Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

29-10-2021 | Año 3 | N°121

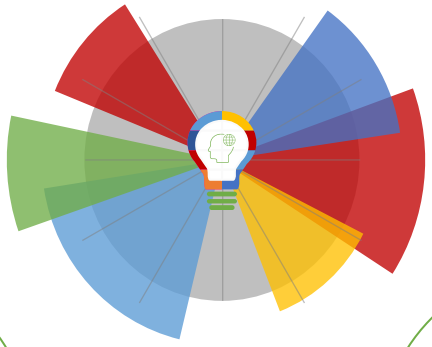
Boletín de Seguridad Cibernética

Semana del 22 al 28 de octubre de 2021

La semana en cifras

Hash
22
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
111
para vulnerabilidades
Las mitigaciones son útiles en productos de Red Hat, Discourse, Apple y Adobe.

IP
15
Informadas
Listado de IP advertidas en múltiples campañas de phishing y de malware.

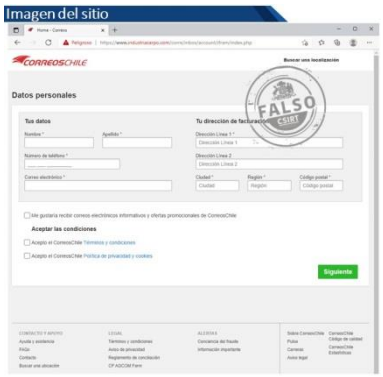
*Los datos recopilados corresponden a información publicada en diferentes secciones del sitio web https://www.csirt.gob.cl.

Contenido

Sitios fraudulentos

CSIRT informa página falsa del Banco Santander	
Alerta de seguridad cibernética	8FFR21-01015-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Octubre de 2021
Última revisión	25 de Octubre de 2021
Indicadores de compromiso	
URL sitio falso	
http://chile-smsseguro[.]com/1635125139/portada/personas/home.asp	
IP	
[51.161.122.78]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01015-01/	
https://www.csirt.gob.cl/media/2021/10/8FFR21-01015-01.pdf	

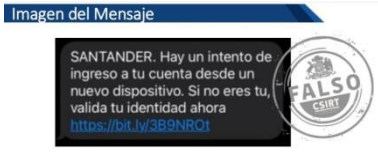
CSIRT advierte sitio web que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR21-01016-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Octubre de 2021
Última revisión	25 de Octubre de 2021
Indicadores de compromiso	
URL sitio falso	
https://www.sms-chilesgurro[.]ovh/1635125730/portada/personas/home.asp	
IP	
[51.161.122.78]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01016-01/	
https://www.csirt.gob.cl/media/2021/10/8FFR21-01016-01.pdf	



CSIRT advierte suplantación de página web de Correos de Chile	
Alerta de seguridad cibernética	8FFR21-01017-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Octubre de 2021
Última revisión	25 de Octubre de 2021
Indicadores de compromiso	
URL sitio falso	
https://www.industriasarpo[.]com/corre/inbox/account/iframe/index.php	
IP	
[185.176.9.146]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01017-01/	
https://www.csirt.gob.cl/media/2021/10/8FFR21-01017-01.pdf	

Phishing

CSIRT advierte de phishing por supuesto cobro de IFE Universal	
Alerta de seguridad cibernética	8FPH21-00438-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Octubre de 2021
Última revisión	26 de Octubre de 2021
Indicadores de compromiso	
URL redirección	
https://bit[.]ly/3gUlllZ	
URL sitio falso	
https://www-personas-banco-estado-web[.]cf/promos-feriadas?235695623ffiof26jqbc	
IP	
[204.12.234.154]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00438-01/	
https://www.csirt.gob.cl/media/2021/10/8FPH21-00438-01.pdf	



CSIRT alerta de campaña de smishing que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FPH21-00439-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Octubre de 2021
Última revisión	27 de Octubre de 2021
Indicadores de compromiso	
URL de SMS	
https://bitly[.]com/3B9NROt	
URL sitio falso	
http://mundodinamico[.]ovh/?sms=santander	
http://wsananz.cluster051.hosting.ovh[.]net/1635341024/portada/personas/home.asp	
IP	
[51.161.122.78]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00439-01/	
https://www.csirt.gob.cl/media/2021/10/8FPH21-00439-01-1.pdf	

CSIRT informa de smishing que suplanta al Banco de Chile	
Alerta de seguridad cibernética	8FPH21-00440-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Octubre de 2021
Última revisión	28 de Octubre de 2021
Indicadores de compromiso	
URL de SMS	
https://bit[.]ly/MiPaSs-cl	
URL sitio falso	
https://login-chilebanca.cl-kdtc[.]xyz/1635361063/bcochile-web/persona/login/index.html/login	
IP	
[104.21.2.248]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00440-01/	
https://www.csirt.gob.cl/media/2021/10/8FPH21-00440-01.pdf	

Malware

CSIRT informa campaña de phishing con malware por falso envío de DHL	
Alerta de seguridad cibernética	2CMV21-00239-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de Octubre de 2021
Última revisión	19 de Octubre de 2021
Indicadores de compromiso	
SHA256	
682C6CEECD131B1D921137C402CBD0FDFE3921CBB07342082D379FC0D463C8AC 3B8333C95F03BCEFC683AC075A6F3629DE98D38B3766498323E95F6C73CA6BEB	
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://63.250.40.204/~wpdemo/file.php?search=8376882	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv21-0240-01/	
https://www.csirt.gob.cl/media/2021/10/2CMV21-00239-01.pdf	

Vulnerabilidades

CSIRT alerta ante vulnerabilidades en productos Red Hat	
Alerta de seguridad cibernética	9VSA21-00510-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Octubre de 2021
Última revisión	22 de Octubre de 2021
CVE	
CVE-2016-4658	CVE-2021-34428
CVE-2016-4658	CVE-2021-35550
CVE-2020-25648	CVE-2021-35556
CVE-2021-21670	CVE-2021-35559
CVE-2021-21671	CVE-2021-35561
CVE-2021-22543	CVE-2021-35564
CVE-2021-22922	CVE-2021-35565
CVE-2021-22923	CVE-2021-35567
CVE-2021-22924	CVE-2021-35578
CVE-2021-23017	CVE-2021-35586
CVE-2021-23840	CVE-2021-35588
CVE-2021-23841	CVE-2021-35603

CVE-2021-25741 CVE-2021-28169 CVE-2021-32626 CVE-2021-32627 CVE-2021-32628 CVE-2021-32672 CVE-2021-32675 CVE-2021-32687 CVE-2021-32690	CVE-2021-36222 CVE-2021-3653 CVE-2021-3656 CVE-2021-36980 CVE-2021-37576 CVE-2021-37750 CVE-2021-41099 CVE-2021-33196
Fabricante	
Red Hat	
Productos afectados	
java-1.8.0-openjdk (Red Hat package): before 1.8.0.312 b07-1.el8_1 java-1.8.0-openjdk (Red Hat package): before 1.8.0.312 b07-1.el8_2 java-1.8.0-openjdk (Red Hat package): before 1.8.0.312 b07-1.el8_4 java-11-openjdk (Red Hat package): 11.0.11.0.9-0.el8_2, 11.0.12.0.7-0.el8_2 java-11-openjdk (Red Hat package): 11.0.11.0.9-1.el7_9, 11.0.12.0.7-0.el7_9 java-11-openjdk (Red Hat package): 11.0.12.0.7-0.el8_4 java-11-openjdk (Red Hat package): 11.0.6.10-0.el8_1, 11.0.7.10-1.el8_1, 11.0.11.0.9-0.el8_1, 11.0.12.0.7-0.el8_1 openvswitch2.11 (Red Hat package): 2.11.3-77.el7fdp, 2.11.3-86.el7fdp Red Hat Advanced Cluster Management for Kubernetes 2.1 Red Hat Advanced Cluster Management for Kubernetes: 2.3.0, 2.3.1, 2.3.2 Red Hat CodeReady Linux Builder for ARM 64 – Extended Update Support: 8.4 Red Hat CodeReady Linux Builder for ARM 64: 8.0 Red Hat CodeReady Linux Builder for IBM z Systems – Extended Update Support: 8.4 Red Hat CodeReady Linux Builder for IBM z Systems: 8.0 Red Hat CodeReady Linux Builder for Power, little endian – Extended Update Support: 8.4 Red Hat CodeReady Linux Builder for Power, little endian: 8.0 Red Hat CodeReady Linux Builder for x86_64 – Extended Update Support: 8.4 Red Hat CodeReady Linux Builder for x86_64: 8.0 Red Hat Enterprise Linux Desktop: 7 Red Hat Enterprise Linux for ARM 64 – Extended Update Support: 8.1 Red Hat Enterprise Linux for ARM 64 – Extended Update Support: 8.4 Red Hat Enterprise Linux for ARM 64: 8 Red Hat Enterprise Linux for IBM z Systems – Extended Update Support: 8.1 Red Hat Enterprise Linux for IBM z Systems – Extended Update Support: 8.4 Red Hat Enterprise Linux for IBM z Systems: 7 Red Hat Enterprise Linux for IBM z Systems: 8 Red Hat Enterprise Linux for Power, big endian: 7 Red Hat Enterprise Linux for Power, little endian – Extended Update Support: 8.1 Red Hat Enterprise Linux for Power, little endian – Extended Update Support: 8.4 Red Hat Enterprise Linux for Power, little endian: 7 Red Hat Enterprise Linux for Power, little endian: 8 Red Hat Enterprise Linux for Scientific Computing: 7	

Red Hat Enterprise Linux for x86_64 – Extended Update Support: 8.1 Red Hat Enterprise Linux for x86_64 – Extended Update Support: 8.4 Red Hat Enterprise Linux for x86_64: 8.0 Red Hat Enterprise Linux Server – AUS: 8.4 Red Hat Enterprise Linux Server – TUS: 8.2 Red Hat Enterprise Linux Server – TUS: 8.4 Red Hat Enterprise Linux Server – Update Services for SAP Solutions: 8.1 Red Hat Enterprise Linux Server – Update Services for SAP Solutions: 8.4 Red Hat Enterprise Linux Server (for IBM Power LE) – Update Services for SAP Solutions: 8.1 Red Hat Enterprise Linux Server (for IBM Power LE) – Update Services for SAP Solutions: 8.4 Red Hat Enterprise Linux Server: 7 Red Hat Enterprise Linux Workstation: 7 Red Hat OpenShift Container Platform 4.9 Red Hat Software Collections: 1 for RHEL 7, 1 for RHEL 7.7 Red Hat Virtualization for IBM Power LE: 4 Red Hat Virtualization Host: 4 Red Hat Virtualization: 4 redhat-release-virtualization-host (Red Hat package): 4.3.4-1.el7ev, 4.3.5-2.el7ev, 4.3.5-4.el7ev, 4.3.6-2.el7ev, 4.3.6-5.el7ev, 4.3.9-2.el7ev, 4.3.11-1.el7ev, 4.3.12-4.el7ev, 4.3.13-2.el7ev, 4.3.14-2.el7ev, 4.3.16-1.el7ev, 4.3.17-1.el7ev, 4.3.18-1.el7ev redhat-virtualization-host (Red Hat package): 4.3.11-20200922.0.el7_9, 4.3.12-20201216.0.el7_9, 4.3.13-20210127.0.el7_9, 4.3.14-20210322.0.el7_9, 4.3.16-20210615.0.el7_9, 4.3.17-20210713.0.el7_9, 4.3.18-20210903.0.el7_9 rh-redis5-redis (Red Hat package): before 5.0.5-3.el7
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00510-01/
https://www.csirt.gob.cl/media/2021/10/9VSA21-00510-01.pdf

CSIRT alerta ante vulnerabilidad crítica en Discourse	
Alerta de seguridad cibernética	9VSA21-00511-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	26 de Octubre de 2021
Última revisión	26 de Octubre de 2021
CVE	
CVE-2021-41163	
Fabricante	
Discourse	
Productos afectados	
Discourse 2.7.8 y anteriores.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00511-01/	
https://www.csirt.gob.cl/media/2021/10/9VSA21-00511-01.pdf	

CSIRT alerta ante vulnerabilidades en productos de Apple	
Alerta de seguridad cibernética	9VSA21-005012-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Octubre de 2021
Última revisión	27 de Octubre de 2021
CVE	
CVE-2021-30821	CVE-2021-30903
CVE-2021-30824	CVE-2021-30906
CVE-2021-30834	CVE-2021-30907
CVE-2021-30868	CVE-2021-30908
CVE-2021-30876	CVE-2021-30909
CVE-2021-30877	CVE-2021-30910
CVE-2021-30879	CVE-2021-30911
CVE-2021-30880	CVE-2021-30912
CVE-2021-30881	CVE-2021-30913
CVE-2021-30883	CVE-2021-30915
CVE-2021-30888	CVE-2021-30916
CVE-2021-30899	CVE-2021-30917
CVE-2021-30900	CVE-2021-30918
CVE-2021-30901	CVE-2021-30919
CVE-2021-30902	
Fabricante	
Apple	
Productos afectados	
MacOS 11.0 20A2411 a 11.6 20G165.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00512-01/	
https://www.csirt.gob.cl/media/2021/10/9VSA21-00512-01.pdf	

CSIRT alerta de vulnerabilidades en productos Adobe	
Alerta de seguridad cibernética	9VSA21-005013-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Octubre de 2021
Última revisión	28 de Octubre de 2021
CVE	
CVE-2021-40718	CVE-2021-42267
CVE-2021-40733	CVE-2021-42268
CVE-2021-40743	CVE-2021-42269
CVE-2021-40746	CVE-2021-42270
CVE-2021-40747	CVE-2021-42271
CVE-2021-40748	CVE-2021-42272
CVE-2021-40749	CVE-2021-42524
CVE-2021-40776	CVE-2021-42525
CVE-2021-40785	CVE-2021-42526

CVE-2021-40786	CVE-2021-42527
CVE-2021-40787	CVE-2021-42528
CVE-2021-40788	CVE-2021-42529
CVE-2021-40789	CVE-2021-42530
CVE-2021-40792	CVE-2021-42531
CVE-2021-40793	CVE-2021-42532
CVE-2021-40794	CVE-2021-42731
CVE-2021-40796	CVE-2021-42732
CVE-2021-42263	CVE-2021-42734
CVE-2021-42264	CVE-2021-42735
CVE-2021-42266	CVE-2021-42736
Fabricante	
Adobe	
Productos afectados	
Adobe Illustrator CC: 25.0 a 25.4.1. Adobe Premiere Elements: 2021.19.0 20210809.daily.2242976. Adobe InDesign: 9.1.0 a 2015. Adobe Lightroom Classic: 10.3 Adobe Animate 21.0.9. Adobe Photoshop: 20.0 a 22.5.1. Adobe Premiere Pro 13.1.0 a 15.4.1. Adobe Premiere Elements: 2021.19.0 20210809.daily.2242976 Adobe InDesign: 9.1.0 a 2014.2, 2015. Adobe Lightroom Classic 10.3.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00513-01/	
https://www.csirt.gob.cl/media/2021/10/9VSA21-00513-01.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 de archivos maliciosos	Tipo de malware	Documento web
35056762755603176fdd69583d03f154c6b5a7dbac3ae758b9a1d4cd04ff4e32	MSOffice/Agent.GV!tr	2CMV21-00240-01
134d2e46618207db5a72d7ca0fb39310491a5e3c4337dc459d623dbec2beaf06	MSOffice/Scam.2ED7!tr	2CMV21-00240-01
a3d56f9820ec00991790b130b88f0b7fa36f9366b3ac287db58c70c5a4a5dc53	MSOffice/CVE_2017_11882	2CMV21-00240-01
429200fcff319513ff946fae51d5bb4500f969e02f5dcc02bc7333506b77635b	MSIL/GenKryptik.FLEY!tr	2CMV21-00240-01
4fe4931ff2df16ba3943c1380dd21e9c32ce29a708068b3190c10de20b5a1d99	PossibleThreat	2CMV21-00240-01
fbf3874618c8de5a447f5d757b707e6680e83dd6a2edf4a11dcf566de65064e9	PossibleThreat	2CMV21-00240-01
78efeb17c061e887abd631e616e44139a92ffc4d82f709c6cd062c23805cfcb7		2CMV21-00240-01
1151e2239b24e43cc43e43f1f3ef5241f7ea4831443e7fbf1981e7b2f7b116c8		2CMV21-00240-01
abd12aba01515d8829dba0e20a08420925265346bf63b0d0f25fa8dd72c33de9		2CMV21-00240-01
115239f3a4c673dbbcf990b8a81594c350a0e8c7c5216d1ffca4ffc7751d35b5	VBA/Agent.D795!tr	2CMV21-00240-01
1845ebd6aaa37eb8a9665af93db7b53e6133a864ba613a376882107d2b1b582c	MSIL/Agent.AES!tr	2CMV21-00240-01
02775b6ac6554e57854050cd6462a2bb1086a45607b6a5f22b6fb111e6880391	MSIL/Kryptik.ADCZ!tr	2CMV21-00240-01
d3444dae388a8d1671d53edcd75a3ca92a427d0d7db8acfae89e2a92e264812b	MSIL/Agent.AES!tr	2CMV21-00240-01
d7677d8ae3578e42bc4e7802420b14f63eb7ff9425f46c413c57eca2d8420e68	W32/Malicious_Behavior	2CMV21-00240-01
7a4e256a50649d821899a58c8e401b205875027fbd871447f952e2582f4931c1		2CMV21-00240-01
df20110a040aae764dd95bdfb474fa2f9929d5e78f6280ddc6a9667d18da54cc	MSIL/Agent.AES!tr	2CMV21-00240-01
741b738edb136abc66219d1ad8a4cbdbcc97f99d6ad85539a4881c39a0d62702	MSIL/Agent.AES!tr	2CMV21-00240-01
61fa21c4f1d716dd406241273bd1763af497d919b8008c53f4c85bbbb48d1b64	MSIL/Kryptik.FVA!tr.dldr	2CMV21-00240-01
069cf47ec8964fdae9009421489242faf2be3078b2f986874a3d4f0c67fda0a2	MSIL/Kryptik.FVA!tr.dldr	2CMV21-00240-01
d2a3560a21206f97042705f8716f3b4e05088eaa202c601016d772b6afa73b79		2CMV21-00240-01

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
77.247.110.105	ABC Consultancy	2CMV21-00240-01
165.232.135.241	DIGITALOCEAN-ASN	2CMV21-00240-01
142.11.234.209	142.11.234.209	2CMV21-00240-01
185.222.57.168	RootLayer Web Services Ltd.	2CMV21-00240-01
185.222.57.214	RootLayer Web Services Ltd.	2CMV21-00240-01
193.56.29.111	Web Hosted Group Ltd	2CMV21-00240-01
195.242.110.72	Internet It Company Inc	2CMV21-00240-01
212.193.30.87	Des Capital B.V.	2CMV21-00240-01
37.221.113.41	M247 Ltd	2CMV21-00240-01
45.137.22.144	RootLayer Web Services Ltd.	2CMV21-00240-01
45.137.22.49	RootLayer Web Services Ltd.	2CMV21-00240-01

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
UOtBQlxt6rYmlyY.exe	2CMV21-00240-01
SWIFT.rar	2CMV21-00240-01
RPLTFL024962021.GZ	2CMV21-00240-01
Proforma Invoice.pdf.z	2CMV21-00240-01
PO-18102021.xlsx	2CMV21-00240-01
PO # 11002021.zip	2CMV21-00240-01
Order Confirmation & payment.,pdf.ppam	2CMV21-00240-01
NEW ORDER AST 27-28 October.xlsx	2CMV21-00240-01
Invoice.shtml	2CMV21-00240-01
IMG_RFQ70103260100057.r12	2CMV21-00240-01
HO-MA PO-7741.xlsx	2CMV21-00240-01
HLG 21665-PSI-October -2021.zip	2CMV21-00240-01
data24422.pif	2CMV21-00240-01

Copy BL and Debit Note.rar	2CMV21-00240-01
Bank slip.rar	2CMV21-00240-01
ADNOC DOCUMENTS.rar	2CMV21-00240-01
70654 SSEBACT.zip	2CMV21-00240-01

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
74.201.28.192	DEDIPATH-LLC	4IIA21-00045-01
141.98.10.252	UAB Host Baltic	4IIA21-00045-01
41.216.201.78	rain	4IIA21-00045-01
31.210.20.229	Delis LLC	4IIA21-00045-01
195.133.40.210	Delis LLC	4IIA21-00045-01

Ip reportadas en informes anteriores y que aún se encuentran activas hasta el informe del 25 de octubre:

IP
194.61.24.154
194.61.24.155
194.61.24.151
194.61.24.153
194.61.24.152

Actualidad

Ciberconsejos para guiar a las personas mayores en el mundo digital

Continuando con nuestras guías de uso seguro del internet y la tecnología, que preparamos durante el Mes de la Ciberseguridad (la primera, dirigida a niños, niñas y adolescentes, la pueden ver aquí: Siete grandes riesgos para NNA), hoy les presentamos ciberconsejos dedicados especialmente a las personas mayores, aunque sirven para todos quienes quieran reforzar algunos conceptos básicos del uso de internet y también conocer buenas prácticas que debemos aplicar a toda edad.

Pueden descargar y compartir «Ciberconsejos para guiar a las personas mayores en el mundo digital» en este enlace: https://www.csirt.gob.cl/media/2021/10/Cibergui%CC%81a-para-el-adulto-mayor-OK.pdf

Las personas mayores fueron el foco central de la campaña semanal del CSIRT de Gobierno y CSIRTAmericas por el Mes de la Ciberseguridad.

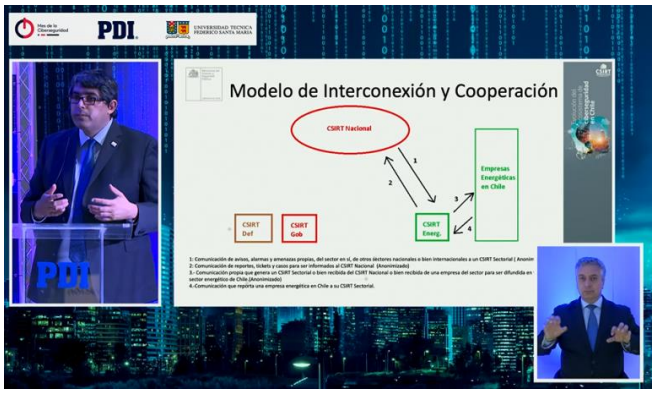
Octubre es el Mes de la Ciberseguridad y por eso 12 CSIRT del continente — reunidos en CSIRTAmericas— y el Programa de Ciberseguridad de la Organización de los Estados Americanos (OEA) hemos compartido una serie de ciberconsejos de concientización alineados según cuatro temas, uno cada semana.

En esta última semana de campaña, los CSIRT de Ecuador, Colombia y República Dominica enfocaron los ciberconsejos para las personas mayores. Las recomendaciones tuvieron como objetivo enseñar cómo navegar por internet y utilizar las distintas plataformas de forma segura.

La idea, presentada por el CSIRT del Gobierno de Chile a CSIRTAmericas y adoptada rápidamente, ha sido plasmada en imágenes en nuestro país recopilando consejos enviados por cada uno de los CSIRT partícipes: Buenos Aires y Neuquén en Argentina, Chile, Colombia, Costa Rica, Ecuador, Estados Unidos, Jamaica, Panamá, Paraguay, República Dominicana y Uruguay. Las publicaciones son hechas en inglés y castellano y podrán verlas aparecer durante todo el mes en https://twitter.com/CSIRTGOB

Director del CSIRT resalta urgencia de nueva institucionalidad en Cuarto Seminario de Ciberseguridad de la PDI y la Universidad Santa María

El jueves 28 de octubre se realizó el Cuarto Seminario Internacional de Ciberseguridad, organizado por la Policía de Investigaciones y la Universidad Técnica Federico Santa María, que bajo el título «Hiperconectados: Riesgos, desafíos y responsabilidades» reunió a destacadas personalidades de la ciberseguridad en nuestro país, como el senador Kenneth Pugh, el académico Xavier Bonaire y el director del CSIRT de Gobierno, Carlos Landeros.



El seminario se realiza cada año en el marco del Mes de la Ciberseguridad (https://www.mesdelaciberseguridad.cl/seminario/).

Landeros entregó en su presentación «Evolución del ecosistema de la ciberseguridad en Chile» una muestra de cómo el ambiente en esta materia ha ido cambiando en los últimos años, en medio de un crecimiento exponencial de los ataques informáticos y el avance de la transformación digital y la inteligencia artificial, entre otros cambios que exigen la creación de una Agencia Nacional de Ciberseguridad (ANC) como la que busca generar el proyecto de Ley Marco de Ciberseguridad.

La ANC será parte así de una nueva institucionalidad de la ciberseguridad en Chile, de la que participarán también el Comité Interministerial de Ciberseguridad, un CSIRT Nacional, y CSIRT sectoriales.

Más aún, explicó el director del CSIRT de Gobierno, esta ley también contempla medidas para mejorar la colaboración y comunicación público-privadas en esta materia, las que han sido adaptadas de las experiencias exitosas de socios extranjeros con los que el CSIRT mantiene acuerdos de cooperación, como sus entidades homólogas en Israel, España y Estados Unidos.

Un elemento clave es la definición de activos que correspondan a infraestructura crítica de la información, que sería regulada y supervisada por esta nueva agencia.

Ministerio de Ciencia presenta primera Política Nacional de Inteligencia Artificial del país, con un importante componente de ciberseguridad

El Ministerio de Ciencia, Tecnología, Conocimiento e Innovación presentó ayer la nueva Política Nacional de Inteligencia Artificial (disponible para su descarga aquí Política Nacional de Inteligencia Artificial (minciencia.gob.cl)), iniciativa inédita en el país y que define los lineamientos estratégicos que seguirán las decisiones de la autoridad en términos de inteligencia artificial por la próxima década.

Esta «hoja de ruta» presenta 180 iniciativas y 70 acciones prioritarias, organizadas alrededor de tres ejes: factores habilitantes, uso y desarrollo de Inteligencia Artificial en Chile y aspectos de ética y seguridad, y fue desarrollada con la participación de 9 mil personas, indica el ministerio, liderados por un comité asesor multidisciplinario de 12 expertos.

La Política nace de una solicitud efectuada por el Presidente Sebastián Piñera en agosto de 2019, y hace mención explícita y reiterada a la ciberseguridad, y a las implicancias para bien y para mal que tiene la extensión del uso de inteligencia artificial (IA) para estas materias.

Así, la ciberseguridad y sus ramificaciones vienen analizadas directamente en su propia sección del capítulo sobre Ética, Aspectos Legales y Regulatorios. Es indispensable ignorar la ciberseguridad como parte de la discusión sobre IA, explica el documento, ya que «el significativo aumento y complejidad de los ciberataques ejecutados diariamente se suma a los diversos propósitos e intereses que ellos persiguen, así como también a la multiplicidad de brechas, vulnerabilidades y vectores de ataque. Un ciberataque puede llegar a ser tan efectivo y perjudicial como un ataque armado, y más aún ante posibles usos bélicos de estos sistemas automatizados».

Estos riesgos aumentan con la aplicación de IA, agrega el texto, algo que ya está sucediendo. Pero al mismo tiempo «la IA se presenta como una nueva herramienta para mantener el ciberespacio libre, abierto, seguro y resiliente y, con ello, cumplir los objetivos señalados en nuestra actual Política Nacional de Ciberseguridad. De ahí la vinculación entre ambas Políticas. La IA, en general, puede contribuir optimizando los tiempos de respuesta, la identificación de vulnerabilidades, la detección de intrusiones, fraudes o identificación de malwares, además de identificar tendencias y/o elaborar rankings de los riesgos relevantes en la red y analizar grandes volúmenes de información de contexto reduciendo al mismo tiempo la intervención humana».

En resumen, la Política Nacional de Inteligencia Artificial llama a:

Incorporar la IA en las estrategias de ciberseguridad y ciberdefensa, así como en proyectos de ley asociados a ellas: incorporaremos la IA como un componente en las próximas actualizaciones de la Política Nacional de Ciberseguridad y así también en las políticas de ciberdefensa por medios de diálogos multiactor.

Además, analizaremos el marco legal vigente en cuanto a las implicaciones del usode IA en el ámbito de la ciberseguridad, y le daremos impulso a proyectos de ley de relevancia en este aspecto, como el Proyecto de Ley Marco de Ciberseguridad e Infraestructura crítica y el Proyecto de Ley sobre Delitos Informáticos.

Fomentar el uso de sistemas de IA para reaccionar a los ataques informáticos en el Estado: Generaremos recomendaciones para el uso de IA en los sistemas del Estado para combatir los ataques informáticos. Esto lo haremos en conjunto con los actores con competencias en materias de ciberseguridad, para aprovechar la potencialidad de la tecnología.

Fomentar la capacitación en las áreas asociadas a la ciberseguridad: Incorporaremos en las Políticas de Ciberseguridad y Ciberdefensa planes de capacitación sobre IA de los profesionales que desarrollan, implementan y tienen a su cargo sistemas informáticos. Adicionalmente, en cuanto el avance es constante tanto de la sofisticación de los ataques como de técnicas defensivas, se promoverá mayor investigación, desarrollo e innovación en tecnologías del futuro, por ejemplo, tecnologías cuánticas, que proveerán mejores herramientas para abordar estas técnicas defensivas y formación de expertos y profesionales.

Incorporar la IA en la institucionalidad pública de ciberseguridad: El Decreto Supremo N°533, de 2015, del Ministerio del Interior y Seguridad Pública, creó el Comité Interministerial sobre Ciberseguridad (“CICS”), con la misión de confeccionar la Política Nacional de Ciberseguridad del país. Actualizaremos este Comité para que se posicione como un espacio intersectorial propicio para impulsar y concretar acciones en materia de ciberseguridad que incluyan IA.

El Comando de la Semana | No. 23 Bing-IP2Hosts

El protagonista en una nueva edición de El Comando de la Semana es Lynis, una herramienta de El Comando de la Semana es hoy Bing-IP2Hosts, una herramienta que aprovecha una función única del motor de búsqueda de Microsoft, Bing, para buscar sitios web alojados en una dirección IP específica.

Bing-IP2Hosts utiliza esta función para enumerar todos los nombres de host que Bing ha indexado para una dirección IP específica. Esta técnica se considera la mejor práctica durante la fase de reconocimiento de una prueba de penetración, para descubrir una superficie de ataque potencial más grande. Bing-IP2Hosts está escrito en el lenguaje de secuencias de comandos Bash para Linux.

Con los comandos que compartimos semanalmente no pretendemos reemplazar una auditoria de código o evaluación de vulnerabilidades, sino que establecer capacidades básicas de chequeo y obtención de información de manera rápida para temas específicos, como por ejemplo la verificación de la subsanación de alertas o vulnerabilidades reportadas por el CSIRT de Gobierno.

Encuentra el comando de esta semana aquí:
https://www.csirt.gob.cl/media/2021/10/Comando-de-la-semana-23-BING-IP2HOSTS.pdf

El Control de la Semana | No. 17 Restricciones sobre la instalación de software

Esta semana, la Ficha de Control Normativo detalla las Restricciones sobre la instalación de software, incluyendo recomendaciones y mejores prácticas.

Las organizaciones deben definir y poner en vigencia una política estricta sobre qué tipos de software pueden instalar sus usuarios en los equipos y dispositivos institucionales. Cabe tener presente que las instalaciones de software puede ser realizadas por el usuario de manera intencional o no, y que esta instalación puede ser también maliciosa o benigna, lo que determinará los impactos positivos o negativos que pueda tener sobre la organización y sus controles.

También es necesario entender que la instalación de software puede ser realizada por terceras partes (soporte u otras personas) y más aún, un software puede ser instalado por otras piezas de software (malware, por ejemplo) que se propagan lateralmente dentro de una organización desde una máquina contaminada a otra vulnerable.

En este contexto, es necesario establecer controles que ayuden a mitigar los impactos negativos de instalaciones de software malicioso o, desde otra óptica, software no licenciado (con impacto en el cumplimiento legal de la institución exponiéndola a multas e infracciones por uso ilegal de software con propiedad intelectual).

En el documento descargable a continuación encontrarán todos los detalles del control de esta semana: https://www.csirt.gob.cl/media/2021/10/El-Control-de-la-semana-N%C2%B017-A12.6.2_v1.pdf

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.

- Fernando Enrique González Rojas
- Javier Ignacio Candia Tapia
- Alonso Alejandro Pasten Guajardo
- Francisco Gutiérrez
- Milena Lagos Carrasco
- Sebastián Urquiza Rojas
- Christian Abarca
- Víctor Cofré

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.10.29 16:49:50 -03'00'