CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

21-01-2021 | Año 3 | N°81

Boletín de Seguridad Cibernética

Semana del 14 al 20 de Enero de 2021

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

68

Sha 256

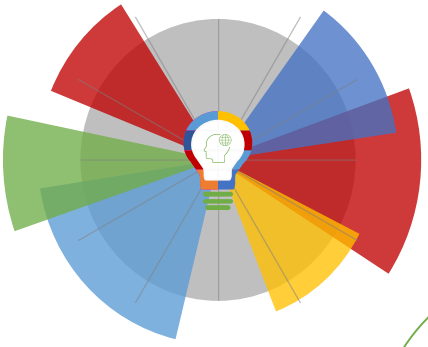
Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron

7

URLs

Asociadas a sitios fraudulentos y campañas de phishing



Parches

92

para vulnerabilidades

Las mitigaciones son útiles para productos Cisco, Red Hat, Apache y Laravel.

IPs

66

Informadas

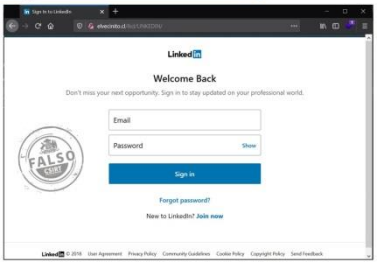
Listado de IPs advertidas en múltiples campañas de phishing y de malware.

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

Contenido

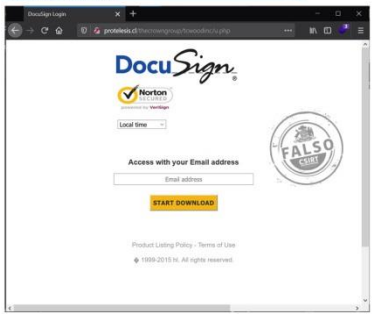
Sitios fraudulentos

Imagen del sitio



CSIRT advierte sitio de red social fraudulento	
Alerta de seguridad cibernética	8FFR21-00874-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Enero de 2021
Última revisión	15 de Enero de 2021
Indicadores de compromiso	
URL	
http[:]//elvecinito[.]cl/lkd/LINKEDIN/	
IP	
162[.]241.2.177	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00874-01/	
https://www.csirt.gob.cl/media/2021/01/8FFR21-00874-01.pdf	

Imagen del sitio



CSIRT informa portal falso de plataforma de firma electrónica	
Alerta de seguridad cibernética	8FFR21-00875-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Enero de 2021
Última revisión	18 de Enero de 2021
Indicadores de compromiso	
URL	
http[:]//protelesis[.]cl/thecrowngroup/tcwoodinc/u.php	
IP	
186[.]64.116.220	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00875-01/	
https://www.csirt.gob.cl/media/2021/01/8FFR21-00875-01.pdf	

Phishing

Imagen del mensaje

CSIRT informa phishing de SúperClave bloqueada	
Alerta de seguridad cibernética	8FPH21-00353-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Enero de 2021
Última revisión	18 de Enero de 2021
Indicadores de compromiso	
URL	
https[:]//santander-persona-cl.decoracaos[.]com/1610972250/index.asp	
IP	
[92.223.65.46]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00353-01/	
https://www.csirt.gob.cl/media/2021/01/8FPH21-00353-01.pdf	

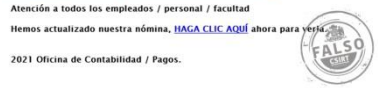
Imagen del mensaje

CSIRT advierte phishing de correo electrónico con almacenamiento completo	
Alerta de seguridad cibernética	8FPH21-00354-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Enero de 2021
Última revisión	18 de Enero de 2021
Indicadores de compromiso	
URL	
https[:]//xn--administractincorreo227-ijc[.]weebly.com/	
IP	
[92.223.65.46]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00354-01/	
https://www.csirt.gob.cl/media/2021/01/8FPH21-00354-01.pdf	

Imagen del mensaje

CSIRT informa phishing de SúperClave bloqueada	
Alerta de seguridad cibernética	8FPH21-00355-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Enero de 2021
Última revisión	18 de Enero de 2021
Indicadores de compromiso	
URL	
https[:]//www.santaandercl[.]com/1610975926/index.asp	
IP	
[103.248.146.11]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00355-01/	
https://www.csirt.gob.cl/media/2021/01/8FPH21-00355-01.pdf	

Imagen del mensaje



CSIRT advierte phishing con nómina de personal	
Alerta de seguridad cibernética	8FPH21-00356-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Enero de 2021
Última revisión	18 de Enero de 2021
Indicadores de compromiso	
URL	
http[:]//site-6nqqpbj5.websiteserver2[.]com/	
IP	
[85.132.27.124]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00356-01/	
https://www.csirt.gob.cl/media/2021/01/8FPH21-00356-01.pdf	

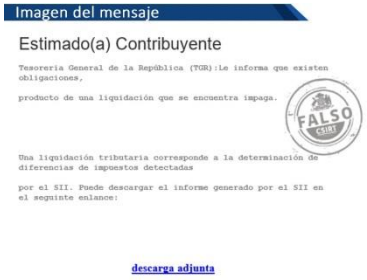
CSIRT informa phishing de Súper Clave no asignada	
Alerta de seguridad cibernética	8FPH21-00357-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de Enero de 2021
Última revisión	19 de Enero de 2021
Indicadores de compromiso	
URL	
https://apex-financials[.]net/1611082149/index.asp	
IP	
[136.243.107.47]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00357-01/	
https://www.csirt.gob.cl/media/2021/01/8FPH21-00357-01-1.pdf	

Malware

CSIRT advierte campaña malware con supuesto recibo de compra	
Alerta de seguridad cibernética	2CMV21-00131-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de Enero de 2021
Última revisión	19 de Enero de 2021
Indicadores de compromiso	
SHA256	
DF2A605BDC1D3B7107267BCBAE998B3EC1EBA7C8CA2347286FA733B22C418397	
DB40B329C1ECEA2045D4E2BC27FE712B52BBFC1D51FF1B55DCD3C8BB72258710	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv21-0031-01/	
https://www.csirt.gob.cl/media/2021/01/2CMV21-00131-01-1.pdf	

CSIRT informa campaña de malware con documentos para envío	
Alerta de seguridad cibernética	2CMV21-00132-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de Enero de 2021
Última revisión	19 de Enero de 2021
Indicadores de compromiso	
SHA256	
EF010AB0B64D78722402FF110720418C7AC4DE280EB1F75B2B93353FE34B4986	
E0FA6C966F07E112CF5C5E78A8D421ABA10D7A05E0E3A7F352BE03E0AD5389B1	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv21-00132-01/	
https://www.csirt.gob.cl/media/2021/01/2CMV21-00132-01.pdf	

CSIRT advierte correo con malware con precio de productos solicitados	
Alerta de seguridad cibernética	2CMV21-00133-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de Enero de 2021
Última revisión	19 de Enero de 2021
Indicadores de compromiso	
SHA256	
C069320CF1B5C2D0DD66A40F85E2A84FD4A2E07EB37D9684DF6C8AEC4DAD34B	
1F05B369246B2867A66ABA3CACD9DA9C2F29C03ADC4D45883C91054C35AC3345	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv21-00133-01/	
https://www.csirt.gob.cl/media/2021/01/2CMV21-00133-01.pdf	



CSIRT advierte correo con malware con falsas diferencias de impuestos	
Alerta de seguridad cibernética	2CMV21-00134-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de Enero de 2021
Última revisión	19 de Enero de 2021
Indicadores de compromiso	
SHA256	
73971DEF779F56A49EC351448AD503CDE9D5EE66B8F545CE2C173B9538F77730	
CEAFE328D30E20E8F5D10F5FBDDA20BCE8D6FCECF6C01769E1986728C6CBDA4A	
55B73B260F31C2E2A466D99804FEBF5973D29C93F3A71CE71347B1523AA98F12	
500F9E4F5CDEB6F49A8EE8FA0BF8F52A819AA961CDE619FD84311B7D269FC527	
3CF21F31C5281600CA70D4C87F4F829F0011C6740084D26C3665D2729B092DA2	
640D680A6DA84E0208D1C3D042CAFB728137960A3157C535A5C16AC5A0DA1F0	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv21-00134-01/	
https://www.csirt.gob.cl/media/2021/01/2CMV21-00133-01.pdf	

Vulnerabilidades

CSIRT comparte vulnerabilidades obtenidas de Cisco	
Alerta de seguridad cibernética	9VSA21-00364-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Enero de 2021
Última revisión	14 de Enero de 2021

CVE

CVE-2021-1144	CVE-2021-1179	CVE-2021-1201
CVE-2021-1146	CVE-2021-1180	CVE-2021-1202
CVE-2021-1159	CVE-2021-1181	CVE-2021-1203
CVE-2021-1160	CVE-2021-1182	CVE-2021-1204
CVE-2021-1161	CVE-2021-1183	CVE-2021-1205
CVE-2021-1162	CVE-2021-1184	CVE-2021-1206
CVE-2021-1163	CVE-2021-1185	CVE-2021-1207
CVE-2021-1164	CVE-2021-1186	CVE-2021-1208
CVE-2021-1165	CVE-2021-1187	CVE-2021-1209
CVE-2021-1166	CVE-2021-1188	CVE-2021-1210
CVE-2021-1167	CVE-2021-1189	CVE-2021-1211
CVE-2021-1168	CVE-2021-1190	CVE-2021-1212
CVE-2021-1169	CVE-2021-1191	CVE-2021-1213
CVE-2021-1170	CVE-2021-1192	CVE-2021-1214
CVE-2021-1171	CVE-2021-1193	CVE-2021-1215
CVE-2021-1172	CVE-2021-1194	CVE-2021-1216
CVE-2021-1173	CVE-2021-1195	CVE-2021-1217
CVE-2021-1174	CVE-2021-1196	CVE-2021-1237
CVE-2021-1175	CVE-2021-1197	CVE-2021-1307
CVE-2021-1176	CVE-2021-1198	CVE-2021-1360
CVE-2021-1177	CVE-2021-1199	CVE-2021-1147
CVE-2021-1178	CVE-2021-1200	CVE-2021-1148
CVE-2021-1150	CVE-2021-1149	

Fabricante

Cisco

Productos afectados

Cisco AnyConnect Secure Mobility Client for Windows, versiones anteriores a la 4.9.04043.
Cisco Connected Mobile Experiences (CMX), versiones 10.6.0 a la 10.6.2.
Routers Cisco Small Business RV110W, RV130, RV130W y RV215W.

Enlaces para revisar el informe:

https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00364-01/
https://www.csirt.gob.cl/media/2021/01/9VSA21-00364-01.pdf

CSIRT comparte vulnerabilidades entregadas por Red Hat	
Alerta de seguridad cibernética	9VSA21-00365-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Enero de 2021
Última revisión	16 de Enero de 2021
CVE	
CVE-2020-24553 - CVE-2020-28362 - CVE-2020-28366 CVE-2020-28367	
Fabricante	
Red Hat	
Productos afectados	
Paquetes Red Hat OpenShift Serverless 0.2.3-1.el8 a 0.12.0-1.el8.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00365-01/	
https://www.csirt.gob.cl/media/2021/01/9VSA21-00365-01.pdf	

CSIRT comparte mitigaciones obtenidas de Apache Tomcat	
Alerta de seguridad cibernética	9VSA21-00366-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Enero de 2021
Última revisión	18 de Enero de 2021
CVE	
CVE-2021-24122	
Fabricante	
Apache	
Productos afectados	
Apache Tomcat 10.0.0-M1 a 10.0.0-M9. Apache Tomcat 9.0.0.M1 a 9.0.39. Apache Tomcat 8.5.0 a 8.5.59. Apache Tomcat 7.0.0 a 7.0.106.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00366-01/	
https://www.csirt.gob.cl/media/2021/01/9VSA21-00366-01.pdf	

CSIRT advierte vulnerabilidades entregadas por Cisco	
Alerta de seguridad cibernética	9VSA21-00367-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Enero de 2021
Última revisión	08 de Enero de 2021

CVE

CVE-2021-1242 - CVE-2021-1311 - CVE-2021-1145
CVE-2021-1224 - CVE-2021-1236 - CVE-2021-1258
CVE-2021-1240 - CVE-2021-1127 - CVE-2021-1245
CVE-2021-1246 - CVE-2021-1131 - CVE-2021-1267
CVE-2021-1238 - CVE-2021-1239 - CVE-2021-1126
CVE-2021-1130 - CVE-2021-1226 - CVE-2021-1143

Fabricante

Cisco

Productos afectados

CVE-2021-1242
Cisco Webex Teams, versiones anteriores a la 40.12.0.17293.
CVE-2021-1311
Cisco Webex Meetings Server. 0MR3 anteriores al Parche de Seguridad 5.
4.0MR3 anteriores al Parche de Seguridad 4.
CVE-2021-1145
Routers Cisco ASR 5000 Series si están ejecutando una versión de Cisco StarOS previa a la 21.19.7.
CVE-2021-1224
Aparatos que usen el siguiente software
Software Cisco FTD anteriores al 6.6.0.
Software Snort Intrusion Protection System (IPS) para Cisco Unified Threat Defense (UTD) para Cisco IOS XE anteriores a la version 17.2.1r.
Snort de Código abierto, versiones anteriores a la 2.9.16.
CVE-2021-1223
Aparatos que usen el siguiente software
Cisco Firepower Threat Defense (FTD) anteriores a la version 6.7.0.
Cisco UTD Snort IPS Engine para IOS XE, versiones anteriores a la 17.4.1.
Snort de código abierto, versiones anteriores a la 2.9.17.
CVE-2021-1236
Aparatos que usen el siguiente software:
Cisco Firepower Threat Defense (FTD) anteriores a la ersion 6.5.0.5.
Cisco UTD Snort IPS Engine para IOS XE, versiones anteriores a la 17.4.1.
Snort de código abierto, versiones anteriores a la 2.9.14.10.
CVE-2021-1258
AnyConnect Secure Mobiliy Client para Linux: versiones anteriores a la 4.9.03047.
AnyConnect Secure Mobiliy Client para MacOS: versiones anteriores a la 4.9.03047.
AnyConnect Secure Mobilty Client para Windows, versiones anteriores a la 4.9.03049.

CVE-2021-1240 Cisco Proximity Desktop para Windows, versiones anteriores a la 3.1.0. CVE-2021-1127 Aparatos Cisco Enterprise NFVIS con versiones anteriores a la 4.4.1. CVE-2021-1245 Cisco Finesse, versiones anteriores a la 12.0 ES05 y 12.5 ES.05. CVE-2021-1246 Cisco Finesse, versiones anteriores a la 12.0 ES05 y 12.5 ES.05. CVE-2021-1131 Cámaras IP Cisco Video Surveillance 8000 Series con versiones de firmware anteriores al 1.0.9-8 con el Cisco Discovery Protocol activado. CVE-2021-1267 Cisco FMC, versiones anteriores a la 6.6.1. CVE-2021-1238 Cisco FMC, versiones anteriores a la 6.7.0. CVE-2021-1239 Cisco FMC, versiones anteriores a la 6.7.0. CVE-2021-1126 Cisco Firepower Management Center versiones anteriores a la 6.7.0. CVE-2021-1130 Cisco DNA Center, versiones anteriores a la 2.2.1.0. CVE-2021-1226 Unified Communications Manager (Unified CM) Unified Communications Manager Session Management Edition (Unified CM SME) Unified Communications Manager IM & Presence Service (Unified CM IM&P) Unity Connection Emergency Responder Prime License Manager CVE-2021-1143 Cisco CMX, versiones 10.6.0, 10.6.1. y 10.6.2.
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00367-01/
https://www.csirt.gob.cl/media/2021/01/9VSA21-00367-01.pdf

CSIRT comparte mitigaciones para una vulnerabilidad de Laravel	
Alerta de seguridad cibernética	9VSA21-00368-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de Enero de 2021
Última revisión	20 de Enero de 2021
CVE	
CVE-2021-3129	
Fabricante	
Laravel	
Productos afectados	
Laravel versiones de la 8.0.0. a la 8.4.2.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00368-01/	
https://www.csirt.gob.cl/media/2021/01/9VSA21-00368-01.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
354e51b2ad7dd7ae40aa58987a27041b0a2ae4490a1177e983b47fcba19423c9
689c85c9bf479544446c251bdc7c4d743ee2c6005f52a0bfa69b5debe26ad0be
cdffc1adc6130ea4ac7b0a16d581c8db0b88ea84fda2c1edb12ee302418dd530
76ffbc488b52655000facf0b042eba699d17270c09e24b5703ac3c5a6859ebfb
f5e146e75878be0e926a587ae7c2ea9663e7873c2aaf63783f6675813fcf4200
90676a5067149360647a5ff7374dba0e94711d70c444f000663bf5d4a6b21f98
b439ae33bd80f4011660b3ceeb8659f3f1298ea36e79bf80e2accc12abfc2b94
9085abde0721f2f03e9e9d2afb9054c3bbdc937c32b099ec798850641f760fda
0568208fcaa7f6fa90c4abad9ea4c0676a155d09c3c51e4d8a6bdb5e55bafc3b
bc33d6bc28fc97ffb5eaae725a7c505357873a471fc928911fdc4c1bdce9a799
a2bf56911e84445f16ca2c0477de6a5592a55610ad56fffe5e65b08728bdbd08
eae24d230cc1c80d0a12778d3436c87ac52581ed5fb8840a618b8fafc5f34da8
93ecbff92cfadfdaf26093aa377048328d19821c09fdb6c8a926d3751f28ceab
0dba6290a0f9faafc903c56c6e9016f7654d7514188b6b41bfab5ecf6b41a1df
8b1bffbc02fafbfbf0dedf65e6b42dd3a12b6e8e6729b8460fadc8e528cbdea7
f63e6c0d5d4fa2e878b16720402523ad433d57bf4f32d7b7588cdcef7bf998bd
6ff6c454e8fe34e2d87a20fc6f6a1a28e463e4f29e5ca5e8b28134cf416d9356
4bcd9f19f8f8429746d3db3ce167f53b33d72116f7ab178e80f1115a0cb9b995
cd6726bcbd4e3241444d8bfb0da56997fefa4a614c3f2e6509f615d43b95f004
2aa5c3ef55242ccb530f5ae466e0ccf5eff7ee0e99a14dfbab77b84b1f231a24
997ef8fc2e605fe96c860961640c040cd4e4e850ae6ef4f7ff0f42582364694d
c8532382f27748bba7557246d4a6e66a084dd6748c4af5f75ab8f59b0d522558
7e6c8d2b812feb9ce8686b301f9df78d69bf9a7bde4572ec7da309a59ec62dab
ecccba19ec91e0fd9fd4e599bd95f5f465d5c68bf774f17e7f8e4b3162ccb97b
bfccc1d871347a0f216cd12e591faafc8cc1150b0e013de934288e20739b065b
5a17dee61b79152ce451f560a17603b291bd0934b4c0bdb69a3328fca8b36771
743b0489a94f04569f1dd9ea1c62d1d5d6ce22b642369e87f974b3635990edb8
11e1780e215a9521853152536320 33b1e42e269f59252e80ccc002e7ed15c086
c4f94c6960792fe6e062b42c6c149482152a96588a9a5b9c3f7c4a35c974ac50
4142cfc2bb8a067a21c0439bef1d08e1742025b00b3cb1c9619ff7bf0a2b42d6

1fa18e851ad74226caf71eaca19ccba3ba2b1457521c4a4fbe6ba07fb3008333
17420055c7c1b85137e8f5e78a7eab811ae1b4f00b33ce05590e19399286fe2f
fb4541bb676e36bc08711601b21c85ec6a0eec67fa65a2ac53a7e70a8f01c628
75d4b326ca471055fba9d3e4dfbb994e191135130d15f7f1e75fa6a8346bf89d
1b2b0f6f229f819f49cefa1af565aa4e83bf8b1f9df047bebfa9143dbebbb349
51d0ab773047ebaac512a5d397e79534ac5b266afd4ee691d6356a8bd7fe4b11
3602f8e737829acb355fceaf51908fe8a199a2ae44099cedd08d3cb298fc8b53
58bd78843e708ee76feee70fd020e5e0ff29c4ad4df2aebbd48ca6d587b15912
0f0061b80732fc11150a67c1807a75989ce897eb2be6e22d425c4b41f88f98ee
c84de615620cd1a69411f262b2f431ac07909b7705e43c1a97d80f5bfdc3ea33
57c0a7e0c8c758419617cbb0493789572ffd9bad491e5e98ecb0754de052efe3
fafa1cf428d6c5e3cc4e6538a098ed38e2ffbd8c9dc5ea06313648aafe2fa0a4
5f6d69e58850b0965c708c5e8cbf7f3f0a769a42c33abe4a82595f903ad92dbe
922d235666c1b57e9aff2834a273334b7e72c3963d98f1a4d8d02287c540a997
849af1e2dd0cefe909b1e37a24266f716af4687eab7ace3bb9bc28c921c4f999
a6b87278bb77d9a04427862b72b0c109e770f31d1c6c6da47644a2dbd82cad11
fcb1b3759243a11409e9c374d7feef2bd785139f1871e23eb04a745e492b0d84
0ded59b8e793df139715fe181350639f9f92855d28917d5321a8c7ee5ca178dd
13fa691fa4a6d36f4aa041d3159233a3272fe9d6a2837dfafa1a34235833221b
8a4ec0ca950a390ef42dca2eba4cb2baea9d9239ab969b07b0596fa2e601e01c
bd207412e6350e4c7e0f4149a5e2e5f607193dbd98360ec8e696ef42cd6ba4ad
3fe9826f416743be9ec86023808b246c046a0384db9c9c81268ce8fd008c792d
24ff39d73f1df07521eae970f57ccb4c214adec5a1a9e3941890abea7f59810b
4d972e37eedaf19d2f0e71ed55568cce27b0860e54906c5442ca69c2e2f0d360
54accdc2c15133ddabb1dd67159f363044ec299963688259f2947ef9b8160093
f773095273ff78e1678a13fcec9c17b2cce0412f13c0f12e09cdd6173ffc82c3

Correos electrónicos de donde son enviados los archivos adjunto con malware

5057040@qq.com
accounting@ocs.co.id
amy.gan@jcb.com
anna@findaproperty.gi
delivery@bedslide.com
info@absolare.com
info@dhlexpressgrp.pw
info@dhlexpressint.pw
info@howw.com
jhewitt@wayfair.com

jquijano@plantacmm.com
Nancy@riversideprojects.com.au
paule.a@mageneet.com
redirect@amgeneralinsurance.com
sabrina@comitras.com
sandeepgill@combytellc.com
scott@webbimpressions.com
shelly@royal-bike.com
sscrm@cmhk.com
terence.so@otlsystems.com
tien.mai@r-pac.com
vnsales6@juwonmetal.com
silvia.almaraz@loubet.com.mx
christian.sagadraca@nfc.gov.ph
visas2@siecindia.com
vikki.tambe@sysnetglobal.com
dnduw@nduwsfamily.com
ych512@ms75.hinet.net
asif@regrowz.in
gemma.miaventilation@miachina.net
walaa@metrofiresystems.com
pedidos@laveiga.com
zahid@roshnimm.com
sherrera@makler.com.ve
jean-yves.lameyse@paris.notaires.fr
ehernandez@decimas.es
finance@pinstarauto.com
mail@libertylease.nl
seiaprod@seia.cl
3d@threenarrewarren.com.au
info@caa-ingenieria.com.ar
toanbui@benhvienranghammat.vn
submission@najmedicine.us
info@turismoproclusone.it
esperanza@protools.mx
progettazione.p@rossini1969.it
accounts@stopl.in
n.gouveia@qualiconsig.com.br

spg@spgbrindisi.it
ruben@granimarloranca.com
branchmanager.skp@shaheen-traders.com
r_kakita@hamaoka-industry.com
compras@josehuespeehijos.com.ar
Samiuddinr@hotmail.com
SHALEY.NG@ienergy.com.sg
recruitment@shengtai.co.th

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.

185.222.57.238
77.139.57.60
192.185.201.2
192.185.149.46
98.187.237.162
45.145.185.72
37.49.225.241
193.239.147.142
160.20.147.58
159.89.224.7
180.214.237.140
64.225.53.63
172.93.201.206
103.141.138.130
103.199.17.185
45.133.203.50
117.102.98.79
192.158.231.119
128.199.15.190
37.46.150.218
185.244.216.174
155.94.136.43
164.90.152.242

144.208.127.207
69.89.20.226
192.185.50.93
216.10.244.214
172.104.61.201
168.95.4.114
162.210.70.184
162.210.70.2
162.251.83.181
175.107.198.7
50.116.124.69
170.249.199.130
162.252.57.42
114.31.72.17
207.21.192.5
103.45.230.198
103.120.176.28
198.71.225.36
201.76.49.59
69.89.25.95
219.99.187.7
189.126.112.61
181.31.135.145
193.56.28.234
217.74.103.244
116.202.193.189
145.131.7.81

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
78.128.113.66
212.70.149.54
212.70.149.85
5188206204
37.49.225.207
141.98.80.101
72.11.135.222
193.105.134.232
190.21.158.16

Actualidad

CSIRT inicia mesa de ciberseguridad del sistema sanitario, parte del desarrollo protocolos comunes para los sectores regulados

El CSIRT de Gobierno fue el primer expositor en la Mesa de Ciberseguridad de la Superintendencia de Servicios Sanitarios, que comenzó a trabajar de forma telemática esta semana. La instancia, surgida a partir de un requerimiento del Comité Interministerial de Ciberseguridad, tiene el objetivo de desarrollar estandares de ciberseguridad para los sectores regulados de la economía.

Es así que el CSIRT ya ha realizado esta misma labor con la Subsecretaría de Telecomunicaciones, Superintendencia de Seguridad Social, el Coordinador Eléctrico, la Superintendencia de Casinos y la de Salud, entre otros organismos.

La idea es que las distintas empresas y organizaciones que participan de los mercados regulados desarrollan protocolos de ciberseguridad unificados y criterios de notificación comunes, para contar con la mayor coordinación ante ataques cibernéticos a la infraestructura del país, que suelen afectar de forma transversal a varios sectores del ecosistema digital de una nación.

Todo lo anterior, para avanzar en el desarrollo de protocolos para la coordinación en ciberseguridad, mientras se espera que el Congreso apruebe la Ley Marco de Seguridad, que establecerá los estándares definitivos, cuya implementación se facilitará gracias al trabajo que ya están realizando el CSIRT y los distintos grupos sectoriales.

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.

- Fernando Cid
- Boris López

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.01.22 14:26:18 -03'00'