08-10-2020 | Año 2 | N°66

Boletín de Seguridad Cibernética

Semana del 01 al 07 de Octubre de 2020

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

División de Redes y Seguridad Informática.
Gobierno de Chile

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

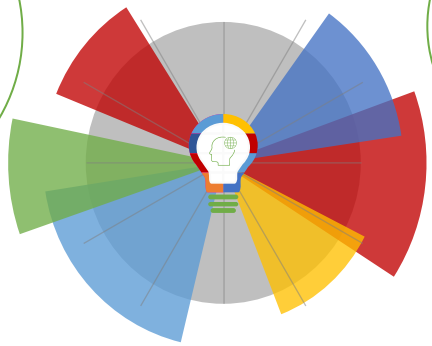
Resumen de la semana en cifras

Body Hash

52

Sha 256

Asociadas a múltiples campañas de phishing son archivos que contienen malware



Se advirtieron

28

URLs

Asociadas a sitios fraudulentos y múltiples campañas de phishing y malware

IPs

49

Informadas

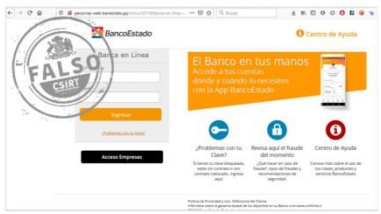
Listado de IPs advertidas en múltiples campañas de phishing y de malware.

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

Contenido

Sitios fraudulentos

Imagen del sitio



CSIRT advierte de sitio de suplantación bancario	
Alerta de seguridad cibernética	8FFR20-00765-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Octubre de 2020
Última revisión	01 de Octubre de 2020
Indicadores de compromiso	
URL	
personas-web-banestado[.]gq	
IP	
101[.]99[.]90[.]35	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00765-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00765-01.pdf	

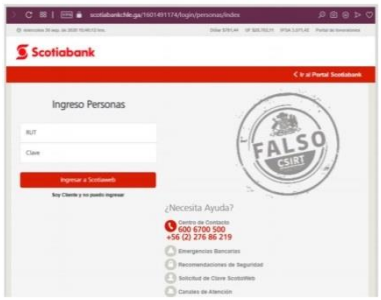
Imagen del sitio

CSIRT informa de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00766-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Octubre de 2020
Última revisión	01 de Octubre de 2020
Indicadores de compromiso	
URL	
portal-web-banestado-cl[.]cf	
IP	
101[.]99[.]90[.]35	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00766-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00766-01.pdf	

Imagen del sitio

CSIRT advierte de portal que suplanta web bancaria	
Alerta de seguridad cibernética	8FFR20-00767-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Octubre de 2020
Última revisión	01 de Octubre de 2020
Indicadores de compromiso	
URL	
www-consulta-banestado-chile[.]ga	
IP	
101[.]99[.]90[.]35	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00767-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00767-01.pdf	

Imagen del sitio

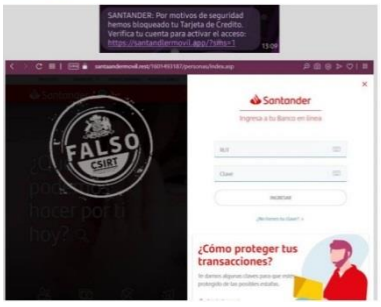


CSIRT advierte de sitio que suplanta a web de banco	
Alerta de seguridad cibernética	8FFR20-00768-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Octubre de 2020
Última revisión	01 de Octubre de 2020
Indicadores de compromiso	
URL	
scotiabankchle[.]ga	
IP	
178[.]159[.]36[.]141	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00768-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00768-01.pdf	

Imagen del sitio

CSIRT advierte de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00769-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Octubre de 2020
Última revisión	01 de Octubre de 2020
Indicadores de compromiso	
URL	
santandler-personas-cl[.]manikganjbigbazar[.]com	
IP	
66[.]206[.]9[.]194	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00769-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00769-01.pdf	

Imagen del sitio

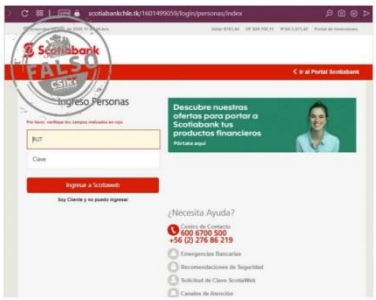


CSIRT informa sobre sitio de suplantación bancario	
Alerta de seguridad cibernética	8FFR20-00770-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Octubre de 2020
Última revisión	01 de Octubre de 2020
Indicadores de compromiso	
URL	
hxxps://santandlermovil[.]app/?sms=1	
santaandermovil[.]rest	
IP	
68[.]65[.]123[.]56	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00770-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00770-01.pdf	

Imagen del sitio

CSIRT advierte de portal que suplanta web bancaria	
Alerta de seguridad cibernética	8FFR20-00771-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Octubre de 2020
Última revisión	01 de Octubre de 2020
Indicadores de compromiso	
URL	
bancochile-actualizacion-dispositivos[.]cf	
IP	
178[.]159[.]36[.]141	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00771-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00771-01.pdf	

Imagen del sitio

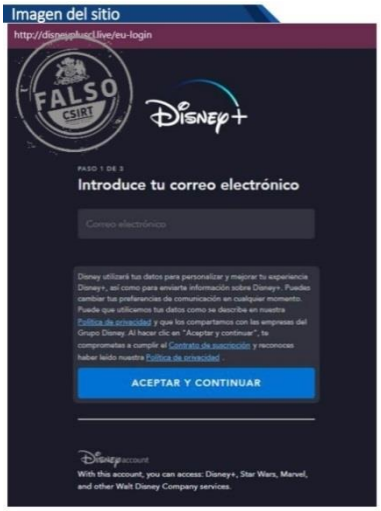


CSIRT advierte de web de suplantación bancario	
Alerta de seguridad cibernética	8FFR20-00772-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Octubre de 2020
Última revisión	01 de Octubre de 2020
Indicadores de compromiso	
URL	
scotiabankchle[.]tk	
IP	
178[.]159[.]36[.]141	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00772-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00772-01.pdf	

CSIRT advierte de sitio de suplantación bancario	
Alerta de seguridad cibernética	8FFR20-00773-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Octubre de 2020
Última revisión	02 de Octubre de 2020
Indicadores de compromiso	
URL	
bancestadochile[.]ddns[.]net	
IP	
217[.]195[.]153[.]128	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00773-01/	
https://www.csirt.gob.cl/media/2020/10/8FFR20-00773-01.pdf	

CSIRT advierte de sitio que suplanta una web bancaria	
Alerta de seguridad cibernética	8FFR20-00774-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Octubre de 2020
Última revisión	02 de Octubre de 2020
Indicadores de compromiso	
URL	
saantandeesms-security[.]website	
IP	
162[.]0[.]232[.]231	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00774-01/	
https://www.csirt.gob.cl/media/2020/10/8FFR20-00774-01.pdf	

Imagen del sitio



CSIRT advierte de portal que suplanta a web de streaming	
Alerta de seguridad cibernética	8FFR20-00775-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Octubre de 2020
Última revisión	02 de Octubre de 2020
Indicadores de compromiso	
URL	
disneypluscl[.]live	
IP	
185[.]186[.]245[.]22	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00775-01/	
https://www.csirt.gob.cl/media/2020/10/8FFR20-00775-01.pdf	

Imagen del sitio

CSIRT informa de portal de suplantación bancaria	
Alerta de seguridad cibernética	8FFR20-00776-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Octubre de 2020
Última revisión	02 de Octubre de 2020
Indicadores de compromiso	
URL	
www-bancoestado-cl[.]dreampleasuretours[.]net	
IP	
98[.]142[.]221[.]42	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00776-01/	
https://www.csirt.gob.cl/media/2020/10/8FFR20-00776-01.pdf	

Imagen del sitio

CSIRT advierte de sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00777-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Octubre de 2020
Última revisión	02 de Octubre de 2020
Indicadores de compromiso	
URL	
netflix[.]mr-19[.]com	
IP	
108[.]177[.]111[.]121	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00777-01/	
https://www.csirt.gob.cl/media/2020/10/8FFR20-00777-01.pdf	

Imagen del sitio

CSIRT advierte de web que suplanta a sitio bancario	
Alerta de seguridad cibernética	8FFR20-00778-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Octubre de 2020
Última revisión	03 de Octubre de 2020
Indicadores de compromiso	
URL	
bancaponinternet[.]miestadocrediticio-cl[.]com	
IP	
68[.]65[.]123[.]56	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00778-01/	
https://www.csirt.gob.cl/media/2020/10/8FFR20-00778-01.pdf	

Imagen del sitio

CSIRT informa de portal de suplantación de banco	
Alerta de seguridad cibernética	8FFR20-00779-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Octubre de 2020
Última revisión	03 de Octubre de 2020
Indicadores de compromiso	
URL	
www-bancoestado[.]cl[.]myworkspace[.]ga	
IP	
98[.]142[.]221[.]42	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00779-01/	
https://www.csirt.gob.cl/media/2020/10/8FFR20-00779-01.pdf	

Imagen del sitio

CSIRT advierte de web de suplantación de banco	
Alerta de seguridad cibernética	8FFR20-00780-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Octubre de 2020
Última revisión	03 de Octubre de 2020
Indicadores de compromiso	
URL	
bci-accesos-cl[.]xyz/personas	
IP	
188[.]227[.]86[.]115	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00780-01/	
https://www.csirt.gob.cl/media/2020/10/8FFR20-00780-01.pdf	

Imagen del sitio

CSIRT advierte de portal de suplantación bancario	
Alerta de seguridad cibernética	8FFR20-00781-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Octubre de 2020
Última revisión	03 de Octubre de 2020
Indicadores de compromiso	
URL	
bancascotiabank[.]cl/login_personas[.]html	
IP	
190[.]107[.]177[.]36	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00781-01/	
https://www.csirt.gob.cl/media/2020/10/8FFR20-00781-01.pdf	

Imagen del sitio

CSIRT advierte de sitio que suplanta web de banco	
Alerta de seguridad cibernética	8FFR20-00782-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Octubre de 2020
Última revisión	03 de Octubre de 2020
Indicadores de compromiso	
URL	
www-bancoestado-cl[.]digitalmktplus[.]com[.]br	
IP	
98[.]142[.]221[.]42	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00782-01/	
https://www.csirt.gob.cl/media/2020/10/8FFR20-00782-01.pdf	

Imagen del sitio

CSIRT advierte sitio de streaming falso	
Alerta de seguridad cibernética	8FFR20-00750-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Octubre de 2020
Última revisión	06 de Octubre de 2020
Indicadores de compromiso	
URL	
unholdnetflix[.]com	
IP	
35[.]214[.]168[.]224	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00783-01/	
https://www.csirt.gob.cl/media/2020/10/8FFR20-00783-01.pdf	

Imagen del sitio

CSIRT informa página fraudulenta bancaria	
Alerta de seguridad cibernética	8FFR20-00751-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Octubre de 2020
Última revisión	06 de Octubre de 2020
Indicadores de compromiso	
URL	
scotiabankchle-info[.]ml	
IP	
154[.]16[.]173[.]147	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00784-01/	
https://www.csirt.gob.cl/media/2020/10/8FFR20-00784-01.pdf	

Imagen del sitio

CSIRT advierte de portal de suplantación bancario	
Alerta de seguridad cibernética	8FFR20-00785-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Octubre de 2020
Última revisión	07 de Octubre de 2020
Indicadores de compromiso	
URL	
banceoestadochile[.]ddns[.]net	
IP	
45[.]155[.]37[.]10	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00785-01/	
https://www.csirt.gob.cl/media/2020/10/8FFR20-00785-01.pdf	

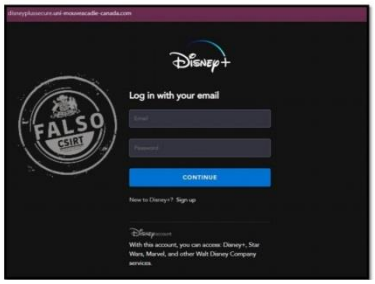
Imagen del sitio

CSIRT informa sobre sitio de suplantación de web de banco	
Alerta de seguridad cibernética	8FFR20-00786-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Octubre de 2020
Última revisión	07 de Octubre de 2020
Indicadores de compromiso	
URL	
bancestadodchile-cl[.]ddns[.]net	
IP	
45[.]155[.]37[.]10	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00786-01/	
https://www.csirt.gob.cl/media/2020/10/8FFR20-00786-01.pdf	

Imagen del sitio

CSIRT advierte de sitio de suplantación bancaria	
Alerta de seguridad cibernética	8FFR20-00787-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Octubre de 2020
Última revisión	07 de Octubre de 2020
Indicadores de compromiso	
URL	
hxxps://santande-r-movil[.]app/?sms=1	
santande-r-movil[.]link	
IP	
68[.]65[.]123[.]56	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00787-01/	
https://www.csirt.gob.cl/media/2020/10/8FFR20-00787-01.pdf	

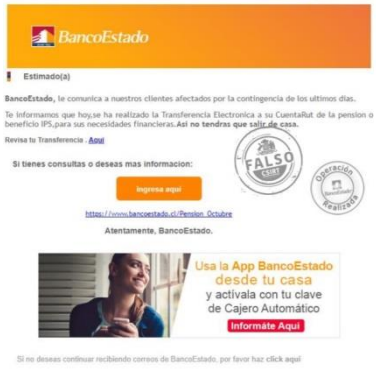
Imagen del sitio



CSIRT advierte de portal de suplantación de sitio de streaming	
Alerta de seguridad cibernética	8FFR20-00788-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Octubre de 2020
Última revisión	07 de Octubre de 2020
Indicadores de compromiso	
URL	
disneyplussecure[.]uni-mouveacadie-canada[.]com	
IP	
146[.]0[.]76[.]81	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00788-01/	
https://www.csirt.gob.cl/media/2020/10/8FFR20-00788-01.pdf	

Phishing

Imagen del mensaje



CSIRT informa phishing con falsa transferencia bancaria	
Alerta de seguridad cibernética	8FPH20-00311-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Octubre de 2020
Última revisión	07 de Octubre de 2020
Indicadores de compromiso	
URL	
hxxp://fhbhairnbeauty.com[.]au/wp-includes/js/enviar.php?l=945430361	
hxxp://webinar.vouchpro[.]in/www.bancoestado.cl/	
IP	
[193.227.5.25]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00311-01/	
https://www.csirt.gob.cl/media/2020/10/8FPH20-00311-01.pdf	

Imagen del mensaje

CSIRT advierte phishing de supuesta cuenta suspendida	
Alerta de seguridad cibernética	8FPH20-00310-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Octubre de 2020
Última revisión	07 de Octubre de 2020
Indicadores de compromiso	
URL	
https://tomatobank-dev.yapp[.]li/registerr/	
https://street.todomodaa.com/login/?id=TnJSQzFBMG1Ea2huT29zM3ZJa3lTUDBwQnVSZDBXRlpjVzNVdzFycEs0eG0wTGJqeEc=	
IP	
98.142.221.133	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00312-01/	
https://www.csirt.gob.cl/media/2020/10/8FPH20-00312-01.pdf	

Indicadores de Compromisos

Se comparte a continuación el listado de IPs que fueron detectadas durante la pasada semana por el Equipo del CSIRT intentando ejecutar escaneaos puertos, ataques de denegación de servicios o tratando de infectar con códigos maliciosos, entre otros ataques, para el conocimiento de la comunidad.
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 reportados (se recomienda bloquear)

05bdf1741db77795ab66ba0a32a02ee8b28dd5f31bcf4d27c7e06ba17ee748ca	d87ccceefffcf29b4acd58d73b786e8d15c052d61aa1fc5523d93b5b900cd5941
18de75f79cac64d283e6e175419bc19dc929ee104969c535a8979a036aa4c318	d98caa065accb367a0183450b1cd04eceb9b6bb6e998b436380ba6545fe9dcea
1a9c7d9da3cd0d83b20d0a627f02507c6b0f5ce5a283bdc92ec83186df4173be	e01fdae3d2db9fc1e5b5d456e0ce929a7a2b5631d267cbb908dd72d84fcb04d0
2f1d0226cd0085a97629ba3eacadc3fc5c70231bff78a41f6dfb574353451d9c	ea0a6f7187a27e0a7b61c2263925e116530df8dfcd4f3d1c0a61caf64faa51c6
35073f104c76640759c890c252c3537f0a523fc88e1815db28a7dd01fa4b5211	ef6ecd78893ea4323725b4918035fbc8aa255fe6565f152a12b03272f4fc2152
42b428a3693896899501a83f0c3fe3282be45101e640474f03d27fe15b06ce23	f6f3dcc2015caa0a9a11bf8106778f74f937b6d0643fccbaf05a8d94d4e7a67f
43becee6bd1d68fe76079ffdca0daff93003664a7c1428880045a171c69e8208	ff6b7c52f3b700f8c61f16fc11a192630ecfa7f39273b809682573b1ada2e497
47146f8d8b46a395adabd4c961732aa28c28b08776d1a0e91a71b66da0eb767b	27639748702e6247fa78b4ac51033308a8a975c883ddc62cb9ad972bb93a338f
47279865cf49798bddde8288d927890cc389cd80ffdab912a3db6802495c7e8f	47884ca1a17794d493809c9644958d7724130a9acaf925cc022c213238a6613c
5723816fec8f9c48c2600b941206787a633a09e066e39f73eb8ecd0f55f2fe7d	53285bf2aff7155aaf4d28de40e67449f704eb1233bfc3fff6af913c92fe7b88
57270ee47ca234d75c97bf67c5e665c182b147d0af0de427fa9b7201a4e8fa47	53e480ae08a501cf7f275325ddf80486264b6da9bb98a1dde66bd7337854879e
578fbf8d7827d5783958f3574c6710f1062061ef3c81a79ba5bec8609a290fe9	627fc5962ae3a8ed778210a760d3b791b2e5602dcb94f6085bbe544656c53148
5ad634b81d20399114ae02f7586e95f27ac1c82d2cd6fe91943b351ded13d0ea	6840c6aeb9c9cf65a73ff7e39b17318ab4f77f08b9078c4bc1c18ae29de964cd
5adf9414286aaf4b34086f8c50a64e9831082a71ed4e271f87c90ff295ba6b1e	728258695a9707f3c000559ec4b3ceddfc2452dbc0b6ed984286a098d3f2662c
69c39e7554e620e21619b5a851b40009a00d7693245cef0d081c373697d240d0	75def422d0621c915140b20a8554722c137802521402c690c227242cfc5d7ded
8361360346ef3f4a6e6cd8f0e0e3d5a31da21d88883cf3c20dce401384330097	86e0a3810bbcf936f0db47bdee5f01362d0cfa1bee44697bcad02eb9582a574a
9a48c0fb67377f42a590e2e6fd43b5eae5eebea960850954c59cf9471f5cb6b0	92224c3241716a0581e2ccc6da06e6a131622d47ce47a6c0c871a9a0b210dc2c
a2ab266f3224c6cc6403b5bb6f89ce0d537f426973008abea16ae918db0758de	945db9afb877ebc2eddf0f62cf69be7a05508e8bf3bab70ba2f8c0f54b9e4b63
ab79e953e2528491eb420b6bd7c9fe80f1252ece0da70edf2295ae4a665b8fbc	995a7eb3c2f072a0a9ce21155d288ba08e86f0dbc7df70e1e48fc9cb951e3081
ac3da9790f61c14af34276a149b0f37c7b41a3624dc439b039bd18d358fb580a	bcc4a6e6a1f8792a99b8b91920f4b2e628ffd11c47298927fe4a8ffd778c346b
b5c9a44a1c1e7cd771088b3fe0e2a732139e6efadfcf02efd068074c29a23fd2	c60ab85d4915d451570e355916443fdf1e567ad7917fc6cc88dfa5a58dd3410c
b5fc56851f5968ae88851c39e4ed27d8a36335c87fd351010af90a3935fd8d01	cbfa75c9ccecb2e6456741133e99150aee082d62e572463cd77f7a9cde00e047
c7ab3640ce1eec5e3e1fb4588bdfba7065d1471a04187ab0f6fd9b55669a21f7	da7d20b5be05e787fd87068fc8f2b7ffea8e06f79827eb376bbf0407eb9b6505
c86c0ddeb5a64eae729ee5d9cc9fac37354babc3610e4adbf519a086d99d3fc6	daf910305f9777ad7f52b0834e9b4520c428782501d50cc7d2533419ac77ac65
cd3e04eba2b0dd226ba39cad8947c7c4ed58bcaf9e6f4f4eee384dc27b22d779	dca160ca7777f27f7f278ed41853b88a36629d0c2289d6f63b55051a1a229736
d08e4db40506f9ec4d76d8bd321fca200b30157ccaef27af80a7568cb5a0d4dd	f167ba70e0001c7b6666fb49ee581ec02547908fc2048df50a9fa5ae5a22b1eb

Archivos reportados (se recomienda mantener en monitoreo)

103.109.37.111	45.137.22.49
156.96.46.26	45.95.169.122
159.89.233.101	5.8.93.187
185.222.57.162	62.12.115.74
185.222.57.181	88.218.16.126
185.222.57.71	194.31.141.130
185.222.58.111	180.214.238.214
185.254.204.24	96.9.226.52
188.166.89.61	23.106.160.116
191.96.185.245	180.214.238.214
198.55.113.239	104.161.77.84
207.154.254.92	88.218.16.196
37.49.225.236	37.49.225.234
45.137.22.56	

Correo electrónico (Se recomienda mantener monitoreo)

faraz.khawaja@redachem.com
kenjoe@choudharyexports.com
sales@carmens.it
faraz.khawaja@redachem.com
farhan@gstrapinuse.com
omegra.sg.operations@fksgroup.com
hchartering@roxanashipping.com
jkhan@drillservint.com
issasia.enquiries@iss-shipping.com
agency@nortrans.com
supportdesk@cssdubai.com
201@marsans.es
mtunzi.mtembu@oldendorff.com
neha.y@triton-intl.com
xasapi@auto-deal.gr
sales@rdagloballogistics.com

Investigación

Seguridad Digital para PYMES

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, publicó la 18° edición de su publicación sobre amenazas cibernéticas. Carlos Montoya, autor invitado en esta oportunidad (Fundación Whilolab y Universidad Mayor), comparte con nosotros la base técnica para la implementación de un sistema de "ciberdefensa para las PYMES", utilizando herramientas open source, el que debe sostenerse necesariamente en un estrategia general de protección. Este artículo tiene como finalidad servir de guía para el uso integrado de siete herramientas, partiendo de la base de mínima para implementar esta arquitectura.

Ver más: https://www.csirt.gob.cl/reportes/an2-2020-18/

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.

- Joaquín Morales
- Lorena Brun
- Cristián Bravo

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.10.09 18:40:25 -03'00'