CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

03-12-2020 | Año 2 | N°74

Boletín de Seguridad Cibernética

Semana del 26 de Noviembre al
02 de Diciembrede 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

47

Sha 256

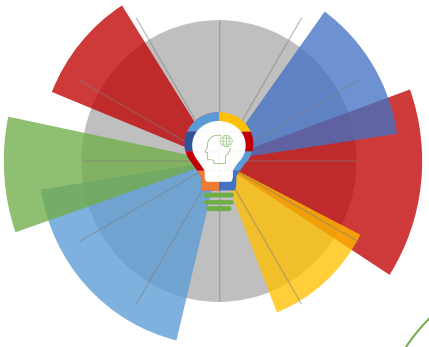
Asociadas a múltiples campañas de phishing son archivos que contienen malware

Se advirtieron

20

URLs

Asociadas a sitios fraudulentos y campañas de phishing



Parches

1

para vulnerabilidades

Las mitigaciones son útiles para productos FortiOS.

IPs

284

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

CSIRT advierte sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00836-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Noviembre de 2020
Última revisión	27 de Noviembre de 2020
Indicadores de compromiso	
URL	
https[:]//bancosantaander-movil[.]app	
IP	
[162.0.235.16]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00836-01/	
https://www.csirt.gob.cl/media/2020/11/8FFR20-00836-01.pdf	

CSIRT advierte sitio de banco falso	
Alerta de seguridad cibernética	8FFR20-00837-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Noviembre de 2020
Última revisión	27 de Noviembre de 2020
Indicadores de compromiso	
URL	
https[:]//araucaniatv[.]cl/wp-admin/maint/css/signin.php	
IP	
[162.241.2.176]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00837-01/	
https://www.csirt.gob.cl/media/2020/11/8FFR20-00837-01.pdf	

CSIRT advierte página fraudulenta de software	
Alerta de seguridad cibernética	8FFR20-00838-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Noviembre de 2020
Última revisión	27 de Noviembre de 2020
Indicadores de compromiso	
URL	
https[:]//www.dispensariosur[.]cl/adobe/	
IP	
[170.84.209.80]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00838-01/	
https://www.csirt.gob.cl/media/2020/11/8FFR20-00838-01.pdf	

CSIRT informa suplantación de sitio bancario	
Alerta de seguridad cibernética	8FFR20-00839-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Noviembre de 2020
Última revisión	27 de Noviembre de 2020
Indicadores de compromiso	
URL	
https[:]//bancosantande-r[.]app/	
IP	
[170.84.209.80]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00839-01/	
https://www.csirt.gob.cl/media/2020/11/8FFR20-00839-01.pdf	

CSIRT advierte sitio fraudulento de servicio de alojamiento de archivos	
Alerta de seguridad cibernética	8FFR20-00840-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Noviembre de 2020
Última revisión	30 de Noviembre de 2020
Indicadores de compromiso	
URL	
https[:]//chileanylgroup[.]cl/wp-admin/documentview/	
IP	
[66.165.231.114]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00840-01/	
https://www.csirt.gob.cl/media/2020/11/8FFR20-00840-01.pdf	

CSIRT informa suplantación de página de una red social	
Alerta de seguridad cibernética	8FFR20-00841-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Noviembre de 2020
Última revisión	30 de Noviembre de 2020
Indicadores de compromiso	
URL	
http[:]//chat-whatsapp.doctorhaddadpediatriayflores[.]cl/login.php	
IP	
[186.64.117.225]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00841-01/	
https://www.csirt.gob.cl/media/2020/11/8FFR20-00841-01.pdf	

CSIRT advierte portal falso de plataforma de firma electrónica	
Alerta de seguridad cibernética	8FFR20-00842-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Noviembre de 2020
Última revisión	30 de Noviembre de 2020
Indicadores de compromiso	
URL	
http[:]//consultax[.]cl/thecrowngroup/tcwoodinc/u.php	
IP	
[186.64.118.155]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00842-01/	
https://www.csirt.gob.cl/media/2020/11/8FFR20-00842-01.pdf	

Phishing

CSIRT informa de phishing bancario por supuesto estado de SuperClave	
Alerta de seguridad cibernética	8FPH20-00330-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Noviembre de 2020
Última revisión	26 de Noviembre de 2020
Indicadores de compromiso	
URL	
https://cutt[.]ly/qhsTsIU	
https://cutt[.]ly/chank2B	
https[:]//santander.logincl[.]site/	
IP	
[173.82.106.16]	
[184.175.85.196]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00330-01/	
https://www.csirt.gob.cl/media/2020/11/8FPH20-00330-01.pdf	

CSIRT informa phishing con supuesta actualización bancaria	
Alerta de seguridad cibernética	8FPH20-00331-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Noviembre de 2020
Última revisión	27 de Noviembre de 2020
Indicadores de compromiso	
URL	
http://supersauna.alfahosting.org/Validacion2.0/Secured/acepting.php	
https://ee.mobile.santander-chile.update.personas.cl.adu-experts.com/	
IP	
107.180.3.96	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00331-01/	
https://www.csirt.gob.cl/media/2020/11/8FPH20-00331-01.pdf	

Imagen del mensaje

CSIRT advierte smishing de súper clave bloqueada	
Alerta de seguridad cibernética	8FPH20-00332-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Noviembre de 2020
Última revisión	27 de Noviembre de 2020
Indicadores de compromiso	
URL	
https[:]//bancosantandder[.]app/?sms=santander	
https[:]//bancosantaander-movil[.]app/1606503657/personas/index.asp	
IP	
162.0.235.16	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00332-01/	
https://www.csirt.gob.cl/media/2020/11/8FPH20-00332-01.pdf	

Malware

Imagen del mensaje

CSIRT informa de malware con supuesta factura para pago	
Alerta de seguridad cibernética	2CMV20-00109-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Noviembre de 2020
Última revisión	27 de Noviembre de 2020
Indicadores de compromiso	
Hash	
435B91F80163B5EAB6677E014A38437D07B408A2E1192412577BF8327CC0DAF8	
AB38630902553668E95037B67283D2FA68951B392679EF60A1DAFC63EB9BE3CC	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00332-01/	
https://www.csirt.gob.cl/media/2020/11/8FPH20-00332-01.pdf	

Vulnerabilidades

CSIRT comparte mitigación para vulnerabilidad de FortiOS	
Alerta de seguridad cibernética	9VSA20-00328-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Noviembre de 2020
Última revisión	28 de Noviembre de 2020
CVE	
CVE-2018-13379	
Fabricante	
Fortinet	
Productos afectados	
FortiOS desde la versión 6.0.0 hasta la 6.0.4, desde la 5.6.3 hasta la 5.6.7 y desde la 5.4.6 hasta la 5.4.12. Solo si el servicio VPN SSL (modo web o modo túnel) se encuentra habilitado.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00328-01/	
https://www.csirt.gob.cl/media/2020/11/9VSA20-00328-01.pdf	

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
16c5cbeda4b5dfad0058c5ade0284c0d02b3dd9f4145306600d991fd1d2dd157
6327d4da5bcd54191d94479582194c30298ebd8dbad980b4a25fa39f95afb60b
56dd20b5bcf436ddb28eca061ca9f6d0458a1dd29d2ec1932d83aa4f75cbd62e
e34317bb799040db5ac6d4821d19f6d0b9dba1ed1151217f3af0cd4ff1cde887
2f1d7661d4fc0cd69804b4c13e79eabdc6a71dcd4dc3adbd71c0a8b908a48213
93a44932c9f69503c3c64526fd393f1f880e8d4c902118938e94611f1b8533a5
35b586adfd3a1223e6e6bf5301a63e66fff0b283170a1dc28432d55ccae36ec7
fbd27e8376e163522d33ecb1bcd8b4aa21cbefc47999705baa2991d187776966
e804f2914ce23f9c3ab3f5bc96799af2222c8f458d3e205369ea77deae2fbf53
e09256c5640b2edb09dd85e28e7b41061d1f9b498a3b0d7c27cd4637b6b869fc
3f84f4066f10a19dbd3a8166e191ce77f9b30cb063bc2958e7adfeb0ff4ba73e
765479a105fd76a3f3793014597a9f96fc9c6b62e9a0752eb0b9ba9b8e8d7221
559414341d8cfd33236037c31aacc503edf05f5babde9ef10e641638d9c2c36e
e2a62f1e976390ab92ba2448f9949bee0fb8b71a41e38c4e9cba597a2f9b12cf
b828f049dfe16d430ab605d22751b7b9d6f09d80072b728b499ba3dbe428f7a2
de16ac1476751c9c3299908201515af30e740c2b6133783b34dccfd9a6416df9
ead62772d0fd68778028df20f10438f39ac93374e6114c9eddeae7c7a5cdea1c
78c1e52c56949d593ebc2c746bf7ed4f0509bb7a43fa26dc42f03ef1d99d9e3e
542ca7ae59a7a502befe37327bf8bbc85b046f0d50e64274dee8a656514146be
a4850a594a6993d7473f9eb17d8aa86abd7bcc10a73cdf4e8cdd59de885f20fa
ff6a9804b88dc44bb751f0d82e8f698d48fed46bcb2202f7f0e91ee5b235bdd7
336950f0069d06c1db6243ab78a872ef90abb7e8beb692c84dc32e650b1b19d9
06df213aaf0d34f89961a302fdd46427a73ef4506f9becb487c57f6bc4845486
1f4d1b50fddb44e5bd891b724268023d4f53c181d36a691d1d3e50bd3d4ed5ac
273b21b626a0d62db668a96bd8629fd6c337562af8d96ba54b4565e7317d392d
27f54b776df2d81372881e08f8f30c6de016b42af253b922daf47610c0994f3a
2ba9db3110899e60daeecb086d4f53adc1cfab127820db3d230c383e74f7172c

2ef7e94a43af91a940c6f95e61c7704cd9e9fa85a29326837b9304432227bbed
39b19d8de9ae16f6d264e859c74f4a94aa5b15457e47956e51afe7932eaad3aa
410daa0d516d732cee201ec712f76ea2201a3f8e75cae4780b8c59704ad7210d
419bb546a0c3f701084e0e8a1747bef2d5c8017084615abb4c398cefa07491c0
45140dd2ab7b443fbab11137844d7aded6a57da3c3b833394fc6fd04ce37387d
4c458adc275a7faedf5c6d94f20c71de8bd853b5bd3cee24311f35c2dd6d6195
5013fc28e8430f52d98897e86b43f8c304ea06eb6cc0458cb24c17146998e53d
5835c6cac6eb6f57d36b3ecf2acd21941b5c2ae646793484db9ee69191420118
613b8dba5d25b203e40c79290fd37d4463c72ba09b22d4680eb8947cec0c951c
6d535b5e5a0ebb2e85af8667e6ef7c5ed1c4851d2cd6546a4bffddb6d1e06eac
78ad819ae78dde1cebf9e56773ba9e9932e16ba223c1610914a6a9b3562584f6
84814a4e998b3ccc23438707923f0e3dba5238a7e52c4641d7cf0ae9c3384ecb
87f6c0a7b49247b2009bbaa8995dde20ba9bb8a1c66731c450ebbaea566ec962
be0de7bcb47424c202d39f09e09b5a05b1441d16af3227315aea4b56bf7f644d
cc4ffbe82cc4d419110401a56146ee7dab7d02cb745b4a4aa37435c2a3872180
cf1526e4f848aa6b5d2131e3de2241fbd89562e3bede450ca608a18ea338ad46
d02f316f4605b93bf187a25a625b7f2d91d8f644c048ec4e091b99d817d52c5b
dc0b3a41288d7bf453ec5ee9d453777365b9d14c3991230023fb1f767db7aa5b

Correos electrónicos de donde son enviados los archivos adjunto con malware

61@hkstar.com
ebrolibro@teleline.es
ahmed.akram@mediaminds.biz
syeon@ra.rockwell.com
sales.coate@greenroad.com.cn
jdlouhy1@bloomberg.net
info@nyheder.danskespil.dk
ali.alzoubaidi@trust.com.jo
export@tesartesisat.com
jetchehu@zeni.com.ar
pt@hinewdubai.pw
support@hengfengsteel.org
Feray.Kozan@dhl.com
mechanic@cement.kz
Jenny.Jiang@bmo.com
itcqs1@nawaloka.net

procurement@relsuninternational.com
noreply@wetransfer.com
ANCHELENE@curtidoscabezas.com
Bankalerts@kotak.com
corinna.li@dhl.com
magna@magnaexport.cl
kadriye@ekinteksmoda.com
fiona@hamoasia.com
expressshipping@dhl.com
chartering@roxanashipping.com
crisbcn7@yahoo.es
ob_prokuplje@mojdoktor.gov.rs
alexh.tampa@gmail.com
dep.finaceiro@famplac.com.br
libing@limkimhai.com.sg
accounts@eurobank.gr
sangyoung.kr@samsung.com
jeffrea@cqv.co.kr

Direcciones IP de servidor SMTP donde es enviado el correo malicioso

195.254.241.251
185.222.57.221
185.222.58.144
103.141.138.125
45.147.229.20
185.222.58.157
202.230.222.70
202.230.222.69
188.93.233.117
202.230.222.68
202.230.222.67
202.230.222.66
202.230.222.65
202.230.222.64
202.230.222.63
202.230.222.62
202.230.222.71
104.168.245.162

92.60.142.98
103.145.252.171
193.193.228.225
89.44.9.240
45.137.22.94
202.230.222.109
202.230.222.108
202.230.222.107
202.230.222.106
202.230.222.105
85.204.116.137
202.230.222.104
202.230.222.103
202.230.222.102
202.230.222.111
202.230.222.110
104.168.172.23
37.49.225.134
104.168.211.132
194.31.141.131
212.175.100.142
185.239.242.143
185.29.11.102
212.200.253.238
103.133.109.32
103.225.25.74
37.49.225.135
143.110.246.188
139.59.66.50
206.189.89.96

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		
5.196.217.176	171.242.66.110	186.179.100.199
14.186.196.217	188.255.237.206	186.239.155.106
14.226.246.151	190.197.113.149	78.189.26.51
37.221.178.100	200.155.181.198	124.182.230.85
37.221.179.151	201.131.180.160	134.90.254.119
37.221.179.187	212.126.121.254	138.0.7.222
37.221.182.229	220.180.171.199	138.97.54.58
37.221.183.192	1.9.78.181	14.177.138.53
60.211.217.154	101.85.226.21	79.98.222.39
76.184.134.253	109.233.17.8	79.98.223.80
88.148.113.227	109.90.75.248	89.214.212.89
109.166.168.111	110.36.219.242	183.102.114.251
111.202.130.168	110.39.184.230	186.179.100.104
121.160.165.136	110.39.196.2	186.179.100.118
178.254.171.149	111.224.52.169	84.253.185.234
178.254.171.178	111.50.110.214	111.224.166.206
178.254.179.153	113.172.231.25	111.224.166.221
178.254.179.198	113.195.164.74	113.173.186.175
178.254.179.250	115.84.91.38	119.199.253.216
186.179.100.115	116.199.63.218	121.142.146.167
186.179.100.203	117.1.23.94	124.195.191.112
186.239.134.158	117.222.94.93	124.207.159.249
188.255.131.183	117.70.93.251	141.105.105.142
188.255.131.245	118.200.63.97	141.105.105.158

188.255.132.165	118.212.37.33	177.154.230.156
188.255.132.181	119.62.184.137	178.254.179.110
188.255.132.221	119.75.76.252	45.14.250.76
188.255.132.239	121.175.243.75	45.4.171.114
188.255.237.161	123.20.3.29	58.57.178.30
188.255.237.188	124.131.28.137	59.103.198.85
188.255.237.208	113.173.186.175	59.40.82.205
191.102.120.181	154.127.82.93	59.53.183.198
102.68.7.160	171.242.66.110	60.173.241.87
103.89.89.210	171.35.162.223	60.186.32.225
104.136.140.15	171.35.163.67	60.212.48.55
120.33.137.113	171.35.175.84	60.223.242.27
121.133.34.48	174.66.106.22	60.23.191.75
123.24.186.225	176.31.24.26	61.157.84.57
124.88.218.106	177.125.20.118	61.183.93.110
128.92.1.162	177.152.64.255	70.112.177.13
14.177.18.134	177.154.238.41	195.32.74.7
14.179.15.195	177.99.217.233	195.32.75.143
14.186.48.196	178.254.171.40	195.32.75.37
141.105.104.43	180.107.229.90	197.153.91.74
141.98.80.80	180.162.249.82	212.160.230.88
155.12.21.118	182.110.184.10	71.219.71.232
158.69.157.46	182.47.24.147	77.71.48.222
170.233.69.109	183.157.170.63	74.51.2.240
170.250.245.40	183.239.203.40	80.210.22.96
178.156.67.180	185.64.221.11	85.105.206.68
186.179.100.10	185.64.221.7	95.38.101.206
186.68.86.234	186.179.100.22	78.128.113.66
187.25.227.218	186.215.197.15	141.98.80.81
188.255.131.70	186.47.153.126	5.188.206.202
189.114.93.191	187.71.9.181	103.88.127.48
191.102.83.167	189.114.67.213	1.234.172.251
194.208.93.9	189.44.20.193	42.243.218.138
195.32.73.160	189.59.69.3	45.115.171.144
195.32.73.73	189.93.18.159	45.238.121.154
197.248.20.2	195.32.73.38	45.238.121.198
198.27.110.178	91.134.169.23	50.198.244.241
200.91.55.236	212.160.230.96	59.103.195.235

212.69.22.168	218.64.57.12	59.103.196.245
212.69.22.190	219.159.201.66	59.103.197.108
212.69.22.20	220.164.2.67	61.133.247.224
212.69.24.226	220.172.105.39	66.248.171.120
212.69.27.222	220.225.7.99	73.232.102.183
218.22.180.146	222.173.98.202	82.141.161.190
218.85.143.78	222.179.42.134	41.212.26.36
221.13.140.88	222.181.146.60	41.60.85.155
23.240.136.91	222.189.163.82	41.60.86.112
31.170.59.35	222.82.252.238	42.231.254.65
37.221.181.3	27.71.8.94	42.243.96.20
37.221.181.51	37.99.251.248	45.165.214.24
37.221.181.69	37.99.252.87	5.196.201.7
37.221.182.8	37.99.253.2	60.29.37.54
37.99.254.197	39.129.25.5	60.30.162.38
41.202.170.77	39.71.221.116	62.20.175.84
41.86.238.176	41.202.168.50	

Actualidad

Ciberconsejos para reconocer apps fraudulentas

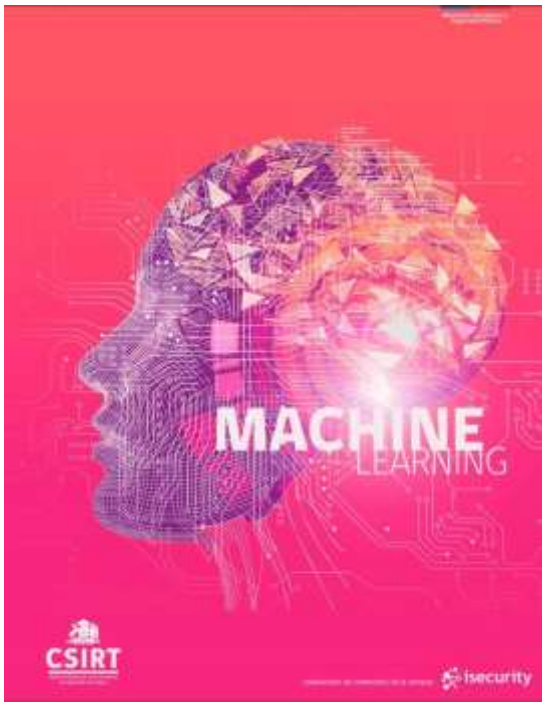
Si bien las aplicaciones o juegos para los smartphones pueden ser muy útiles o entretenidas, hoy debemos tener mucho cuidado al descargarlas, ya que algunas son creadas con fines maliciosos, como espionaje, acoso o suplantación de identidad.

Ver más: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-reconocer-apps-fraudulentas/

Investigación

Machine Learning

La versión 23 del Análisis de Amenazas Cibernéticas fue elaborada por el investigador Jaime Gómez Gonzalez, quien de profesión es Ingeniero Civil Electrónico de la Pontificia Universidad Católica de Valparaíso, posee un MBA de la Universidad Adolfo Ibáñez, y actualmente se desempeña como Líder de iSecurity Labs, responsable del área de nuevas tecnologías de la compañía, quien en este trabajo aborda el fenómeno de inteligencia artificial conocido como "Machine Learning".
El autor explica que en materia de ciberseguridad el Machine Learning es una de las aplicaciones más prometedoras en el campo de la seguridad cibernética. Así, el también conocido como aprendizaje automático permite que los sistemas de red y ciberseguridad hagan cosas bastante sorprendentes, pudiendo determinar y detectar con precisión anomalías en los patrones de tráfico, las conexiones y la actividad del usuario, entre otros aspectos de la red.
Hay dos términos que se usan con mucha frecuencia cuando se habla de ciberseguridad: sistemas de detección de intrusos (IDS) y sistemas de prevención de intrusos (IPS). IDS es la detección de cualquier ataque que haya ocurrido. IPS es la prevención de cualquier tipo de ataque. Es más fácil detectar un ataque que prevenirlo completamente.



Ver más: https://www.csirt.gob.cl/reportes/machine-learning/

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.

- Christian Vidal
- Camilo Orellana
- Rodrigo Machado

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.12.04 13:40:12 -03'00'