y Bio Bio

Hoy queremos agradecer a Las Últimas Noticias, Emol y Radio Bío Bío por compartir en sus medios la detección que realizamos, como CSIRT de Gobierno, de 41 sitios fraudulentos que imitan las webs de marcas reales de vestuario, calzado y accesorios para robar información financiera y recibir pagos de quienes creyendo que son páginas legítimas tratan de comprar en ellas.

La detección de los sitios falsos corresponde a usos ilícitos de los logos de conocidas marcas. Las páginas detectadas suplantan a Women´secret, Bruno Rossi, Amphora, Calzedonia, CAT, Merell, Oster, Romano, Bimba y Lola, Azaleia, Cannon, Doite y Lippi, entre otras.

La colaboración de los medios de comunicación con nuestras noticias y campañas es clave para llegar a más potenciales víctimas y evitar que caigan en estafas virtuales.

Pueden leer a continuación lo que escribieron sobre el trabajo del CSIRT y el Ministerio del Interior respecto de estos sitios fraudulentos. También recomendamos mirar nuestros ciberconsejos para evitar caer en fraudes al comprar esta Navidad: https://csirt.gob.cl/recomendaciones/ciberconsejos-navidad-2021/

Las Últimas Noticias: https://www.lun.com/Pages/NewsDetail.aspx?dt=2021-12-14&NewsID=482629&BodyID=0&PaginaId=15

Emol: https://www.emol.com/noticias/Tecnologia/2021/12/13/1041050/detectan-41-sitios-web-suplantados.html

Radío Bío Bío: https://www.biobiochile.cl/noticias/economia/tu-bolsillo/2021/12/14/detectan-41-paginas-falsas-con-supuestos-descuentos-navidenos.shtml

Actualidad

Ciberconsejos para evitar riesgos digitales con nuestros regalos navideños

La tecnología es uno de los regalos cotizados en Navidad. Smartphone, Tablet, consolas de video juegos o membresías para juegos en línea son algunas de las peticiones de niños, niñas y adolescentes. Pero antes de comprar, es importante que quienes hagan este tipo de regalos se informen sobre los peligros del uso de dispositivos conectados a Internet y saber qué productos es seguro utilizar en cada edad de los menores.

A continuación, les entregamos algunas recomendaciones para comprar regalos digitales según la edad de cada niño y niña en esta Navidad. Puedes descargar el PDF aquí: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-riesgos-digitales/

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 problemas de seguridad y vulnerabilidades descubiertas.

El CSIRT de Gobierno destaca en este segmento a quienes reportaron incidentes utilizando canales formales (https://www.csirt.gob.cl o al teléfono +(562) 2486 3850) siempre que hayan aportado información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- Juan Pablo Berríos
- Eduardo Omerovic
- Víctor Cofré
- Juan Carlos Rodríguez
- Gustavo Vidal
- Darío Morandé
- Simón Schoihet
- Roberto Plaza
- Iván González
- Hans Sandoval
- Víctor Cofré
- Andrea Galleguillos
- Jorge Torlaschi
- Gustavo Vidal
- Bárbara Palacios
- Esteban Vásquez
- Elisa Molina

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.12.17 16:17:39 -03'00'