CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

17-12-2020 | Año 2 | N°76

Boletín de Seguridad Cibernética

Semana del 10 al 16 de Diciembre de 2020

División de Redes y Seguridad Informática. Gobierno de Chile

Ministerio del Interior y Seguridad Pública. Gobierno de Chile

Resumen de la semana en cifras

Hash

109

Sha 256

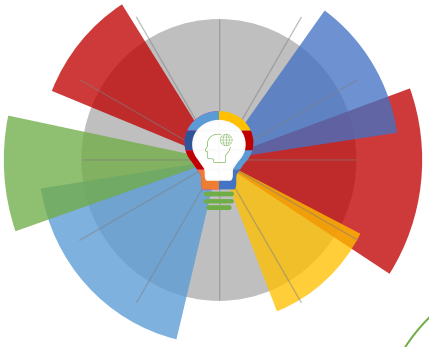
Asociadas a múltiples campañas de phishing son archivos que contienen malware

Se advirtieron

23

URLs

Asociadas a sitios fraudulentos y campañas de phishing



Parches

38

para vulnerabilidades

Las mitigaciones son útiles para productos Haxx, Mozilla, Cisco, Wireshark, GitLab y OpenSSL.

IPs

132

Informadas

Listado de IPs 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 3
Phishing 9
Vulnerabilidades 12
IoC - Malware 15
IoC - Ataques de Fuerza Bruta 20
Actualidad 21
Investigación 22
Recomendaciones y Buenas Prácticas 23
Muro de la Fama 24

Sitios fraudulentos

CSIRT informa de página bancaria fraudulenta	
Alerta de seguridad cibernética	8FFR20-00844-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Diciembre de 2020
Última revisión	11 de Diciembre de 2020
Indicadores de compromiso	
URL	
https://santcnder-cl[.]info/1607697116/index.asp	
IP	
[188.166.90.21]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00844-01/	
https://www.csirt.gob.cl/media/2020/12/8FFR20-00844-01.pdf	

CSIRT advierte suplantación de sitio bancario	
Alerta de seguridad cibernética	8FFR20-00845-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Diciembre de 2020
Última revisión	11 de Diciembre de 2020
Indicadores de compromiso	
URL	
https://login.personascl.online/1607698337/index.asp	
IP	
[35.193.13.30]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00845-01/	
https://www.csirt.gob.cl/media/2020/12/8FFR20-00845-01.pdf	

CSIRT informa sitio fraudulento de almacenamiento de archivos	
Alerta de seguridad cibernética	8FFR20-00846-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Diciembre de 2020
Última revisión	11 de Diciembre de 2020
Indicadores de compromiso	
URL	
http://findingbuyerstraining[.]com/alex/stone/	
IP	
[173.254.237.250]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00846-01/	
https://www.csirt.gob.cl/media/2020/12/8FFR20-00846-01.pdf	

CSIRT informa portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00847-01
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 2020
Última revisión	14 de Diciembre de 2020
Indicadores de compromiso	
URL	
https[:]//www.superclave-actualizar[.]app/1607949105/personas/index.asp	
IP	
[162.0.235.23]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00847-01/	
https://www.csirt.gob.cl/media/2020/12/8FFR20-00847-01.pdf	

CSIRT advierte página falsa de empresa de almacenamiento de archivos	
Alerta de seguridad cibernética	8FFR20-00848-01
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 2020
Última revisión	14 de Diciembre de 2020
Indicadores de compromiso	
URL	
https://rucalafchiloe[.]cl/lok/FBG/	
IP	
[185.50.196.201]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00848-01/	
https://www.csirt.gob.cl/media/2020/12/8FFR20-00848-01.pdf	

CSIRT informa suplantación de página de software	
Alerta de seguridad cibernética	8FFR20-00849-01
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 2020
Última revisión	14 de Diciembre de 2020
Indicadores de compromiso	
URL	
http://vcv-custom[.]cl/fax/office/Login.php	
IP	
[192.141.168.137]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00849-01/	
https://www.csirt.gob.cl/media/2020/12/8FFR20-00849-01.pdf	

CSIRT advierte sitio de empresa de mensajería falsa	
Alerta de seguridad cibernética	8FFR20-00850-01
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 2020
Última revisión	14 de Diciembre de 2020
Indicadores de compromiso	
URL	
http://solojoyas[.]cl/js/jquery/ui/themes/base/ui/Dhl2/Dhl/Dhl/	
IP	
[190.107.177.235]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00850-01/	
https://www.csirt.gob.cl/media/2020/12/8FFR20-00850-01.pdf	

CSIRT advierte página bancaria fraudulenta	
Alerta de seguridad cibernética	8FFR20-00851-01
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 2020
Última revisión	15 de Diciembre de 2020
Indicadores de compromiso	
URL	
https://validasanta-sms[.]online/1608053655/personas/index.asp	
IP	
[198.54.114.240]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00851-01/	
https://www.csirt.gob.cl/media/2020/12/8FFR20-00851-01.pdf	

CSIRT advierte suplantación de sitio bancario	
Alerta de seguridad cibernética	8FFR20-00852-01
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 2020
Última revisión	15 de Diciembre de 2020
Indicadores de compromiso	
URL	
https://service-santder-cl[.]info/1608061556/index.asp	
IP	
[167.71.233.97]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00852-01/	
https://www.csirt.gob.cl/media/2020/12/8FFR20-00852-01.pdf	

CSIRT informa de página de banco fraudulenta	
Alerta de seguridad cibernética	8FFR20-00853-01
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 2020
Última revisión	14 de Diciembre de 2020
Indicadores de compromiso	
URL	
https://www.superclave-sitio-seguro[.]com/1608118519/personas/index.asp	
IP	
[162.0.235.6]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00853-01/	
https://www.csirt.gob.cl/media/2020/12/8FFR20-00853-01.pdf	

CSIRT advierte sitio falso de empresa de almacenamiento en la nube	
Alerta de seguridad cibernética	8FFR20-00854-01
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 2020
Última revisión	16 de Diciembre de 2020
Indicadores de compromiso	
URL	
https://rucalafchiloe[.]cl/lok/FBG/	
IP	
[185.50.196.201]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00854-01/	
https://www.csirt.gob.cl/media/2020/12/8FFR20-00854-01.pdf	

Phishing

CSIRT informa de phishing por supuesta suspensión de cuenta	
Alerta de seguridad cibernética	8FPH20-00336-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Diciembre de 2020
Última revisión	10 de Diciembre de 2020
Indicadores de compromiso	
URL	
http://www.cetpline[.]com/Activacion/cuenta-lfgd/	
https://valpanet[.]com/r4t4tu1lxx25/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[170.239.87.68]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00336-01/	
https://www.csirt.gob.cl/media/2020/12/8FPH20-00336-01.pdf	

CSIRT advierte phishing de falso correo que superó el límite	
Alerta de seguridad cibernética	8FPH20-00337-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Diciembre de 2020
Última revisión	10 de Diciembre de 2020
Indicadores de compromiso	
URL	
https://mastermaq[.]weebly.com/	
IP	
199.34.228.53	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00337-01/	
https://www.csirt.gob.cl/media/2020/12/8FPH20-00337-01.pdf	

CSIRT advierte phishing por actualización de cuenta en sitio de streaming	
Alerta de seguridad cibernética	8FPH20-00338-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Diciembre de 2020
Última revisión	09 de Diciembre de 2020
Indicadores de compromiso	
URL	
https://www.fichetbarcelona[.]info/wp-admin/css/es/NTFlX/app/login	
IP	
[86.109.178.157]	
[185.37.228.137]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00338-01/	
https://www.csirt.gob.cl/media/2020/12/8FPH20-00338-01.pdf	

CSIRT advierte phishing por cuenta suspendida	
Alerta de seguridad cibernética	8FPH20-00339-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Diciembre de 2020
Última revisión	14 de Diciembre de 2020
Indicadores de compromiso	
URL	
http[:]//cetpline[.]com/Activacion/cuenta-ifli/	
https[:]//valpanet[.]com/3qu1n0x25x23/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[45.236.130.10]	
[186.64.117.245]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00339-01/	
https://www.csirt.gob.cl/media/2020/12/8FPH20-00339-01.pdf	

CSIRT advierte phishing de SúperClave bloqueada	
Alerta de seguridad cibernética	8FPH20-00340-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Diciembre de 2020
Última revisión	14 de Diciembre de 2020
Indicadores de compromiso	
URL	
https://bit[.]ly/3meAPIi?l=www.santander.cl	
http://www.sohbetnetyap[.]com/wp-content/cli/enviar.php?l=2135998240	
https://www.breathingforward[.]com/activacion/cuenta-qeuq/	
https://syedfoundation.org[.]uk/transa/www.santander.cl/pagina/login.asp	
IP	
[80.77.122.111]	
[186.64.117.245]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00340-01/	
https://www.csirt.gob.cl/media/2020/12/8FPH20-00340-01.pdf	

CSIRT informa phishing de cuenta temporalmente suspendida	
Alerta de seguridad cibernética	8FPH20-00341-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Diciembre de 2020
Última revisión	15 de Diciembre de 2020
Indicadores de compromiso	
URL	
http://ferreirainvestig.com[.]br/Activacion/cuenta-cdqd/	
https://www.tenews.org[.]ua/cmfchile/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[186.64.121.153]	
[45.236.130.202]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00341-01/	
https://www.csirt.gob.cl/media/2020/12/8FPH20-00341-01.pdf	

Vulnerabilidades

CSIRT comparte vulnerabilidades obtenidas de Haxx	
Alerta de seguridad cibernética	9VSA20-00334-01
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 2020
Última revisión	10 de Diciembre de 2020
CVE	
CVE-2020-8284 - CVE-2020-8285 - CVE-2020-8286	
Fabricante	
Haxx	
Productos afectados	
cURL desde la versión 4.0 hasta la 7.73.0 (incluida). cURL desde la versión 7.21.0 hasta la 7.73.0 (incluida). cURL desde la versión 7.41.0 hasta la 7.73.0 (incluida).	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00334-01/	
https://www.csirt.gob.cl/media/2020/12/9VSA20-00334-01.pdf	

CSIRT comparte mitigación obtenida de OpenSSL	
Alerta de seguridad cibernética	9VSA20-00335-01
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 2020
Última revisión	10 de Diciembre de 2020
CVE	
CVE-2020-1971	
Fabricante	
OpenSSL	
Productos afectados	
Todas las versiones 1.1.1 y 1.0.2 de OpenSSL son vulnerables, no se revisaron versiones sin soporte.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00335-01/	
https://www.csirt.gob.cl/media/2020/12/9VSA20-00335-01.pdf	

CSIRT comparte mitigaciones entregadas por Cisco	
Alerta de seguridad cibernética	9VSA20-00336-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Diciembre de 2020
Última revisión	11 de Diciembre de 2020
CVE	
Críticas CVE-2020-26085 - CVE-2020-27127 - CVE-2020-27132 CVE-2020-27133 - CVE-2020-27134 Altas CVE-2020-3512 - CVE-2020-3409 Medias CVE-2020-3419	
Fabricante	
Cisco	
Productos afectados	
Esta vulnerabilidad afecta a los dispositivos Cisco Industrial Ethernet si están ejecutando una versión vulnerable del software Cisco IOS o IOS XE y si tienen habilitada la función PROFINET. La función PROFINET está habilitada de forma predeterminada en las plataformas que la admiten.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00336-01/	
https://www.csirt.gob.cl/media/2020/12/9VSA20-00336-01.pdf	

CSIRT comparte mitigaciones obtenidas por GitLab	
Alerta de seguridad cibernética	9VSA20-00337-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Diciembre de 2020
Última revisión	16 de Diciembre de 2020
CVE	
CVE-2020-26407 - CVE-2020-26408 - CVE-2020-13357 CVE-2020-26411 - CVE-2020-26409 - CVE-2020-26413 CVE-2020-26417 - CVE-2020-26416 - CVE-2020-26415 CVE-2020-26412	
Fabricante	
GitLab	
Productos afectados	
GitLab Community Edition: Versiones 0.1.5 y de la 0.8.0 a la 13.6.1 GitLab Enterprise Edition: Versiones de la 6.2.0 a la 13.6.1	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00337-01/	

https://www.csirt.gob.cl/media/2020/12/9VSA20-00337-01.pdf

CSIRT comparte mitigaciones de Wireshark	
Alerta de seguridad cibernética	9VSA20-00338-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Diciembre de 2020
Última revisión	16 de Diciembre de 2020
CVE	
CVE-2020-28030 - CVE-2020-26575	
Fabricante	
Wireshark	
Productos afectados	
Desde la versión 3.2.0 hasta la 3.2.8.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00338-01/	
https://www.csirt.gob.cl/media/2020/12/9VSA20-00338-01.pdf	

CSIRT comparte vulnerabilidades obtenidas de Mozilla	
Alerta de seguridad cibernética	9VSA20-00339-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Diciembre de 2020
Última revisión	16 de Diciembre de 2020
CVE	
CVE-2020-16042 - CVE-2020-26971 - CVE-2020-26972 CVE-2020-26973 - CVE-2020-26974 - CVE-2020-26975 CVE-2020-26976 - CVE-2020-26977 - CVE-2020-26978 CVE-2020-26979 - CVE-2020-35111 - CVE-2020-35112 CVE-2020-35113 - CVE-2020-35114	
Fabricante	
Mozilla	
Productos afectados	
La vulnerabilidad afecta al explorador web Firefox Mozilla versiones anteriores a la 84, de Firefox ESR anteriores a la 78.6 y de Thunderbird anteriores a la 78.6.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00339-01/	
https://www.csirt.gob.cl/media/2020/12/9VSA20-00339-01.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

081b3cdf1ea46b99269d315df93fed21d47288df2139fb227ed3768b3435c139	7123697173acfb4a007517ac817c37baa4f845bd8f57c972b9a554655f8746a2
090c4f9e11431a29dcddd52948422655187024fbccd7f1c62df43d1249368d48	55cd40119050214a5b6d4c0cec5a53b45ac687f7e721909f5017c4d546868e00
0952ac64295f01b82857f1508bb39163fafe8f6ed3cc9acfb5acdebdf1e7e972	abdf5b91c52e3318ab4837fab1658c87c6dba52aacd267fdf9db67a68c597f44
0dd095b4a46b0973b095bcc02ee36c8460ce7fd936688cf9037cb1bd2482a7b0	3ecc2dc3ca4976a798f1aa3b6b050a4bec65f4cd21ad3818cd748df2cb446733
0e5cd1988af1addf8bf0de7a91268f53a28c71cccee4aa32c916adc076329efd	98b40fa7dffdf75b7d25aa8359a00d5a52c47fd0acc6e20c2ad26a734681c4fe
112f8c09f8427da46f5185113c9ab42a7eb7f4eb856daa7c63ff5ebb9a234560	110138c714087e37609b57da0143acb1c498553837302349ac8b01b06d26d90b
12885b0462e6977afc7c42d03c8e039a5df25f70b610177b8e02f6642847584b	d1a0be9963f086960034166c0f85601a720fbcf3f3d361e6102f7eb6123a4199
1be9290abb7d0f70f131ba77da664ce1d8a8c8e95097e7535c9ab6205c9f07ee	349f95f8838f5defa6bf105b34530664b52cb3d041fa7ddfd4f881d75b1b5ff5
20dacea91be5056315789204f743fd6293c3e0248b432982fde33e91d826d2c4	742386b285d1ca558bb4d0aca6b30df36b83866e36fd9d26b680cff721de0182
2538dfa787f159cf3d773d8b7c3f089378009fab4174dcbd136ff6f299db739a	8413f5b1c07582de5020575251ad37dce44d725ce0a04cf1b6ca446063f3f3e4
297c9f0e6fcbfe3d178c29bbe8da51020fce24fef21b33c2239eb983f4d7e9d2	ae84be04120bc075561e75f8becdbd693773a020f90ae0fc3693ff2b0d72f78b
2c552791b2eb73d09025a0f02827e8ca11cf5902534baec987a7f8babdf7a62b	180bed3d9b16d8da10d85078b967ea926838a4ecded1e5779d7d5306105cd0c7
2d03714006fbc19b4923d2de4718441c80bb4862c7fde2996f2bc72d48115089	bb4b4d36e73143f13e28e331cb6392007041874f7fd65c770dc74414f37f647c
2d3ea1d4f9b676e6132eee87b86981321a91e04105df6ee8fbff8c999dce19b8	6823554e87d94f940123caa646a156231e4c37a4fce1d696c25f65252e6b483a
2d81a4863eb4e3eb5cc32d13d8c2742c54ad5397b3a480159af0b2a78478ddcb	be79443c0b4eaf793c5513f47bb589a57cd734dd8467272baf612b21894cae8a
4b8b7c8ce9fbc818ce1691b84fb5bca202420b23398c64c67ee7dec8d86092f6	eece226f5fc0fb7b309f30c682f2f5616a82170998d1306d89c6d8753664d497
4d9c56d5a04e971930cf23af55f87704d3883ae725b4b3992a6f566385f4f5e5	800ae626585bcd63a5bbbb43e3047846bc792110736a273941a89c7ebcc1a4e0
4ff7894020de3130a36027e8fe49456d4d565123c2280178a89a21c8129097a3	edd079134004b9585cc1f49712b760be6b82922b9c950cff0c3b70c0df7c3802
524ef8359854ea0b7db3ee74859ead68addc643a80ca2f262b61c3884c3df1cd	0ca02b271e05470bab38ce94781f906d7a549e479670db85cbc24b82111c8533
52ecfc52692253af3694d2e6a11bb3b21af8ea05e76ab2bc9127cb391d6ca709	2335dd98b0f7c6310c2a0473eb5a2ee46bf473f960382b9d50a4972fad5597a4
5760f8e07801033ec690d78c481f9b036b847f286c9696942472eca1a863daf5	d5c990d38188b6cbf497c2cb4f1498d0ca7045b2379475ce7db3b2bdcb1b947c
592070013868e01377a6393228148f68a7da866637b28243f80f7479f5ffe270	22fe1af79a86c8514131fa8f9ae5c913101592a0f7ed9ecd3d3c18d9097691b5
5920c2d65af6603c40f9343e6f9ce3f0795f3b810467ea0572897de9e32ef0b1	4319771cc6f5370499167b30b80e76e333204fbe70428ca39492c0af19749f78
5ffe25993311b635efcf95d9d1a617348696580d79b1d1c9b8e3a68594f4eb0b	cb23bcf0d2b097cafd9ba420dfdbbd995e882ffa0f2a22c73966a7e54e55947c
70b7824cc752cdc432dc6ba1a2c820408231cf719dcb8e84ed9286c0d6c5bea3	8df34f6c5dca55e6dbc826b143f5471df7c79748e2ac9c9a141fa7c43498179c
72608b24c7a3e879a23892cba985a4af2b9965519564f58682a7d060a02377c6	729429c708e71d2fd3a5e8f1ae48df56c3967c71ca75c46254bce5fe52ba01fe
760dde4766f321bfd3bc991e78b3802e185907300439297b31784b84bc28cca9	995f2f30b23dc76600c4c54fb572dbc35230a036d76d129143c5f61a23df1e1a
862090e9b5e18026ec5027bbd02f5f516f46ec34b2dc73cde2aebf46757c4bb9	9de4d094d14083a2655427dcc8314013cf28b7116b7c7f3eadd5f3d4561daff9
876fb96ee19bf5761dfa0bc64f1131509594d37e8c77933dbd6ed1537cfc9e09	0b82357aecfede97b3cfadee8a9c8be165bcb361d2af5054aa809ddcda70f01b
88e48976bfc503ba9139d0494a48564709960a51e99fc5ad0ad5191775d1a502	72243306a41b6f1cd5a13e3097805ffdb0c6d49bcb92497d130ba7c42d521da0

8ca15f24efed9f67b10fb5cca3bd3cb5da365e5e90048e47fabb0866a42cf911	29503850c8b7ba352544c70cee1f7bb2bcf60e67aca4d3677be6c4f44ae812b7
9078a9959174b1db5ca84886d629dff6e02518d16fd4f4e0afda6affffc3d3e	1c7b7a542859113679131de1ac7797a4a65c0650811682010e990ce2eae9538b
93c336215eaa54d88b98eee5da569a9709fd351890271d591b7e9b4b1ac9011f	9de7df8b38954c9d93fa69070d28d5b587d1ede9193fbc0c0a6a565955a88fbd
945e33c4eb8e89fa874bfaf5471a3fcb0a9ca0d9d72a3581dfdef27ccc8d5a42	f469d7a84ba48d8c9a9ae5bfbfa38b708a74d330a2507a7a527d8eb32c0c40af
99ad43fdd25f8c86dd3e95c64be4545a6067dfbd503d60b4513237640b41560a	5de89393ff5a01bf9f790962c2cc5298c289ecaf99ca78611a86fa90c9d9b58b
a100076d42b558843be9617745b750519c4e75e4805a358ca282cf5bf1ae50f8	99975fa5c19cbe2b174de1f227beadd6c04256e1428bea86491f965cdbe90cd8
c0aebd735a0581eee88997334dcf4d98ec9fb188af7bed95106419e1c4ee99ee	ea9976cebb98e32374c7bc02123b185169c27232abe3578a39001451b4b27bfa
cdc5df1dcea9450ee7111f17e3a66dc903fdba4fa4adb8ec95e0b83d3e2e0c8d	81d7d4b3560d7ad69ac41afd0bf67d99a3986d9704754b11221e6a67a2630829
d1aa557c2013a91a84574b2664797fddad6ed4377b8ddc783883405b51d32405	33dcdaad80453451ab94299814bdd08766436af6f79bc1b19f7c05335e85ddc5
d9ffb075db2c72df631ead4fff17393a8bbc443961847db4ee7ac1ff6f5509c6	5491593e9f76a18a85972662a47de82ac3786b473faa05a88518ebaef57bc1e3
ef555838cd9305aa939e45414d3b7de65cd944fa3915309af7d913022e406466	6dcdd0af7032e97516308bf8f6b0d8a75f69697ac34ff9ac567716fc35192cff
f6939e07b9448b922f4f021204cf58c4587a81b286e89aa6627f00a44e3c2b44	0a9e3fa71406b6678645937c466c02d671138b2eb449419001cf16e08dc960f1
f962fd8a34ee53667338e25fbb1653dc03d77af53c5c98568d560436c8263899	784a771a6c4bebd30e298277853632f485a14867a262295fe5dfd2c4087f6e97
fdd325f347c0da52bfac266dfce0be0eb6cbaf5cb17f3cc1b34196d50b965cf5	7205dba904395dfb5f958d3a2781ed25ed9bcde885956ce34c2a0ec1b9ae55c6
52ccb3c0fdf5a051df5ba003ce61ffe915ecf257bd9d68297648ab5b086a3d0d	476ec5a648c3159681feb1040aeffc59f4913d6f1fc29f8f5a03bd04be62694d
4c91df648f693ae2debf244e2c420e33a1bc64fe7e93a52eaa0667e9a9fbd708	b48d12b7623bfed724e8d19c7d93fae540295f2490eaf3702be3d2a5a5751bc3
6d7b3f594dd9ab03414918168e22ffb656b5c247a1b9f0c87070d12b5f4a81fd	75dbeb9d3c43cf8ad17eca74dc39bd0d230731df3e37a5aa4cad4717bfd7e163
9d55d503a67cb2737b27c0ea77bda519f470fa55053c1cb981b39fce2268dc5e	4524f84146912b008015a0baf214e6f950281d45278426ff183aa4ce6690da44
2886e712b761941f8ee425aef938e646c7f402d96ae5a7bbe65dd67bd26f616f	f2143634b15c89c84f9086c891c2bd51bd03411b625bfa43ba40a16836ed8cf3
8f054ae222c2b0e317e614335ddb5e35590f6669191805e0e0c6961b92570ed7	d4f4e52c7ebf5c75e74ff3dcd32f2944e0595da63e9ee70541b83e1ccb80275c
8a5d1545a4f74c34fb41ff8ea74d35aa53d30742bac51ea30c9bf6d49c4eb59b	5e201ff705d6225abee529b228670b2f9bce7a3cf5b99a7475c40df0a511caf2
999e7a8df9428ff11ece63a95ba76bfe4b401cd476e62cc5760972307106ebf2	af1c84e4a3c0f70d7871314c884366e7de3c23afad9594ffb6e04099deacb129
c28ab91f1ba16035aa3c83299f2e6e3cc642c5fd2c6049a6d764d24342f09b24	f554c01536217162995e590ef9c085a25a3af0f2857d3a20f27979fb67b7b2e7
88a285f950e2e3cf1252b5765349b663b041f25cdc0543ac37a3c389ffd2b721	892b3f9200b6dd5cb181cda7e006da91591ff3979efb27188754c6209b28b77b
632fe1c443696ff0f67adb10012caa948046f04ceae3d3e509921e368ae89cbe	

Correos electrónicos de donde son enviados los archivos adjunto con malware

angel.vargas@dopingmaq.com.mx	Hanan@dhl.com
hr-001@asano.com.cn	amundsen02@mail-relay.msc.com
commercial@hongfashipping.com	barefootedx126@msc.com
susana.diaz@freireshipyard.com	leavingz62@msc.com
sales@vuzix.com	packersn96@msc.com
mueblescortes@intermobel.net	sales@omanht.com
remove@mypresent.ru	awhazicoo2@yahoo.com
ignominiespq19@mail-relay.msc.com	Sudheesh_Poyil@mazruiholdings.ae
betrayersdi408@mail-relay.msc.com	sale5@ankainflatable.com
styed2@mail-relay.msc.com	claudio.stella@msg.it
negligeend51@msc.com	dept3.shabbir@alriaz.com

explicitnessfxkj@mail-relay.msc.com	waves@richermoren.gq
antiquatedg605@msc.com	jmtc.import@jaipur.ae
booklxd@msc.com	sales@multiimpact.com.my
validateowc@msc.com	purchasing@iconjamaica.com
lingostp973@mail-relay.msc.com	thaodud5pr@hotmail.com
foibleym605@mail-relay.msc.com	nicola5dswamp@hotmail.com
succincter94@mail-relay.msc.com	kataraquejj@hotmail.com
dionysiand01@mail-relay.msc.com	blainebr07l@hotmail.com
doram5@msc.com	meridith3sdom@hotmail.com
legitimatelyxg7@msc.com	parisru0s@hotmail.com
gruntedvh@msc.com	flickcolwadman@hotmail.com
fluffsvlr@msc.com	cmaisonmf5@hotmail.com
prophylaxiswz08@msc.com	mickqcrgrappe@hotmail.com
gangrenedw541@mail-relay.msc.com	gregs7zynu@hotmail.com
neighbt5@msc.com	irinauhsegur@hotmail.com
dewaynerzql@msc.com	lailayrayl5j@hotmail.com
aesculapiusfi1@mail-relay.msc.com	latdsmisch@hotmail.com
nowadayskts1090@msc.com	anniekhamocek@hotmail.com
praisegr5@mail-relay.msc.com	mafillerxs6x@hotmail.com
foulesty9@msc.com	jennine1kalosb@hotmail.com
radioisotopesycq@msc.com	mickict5sw@hotmail.com
questionablyb@msc.com	holleyb4ihbarut@hotmail.com
annul132@msc.com	marietterwzg@hotmail.com
alcove323@mail-relay.msc.com	jewelfoots1u@hotmail.com
xdisarrangesvh@mail-relay.msc.com	de89cordon@hotmail.com
plectrumsqg94@msc.com	trulaballamwg@hotmail.com
celloh58@mail-relay.msc.com	joyaquipvvm@hotmail.com
frillsul@msc.com	arniedwe@hotmail.com
sharfa.rasheed@villa.com.mv	stellak8artice@hotmail.com
Siti.Noorraishah@dhl.com	calvinmjjs@hotmail.com
marycafm6c@hotmail.com	hyepfv0sb@hotmail.com
ibrserazhudin552@outlook.com	devorabav7@hotmail.com
ffawntg2@hotmail.com	omar@primeglobaldubai.com
egunn7uc4@hotmail.com	mjjimenez@novasoft.es
yyadzal@hotmail.com	roberto.c@copttraba.com
vebmakhir350@outlook.com	wecare.ec@dhl.com
pa4e5hilton@hotmail.com	Aboutmile@bremileintl.ga
elsabannerthh4@hotmail.com	jessica@vortexfield.eu

snowamhrnn@hotmail.com	service@lhexagoneso.com
melodyams7@hotmail.com	ivilopeZ@Orange.es
freyjacdnncage@hotmail.com	sales@jetfleetmgmt.com
scarlettqqhap@hotmail.com	sales6@nomila.com
lcagelxf@hotmail.com	sales@esteelsuppliers.com
zoezuha@hotmail.com	invex@retemail.es
artatrevwfy@hotmail.com	maigranada25@yahoo.fr
sjarvisys2f@hotmail.com	marni@pt-dju.com
gabriellaszgp@hotmail.com	harikrishna@vijayadiagnostic.in
anyacrdeo@hotmail.com	Aboutmile@bremileintl.ga
lavqmgunn@hotmail.com	info@semshred.com
katherine5mjpen@hotmail.com	GBVACCARO@voegol.com.br
jatatumqf9@hotmail.com	rodolfo.torrillo@superdyop.com.ar
cloverz40gu@hotmail.com	Noreply_Nalco_SOA@ecolab.com
floralizg1704@hotmail.com	e_dehghani@mehrarad.ir
youlandal3o@hotmail.com	trf.1850458928.2512675.9@informationservcies.hbsc.co.tk
tammysepux@hotmail.com	webmaster@ft.dk
taml9twb@hotmail.com	grutze2@yahoo.es
romanaalgerp63@hotmail.com	edwin@andalanfluids.com
mprintynz1g@hotmail.com	0000718103@pccity.pccity.es
arianecrainenm@hotmail.com	purchasing05@willing.com
nylaamualgeo@hotmail.com	19933o@dejazzd.net
hayleyoedube@hotmail.com	sales1@mikronix-gauges.com
lou9lzysett@hotmail.com	info@minlmax.com
ardeliafcca@hotmail.com	

Direcciones IP de servidor SMTP donde es enviado el correo malicioso

40.92.42.55	40.92.255.42	93.63.61.132
40.92.9.34	40.92.18.32	213.254.6.99
40.92.254.62	40.92.41.91	93.42.7.100
40.92.51.52	40.92.41.57	95.236.39.161
40.92.253.53	40.92.41.25	185.158.38.29
40.92.51.30	40.92.74.43	91.81.73.226
40.92.255.63	40.92.255.50	94.176.30.71
40.92.253.34	45.137.22.51	98.137.69.84
40.92.255.12	84.38.132.107	98.137.65.84
40.92.253.77	40.92.254.63	95.216.63.47
40.92.254.58	40.92.22.62	98.137.65.148

40.92.66.109	79.110.52.195	98.137.65.31
40.92.255.46	37.120.206.112	206.189.118.13
40.92.40.65	45.137.22.56	5.8.93.86
40.92.254.59	62.36.20.208	84.38.132.53
40.92.10.51	23.83.133.171	45.137.22.125
40.92.75.61	51.79.157.206	40.92.74.29
40.92.16.108	193.56.28.122	40.92.10.56
40.92.255.25	98.137.64.146	40.92.3.16
40.92.254.83	98.137.65.32	40.92.47.46
40.92.253.50	98.137.66.147	40.92.71.21
40.92.41.45	98.137.65.206	40.92.3.30
190.210.215.185	79.110.52.195	40.92.19.64
151.106.27.217	23.108.57.65	40.92.51.94
88.218.16.196	40.107.80.57	103.253.68.172
192.3.3.143	213.236.3.9	77.93.235.250
85.33.179.184	210.236.45.1	122.173.70.104
40.92.253.58	52.162.219.104	40.92.4.62
40.92.67.83	107.150.18.142	40.92.255.62
40.92.255.98	198.23.221.43	40.92.255.82
40.92.254.108	204.44.127.166	40.92.42.75
40.92.254.22	142.11.194.202	40.92.4.108
40.92.253.93	209.198.42.103	40.92.253.43
40.92.21.28	40.92.255.95	40.92.42.81
40.92.71.73	40.92.20.108	

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) para suplantar a los remitentes originales para depositar correos con contenido o enlaces maliciosos en las bandejas de entrada de sus potenciales víctimas.

IP
5.188.206.203
5.188.206.202
114.106.172.195
110.243.25.141

Actualidad

Ciberconsejos para crear contraseñas seguras

Para cuidar nuestros datos e información en internet es importante contar con contraseñas seguras en los distintos sitios donde te registras, para así evitar, por ejemplo, el robo de tu información o que suplanten tu identidad. El CSIRT comparte contigo algunos ciberconsejos de cómo proteger tus datos y cómo crear una contraseña robusta.

Ver más: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-crear-contrasenas-seguras/

Investigación

Consejos y buenas prácticas en la administración de Firewall

Para este número 24 de Análisis de Amenazas Cibernéticas, el CSIRT de Gobierno contó con la ayuda de Jennifer Nilo Andrade —especialista senior de operación en Entel y parte de Hackada, comunidad de mujeres en ciberseguridad—, quien elaboró el presente informe donde explica los detalles de un firewall o cortafuegos y aconseja cómo administrarlos de forma de maximizar la ciberseguridad de una red.

Así, a lo largo de este documento la autora explica los distintos tipos de firewall existentes, además de varios conceptos para ayudar con la administración de los equipos de seguridad. Nilo pone especial atención en el modelo de zero trust (confianza cero) que consiste tratar a todo usuario o equipo como si fuera externo y debiera pedir autorización explícita cada vez que desee acceder a un distinto nivel de seguridad dentro de una red, por lo que su implementación permite a los administradores de los sistemas ser más granulares y minuciosos al momento de otorgar permisos, y así dificultar la creación de brechas de seguridad que permitan la entrada a distintas amenazas, ya sea de origen interno o externo.

Nilo presenta los errores más comunes en la administración de firewalls, ejemplificando con casos y haciendo recomendaciones sobre la forma correcta de administrar la seguridad de los sistemas a través de la adopción de buenas prácticas por parte de usuarios y administradores, para mejorar la seguridad de un sistema incluso cuando no sea posible adoptar un modelo de zero trust como tal.

Ver más: https://www.csirt.gob.cl/reportes/consejos-y-buenas-practicas-en-la-administracion-del-firewall/

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 públicos 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 (en el sitio web https://www.csirt.gob.cl y/o al teléfono +(562) 2486 3850) siempre que hayan aportado con información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución del mismo.

- Robert Arancibia
- Juan Pablo Berríos
- Ricardo Monreal
- Claudio Valderrama
- Nicolás Pizarro

CSIRT Gobierno de Chile