Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

05-11-2021 | Año 3 | N°122

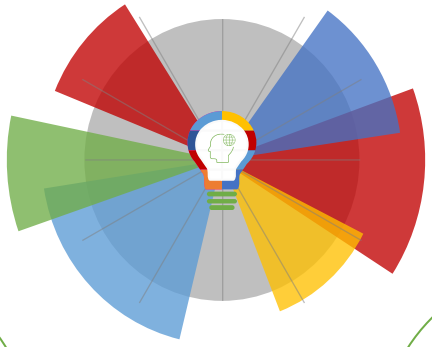
Boletín de Seguridad Cibernética

Semana del 29 de octubre al 04 de noviembre de 2021

La semana en cifras

Hash
34
SHA
Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron
10
URL
Asociadas a sitios fraudulentos y campañas de phishing y malware.



Parches
228
para vulnerabilidades
Las mitigaciones son útiles en productos de Red Hat, Discourse, Apple y Adobe.

IP
16
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 advierte sitio fraudulento de Correos de Chile	
Alerta de seguridad cibernética	8FFR21-01018-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Noviembre de 2021
Última revisión	03 de Noviembre de 2021
Indicadores de compromiso	
URL sitio falso	
https://colispartilive[.]com/LOGIN/inbox/account/ifram/index.php	
IP	
[46.101.193.187]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01018-01/	
https://www.csirt.gob.cl/media/2021/11/8FFR21-01018-01.pdf	

Phishing

CSIRT advierte smishing de falso bloqueo de tarjeta del Banco Ripley	
Alerta de seguridad cibernética	8FPH21-00441-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Noviembre de 2021
Última revisión	02 de Noviembre de 2021
Indicadores de compromiso	
URL de SMS	
https://bit[.]ly/3GtUkrs	
URL Redirección	
https://mantenifactuty[.]com/?sms=ripley	
URL sitio falso	
https://ripleymesonseguro[.]store/1635874265/login/index.html	
IP	
[104.21.58.2]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00441-01/	
https://www.csirt.gob.cl/media/2021/11/8FPH21-00441-01.pdf	

CSIRT advierte phishing que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH21-00442-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Noviembre de 2021
Última revisión	02 de Noviembre de 2021
Indicadores de compromiso	
URL Redirección	
https://bit[.]ly/3nEXWOK?l=www.bancoripley.cl	
URL sitio falso	
https://www-bancoripley-cl.saimshop[.]pk/login	
IP	
[194.107.124.65]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00442-01/	
https://www.csirt.gob.cl/media/2021/11/8FPH21-00442-01-1.pdf	

Imagen del mensaje

CSIRT advierte phishing suplantando a Correos de Chile	
Alerta de seguridad cibernética	8FPH21-00443-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Noviembre de 2021
Última revisión	03 de Noviembre de 2021
Indicadores de compromiso	
URL Redirección	
https://futureexpertsgeophysics[.]com/.well-known/cl	
URL sitio falso	
https://futureexpertsgeophysics[.]com/.well-known/cl/32c929863a793d5ebae5bc7ce7c3fe04/	
IP	
[153.126.163.56]	
[172.67.196.223]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00443-01/	
https://www.csirt.gob.cl/media/2021/11/8FPH21-00443-01.pdf	

Imagen del mensaje

CSIRT advierte smishing por dispositivo de seguridad caducado	
Alerta de seguridad cibernética	8FPH21-00444-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Noviembre de 2021
Última revisión	04 de Noviembre de 2021
Indicadores de compromiso	
URL de SMS	
https://bit[.]ly/3BHZbSq	
URL sitio falso	
https://bchile.apx-chilen[.]xyz/tspqTHnCPeSaGWaBAK8I39t1e/	
IP	
[23.94.50.162]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00444-01/	
https://www.csirt.gob.cl/media/2021/11/8FPH21-00444-01.pdf	

Malware

CSIRT informa campaña de phishing malware con falsa factura	
Alerta de seguridad cibernética	2CMV21-00241-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Octubre de 2021
Última revisión	29 de Octubre de 2021
Indicadores de compromiso	
SHA256	
EF05505D918F4484B9FC6DB920DA8FDAA02A178A36E6CB67F0E0534841D86245 616838E6DFFF493E546F51436EE3C0BBE99D459C18ABBBB71A6207555E9D73E6 D231020E3E3ABCF9F17DE87FAF383AEDC5C6E858767F909CE7F313AAD47572A7	
IoC Red	
www.cjspizza[.]net/rv9n/ www.maintaintest[.]com www.2fastrepair[.]com www.keeptest[.]com www.skandinaviskakryptobanken[.]com	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv21-0241-01/	
https://www.csirt.gob.cl/media/2021/10/2CMV21-00241-01.pdf	

CSIRT informa phishing con malware supuestamente de la TGR	
Alerta de seguridad cibernética	2CMV21-00243-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Noviembre de 2021
Última revisión	03 de Noviembre de 2021
Indicadores de compromiso	
SHA256	
25D8C96E61388BB29EEA3FDA8E1A601A6842350B725E35A193468D8F2BE6368F 77E19EEB9AC37EFB541EF647F401A372F5ED2098690156AE6A42AE65B906DEA6 A15EE764618CC1AA648F341C0419B8A1FB933CD9DA404A27F385CE5FF8BA1405 AC0E0AAFCAB69E4F471BD8C7F91238EAD6931B8BAE074EC5852762AF551037C1 945ADADA6CF6698B949359D9B395A5F905989D0D1EB84F537DE492ECC1263148	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv21-00243-01/	
https://www.csirt.gob.cl/media/2021/11/2CMV21-00243-01.pdf	

Vulnerabilidades

CSIRT alerta de vulnerabilidades zero-day en Google Chrome	
Alerta de seguridad cibernética	9VSA21-00514-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Octubre de 2021
Última revisión	29 de Octubre de 2021
CVE	
CVE-2021-38000 CVE-2021-38003 CVE-2021-37997 CVE-2021-37998 CVE-2021-37999 CVE-2021-38001 CVE-2021-38002	
Fabricante	
Google	
Productos afectados	
Google Chrome anteriores a 95.0.4638.69.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00514-01/	
https://www.csirt.gob.cl/media/2021/10/9VSA21-00514-01.pdf	

CSIRT alerta de vulnerabilidad de riesgo alto en Cisco Firepower Threat Defense	
Alerta de seguridad cibernética	9VSA21-005015-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Octubre de 2021
Última revisión	29 de Octubre de 2021
CVE	
CVE-2021-34781	
Fabricante	
Cisco	
Productos afectados	
Aparatos con una versión del software Cisco FTD vulnerable configurada para operación multi-instance, introducida en Cisco FTD Software 6.3.0. Las únicas plataformas de software Cisco FTD que permiten la operación multi-instance son: Firepower 4100 y Firepower 9300 Security Appliances.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00515-01/	
https://www.csirt.gob.cl/media/2021/10/9VSA21-00515-01.pdf	

CSIRT alerta de vulnerabilidades en productos de Adobe	
Alerta de seguridad cibernética	9VSA21-00516-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Octubre de 2021
Última revisión	30 de Octubre de 2021

CVE	
CVE-2021-36070	**After Effects**
CVE-2021-40775	CVE-2021-40751
CVE-2021-40710	CVE-2021-40752
CVE-2021-40711	CVE-2021-40753
CVE-2021-40712	CVE-2021-40754
CVE-2021-40713	CVE-2021-40755
CVE-2021-40714	CVE-2021-40757
CVE-2021-40715	CVE-2021-40758
CVE-2021-40718	CVE-2021-40759
CVE-2021-40723	CVE-2021-40760
CVE-2021-40725	
CVE-2021-40733	**Animate**
CVE-2021-40734	CVE-2021-40733
CVE-2021-40735	CVE-2021-42266
CVE-2021-40736	CVE-2021-42267
CVE-2021-40737	CVE-2021-42268
CVE-2021-40738	CVE-2021-42269
CVE-2021-40739	CVE-2021-42270
CVE-2021-40740	CVE-2021-42271
CVE-2021-40741	CVE-2021-42272
CVE-2021-40742	CVE-2021-42524
CVE-2021-40744	
CVE-2021-40745	**Audition**
CVE-2021-40746	CVE-2021-40734
CVE-2021-40750	CVE-2021-40735
CVE-2021-40751	CVE-2021-40736
CVE-2021-40752	CVE-2021-40738
CVE-2021-40753	CVE-2021-40739
CVE-2021-40754	CVE-2021-40740
CVE-2021-40755	
CVE-2021-40757	**Bridge**
CVE-2021-40758	CVE-2021-40750
CVE-2021-40759	CVE-2021-42533
CVE-2021-40760	CVE-2021-42722
CVE-2021-40761	CVE-2021-42720
CVE-2021-40763	CVE-2021-42719
CVE-2021-40764	CVE-2021-42728
CVE-2021-40765	CVE-2021-42724
CVE-2021-40770	
CVE-2021-40771	**Character Animator**

CVE-2021-40772
CVE-2021-40773
CVE-2021-40774
CVE-2021-40776
CVE-2021-40777
CVE-2021-40778
CVE-2021-40779
CVE-2021-40780
CVE-2021-40785
CVE-2021-40786
CVE-2021-40787
CVE-2021-40792
CVE-2021-40793
CVE-2021-40794
CVE-2021-42266
CVE-2021-42267
CVE-2021-42268
CVE-2021-42269
CVE-2021-42270
CVE-2021-42271
CVE-2021-42272
CVE-2021-42524
CVE-2021-42526
CVE-2021-42527
CVE-2021-42529
CVE-2021-42530
CVE-2021-42531
CVE-2021-42532
CVE-2021-42533
CVE-2021-42719
CVE-2021-42720
CVE-2021-42721
CVE-2021-42722
CVE-2021-42723
CVE-2021-42724
CVE-2021-42726
CVE-2021-42728
CVE-2021-42731
CVE-2021-42732
CVE-2021-42733
CVE-2021-42735
CVE-2021-42736
CVE-2021-42737
CVE-2021-42738
CVE-2021-43011
CVE-2021-43012

XMP Toolkit SDK
CVE-2021-42529
CVE-2021-42530
CVE-2021-42531
CVE-2021-40763
CVE-2021-40764
CVE-2021-40765

Illustrator
CVE-2021-40718
CVE-2021-40746

InDesign
CVE-2021-42732
CVE-2021-42731

Lightroom Classic
CVE-2021-40776

Media Encoder
CVE-2021-40778
CVE-2021-40777
CVE-2021-40779
CVE-2021-40780

Photoshop
CVE-2021-42735
CVE-2021-42736

Prelude:
CVE-2021-40773
CVE-2021-42733
CVE -2021-40775
CVE-2021-42738
CVE-2021-42737
CVE-2021-40772
CVE-2021-40771

Premiere Elements
CVE-2021-40785
CVE-2021-40786
CVE-2021-40787
CVE-2021-42526
CVE-2021-42527

Premiere Pro
CVE-2021-40792
CVE-2021-40793
CVE-2021-40794

CVE-2021-42532	
Fabricante	
Adobe	
Productos afectados	
Adobe After Effects	
Adobe Animate	
Adobe Audition	
Adobe Bridge	
Adobe Character Animator	
Adobe Illustrator	
Adobe InDesign	
Adobe Lightroom Classic	
Adobe Media Encoder	
Adobe Photoshop	
Adobe Prelude	
Adobe Premiere Elements	
Adobe Premiere Pro	
Adobe XMP Toolkit SDK	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00516-01/	
https://www.csirt.gob.cl/media/2021/10/9VSA21-00516-01.pdf	

CSIRT alerta de nuevas vulnerabilidades en Android	
Alerta de seguridad cibernética	9VSA21-00517-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Noviembre de 2021
Última revisión	03 de Noviembre de 2021
CVE	
CVE-2021-0799	**Vulnerabilidades críticas**
CVE-2021-0921	CVE-2021-0918
CVE-2021-0923	CVE-2021-0930
CVE-2021-0926	CVE-2021-0889
CVE-2021-0933	CVE-2021-1924
CVE-2020-13871	CVE-2021-1975
CVE-2021-0653	
CVE-2021-0922	**Vulnerabilidades de riesgo alto**
CVE-2021-0928	CVE-2021-0799
CVE-2021-0650	CVE-2021-0921
CVE-2021-0918	CVE-2021-0923
CVE-2021-0930	CVE-2021-0926
CVE-2021-0434	CVE-2021-0933
CVE-2021-0649	CVE-2020-13871
CVE-2021-0932	CVE-2021-0653
CVE-2021-0925	CVE-2021-0928
CVE-2021-0931	CVE-2021-0650
CVE-2021-0919	CVE-2021-0434
CVE-2021-0920	CVE-2021-0649

CVE-2021-0924 CVE-2021-0929 CVE-2021-0889 CVE-2021-0927 CVE-2021-0672 CVE-2021-1924 CVE-2021-1975 CVE-2021-1921 CVE-2021-1973 CVE-2021-1979 CVE-2021-1981 CVE-2021-1982 CVE-2021-30254 CVE-2021-30255 CVE-2021-30259 CVE-2021-30284 CVE-2021-1048	CVE-2021-0932 CVE-2021-0925 CVE-2021-0931 CVE-2021-0920 CVE-2021-0924 CVE-2021-0929 CVE-2021-0927 CVE-2021-0672 CVE-2021-1921 CVE-2021-1973 CVE-2021-1979 CVE-2021-1981 CVE-2021-1982 CVE-2021-30254 CVE-2021-30255 CVE-2021-30259 CVE-2021-30284 CVE-2021-1048
Fabricante	
Google	
Productos afectados	
Versiones de Android anteriores al parche de seguridad del 6 de noviembre de 2021.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00517-01/	
https://www.csirt.gob.cl/media/2021/11/9VSA21-00517-01.pdf	

IoC Malware

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

El CSIRT de Gobierno 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
8f2863a64b0bedc09de0340a81b4986410204ecf596586c12287dc4e4419b1e6	MSIL/Kryptik.ADIF!tr	2CMV21-00242-01
070476bb2c0868aba1da672ffdc08ac1dc35f15b654d769963b0950642233c06	RTF/CVE_2017_11882.BX!exploit	2CMV21-00242-01
01692f885523ea188bbf0ba8e5fb8bd80e8e210e92a2f356684e53dda4fde3c1	MSIL/Kryptik.ADIA!tr	2CMV21-00242-01
60c26cd0aa41687b0540da14eca58a567ef7aac49de89397b8d6129e1ac04e6f	MSIL/Kryptik.ADIA!tr	2CMV21-00242-01
8013d96d1bdc09fc119066d5d7e569e69d71cc2e9af25fa192604bc386734cc8	MSIL/Kryptik.ADIA!tr	2CMV21-00242-01
990e906da487384f492c5100fcc7eef0338c584d8686cb16465d7be0512d8484	PossibleThreat.PALLASNET.H	2CMV21-00242-01
7ec569882f9fbee5facb3e50182f4f5b467e7b819f76e3103e5816704dd93d0f	PossibleThreat.PALLASNET.H	2CMV21-00242-01
59a25a572d221f89511803d03c2d085288815bde1ff4e6569f598aa241f1249b	PossibleThreat.PALLASNET.H	2CMV21-00242-01
f986420d0fa4d6222104117785671b984b789ac7fbd1bccf76ce1dee934cc74f	MSIL/Kryptik.ADIA!tr	2CMV21-00242-01
bf47b1cef6852ce946299fdb067942a6dc7873503b2b3c3d2b7eaaed2beeb52f	MSIL/Kryptik.ADIA!tr	2CMV21-00242-01
73fa3c467d88e6e53a85164b80c5b4b3b03c33243f1f2e5e2dec0983c106d83d	HTML/Phishing_Agent.PR!tr	2CMV21-00242-01
77857c131c719ad5ee2f81505ce4f34da33b64fffd212a788636e9ca7f590054	W32/Netsky.R@mm	2CMV21-00242-01
c2c9cb3c22b2f91e1d4c8f2df369592c49074f6094a91b80f79da0f54671cd83	W32/GenKryptik.EKLE!tr	2CMV21-00242-01
051a49bc5bc107ef08ec4fa89e54103cf763bdafb8faa8fdead8bf0b05cde722	Malicious_Behavior.SB	2CMV21-00242-01
b3f7d57603c0422e8a02662ccbb16ae2683e9d56c978cdafcecbfa46b71dfaaf	Riskware/POC_Iframe_CID	2CMV21-00242-01
232306d8d305d6c0e7c66cbb1a14727a79712cd256aaaf5163a3a8417faf3fcc	MSIL/Kryptik.DZG!tr	2CMV21-00242-01
2f7f960f3c5c57727d479a58cfc484dc4c01ab2673ca53023d0a7f00b55f5591	MSIL/Kryptik.DZG!tr	2CMV21-00242-01
9af7d2828acd443d655f9d5b999f206e51c488d4c0e9b562215edcda1c34083b	PossibleThreat.ZDS	2CMV21-00242-01
40e8a5bcf260915b2d0675766cfce42edcfe9c649cfa1b9208a761f872f37b84	MSIL/Kryptik.DZG!tr	2CMV21-00242-01
82f19eb057aacb95606a73b942f8e9e94b7746a0e9f5364a2fa18b503baab685	MSIL/Kryptik.DZG!tr	2CMV21-00242-01
cc23342a64d395f66a610dd3130eeadddc2ee45b28df12c0e1eb90cd6cb45043	MSIL/Kryptik.DZG!tr	2CMV21-00242-01
883d06e8debb0aa746140835ae112e59d681cf5ca2fd9df604fd8f1b11da8358	MSIL/GenKryptik.FMSI!tr	2CMV21-00242-01
b9705aa5da330f3de4454eb974b5f58dfbdc45ccb5e95e33ee3fc7cbc0263b11	W32/GenKryptik.EKLE!tr	2CMV21-00242-01
6edbfbbe9d75835efb5620ba95b660ff74a5075d56518d82ff17a7cf466ee5aa	MSIL/Kryptik.ADIF!tr	2CMV21-00242-01
86b461aa99e460a62e6db125320de4662a2b419ca07a5fe0afb08f4500d18408	MSIL/GenKryptik.FMSI!tr	2CMV21-00242-01
5a8643b89cf1f78061af0226129bc328e0911ca1b43fa2cdf407440525557e69	MSIL/Kryptik.ADGL!tr	2CMV21-00242-01

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	Documento web
136.144.41.67	Delis LLC	2CMV21-00242-01
45.137.22.156	RootLayer Web Services Ltd.	2CMV21-00242-01
45.137.22.142	RootLayer Web Services Ltd.	2CMV21-00242-01
103.167.91.51	VIETSERVER SERVICES TECHNOLOGY COMPANY LIMITED	2CMV21-00242-01
157.230.233.61	DIGITALOCEAN-ASN	2CMV21-00242-01
185.222.57.154	RootLayer Web Services Ltd.	2CMV21-00242-01
103.167.84.87	VIETSERVER SERVICES TECHNOLOGY COMPANY LIMITED	2CMV21-00242-01
87.246.7.39	SS-Net	2CMV21-00242-01
195.181.210.28	INTERNET CZ, a.s.	2CMV21-00242-01
45.137.22.62	RootLayer Web Services Ltd.	2CMV21-00242-01

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
Payment-Copy.doc	2CMV21-00242-01
PRICE QUOTATION.zip	2CMV21-00242-01
SHIPPING DOCUMENTS.zip	2CMV21-00242-01
0987654323456789876545678 9.z	2CMV21-00242-01
PARKING LIST.zip	2CMV21-00242-01
Scan-Copy.doc	2CMV21-00242-01
COSCO BANK INVOICE.arj	2CMV21-00242-01
Details OF Payment.zip	2CMV21-00242-01
Tax receipt.html	2CMV21-00242-01
msg18361.zip	2CMV21-00242-01
SWIFT COPY.LZH	2CMV21-00242-01
DELIVERY NOTE.zip	2CMV21-00242-01
Q.2021.03.17 PFP...zip	2CMV21-00242-01
Order No00020212910.pdf.z	2CMV21-00242-01
SHIPPING ADVICE#ASIA.zip	2CMV21-00242-01
fax45367876545678.tar	2CMV21-00242-01
TFS_TransferSlip.iso	2CMV21-00242-01

Actualidad

Lanzamiento en La Moneda de la campaña de educación escolar en ciberseguridad «Desde la Cuna al Computador»

Este viernes fue presentada la campaña Primera Campaña Nacional de Ciber Higiene Escolar "Desde la Cuna al Computador", que incentivará el uso responsable de internet en niños, niñas y adolescentes del país a través de comunidades educativas y centros de familia e infancia. Para ello, contempla un programa educativo de formación ciudadana dedicado a prevenir situaciones de acoso y vulnerabilidad que dañen o afecten la condición física y emocional de los menores de edad durante su etapa de desarrollo y escolar.

Acudieron al lanzamiento de la iniciativa en el Salón Montt Varas del Palacio de La Moneda el Ministro Secretario General de Gobierno, Jaime Bellolio, el Senador Kenneth Pugh, la Directora ejecutiva de Cuna Cultural, Andrea Henríquez, el Subsecretario del Interior, Juan Francisco Galli, la Subsecretaría de la Niñez, Blanquita Honorato y el Director Nacional de CSIRT Carlos Landeros, como parte además del cierre a las actividades por el Mes de la Ciberseguridad en nuestro país.

Juan Francisco Galli, Subsecretario del Interior, detalló que "estar conectados implica estar expuestos a peligros y las niñas, niños y adolescentes son un blanco muy atractivo. A través de videojuegos o navegando por Internet se expone a los niños y niñas a ver contenido inapropiado, sin adecuada supervisión, y a ser víctimas de delitos como el grooming. Asimismo, hemos conocido el aumento de la incidencia de cyberbullying, a través de las distintas plataformas. Estos hechos nos han llevado como Gobierno a implementar acciones que contribuyan a mantener un ciberespacio más seguro".

Galli explica que ante esta realidad, "la educación es fundamental para la prevención. Por eso, la Subsecretaría del Interior, mediante el CSIRT de Gobierno, desde 2018 ha elaborado diversas campañas de concientización dirigidas a los padres, madres, tutores, niños, niñas y adolescentes". Es así como "en agosto de este año, en la revista de concientización del Gobierno, "CiberSucesos", publicamos un especial de 10 cuentos infantiles, de manera que los niños conozcan los riesgos a los que están expuestos, ya sea en las redes sociales o en los juegos en línea de una forma simple, entretenida y dinámica. Por otra parte, en el Mes de la Ciberseguridad, desarrollamos una guía con 7 ciberriesgos a los que se exponen los menores de edad, cómo enfrentarlos y de qué manera se pueden prevenir", indicó.

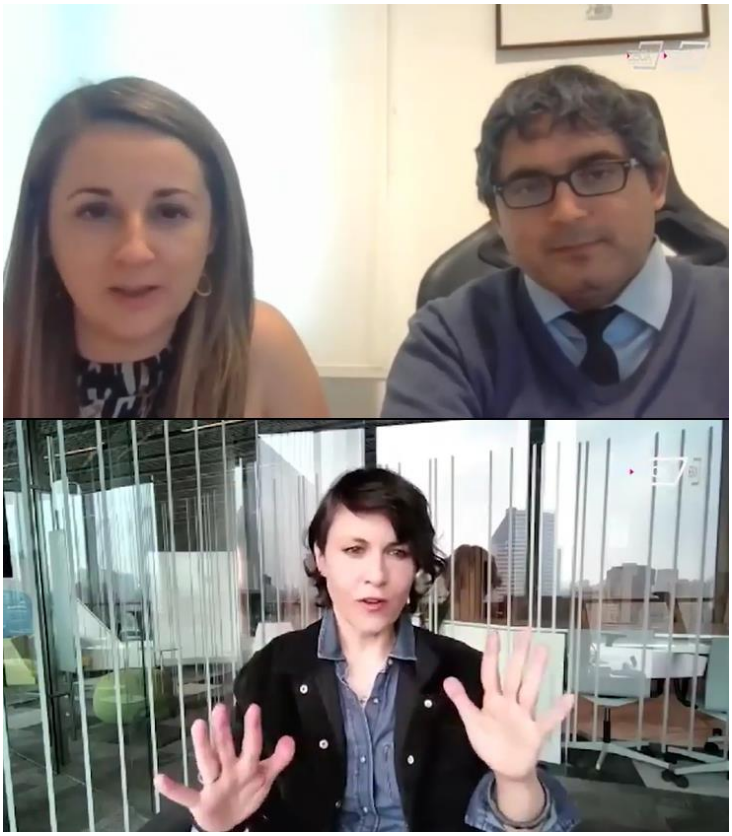
Los creadores de la Fundación Katty Summer junto al Director del CSIRT y su Directora Operacional.

Más detalles y las declaraciones de todas las autoridades que participaron del evento: https://www.csirt.gob.cl/noticias/lanzamiento-de-la-cuna-al-computador/.

El CSIRT de Gobierno participó de podcast Ciudadano Digital en DBoxRadio

El viernes pasado fue emitido el octavo capítulo del podcast Ciudadano Digital de DBoxRadio, al que fueron invitados el Director Nacional del CSIRT de Gobierno, Carlos Landeros, y su Directora Operacional, Katherina Canales, para conversar sobre ciberseguridad con la conductora del segmento, Carmen Gloria Cárcamo, Subgerente de Tendencias y Proyectos de Entel.

La idea del programa fue entregar información sobre conceptos básicos de ciberseguridad como tipos de ataques digitales y cómo prevenirlos, además de los más recientes proyectos de ley que impulsa el Gobierno para mejorar la ciberseguridad del país: Nueva Ley de Delito Informático, Ley de Protección de Datos Personales, y la creación de la Agencia Nacional de Ciberseguridad junto a la definición de los activos críticos de información.



Más información y el enlace para escuchar el podcast en SoundCloud, aquí: https://www.csirt.gob.cl/noticias/csirt-podcast-ciudadano-digital/.

El Comando de la Semana | No. 24 Masscan

En la sección El Comando de la Semana de hoy les traemos a Masscan, Este escáner de puertos de internet promete ser uno de los más rápidos. Su apuesta es que puede escanear todo el internet en menos de 6 minutos, transmitiendo 10 millones de paquetes por segundo. Produce resultados similares a nmap, uno de los escáneres de puertos más populares. Internamente, opera como Scanrand, Unicornscan y ZMap, usando transmisión asincrónica.

La principal diferencia de Masscan es que es más rápido que estos otros escáneres. Además, es más flexible y permite rangos de direcciones y puertos arbitrarios.

Encuentra el comando de esta semana aquí: csirt.gob.cl/estadisticas/el-comando-de-la-semana-no-24/

Recomendaciones y buenas prácticas

Recomendaciones generales de seguridad

- 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.

- Víctor Cofré
- Carlos Benito Queirolo Palma
- Osvaldo Fuentes Escobar
- Hernán Castillo
- Elisa Molina H.
- Germán Fernández
- Christian Feliciano Tapia Morales
- Gonzalo Andrés Ramírez Cabrera
- Francisco Andrés Peñaloza Astudillo
- Ricardo Monreal Llop
- Javiera Alarcón
- Fernando Enrique González Rojas
- Arantza
- Mario Rojas

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.11.05 15:22:26 -03'00'