Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

26-11-2021 | Año 3 | N°125

Boletín de Seguridad Cibernética

Semana del 19 al 25 de noviembre de 2021

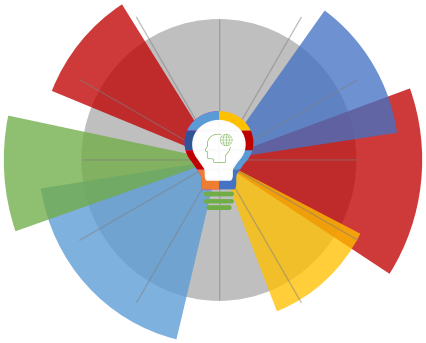
La semana en cifras

Hash

46

SHA

Asociadas a múltiples campañas de phishing con archivos que contienen malware



Se advirtieron

3

URL

Asociadas a sitios fraudulentos y campañas de phishing y malware.

Parches

20

para vulnerabilidades

Las mitigaciones son útiles en productos de Microsoft.

IP

25

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

Imagen del sitio

CSIRT alerta de página fraudulenta que suplanta al Banco Itaú	
Alerta de seguridad cibernética	8FFR21-01022-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de Noviembre de 2021
Última revisión	19 de Noviembre de 2021
Indicadores de compromiso	
URL sitio falso	
https://itau-tarjetaiupp.tarjetaiupp[.]com/2/726a292db52f7f5/mobile/index.php	
IP	
[104.21.84.234]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01022-01/	
https://www.csirt.gob.cl/media/2021/11/8FFR21-01022-01-1.pdf	

Phishing

Imagen del mensaje

CSIRT alerta ante nueva campaña de phishing que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH21-00446-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Noviembre de 2021
Última revisión	22 de Noviembre de 2021
Indicadores de compromiso	
URL Redirección	
http://yashevents.co[.]in/ganador/promo-riwc/	
URL sitio falso	
https://blogs.neloz[.]cl/login	
IP	
[170.239.85.224]	
[200.63.99.33]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00446-01/	
https://www.csirt.gob.cl/media/2021/11/8FPH21-00446-01.pdf	

Malware

CSIRT advierte ante campaña de malware Emotet	
Alerta de seguridad cibernética	2CMV21-00250-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Noviembre de 2021
Última revisión	22 de Noviembre de 2021
Indicadores de compromiso	
SHA256	
c99fea9f7c41af8a448c38aeaf85d200bd508bb84a08a584fa82765104d03e92 d05ec2a0134518ec74fcbee94a522c3837d82b7b5d2f162b8466850fc4f1be0d b8ad4931315f781e7abb33bb193e0ea2419dd4e9302b3ae6c0471ff51c2fc8c4 05f251f9b66d86646b3f9886bbb525414580cf9698cd4918ec79c706fc679a38 b1872d1db76cc8777a35b41478c3e530f40d11e11710ecc4f360066a0d6175a6	
IoC Red	
http://primtalent[.]com/wp-admin/9yt1u/ http://huskysb[.]com/wordpress/6f0qIQlWPaYDfa/ http://ridcyf[.]com/dm7vg/DGWFrJA0kutWTk/ http://manak.edunetfoundation[.]org/school-facilitator/qlwM2RAHhDG8N8/ http://ckfoods[.]net/wp-admin/wPInm2rgMu/ http://adorwelding.zmotpro[.]com/wp-content/Z8ifMTCM2VBWlfeSZmzv/ http://server.zmotpro[.]com/venkat/products/facebook-page/assets/kmIdeXnG/	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv21-00250-01/	
https://www.csirt.gob.cl/media/2021/11/2CMV21-00250-01.pdf	

Vulnerabilidades

CSIRT alerta de nuevas vulnerabilidades en Microsoft Edge	
Alerta de seguridad cibernética	9VSA21-00524-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Noviembre de 2021
Última revisión	25 de Noviembre de 2021
CVE	
CVE-2021-38012 CVE-2021-43221 CVE-2021-38005 CVE-2021-38006 CVE-2021-38007 CVE-2021-38008 CVE-2021-38009 CVE-2021-38010 CVE-2021-42308 CVE-2021-38013 CVE-2021-38011 CVE-2021-38014 CVE-2021-38015 CVE-2021-38016 CVE-2021-38017 CVE-2021-38018 CVE-2021-38019 CVE-2021-38020 CVE-2021-38021 CVE-2021-38022	
Fabricante	
Microsoft	
Productos afectados	
Google Chrome: 79.0.309.71 a 95.0.1020.53	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00524-01/	
https://www.csirt.gob.cl/media/2021/11/9VSA21-00524-01-1.pdf	

IoC Malware

A continuación, se comparten los Indicadores de Compromisos que fueron detectados durante la semana pasada por el CSIRT de Gobierno.

Recomendamos 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
ef22b70669f68fe71d55454f1f94c11fea049c1e2122f1dd25138701151ec2ce	PossibleThreat	2CMV21-0251-01
ed5f1ca94b4152167309005e07b34a79e0d9d6df7516d4e95e99942b3e9267b6	HTML/FPhishing	2CMV21-0251-01
ecb90b01f5fd1a562da3cf732c5e3da673e2af50e0186a781f4c5507c9672cd7	MSIL/FRazy	2CMV21-0251-01
e93fb600997f7665cf6b7665e7e7352dc1b55e2c0f79e9db68fe6e9b4ed354a4	W32/FEQPP/1tr"	2CMV21-0251-01
d3cdf89cf7b7e951833872e37b9530717a444f419b35b3fc67d7d66a4bacf612	RTF/FCVE_2017_11882	2CMV21-0251-01
d3ab411f69aa8200d563361e6827012bd6c32fa29e9efbf5a4d6d9ce32d9d42a	MSOffice/FScam	2CMV21-0251-01
c9a7519cbdf4ef199add00004c3c55316799abc816b129ee2532dfd78d6bacfd	MSIL/FKryptik	2CMV21-0251-01
c842bbd154dd0e75559c9aa451887a125e03f6d3f224c047d81cfc8a08fde7af	MSOffice/FCVE_2017_11882	2CMV21-0251-01
c6f50bb053b2b8364be0e4874f494b8f8ac9e55d6df610e972db619a1f35bca7	PossibleThreat	2CMV21-0251-01
c38b2a3a9498e69a4c2a77801b251a90363d4cc98de9f0c72220033a7bb4e2c6	HTML/FPhishing	2CMV21-0251-01
c054d576bd0cbb6dde7a140a82f1f50dd0302b8f303c038ecb2f2e491f62e114	MSOffice/FCVE_2017_11882	2CMV21-0251-01
b8b7f22de66267a613139041f6f79c94c5a1d6167b3cd75b472ad1aebd5b009a	MSIL/FKryptik	2CMV21-0251-01
b165eb6698c86f8ec711dc6c6a0250996430d2f1daaf52eedf21bfb6d7814b38	Malicious_Behavior	2CMV21-0251-01
acddb11ffbfd3a9b1d45e1948897d40bb1d518fafd4aae21ae765c7f0894765e	HTML/FPhishing	2CMV21-0251-01
ab4879ab5cbb1e4929b32a34ea2c8be7276d587686ee0c49541fb0bbc51dde57	HTML/FPhish	2CMV21-0251-01
a93b818c69c9e1bc47fe8c881753ab9e3bb07ee36502fff22af11ded124f9f55	MSIL/FKryptik	2CMV21-0251-01
9f83e0d42414e2b372d08ec7f1ef0f46d445ba2bb738578fed80326ab46dcba3	MSIL/FKryptik	2CMV21-0251-01
99e3c932ab16020fca8500b72845da601aae12270fad2887f91b6fcc59c26285	MSIL/FKryptik	2CMV21-0251-01
948a6d826607731ce843a34ab2589e86c0b3b5ed74d68b3156c1e83267867817	HTML/FPhishing	2CMV21-0251-01
945e083a833f9496fd9de3bb6739f2ed82609a6a478300b55afb80774fbc8c9c	HTML/FPhishing	2CMV21-0251-01
935df8e4a329b9c33d977a8a54f9f38a25911978fed7f593103b33bf981d364c	MSIL/FInjector	2CMV21-0251-01
8e207089d7f89efba0159ec93a83bdc49d5565f8b8a2dcf980897cd95ee31363	MSOffice/FAgent	2CMV21-0251-01
8d6dc9cddc15e1c8cc9f47246c5d809c12c2db12ed921437405a9a7e274569ed	HTML/FMalphish	2CMV21-0251-01
7829992ef0a0f7ccf3b80fc92660a5d4dc80e875513b239f2585279101b1414e	HTML/FAgent	2CMV21-0251-01
761945b913c6d8b2186baa6a6ca3635492c74dc51d2e9fee347cd3cfe6868879	MSOffice/FCVE_2017_11882	2CMV21-0251-01
7286e945d6db691e71e17a9f123b544ea2b951cb9b02b2119faf090d44f9ad66	MSIL/FKryptik	2CMV21-0251-01
6fccd94dd4ee0c639a795125b4792fe693f323e3ccef86680169a46dafa4b092	MSIL/FKryptik	2CMV21-0251-01
6e7236b8c73931b8ff88f949fd8d772c03640f5e7ef9151b793ed12c9cb567f3	MSIL/FKryptik	2CMV21-0251-01
634c98332c17b0d3c6b6ba8249d4189310f8ec19a60bf612481b00293a8f4197	MSIL/FKryptik	2CMV21-0251-01
60b65b20b9eaa152afab4aaff027271d76ab4ceb65df6bee502be07a23627f2d	HTML/FPhishing	2CMV21-0251-01
5e1045f6d57797cf2fc12417ae45f4440a61d2f8a9851f8087b251f1773195b7	MSIL/FKryptik	2CMV21-0251-01
54c0f4c5ed2e56def68d06b036bd1eacb138c536f7a1ef61d9ce7260304ae65d	Malware_Generic	2CMV21-0251-01
53013780b7d60d96b0ab9aebe155a9f7fcd21e05fb8e4e27c48ce878ec2bdcd3	MSIL/FKryptik	2CMV21-0251-01
3fdbf9221ced7fdd525563d367c0d6b88695f79c99f9f3a931264f5775139e70	HTML/FPhishing	2CMV21-0251-01
3df85a94a8cfd23cb535e158311c5f7e82c5636eadab1b01d072881f7dcda7d3	Malicious_Behavior	2CMV21-0251-01
31122c5f30e28c40a1a1feeaaa1061ac8da82b94ee267407f96ad427dd464edd	MSIL/FKryptik	2CMV21-0251-01

2c895d6478e23de14636e43a3ea4dd3a0a0482f97ac08e31f7ef3b8c3b051a38	HTML/FMalphish	2CMV21-0251-01
2b876350bd686039b76edfe44b51b1bbbd86c83d22a486adb87da8161e481c1f	MSIL/FKryptik	2CMV21-0251-01
297dc3ab02bc9bc07f8b68a78e1da63294690d02dc472b7b9fcf2c91973304e2	MSIL/FKryptik	2CMV21-0251-01
1ad73e5100de22210b26641bfd56bf87f62a08633009cd6206b0deae7f61ae1d	HTML/FAgent	2CMV21-0251-01
05ebb5884e37bc96f7ba5b6193dee22c62ee3d505e9904af2b2a960ea6f7e4f5	MSIL/FKryptik	2CMV21-0251-01

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
45.144.225.109	Delis LLC	AS 211252	2CMV21-00251-01
45.144.225.120	Delis LLC	AS 211252	2CMV21-00251-01
91.250.116.253	Host Europe GmbH	AS 8972	2CMV21-00251-01
103.28.52.162	PT Cloud Hosting Indonesia	AS 136052	2CMV21-00251-01
103.99.0.129	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP	AS 135905	2CMV21-00251-01
103.99.1.233	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP	AS 135905	2CMV21-00251-01
140.227.40.151	NTT PC Communications, Inc.	AS 2514	2CMV21-00251-01
142.93.105.38	DIGITALOCEAN-ASN	AS 14061	2CMV21-00251-01
143.198.42.245	DIGITALOCEAN-ASN	AS 14061	2CMV21-00251-01
159.223.12.59	DIGITALOCEAN-ASN	AS 14061	2CMV21-00251-01
162.240.20.73	UNIFIEDLAYER-AS-1	AS 46606	2CMV21-00251-01
181.30.31.39	Telecom Argentina S.A.	AS 7303	2CMV21-00251-01
185.222.57.144	RootLayer Web Services Ltd.	AS 51447	2CMV21-00251-01
185.222.58.123	RootLayer Web Services Ltd.	AS 51447	2CMV21-00251-01
190.61.219.226	IFX18747	AS 18747	2CMV21-00251-01
194.99.46.217	Des Capital B.V.	AS 213035	2CMV21-00251-01
194.99.46.218	Des Capital B.V.	AS 213035	2CMV21-00251-01
37.0.11.158	Delis LLC	AS 211252	2CMV21-00251-01
45.137.22.163	RootLayer Web Services Ltd.	AS 51447	2CMV21-00251-01
45.137.22.168	RootLayer Web Services Ltd.	AS 51447	2CMV21-00251-01
45.137.22.189	RootLayer Web Services Ltd.	AS 51447	2CMV21-00251-01
45.9.168.115	MAXKO j.d.o.o.	AS 211619	2CMV21-00251-01

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
Euro invoice.zip	2CMV21-00251-01
Contrat SAISS ENVIRONNEMENT.xlsx	2CMV21-00251-01
QUOTATION REQUEST DOCUMENTS - GOTO TRADING.7z	2CMV21-00251-01
2021-24.doc	2CMV21-00251-01
Proforma Invoice 11252021PDF.7Z	2CMV21-00251-01
TRANFER SLIP.zip	2CMV21-00251-01
New AirWayBill.html	2CMV21-00251-01
invoice copy.pdf.z	2CMV21-00251-01
Official Order PDF.7Z	2CMV21-00251-01
465678CN.xlsx	2CMV21-00251-01
LinkedIn.html	2CMV21-00251-01
invoice and packing.zip	2CMV21-00251-01
REVISED_Document_NEW_PROJECT-02826626212.iso	2CMV21-00251-01
Factura proforma para pagos en el extranjero.Html	2CMV21-00251-01
Pago completo.pdf_____.gz	2CMV21-00251-01
Initial Quotation PDF.7Z	2CMV21-00251-01
AWB 281715447283 PDF.7Z	2CMV21-00251-01
PO Approved.xlsx	2CMV21-00251-01
SC-10745.7z.zip	2CMV21-00251-01
IMPORTS INVOICE.rar	2CMV21-00251-01
New Purchase Order 0088870.xlsx.gz	2CMV21-00251-01
documentos de envo.zip	2CMV21-00251-01
PO 675123 y envo de dibujo aprobado.CAB	2CMV21-00251-01
PO-BL00046749.iso	2CMV21-00251-01
ORDER INQUIRY-PVP-SP-2021-58.gz	2CMV21-00251-01
Remittance 10600396.xlsx	2CMV21-00251-01
sample photo.zip	2CMV21-00251-01

El Comando de la Semana | No. 25 DNSRecon

El Comando de la Semana hoy trae a DNSRecon, herramienta que facilita la enumeración, una actividad de reconocimiento en la cual se consigue información de usuarios, grupos o dispositivos, dominios relacionados, vulnerabilidades y demás servicios relacionados con un determinado activo expuesto a Internet.

Todos los detalles, los pueden encontrar en el siguiente documento:
https://www.csirt.gob.cl/estadisticas/el-comando-de-la-semana-no-25/

Ciberconsejos para prevenir estafas en la plataforma de streaming Twitch

Una de las redes sociales que crecen en popularidad, principalmente entre niños y jóvenes, es Twitch, plataforma de videos en vivo poblada principalmente por streamers de videojuegos.

Lamentablemente, todo lo que reúne a una gran audiencia es objetivo de los ciberdelincuentes, y existen ya varias estafas realizadas a través de Twitch, algunas ya vistas con anterioridad y otras diseñadas especialmente para aprovechar esta plataforma.

Puedes ver los ciberconsejos para evitar ser víctima en el siguiente enlace:
https://www.csirt.gob.cl/recomendaciones/ciberconsejos-twitch/

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.

- José Ignacio Parra
- Nicolás Carrasco
- Bárbara Palacios
- Víctor Cofré

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.11.26 15:35:26 -03'00'