CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

24-12-2020 | Año 2 | N°77

Boletín de Seguridad Cibernética

Semana del 17 al 23 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

91

Sha 256

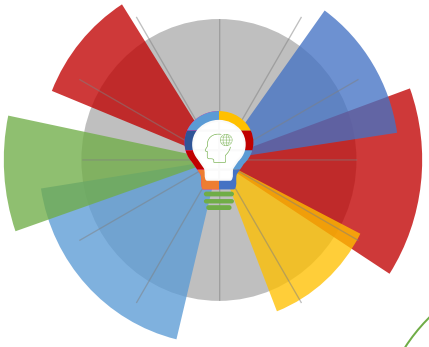
Asociadas a múltiples campañas de phishing son archivos que contienen malware

Se advirtieron

8

URLs

Asociadas a sitios fraudulentos y campañas de phishing



Parches

53

para vulnerabilidades

Las mitigaciones son útiles para productos F5 Network, Android, Contact Form 7, VMware, Dell y Maria DB.

IPs

326

Informadas

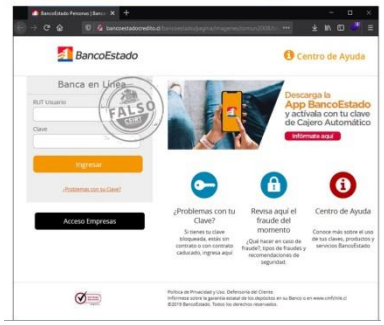
Listado de IPs advertidas en múltiples campañas de phishing y de malware.

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

Contenido

Sitios fraudulentos

Imagen del sitio

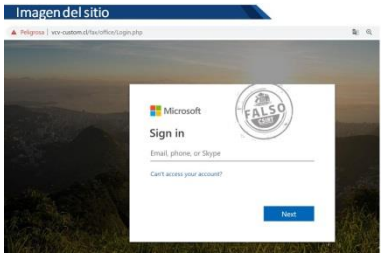


CSIRT advierte sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00855-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Diciembre de 2020
Última revisión	22 de Diciembre de 2020
Indicadores de compromiso	
URL	
http://bancoestadocredito[.]cl/bancoestado/pagina/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
186[.]64[.]118[.]235	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00855-01/	
https://www.csirt.gob.cl/media/2020/12/8FFR20-00855-01.pdf	

Imagen del sitio

CSIRT informa suplantación de página bancaria	
Alerta de seguridad cibernética	8FFR20-00856-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Diciembre de 2020
Última revisión	22 de Diciembre de 2020
Indicadores de compromiso	
URL	
https[:]//newerafitness[.]net/retro/modafck%20page/2/	
IP	
144.208.75[.]114	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00856-01/	
https://www.csirt.gob.cl/media/2020/12/8FFR20-00856-01.pdf	

CSIRT informa suplantación de sitio de empresa de envíos	
Alerta de seguridad cibernética	8FFR20-00857-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Diciembre de 2020
Última revisión	23 de Diciembre de 2020
Indicadores de compromiso	
URL	
https[:]//mutatio[.]cl/wp-admin/js/widgets/widgets./Dhl/	
IP	
[192.141.168.178]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00857-01/	
https://www.csirt.gob.cl/media/2020/12/8FFR20-00857-01.pdf	



CSIRT advierte sitio falso de software	
Alerta de seguridad cibernética	8FFR20-00858-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Diciembre de 2020
Última revisión	23 de Diciembre de 2020
Indicadores de compromiso	
URL	
https[:]//vcv-custom[.]cl/fax/office/Login.php	
IP	
[192.141.168.137]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00858-01/	
https://www.csirt.gob.cl/media/2020/12/8FFR20-00858-01.pdf	

Phishing

Imagen del mensaje

CSIRT informa smishing bancario de Súper Clave bloqueada	
Alerta de seguridad cibernética	8FPH20-00342-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Diciembre de 2020
Última revisión	18 de Diciembre de 2020
Indicadores de compromiso	
URL	
hxxps://superclave-bloqueada[.]app?sms=santander	
hxxps://bancapersonas-superclave-actualizar[.]app/1608320811/personas/index.asp	
IP	
68.65.123.54	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00342-01/	
https://www.csirt.gob.cl/media/2020/12/8FPH20-00342-01.pdf	

Imagen del mensaje

CSIRT informa phishing para realizar una supuesta transacción	
Alerta de seguridad cibernética	8FPH20-00343-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Diciembre de 2020
Última revisión	22 de Diciembre de 2020
Indicadores de compromiso	
IP	
[209.85.215.180]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00343-01/	
https://www.csirt.gob.cl/media/2020/12/8FPH20-00343-01.pdf	

CSIRT advierte phishing de abono del 10% de la AFP	
Alerta de seguridad cibernética	8FPH20-00344-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Diciembre de 2020
Última revisión	22 de Diciembre de 2020
Indicadores de compromiso	
URL	
https[:]//bit[.]ly/34xr5Tr?l=www.bancoestado.cl	
http[:]//mobilewifi[.]rs/Solicitud/www.bancoestado.cl/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[202.69.33.130]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00344-01/	
https://www.csirt.gob.cl/media/2020/12/8FPH20-00344-01.pdf	

Vulnerabilidades

CSIRT comparte mitigaciones obtenidas de F5 Networks	
Alerta de seguridad cibernética	9VSA20-00340-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Diciembre de 2020
Última revisión	18 de Diciembre de 2020
CVE	
CVE-2020-27730	
Fabricante	
F5 Networks	
Productos afectados	
La vulnerabilidad afecta al NGINX Controller, versiones de la 1.0.1 a la 3.9.0.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00340-01/	
https://www.csirt.gob.cl/media/2020/12/9VSA20-00340-01.pdf	

CSIRT comparte mitigaciones obtenidas por Android	
Alerta de seguridad cibernética	9VSA20-00341-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Diciembre de 2020
Última revisión	18 de Diciembre de 2020
CVE	
CVE-2020-0099 - CVE-2020-0294 - CVE-2020-0440 CVE-2020-0459 - CVE-2020-0464 - CVE-2020-0467 CVE-2020-0468 - CVE-2020-0469 - CVE-2020-0458 CVE-2020-0470 - CVE-2020-0460 - CVE-2020-0463 CVE-2020-15802 - CVE-2020-0444 - CVE-2020-0465 CVE-2020-0466 - CVE-2020-0016 - CVE-2020-0019 CVE-2020-0455 - CVE-2020-0456 - CVE-2020-0457 CVE-2020-11225 - CVE-2020-11146 - CVE-2020-11167 CVE-2020-11185 - CVE-2020-11217 - CVE-2020-3685 CVE-2020-3686 - CVE-2020-3691 - CVE-2020-11136 CVE-2020-11137 - CVE-2020-11138 - CVE-2020-11139 CVE-2020-11140 - CVE-2020-11143 - CVE-2020-11119 CVE-2020-11144 - CVE-2020-11145 - CVE-2020-11179 CVE-2020-11197 - CVE-2020-11200 - CVE-2020-11212 CVE-2020-11213 - CVE-2020-11214 - CVE-2020-11215 CVE-2020-11216	
Fabricante	
Android	
Productos afectados	
Dispositivos con el sistema operativo Android.	
Enlaces para revisar el informe:	

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00341-01/
https://www.csirt.gob.cl/media/2020/12/9VSA20-00341-01.pdf

CSIRT comparte mitigaciones obtenidas por Contact Form 7	
Alerta de seguridad cibernética	9VSA20-00342-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Diciembre de 2020
Última revisión	21 de Diciembre de 2020
CVE	
CVE-2020-35489	
Fabricante	
Contact Form 7	
Productos afectados	
Sitios construidos sobre WordPress y que usen el plug in Contact Form 7 en sus versiones 5.3.1. y anteriores.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00342-01/	
https://www.csirt.gob.cl/media/2020/12/9VSA20-00342-01.pdf	

CSIRT comparte vulnerabilidades de VMware	
Alerta de seguridad cibernética	9VSA20-00343-01
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-2020-3999 - CVE-2020-4008	
Fabricante	
VMware	
Productos afectados	
VMware ESXi 7.0, VMware Workstation versiones a 15.x a 16.x, WMware Fusion 11.x y 12.x y WMware Cloud Foundation 4.x.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00343-01/	
https://www.csirt.gob.cl/media/2020/12/9VSA20-00343-01.pdf	

CSIRT comparte mitigaciones entregadas por Dell	
Alerta de seguridad cibernética	9VSA20-00344-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Diciembre de 2020
Última revisión	23 de Diciembre de 2020
CVE	
CVE-2020-29492 - CVE-2020-29491	
Fabricante	
Dell	
Productos afectados	
Dell Wyse ThinOS versiones de la 8.3.0 a la 8.6_511. Dell Wyse ThinOS, versiones de la 8.6_019 a la 8.6_511.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00344-01/	
https://www.csirt.gob.cl/media/2020/12/9VSA20-00344-01.pdf	

CSIRT comparte vulnerabilidad de MariaDB	
Alerta de seguridad cibernética	9VSA20-00345-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Diciembre de 2020
Última revisión	23 de Diciembre de 2020
CVE	
CVE-2020-15180	
Fabricante	
MariaDB	
Productos afectados	
Maria DB versiones desde la 10.1.0 a la 10.5.5.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00345-01/	
https://www.csirt.gob.cl/media/2020/12/9VSA20-00345-01.pdf	

Malware

CSIRT advierte campaña de malware con falsa factura	
Alerta de seguridad cibernética	2CMV20-00120-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Diciembre de 2020
Última revisión	17 de Diciembre de 2020
Indicadores de compromiso	
Hash	
3A3E74C5B52D1CF2308A276952F92C2954A7F6AD064D18334EF0129DD4DD4829	
E6633B5015CAD9D0A683B91202358E01F0E568E1A5F333F0FFBC5B4E3E8B1FB8	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv20-00120-01/	
https://www.csirt.gob.cl/media/2020/12/2CMV20-00120-01-1.pdf	

CSIRT advierte campaña de malware con supuesto pedido realizado	
Alerta de seguridad cibernética	2CMV20-00121-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Diciembre de 2020
Última revisión	17 de Diciembre de 2020
Indicadores de compromiso	
Hash	
69648D3959A59C225107CCFAE22AF07745841655B04DFBD61173E91FB580BC80	
FC956A2B7D33E3DE5063028A0852B2FB1E86EAA91BCF469B157032852F281211	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv20-00121-01/	
https://www.csirt.gob.cl/media/2020/12/2CMV20-00121-01.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

baf9b1f3b396d55191edb05b9ba9dfffca13d739c210382203f3d83897ffbbd3
07981354aad310028a2e5d4bff50a729143af433b99e6c629e4ec15353b9364b
7846211fbc0020448a7a5bc5729d8b01ba6cd441242433f4df9f3b5fced55156
151780de003e4c3e6df80450146734a15a86d0e48e48e925fe093d5964231dca
a91d2a7249086c122bc1a7e697f70bfeec7a0575bbdc6801c710895148fae5cb
e42185ae8dac37175057bc1444a4fe534e21307b3f0814f7e1ea3128ace7fc3b
d532e9feb63d3b871aff64fe5a901dda6a04897f61434b910567315e33ba43b7
f95ba93cf90b89b0abeed62cceee83a008393deb74425ae050775945e8903574
08b1023bf12f8ce09bcad60da88447d1066d6d2ab7b4bcf13261c9d7ec48fdf8
fc60c2d2f89eed099d1b41eb4ed7912549f3e00b8fdd7d7de1ef86e67e619550
cbfeb7245db426440564cc9de2987213b2832fc13876d58864ea9d9774162f60
ad49792b1c23ff2ac87b924a4c6575d0e06f5c2a5520172d85addf0a9b7b5236
454b93f25bcca014d758bf7d8caac0c615c328bd35fa9be0fc03732dfc7209d9
aecd152282def027bfd51b70b018af2c80dabf50c52ba4100c71c1047fe027dd
78cb5ccd1e9ae32d83d8eb6c4144e17150709c210fee9b28a692169809a0f81f
131c0800e1400e25fba579755d90f9a3afcf7fcefe86e5b7178b8c4389cfa89c
2fa4d0c9f754437c49482bceba78a4f36d60b11995ade031ce731028698cb615
81bb2dfe82ab75a170c4d73d51633e7879468a5bb22024eefed8fdc2abf5cab3
697234a66ea01428164440034fcd15f9dc45ff3434f090f641bab6ebf0e95a26
17360343aeba1cad7a0e07554d295d3f84c4a82b5a949272ff89f5ef5dab9a30
c2aa078c0aa7586366efa7b9190004dbdbed735abf183483da41030eba155d0a
ba1218e38d9223acf507cfc1a458681e54567ca72f03040901578a63ffc0ba06
738b80290a3ecd799b197d90b803c1c8468aca688e44caa60902b11075af7f2c
0c2c97f9c94b970cc23cc8f11be9fcbaf1630395d13060ca289eb0d9284b4a7d
939b74068ba5fe714a61e87a3acba52787684f19bc611654a6fc2a644adb57a3
6a7525a409509ac4ff33649e2dab4cc9580795c516cf135dc3a0b5fb5ad0003c
7bec229183b1d7c4db03100936d45560c9c0813f6c13fbe3ac5f215e04b32094
9d2997210a1a3b8a87f557839d44a66180185fc47cae2bc93b209add0619b85e
49bb1d2b789241ba161a41566cf863185c51773cc2e64fda1047cb7c0e562d50
660db63cbeef254c26a647154c7b057b1906ad65d3d95696597f5a2e2e9e2e08

982c30a7783cc20c316d53e0b21cd50fb38445491237219a992c986063c913a2
54138600d3fb1cdeabb57a8d00b7d8a67f80c43c5b95cfe91b904c0bb1008dbe
7364518c41d476610d9c25f8f40f82b61f1d76f005048e84d1d52eebaa6aa997
4cd52a32df2e99b8be2204676b99496a915e89fc236f022b4bd86179cb0785cf
0455a293b2891a1525d2caf8167b28d3776d759110b0069933a0ba39dd773767
0b248f62d10fe7a8464f185674a1d495e20cba826dc512329e873efdf3bfd84e
fcad6f1a48eaeb6b015e4af591a4a7ef6109059795ad66e0254d089bd10595ae
c800fd0a69b586d779e4b21bbab53df82ea3b9614c7abd5c88d3dc9c37b2e4d6
80f2b2eb77f5f4ad8b450ca8cef537d361b130fb1fd5199301f0c75ac7a0861b
47525385713fc7fd6d15cda5b275cd0a26948759f5e9aac9eec2b53a0b634d87
3352962a59f05835697f6f376c443c1113e512c825cb2f74a2b436ec46199d9e
17544fe9da0144c03995cb2eca4c2a6ed8155847d88987bdc1d92584b687dbc4
d43bc64267e70c41ecc4de1a36d3353f1986343e836e1945ce9ffb373f41874c
cd23226808a4884a9c33938bab04ecf6e5f300a24f048c598cd35b17933a750d
84dfb1d345a11c706ea6b239594c00d110714792ea605e96d92bb9e6096c6f4f
4d7781f1ba4a55bb27ddd7719bc00a12c5b29d556369439dd112159f0833d36b
ad4672ae9e5304c4649126a932cea416bddf865fc1d54d49202dbc6c53592b40
da42911fa1b2ed0309eb016f262cf83e1c9dba298c7676d034cd2259f32f2fcd
5c2eb5bb1ad7637e95d3f9a48a34ca84fc39ead486c71dc34bae929f7f848831
91b992d1e6d06d5e535532ffb80e7d1a4a91b5f60da1c6cc792009c398f2774f
1e9e275769a8b2e692b2e83f0650628871a7253f3af1f4ecacb4dc0736e7034a
337169aede64e30a5c9baca172f1a24eba2dae19f7a3ba45b53634b6c5b535ad
83efd75574c148cb3c8b175ee4ad4cd992116523df26ce97808e403a21e07b04
e4bc5123a85ae23ae7f6de9ea1592196b29826ec9d4c2d56c33eaa2ec8ee31f4
514747a4a90a82a28e020de6610765a65eb17b1aa830ec6177635c617d61e34a
8dafa452bf5f5048dc52c1683c18fecdaffe9523c75d390effe407930f7f85e8
b4fb4b88bdfe8696036e969c99c5254ae1f7b6fb08b77e48c324cd6169b45b1a
ce5e471f81a24d25738350faaf78e9b8cc932b38ebd290defc521cd1ddb93ed8
2bae1507a683ce358029fddcdd421bc47e2e507b9a537c6b8a5e1c38f8b5ca23
2600b5e71e52fef021deb05a64f3636e170b2760b35e1586ff90c4d843fca207
56028831a634bfb79343052c82bd948102b570d7453071e64bad7a6b826c912c
11386e19322819ff4a1df2aadbbf46e134f0226a479f9382f5dd1d743b6a0fba
7f1b809897ded160f6d2e1a20f8d35bb379b306960c78da3c0ebb6ec9f1eb8e6
58a9c20c4907988f9dad774601d8ed67cc741790aa4c8d826c3de8e5d17b2fcf
11bce14d289df1a21c0e38653a3859f47140a767cba8297633de6c4d5143cadc
65bc9e2d537db5387ba8c26d2c1a3ff6036d344bb1ba752e252007c7e3b48546
663465856a1af08ad9857d06d44fa89f9733c5fc29230fc32e33b65e54bb855c
fee3266688115210e36c13f2b606b784fa1b1d49637da0d1a69db694d6ba92c8

880fb40e831520a8da92a094bced4092a45952c5c14ef0be4291056c30969ded
0ff4a18e446738277c04650271fb868901c3e7697cdbe1fe989687ecfc29df32
3bf02147cc6adcb05dfbfa2b38035a502d63ccd755fc75d3b84e906faaa6d8e0
073db53be155d3971f7528d1721aff831383ab069116fe6d1d0073c49721a415
e6e59fd682d1212c1b789365f92e5a5e778ca20f2d16440ec6f5b46ddb85d431
d2eccf40d80384b8074417ed6e81e0c0692dabe8517c2f6b379add8e0ad99f24
d81f4600afdc6cc7163c927652257d65473d3716dc40156629d7f391628db3c2
fed4a38bb5982ccbdcd576f36d5cc9b689225c0afd41b4df5fabd6f7fa2decb4
5b70ea2ff1001c9d8c67f0a3df3616d532563d22089b6f56911b81fef84803b1
c50e70faf8aad3f53da8304c5f91bd06c439ef2646bdfdae034ccd44293e12cc
3a22b7fc5a2898ac06725303965a8f56f72b14197e63bddbadad24f5ca5d3a45
250d464f867f99f3dc417c446569b7622da02cfad8ba4cece5bb479f94c1a3d3
617b1a6e3e16f9bd64ef0c3ddf6bbf57ac58ee0d3b6bd6cbffe6b209103995b4
c24af4b0fbeb4317ce9d56b7664a55975aea071583c77f8710a93d7fce3ed010
be04c5e38a1148f9c37a564699d79ec759c01d77826597c4254710c66ae1a42f
d85aae56f6b2d66f6a6b310277616cb151ad6758944f5672ca5b294222d63fd4
8472a12d6fcd977bf47158ea1ecd4ee503312dcf207f72a3bbb941c7f4408858
0e811008e01df70a8a91df197be220251b03e5ff6e09167777b798fc58fea199
12c5b3834d52e34525c8955c29c1ecff760a18f31206b201e5243dde5010e3fe

Correos electrónicos de donde son enviados los archivos adjunto con malware

BStoney@schmersal.com
intetsvar@regionh.dk
tberaia@giantilogistics.ge
sales@crimsonintl.com
Jessicaalba@emcure.com
gunter@efor.es
mueblesvirrey@intermobel.net
smcargo@fourstar.net.in
Info@ejet.com
enquiry@jnkindia.com
kfo@jydepejsen.dk
info@semshred.com
crm@aminequipments.com
jack.miller@chamundeshwari.com
rohit@axonoutsourcing.com
modial@globalnet.es
supply1@tsl-me.com

divakar@integraqatar.com
zguler@betalojistik.org
westrea@juno.com
camp2@alhajricorporation.com
tung.tran@scj.vn
ignacio.segovia@consorciogmq.com
ykato@omega-eng.co.jp
djaya@rpxholding.com
SRS0=7myhev=FZ=dhabicontracting.com=nadyfarahat@eigbox.net
estoquecba@altbrasil.com.br
structura.arhitectsef@csjbacau.ro
himakiran@rcy.com.sg
SRS0=IyY8fO=FZ=bividvietnam.com=thuy.nguyenthidiem@eigbox.net
sitisyou@infoaomori.ne.jp
thuylinh@pap.com.vn
huseyincaglayan@timboocafe.com
m.salman@market786.com.pk
susiec9@mailgw7.chrobinson.com
asbestoss28@mailgw7.chrobinson.com
tsiolkovsky@CHR1PR1EX72.chrobinson.com
nibbledxg276@CHR1PR1EX72.chrobinson.com
englishmenwpv5175@mailgw8.chrobinson.com
tertiaryz8@mailgw7.chrobinson.com
cs02@seaexpertgroup.com
muhasebe@teknommetal.com
murugan.eswer@alhabarigroup.com
stockcontrol@mfsgroup.co.zw
medicenter@medicenter.gr
distribution@perla.com.lb
suzuki@zenkokyo.or.jp
s-hirotsugu-kojima@tusui.jp
n.rosalyn@bageine.co.ug
brisa.castillo@ase-sinaloa.gob.mx
vanessa@frimaster.com.br
duongnt@hpmhanoi.com.vn
thuy.tran@smartsurvey.com.vn
dinardgolf@wanadoo.fr
stefan.cristea@intergameselect.com

georgian.stefan@eastwest.ro
ciro@sunsteel-srl.it
fbmanager@nagoya-mansion.com
Dea@scyachts.com
flozanop@enee.hn
ramona.trif@euro.ro
taj.7@tajcorporation.com
khizer@mail.pakgulf.com
zinmar.soe@dawn.com.mm
kudan@blueribbon.co.zw
melita.urban@zzjzosijek.hr
legal@sascco.com
rljones@processpi.com
junji-sayama@digitechnos.co.jp
amuteiwa@phidepots.co.zw
orion.zwe@bakhresa.com
adminlae@manogeneralservices.com
formalizacionbancaria@mosquerayricci.com
nantes@classcroute.com
whspm@forsan.com.sa
site@flamantvert.com
salmgrai@flyairindia.com.hk
SRS0=r7jXqZ=FZ=valleycollisioncenter.net=estimate3@eigbox.net
satinalma@soffiaks.com
secgen@fijev.org
bibi.hayat@fpapak.org
Simon@Wastewaterservices.com
SRS0=RgCi27=FZ=omni-filtration.com=RobErwin@eigbox.net
kialios@euronics.gr
p.vogiatzis@e-organotiki.gr
admin@nzautomation.com
stolz@stolzsa.com
me@vistar.vn
paul.vanderhulks@sjglobalinvestments.com
ravnatelj@os-fazana.tcloud.hr
enr@maquinariatn.es
info@studioapogeo.com
usuario@miempresa.com

asistente_toluca@grupolaresgoiti.com
stujan.eccleston@virgin.net
simon@plasthane.com
legal2@macndhlovu.com
bdm@icmpk.com
editor@madafu.biz
valentin.radu@ro.fso.ericsson.net
ngoctran@hoangphatcons.com
evancio.njowera@gyproc.co.zw
cangucu@transvidal.com.br
elson.silva@glomes.com.br
hue.tran@scj.vn
apinday@durexporta.com
jorgeheredia@aminco.com.ar
ventasinstitucional@industriasgenio.co
purchase@shahzadigroup.com
dayane@espacial.com.br
hr@harjaguna.com
abdullah@texpandy.com
cumplimiento@adepeshn.org
periodico@maxmedbh.com.br
nvhung@bht.vn
puertomaldonado@macropost.com.pe
bioglio@ptb.provincia.biella.it
chaku@ffa.co.zw
administracao@cadros.com.br
hung.nguyen@ikac.vn
financeiro.sor@piccolitransportes.com.br
bd@shreyapowercontrols.in
nomsa@tigmooeats.com
harun@faksfotokopi.com
steilmaquinas@agrosteil.com.br
Accountant@elcon-in.com
service@elcon-in.com
bomcontracting@gmail.com
getwell@kmchhospitals.com
info@flokelenterprises.com
ops@starocean.cn

purchase@everfreshuk.com

Direcciones IP de servidor SMTP donde es enviado el correo malicioso
34.224.226.104
23.106.223.74
45.137.22.58
172.241.27.109
185.222.57.216
185.222.57.250
45.11.19.69
154.127.53.116
104.47.32.55
45.88.76.19
81.22.97.52
81.22.97.56
64.136.47.15
121.240.21.112
113.61.110.39
184.107.72.134
219.99.208.168
202.158.48.236
66.96.186.10
201.76.49.235
82.77.1.11
118.201.183.130
66.96.185.1
201.76.49.217
66.96.187.8
66.96.185.5
66.96.185.4
201.76.49.125
201.76.49.234
66.96.184.3
189.126.112.117
202.216.97.10
103.254.14.171
81.22.97.55
110.93.216.93
182.183.170.203
159.213.46.250
69.16.230.96
217.116.195.40
37.49.225.154
41.190.32.8
46.226.193.113

23.83.212.25
211.13.204.73
211.13.204.69
211.13.204.71
180.222.84.253
202.158.48.237
158.255.46.94
187.141.164.225
199.201.89.32
210.245.86.42
210.245.95.168
193.252.22.211
89.111.63.34
5.2.183.109
62.149.156.48
101.50.2.87
45.137.22.136
181.210.30.228
149.202.26.4
202.63.193.60
115.186.188.156
162.144.89.19
79.110.52.80
41.79.28.6
108.166.43.79
204.12.102.37
114.179.24.146
146.20.161.126
136.0.111.34
146.20.161.127
146.20.161.122
184.106.54.100
184.106.54.103
184.106.54.99
202.1.207.3
195.68.98.212
212.118.123.8
151.80.83.89
199.193.202.43
66.96.185.8
78.135.79.21
94.231.106.230
178.63.179.254
72.18.137.99
185.78.221.99
46.105.49.92

49.236.208.86
104.247.72.74
141.136.57.17
51.77.245.79
192.185.70.14
192.185.51.139
192.185.179.30
80.0.253.75
23.233.128.31
188.121.43.194
192.185.45.175
192.185.47.206
198.147.25.114
194.102.93.7
45.117.170.227
197.211.215.18
147.135.97.58
187.73.32.147
192.185.50.161
74.220.209.114
181.143.117.62
192.185.47.65
162.144.70.207
103.7.8.218
69.89.30.156
192.185.151.58
192.185.63.14
192.185.51.35
192.185.145.122
103.15.48.235
77.242.176.250
189.113.8.82
103.45.236.12
189.126.112.42
199.250.216.146
192.206.5.175
78.142.210.230
107.191.39.183
185.222.57.189
45.82.178.31
185.222.57.87

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	187.1.57.178
14.161.111.153	187.111.54.189
14.248.108.145	187.8.226.10
45.164.201.107	187.85.210.57
45.165.215.168	187.87.1.87
45.179.191.155	187.87.14.204
45.238.121.129	187.87.8.251
60.171.100.234	187.94.84.242
61.148.196.114	187.95.59.45
62.193.129.232	188.92.209.217
89.211.154.215	188.92.213.91
89.231.138.202	189.114.67.213
103.213.194.230	189.41.247.50
111.224.167.249	189.51.103.125
168.205.109.229	189.90.208.196
168.205.111.185	189.90.209.114
177.126.200.103	189.91.4.148
177.154.226.242	189.91.4.205
177.154.238.159	190.109.43.107
177.184.245.115	190.109.43.151
179.125.118.189	190.181.108.45
186.124.218.116	190.181.109.13
186.179.100.229	190.80.159.182
186.250.203.222	191.102.120.50
189.126.169.171	191.53.195.93
200.152.107.158	191.53.196.215
213.108.162.209	191.53.220.221
222.185.243.130	191.53.220.237
102.23.227.61	191.53.220.255

103.198.10.194	191.53.221.13
103.198.80.88	191.53.237.0
103.237.57.254	191.53.237.51
103.25.134.143	191.53.238.165
103.53.113.78	191.53.52.232
103.89.90.115	191.7.116.16
106.5.58.88	193.56.28.190
108.51.98.116	196.52.107.216
109.175.11.143	197.237.161.58
109.224.12.58	198.36.30.144
111.224.53.125	199.192.16.253
112.253.33.14	200.206.16.105
114.100.48.187	200.66.113.3
114.111.195.34	201.247.40.170
118.127.122.67	201.247.47.246
121.150.28.217	201.55.159.114
123.146.82.68	201.55.159.25
123.20.63.12	201.62.66.106
138.36.200.179	209.42.78.84
138.36.201.159	210.16.88.219
138.97.92.107	211.181.193.2
14.177.60.53	211.198.60.22
141.98.80.87	212.181.80.144
143.208.248.53	212.244.23.161
143.208.249.57	212.244.23.165
151.80.237.221	212.69.17.195
154.127.39.2	213.92.204.228
167.250.190.46	221.210.80.136
167.250.96.31	27.14.211.95
167.250.98.0	27.66.125.55
170.239.138.95	31.170.53.48
170.246.61.165	31.170.61.98
170.80.204.89	37.49.225.185
171.228.164.11	37.49.225.204
171.240.34.95	37.49.225.208
171.35.170.152	37.49.225.209
171.38.71.240	37.49.225.21
177.10.241.117	37.99.251.98

177.128.122.75	37.99.252.137
177.154.238.47	39.72.60.136
177.154.238.84	45.160.138.59
177.21.213.213	45.162.21.203
177.37.198.241	45.165.213.98
177.52.74.137	45.165.214.80
177.85.130.114	45.169.17.246
177.92.244.247	45.181.30.165
178.156.67.181	45.181.30.226
178.219.120.63	45.181.31.52
178.32.144.167	45.224.161.62
179.124.19.158	45.4.169.61
179.189.197.35	45.4.170.82
179.243.53.222	49.130.26.194
179.97.10.51	49.130.68.133
179.97.9.20	49.130.97.105
180.109.39.7	5.239.15.162
185.129.113.35	72.11.135.222
185.235.165.42	77.153.210.44
185.235.165.77	78.128.113.66
186.216.156.31	78.128.113.67
186.216.68.126	78.8.189.103
186.216.70.145	79.9.176.106
186.216.70.223	79.97.177.78
186.224.248.87	82.202.65.70
186.249.85.207	84.22.36.53
91.83.160.181	91.148.68.194
91.83.160.199	91.245.30.79

Actualidad

Ciberconsejos de protección ante ataques de Fuerza Bruta

Las contraseñas que utilizamos en los distintos sitios web son un atractivo para los ciberdelincuentes, ya que gracias a ellas pueden acceder a información personal, bancaria u obtener datos importantes. Y para conseguir las claves, los atacantes utilizan una técnica conocida como ataque de Fuerza Bruta. A continuación, te explicamos cómo protegerse.

Ver más: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-de-proteccion-ante-ataques-de-fuerza-bruta/

Investigación

Troyanos al descubierto: Características, análisis y prevención

La actual edición 25 de Análisis de Amenazas Cibernéticas estuvo a cargo de Elsa Bravo Arellano, especialista senior en ciberseguridad del Banco de Chile y miembro de las comunidades chilenas de hackers Party Hack y Hackada, esta última la cual reúne únicamente a mujeres que contribuye con conocimiento y orientación en temas de ciberseguridad a potenciar y empoderar a otras mujeres.

En el transcurso de la presente investigación —"Troyanos al descubierto"— la autora presenta cómo funciona este tipo de malware, los métodos de infección y algunos consejos sobre cómo protegerse. Su intención es principalmente que este conocimiento sirva a las personas para estar atentos y no realizar acciones riesgosas que comprometan la seguridad, tanto de sus entornos personales como de empresa. Todo lo que se describe a continuación es con fines educativos, advierte Bravo.

Se revisa, por tanto, la forma de infección con un troyano y cómo se aprecia esta desde el equipo del atacante. Las muestras son analizadas en un sandbox gratuito. Esto para revisar también cómo son detectadas estas muestras, y como, en la medida en que se utilizan métodos de cifrado y compresión, el malware se hace menos detectable por los motores de antivirus.

Ver más: https://www.csirt.gob.cl/reportes/troyanos-al-descubierto-caracteristicas-analisis-y-prevencion/

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.

- Nicolás Aguilera
- Claudio Valderrama
- Francisco Sariego
- Alberto Corrales

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.12.24 11:26:54 -03'00'