29-10-2020 | Año 2 | N°69

Boletín de Seguridad Cibernética

Semana del 22 al 28 de Octubre de 2020

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

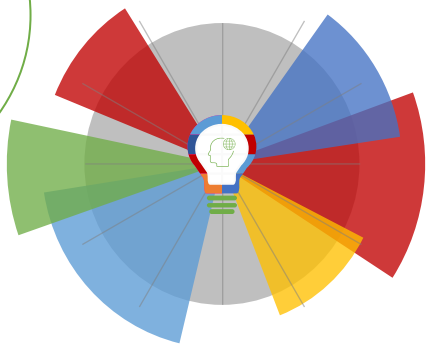
División de Redes y Seguridad Informática.
Gobierno de Chile

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Resumen de la semana en cifras

Hash
102
Sha 256
Asociadas a múltiples campañas de phishing son archivos que contienen malware

Se advirtieron
10
URLs
Asociadas a sitios fraudulentos y múltiples campañas de phishing y malware



Parches
40
para vulnerabilidades
Windows, VMWare, Mozilla, Samba y Google

IPs
213
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

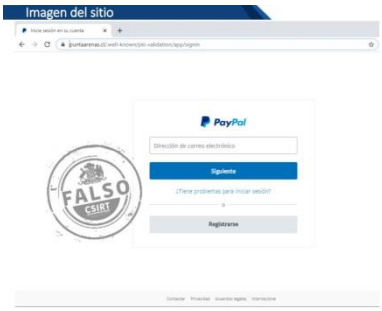
Imagen del sitio

CSIRT advierte sobre sitio que suplanta web de pagos en línea	
Alerta de seguridad cibernética	8FFR20-00807-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Octubre de 2020
Última revisión	24 de Octubre de 2020
Indicadores de compromiso	
URL	
http[:]//amormisericordioso[.]cl/PAYPALINFO	
IP	
162[.]214[.]115[.]150	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00807-01/	
https://www.csirt.gob.cl/media/2020/10/8FFR20-00807-01.pdf	

Imagen del sitio

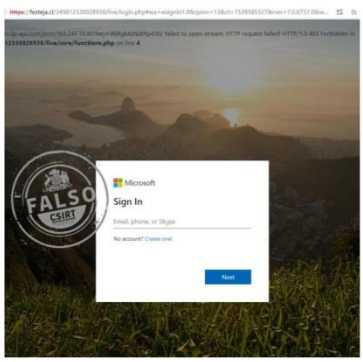
CSIRT advierte de portal que suplanta acceso de sitio web	
Alerta de seguridad cibernética	8FFR20-00808-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Octubre de 2020
Última revisión	24 de Octubre de 2020
Indicadores de compromiso	
URL	
http[:]//www[.]elvecinito[.]cl/of/1ive[.]com/	
IP	
162[.]241[.]2[.]177	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00808-01/	
https://www.csirt.gob.cl/media/2020/10/8FFR20-00808-01.pdf	

CSIRT advierte de web que suplanta a sitio de envíos	
Alerta de seguridad cibernética	8FFR20-00809-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Octubre de 2020
Última revisión	24 de Octubre de 2020
Indicadores de compromiso	
URL	
http[:]//chivasgrillconcepcion[.]cl/dh//DHLAUTO/dhl[.]php?rand=13InboxLighta spxn.1774256418	
IP	
190[.]107[.]177[.]249	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00809-01/	
https://www.csirt.gob.cl/media/2020/10/8FFR20-00809-01.pdf	



CSIRT advierte de sitio de pagos on line fraudulento	
Alerta de seguridad cibernética	8FFR20-00810-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Octubre de 2020
Última revisión	26 de Octubre de 2020
Indicadores de compromiso	
URL	
https://puntaarenas.cl/.well-known/pki-validation/	
IP	
200.91.27.21	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00810-01/	
https://www.csirt.gob.cl/media/2020/10/8FFR20-00810-01.pdf	

Imagen del sitio



CSIRT advierte de portal que suplanta al acceso de sitio web de cuenta de correo electrónico	
Alerta de seguridad cibernética	8FFR20-00811-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Octubre de 2020
Última revisión	26 de Octubre de 2020
Indicadores de compromiso	
URL	
http[:]//festeja[.]cl/349812330928938/live/login.php	
IP	
131.72.237.67	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00811-01/	
https://www.csirt.gob.cl/media/2020/10/8FFR20-00811-01.pdf	

Imagen del sitio

CSIRT advierte de sitio de suplantación bancario	
Alerta de seguridad cibernética	8FFR20-00812-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Octubre de 2020
Última revisión	26 de Octubre de 2020
Indicadores de compromiso	
URL	
http[://]banca-enlinea[.]cl/scotiabank/	
IP	
201[.]148[.]104[.]65	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00812-01/	
https://www.csirt.gob.cl/media/2020/10/8FFR20-00812-01.pdf	

Imagen del sitio

CSIRT advierte de sitio de suplantación de popular red social	
Alerta de seguridad cibernética	8FFR20-00813-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Octubre de 2020
Última revisión	28 de Octubre de 2020
Indicadores de compromiso	
URL	
http[:]//ac-62696748[.]bidsolutions[.]cl/nextVRF[.]html?location=a1604b9aec6d3ac8c9ff1f8474f08774	
IP	
162[.]241[.]37[.]210	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00813-01/	
https://www.csirt.gob.cl/media/2020/10/8FFR20-00813-01-1.pdf	

Imagen del sitio

CSIRT advierte de sitio que suplanta a web de salud extranjero	
Alerta de seguridad cibernética	8FFR20-00814-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de Octubre de 2020
Última revisión	20 de Octubre de 2020
Indicadores de compromiso	
URL	
https[:]//hhs[.]gov[.]procurement[.]auth[.]atacamalex[.]cl/auth/login[.]html	
IP	
99[.]198[.]101[.]234	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00814-01/	
https://www.csirt.gob.cl/media/2020/10/8FFR20-00814-01.pdf	

Phishing

CSIRT advierte de phishing por bloqueo de tarjeta de crédito	
Alerta de seguridad cibernética	8FPH20-00320-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Octubre de 2020
Última revisión	29 de Octubre de 2020
Indicadores de compromiso	
URL	
http[:]//cetpline[.]com/Activacion/cuenta-lthk/	
https[:]//valpanet[.]com/xtremera/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[45.236.129.38]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00320-01/	
https://www.csirt.gob.cl/media/2020/10/8FPH20-00320-01.pdf	

Vulnerabilidades

CSIRT comparte mitigaciones obtenidas de Microsoft para Windows y Visual Studio Code	
Alerta de seguridad cibernética	9VSA20-00303-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Octubre de 2020
Última revisión	22 de Octubre de 2020
CVE	
CVE-2020-17022 - CVE-2020-17023	
Fabricante	
Microsoft	
Productos afectados	
Windows 10 versión 1709 para sistemas 32-bit Windows 10 versión 1709 para sistemas ARM64-based Windows 10 versión 1709 para sistemas x64-based Windows 10 versión 1803 para sistemas 32-bit Windows 10 versión 1803 para sistemas ARM64-based Windows 10 versión 1803 para sistemas x64-based Windows 10 versión 1809 para sistemas 32-bit Windows 10 versión 1809 para sistemas ARM64-based Windows 10 versión 1809 para sistemas x64-based Windows 10 versión 1903 para sistemas 32-bit Windows 10 versión 1903 para sistemas ARM64-based Windows 10 versión 1903 para sistemas x64-based Windows 10 versión 1909 para sistemas ARM64-based Windows 10 versión 1909 para sistemas x64-based Windows 10 versión 2004 para sistemas 32-bit Windows 10 versión 2004 para sistemas ARM64-based Windows 10 versión 2004 para sistemas x64-based	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00309-01/	
https://www.csirt.gob.cl/media/2020/10/9VSA20-00309-01.pdf	

CSIRT comparte actualizaciones obtenidas de VMware	
Alerta de seguridad cibernética	9VSA20-00304-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Octubre de 2020
Última revisión	22 de Octubre de 2020
CVE	
CVE-2020-3981 - CVE-2020-3982 - CVE-2020-3992 CVE-2020-3993 - CVE-2020-3994 - CVE-2020-3995	
Fabricante	
VMware	
Productos afectados	
VMware ESXi versiones 7.0, 6.7 y 6.5. VMware Cloud Foundation (ESXi) versiones 4.x y 3.x.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00310-01/	
https://www.csirt.gob.cl/media/2020/10/9VSA20-00310-01.pdf	

CSIRT comparte actualizaciones obtenidas de Mozilla	
Alerta de seguridad cibernética	9VSA20-00311-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Octubre de 2020
Última revisión	26 de Octubre de 2020
CVE	
CVE-2020-15675 - CVE-2020-15676 - CVE-2020-15677 CVE-2020-15678 - CVE-2020-15673 - CVE-2020-15674 CVE-2020-15969 - CVE-2020-15254 - CVE-2020-15680 CVE-2020-15681 - CVE-2020-15682 - CVE-2020-15683 CVE-2020-15684	
Fabricante	
Mozilla	
Productos afectados	
Explorador web Mozilla Firefox. Actualizar a la versión 78.3 de Mozilla Firefox ESR. Cliente de correo Mozilla Thunderbird.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00311-01/	
https://www.csirt.gob.cl/media/2020/10/9VSA20-00311-01.pdf	

CSIRT comparte actualizaciones obtenidas de Google para Chrome	
Alerta de seguridad cibernética	9VSA20-00312-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Octubre de 2020
Última revisión	26 de Octubre de 2020
CVE	
CVE-2020-15993 - CVE-2020-13871 - CVE-2020-15994 CVE-2020-15995 - CVE-2020-15996 - CVE-2020-15997 CVE-2020-15998 - CVE-2020-16000 - CVE-2020-16001 CVE-2020-16002 - CVE-2020-15999 - CVE-2020-16003	
Fabricante	
Google	
Productos afectados	
Google Chrome versiones anteriores a la 85.0.4183.121.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00312-01/	
https://www.csirt.gob.cl/media/2020/10/9VSA20-00312-01.pdf	

CSIRT comparte actualizaciones obtenida de Samba	
Alerta de seguridad cibernética	9VSA20-00307-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Octubre de 2020
Última revisión	29 de Octubre de 2020
CVE	
CVE-2020-14318 - CVE-2020-14323 - CVE-2020-14383 CVE-2020-10730 - CVE-2020-10745 - CVE-2020-10760 CVE-2020-14303	
Fabricante	
Samba	
Productos afectados	
Explorador web Mozilla Firefox.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00313-01/	
https://www.csirt.gob.cl/media/2020/10/9VSA20-00313-01.pdf	

Indicadores Compromisos

Se comparte a continuación el listado de IPs que fueron detectadas durante la semana pasada por el Equipo del CSIRT intentando ejecutar escaneos de 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)
020c4c5ec77f2397cbe6dcd0c0b9b7c8359b33e488d5d90d34072105f9dfccde
50bba578b7f1c0891c3103f10f15962974f23552a42e0494caa2a405eb48ef2d
a56716bb821cec6e73598f031e0c0600419391626088398fccc2b411af49c62
d9f7e4ed5fd5310ffb109882b91f1d776c3fa1277692a8a5803ca593856eba67
7e410d1fafaea1366356e7c1508d7ca25c84d60944aca09a2cb782bd3a77800b
74bb469bc2970d9c977de84177c8f97cf95b8bbe35cceddd9743ad50bbf05d34
ef325d7dfb28bfd2b7cc344a890502ac41582a49511edbc612392ceee5613bc4
5542c37ee5faeeea86b317db009b24a38f581860e468db0ae1d61b0850aa3463
73ec8c19dee20cdb22bfcbbb69af46b2793ac339206e86714bc0a05142f77b3c
61c236b3335da67d5ce186d5ea15068dfb751357b115f9002a3627f7e801013e
66bec951e026a392e0adfc69b614a9ef4e22bad0ed2bf7b99ea2c1a3a83800ef
7b49b43e3ba684119491279e4899a1685e71d8a9c2cf8cad40623ce9b17cb974
9e61f8e3adea7c7d90d06a028415b58475a5224bfabdde4955e82646eb9d6735
ad10b386d964b6056e529c2bdb70ccb19ba21b3b0a59ac606113fedc49626b81
c4576ef3b6d4f5bc1728a25cfce9f3574e9fa60a5f6aa8874a625255ae74deec
ed51269c3602786ff6ddef3a808d8178d26e4e5960f4ac7af765e4bd642128dd
6793bb2d87fdd82f3f3be7463704436bae5b6dd4c0f25b34d2da3caf0ec5548a
fc1b6ab8e7c3ccf173d0bc6d16116aac495b7f348ce2744164028f6dbb76576d
b47fd0ecc1650de120a1cea2fdaccafaa095d11c14fcf6fed8d54b63ca86fc00
4c93e3f5f2284ba00c90f868322678a4639d2cdaba64affbb88860796fb52241
c639ec18eb060e72b5377a99575d50eaf280703d4d8027c1e133c13aeb663507
d94833fa6c0671d510dd2f44d2cc25c3dff5eda7cf98e160177008d91d093210
905947361d899803ce2a950532c96a566894299116eb264d5efe86df0db596f8
cf639b43ae88211e385838a6a9323afc70149af496ffde9255dae43f8bd11da3
be84537bcc865e8a7b57e55d6755d97f920fac9c0ead75706c64888a8a39de8b
20557abb7e18f9b4d279a25980e9858441be3f6198b35eca3d9f537a706a9760
642139f4b297a7c0f5aaf7dcf848d68e15acea73035637eb22188afb9a92513c
09b8d65b64218ad504489c3b2bc0e3cd74300774ddc3e908c0628f95234fc3be
3f0adda973b6cd3223fa0d4c21c9af228f0db125a0ed255cae4fc949664d7ee6
e13e1b5db38b6d366f7ab841db3b6a383d28d78df1fbcdba3754178064563746
bd3531875b303e0395178fb8d3aa3dedabada2cb53d5b937c2d75d18aebd1ccd
1b6052882a685f2b15ca328318000329551b02dc7e44e231223671e4763165e1

6c1df8bf751a607c2ca0d6f1455aa3318f8ce8644d6e0998847c292438cd7db0
e895c7a1014ab6e9d57b711022b94f17023499b324506905016ce082116e1ee9
9b99d468b6dcb5431a52fd59d05e5984dc4718501c806681668cf3d8a2dcb599
acf8f0958861f638caf265028426240804d2c3d90bfd008fad6a1b5a937f42a1
1f6b1ea621fb46aa988a87540edd2bf95cf79547b2f8e16f40ff22d3ba862e8e
2504bfe6f4638ca673793d5db9c066cdd99e889e351c575fdff4b20dccdf228e
90d7c48b4b9e02a2abbc448e9cc410d5bbf87e8280c47699e6a3654c4555c2f0
b1cd111d50c59c23649c48b00542530a7bcff88b6392a887860a99baac1c75be
35efa253e3dac2aa85604541651aa8ba6424fab68fb76962bf33eb787584ad58
d37e36ccf1d1d6305c792cf1fa6646b2ea51b0caab3d7c9c5b26e852d14c0b89
665ea7994646d6f55327063f07c46e3d51cce78766dc14fc03031b5581283b10
f22f6b796d73cadef21281fb4120d425395b7c6457e38524dde128830ccfc02d
76ec500ee8ac08b386df3fba782437637ef36d46c8b0082ce152cdd7bed864e3
aa5e7414db596bbbac651408e85b19557a2415a2e42a4a2689cf37c1f3dc1c10
14a231cb5f18f89a77a9267b2f7907a57258406d712c3795e5608bf04f702865
283e6d40d0814da95cb0ec7fe6dc4e4ccdfa1dcaaaf61646c01bc0f0250d62b1
88b6d8de1eefcb2999565bd62061ab7a92c0aa565784b6b2f45e8f1d90f5f10e
2373e849718b4f729d4cc542754b76cc7701b468389795a9e9cf7286135f6d17
d6a6701bc63354fa0f34492bdbe6c22bfee5f624d5714b329a8795508ff5b6e4
2ca941346e2ed5e72b8dfc5b700d4c93e0664d32d3b883853d13d8d6a8f8b55a
8b528ffc8ad5402c0f7d33d8523210015ebc1c326c8694ce27e1f13ab28ceb98
4dd9ccbc69cc0fb1602f98fdca26e4640438a65c18e5810ffdc62cba2a636879
cb2de094d6518308daefaa75867659fdee298e4a0617b473ce48c4dcdea085de
bd17ceae08c87f45c042d5893ecd4547b333d49f07e732df28e2000b4b52c46b
f9d2d23fc1bc25ae778e7b8d25a8a846518eacb6f9700b37becb36162b59f6be
8ec484a33a9d6faa812349834788233eb6831589c4190ec8431302da9c9e0757
716c112ebcee979e93345ccc79914c4b31d6067f2473cfddda1f8d265d479065
f3d5aa54e6cfd95c252d912cbfe86be874ce87133282c24af39ac90e46dfc3f3
c70212938d5d4390ba1af7a40fbc16bfe9632cfee0a075e88b4c98a80a3e0c54
e16ff7cfe983a96aa9baabd56c3f8ee53b910bfbcd8c69c062417cfad241e2dd
12aa0b900bd3625b019741d028ec231a4d10c73a0c34aec9fbd07ded33d1df4d
83d5e426acb354f79d4d34753eb72ca59aaa11a64226334ade780226e22a8df1
48a6948505d42f70d05ebe07c311c91dd6ade0cd6ff091c0fae441e82ae57126
4099625585c58edcd07383d898ca0e64e51e6a7751c4b45cf9a52c02cf51c1a9
5da940231b1ebc70e4c974d89da825e72365c081f4b224b0308a7298de66a788
9b1645995b3ff4a25c04f9960fc1d46a55ac23288f5aae592833bacbc8b32d7e
c86d1109c5d349eb65a1d297477a57d75044168dfaa0dd9b40086b9fefac2a8e
e1fa5d543e2d0cc2a52a1af4c34bcd3b5f4ca62e72366ba657d1481307dcff90
1beec5bb24132a128d8578e0a58f3f03deebe026ca66c2066aa03d598ce48959
8154fc4456265f75835be9f6565d293b78fd9ef0f7a5002acc2a0e2dbcb60779
c52d7a70e6ae1edec10a02951f1668f6442e8837619245733d206aa4f669bb2f

28abcf40bb9189d3f74104c3b778daf9a8ab6ff7619774bb2e5e8cba8f1a52b8
8ff6258aa02f76f35f8a2a22164c938e0c28b2b8b906c2e1530d70d2675ce356
9bb6387f29a3a1d92ee730451d52759023a12968fc6c36ab729002d89d085318
941dc42e68ed58a3e797724f248c30d20e035734f6e3193a1e0c39b5ee751512
1029a93c4312651001128b1973e428ac1a6de1dd4b3ed70391fa7f308743abbb
3d531db12abce6a6b59476d4c5816866bed03126306e1c2042a0406618ec2653
7cd5248f6eed960168d2898ffde985d947702c9dc04b50d021161ffbed128e95
51145b793e4c1d8c57e52b53e8301cdb86d9ca5f64e055be118a4f00fb138433
155199a6a7f65483449db4bfcae3985bccf5be64145b1afcc201ba77e6940f50
f9a91d272a070ab3d9adf00c68d2e993cb62d8f33046195ea638cf887b19a7ae
ad588eaa915b7d4dcfdf7b26676ad8ab591db9fba7252d22b3b211cd0cf8dbe1
184579c65c05ec7ef55ae9dce95a34f32b2089bbd035c06a398c7551379117cd
d2d159ebded0bf1265e6d5504c604640a052723ba24cd4893266b03659b569c1
5889f2806952698235cfc4c29fcaec44f4f9bf6aab0dac87de568fc928e6665c
32fecc60c5ad5628caed3644dcff3a29ba6a97fa44cf37911169801f1dd79738
73d3fff5800c071f5250a4aede30e51c32ffe2d5d963da3336c439c795e4233f
9e29ec412872484ab6b0a14d625d6bc7ff0f5205ee410912e6cd2abd82cf4b6c
e7685f0f198129a74f92f5da4d49f1dfbc7d8e726c2ad293428a757a0c2dda86
a6a7e5b85f48751b8fff1a7bf44cc4e8ec3590a252fa93fde41b1cebffe7adde
2ce0b1b64893c2e1bc8708ef881ff4d10eecb5ca1599b25d67e7f20f9cf64eb8
5579980d54ae224a98b4821bcade4d6ae831f02a98d71113574af4a307c7c736
d0f4e7dc356c7d37666d84595bf2a5f6b16ad92b9858b4e921534269d460d1bd
0a2dc11d95176b9aaf5668ba60308fb823187e808fb7955b9483459e7dcb7dac
3a42d565cc18af8b48926bccb2b06179f7e6210c0e2cfe4e313c2bb86f81e682
eb7342e956ea7f0a234e89063bf36cbdb9e2bf4d6478141379a0eaf2efaf711f
a4d1178f3a923b023599d331b6772e92a0728644f27f4ad372f74a28b6a5a096
e225005a6da2c501109a5d73599e7697179f449c42e91f675b4fcb81e49bda29
e33834d79ac6b183fe39b1f2f93348871be890c7b6cbf93bc10ad438c003a068
95d417c5e1d71c30625a95f40fb7d368da11fb8052ed9cf36b2e811f6200846f

Archivos reportados (se recomienda mantener en monitoreo)

162.241.156.197	45.56.111.158	186.202.7.192
89.161.168.9	201.76.49.161	186.202.7.191
186.202.7.183	201.76.49.99	186.202.7.189
186.202.7.182	201.149.15.150	186.202.7.188
200.41.76.132	201.221.252.197	186.202.7.186
103.195.31.205	169.1.24.205	186.202.7.185
186.202.7.180	201.76.49.181	125.234.100.97
186.202.7.179	189.126.112.48	77.78.95.8
194.187.193.118	186.202.7.168	210.172.87.226
113.61.110.39	186.202.7.167	139.138.33.22
72.249.49.223	179.49.120.4	87.118.110.6
186.202.7.177	200.85.158.17	200.25.214.139
186.202.7.176	189.126.112.66	196.11.146.229
58.137.249.55	189.126.112.5	196.11.146.231
195.167.195.190	201.76.49.171	179.127.61.82
186.202.7.174	58.137.254.25	160.119.248.33
186.202.7.173	201.55.56.216	190.210.186.130
201.76.49.64	200.147.34.187	45.126.133.29
201.130.73.235	186.202.7.165	103.239.139.219
52.193.27.110	186.202.7.164	91.90.195.75
203.146.58.25	77.242.176.250	222.165.180.108
87.26.7.173	65.60.53.2	62.149.156.135
94.103.141.82	200.147.32.46	105.187.200.242
185.210.218.116	186.202.7.243	185.138.42.100
200.68.105.191	186.202.7.242	49.236.208.86
113.20.90.118	52.3.166.93	58.137.254.25
162.221.186.245	201.76.49.94	200.189.1.85
101.102.238.150	186.202.7.240	37.220.100.154
162.214.110.181	186.202.7.239	66.96.184.6
61.100.7.39	200.147.32.42	103.3.178.117
189.126.112.51	200.147.34.64	203.124.39.170
201.76.49.229	200.147.32.141	201.76.49.107
189.126.112.42	200.147.34.185	189.113.8.80
201.76.49.87	189.126.112.199	194.244.46.21
58.137.255.125	189.39.29.170	201.76.49.172
185.99.123.99	186.202.7.237	94.103.141.81
110.50.207.200	186.202.7.236	200.152.40.96
203.177.252.48	186.202.7.234	201.76.49.213
189.126.112.200	186.202.7.233	62.149.156.135
189.126.112.9	186.202.7.231	104.47.41.53

189.126.112.67	186.202.7.230	202.39.59.158
200.147.34.45	186.202.7.228	49.249.224.212
200.147.33.240	186.202.7.227	108.179.220.149
201.76.49.143	186.202.7.225	200.6.112.44
189.126.112.28	186.202.7.224	41.221.32.195
201.76.49.118	186.202.7.222	201.76.49.7
201.76.49.61	186.202.7.221	201.76.49.246
189.126.112.23	186.202.7.219	189.50.16.22
201.76.49.241	186.202.7.218	189.126.112.63
189.126.112.53	186.202.7.216	158.255.47.178
189.126.112.3	186.202.7.215	77.242.176.250
201.76.49.198	200.107.202.40	185.104.182.48
201.76.49.119	186.202.7.213	185.22.110.248
201.76.49.228	186.202.7.212	212.227.126.187
203.146.237.187	186.202.7.210	194.63.239.113
189.126.112.65	186.202.7.209	222.165.180.108
201.76.49.148	186.202.7.207	5.79.95.35
186.202.7.171	186.202.7.206	91.212.23.32
186.202.7.170	178.23.78.56	5.149.182.43
194.244.46.112	186.202.7.204	69.10.34.98
103.252.254.47	186.202.7.203	94.126.171.188
146.20.161.78	186.202.7.201	195.22.10.226
200.147.32.40	186.202.7.200	194.187.193.118
200.147.35.72	186.202.7.198	195.167.195.190
200.147.35.74	186.202.7.197	203.124.39.170
200.107.200.16	186.202.7.195	195.167.195.169
201.76.49.182	186.202.7.194	195.167.195.185
213.142.130.73	72.249.49.223	119.82.73.28

Correos electrónicos

xiubin_shen@avc.co	compras@triospuma.com.br
accountsfinance@findhorn.org	gustavo.pereira@preamarbr.com.br
arun.natarajan@pff-group.com	sac@innovapharma.com
m.kosowski@smlogistic.net	enfermagem@nutriex.com.br
finances@transfopam.com	maria@telelog.gr
Purchasing@subli-sport.com.cn	linh-bt@saigonco-op.com.vn
xiubin_shen@avc.co	pavolka@alustav.sk
faturamento2@redeforte.com	i_maruyama@intermarine.co.jp
jefeadmvalledupar@yupi.com.co	rose.le@kyungseung.com
ddg_herdiana@kiselgroup.com	headoffice@aa-namibia.com
acouprie@piveteau-immo.fr	mlayedra@zenix.com.ec
hue.tran@scj.vn	jacodejager@vodamail.co.za
info@brightwell.lk	ncaqua@vodamail.co.za
thanaporn_v@srikrungbroker.co.th	jackson.rodrigues@multicobra.com.br
marina.doreau@bouscasse.fr	ekhokhong@joemorolong.gov.za
asistentedtocali@yupi.com.co	wilawan_s@srikrungbroker.co.th
celia.santos@cordeiromaquinas.com.br	dsabetta@dsagroargentina.com
seguros@toyotacoacalco.com.mx	info@telelog.gr
thin@g-fac.jp	admfaktur.hondabks@nusantara-group.com
info@ortosi.com	ak@foxpetroleum.net
bruxelles1@troc.com	info@cigsweb.com
liliana.duta@cmeb.com.ro	pattm@juliusandcreasy.lk
jjlovera@premieriluminacion.com.ar	m.mariniello@ambraenergie.it
biomedsolutions@kidanet.net.fj	a.okgansbaai@telkomsa.net
christopherrendon@grupofame.com	info@interhealth.gr
hiroaki-t@wakou-co.net	me@vistar.vn
flavia@monacoes.com.br	numpon_s@srikrungbroker.co.th
hryun@cmship.co.kr	atupe@cdlnet.com.br
pedro@okacont.com.br	kyriakos@interscala.com
tacocean@loxinfo.co.th	SRS0=pMFuZr=ED=grupovenado.com=ernestoaliaga @eigbox.net
preshenc@trisolar.co.za	kasem.k@asa.co.th
ya-matsumoto@saegusa-pat.co.jp	fahad.baig@aasenterprises.com.pk
jflumangaya@wyntron.com.ph	suprimentos@viafertil.com.br
marcas.famosas@uol.com.br	bruna.melo@dnr.com.br
samuel.azevedo@tye.com.br	administracao@cadros.com.br
postmaster@lapiramidesrl.it	gianna@lapiramidesrl.it
trangptn@daiphuc.com.vn	projetos@timejardimdasperdizes.com.br
rafael.silva@vonex.com.br	lucia.hoffmann@dataprev.gov.br
cler.mazon@ulsanhyundai.com.br	operacao@segbemlog.com.br

rachmat_kurnia@ptkut.co.id	montesantangelo@tecnecosrl.com
proveedores@triler.com	administracion@paymar.com.mx
gerenciaadm.financeira@angelsvigilancia.com.br	factory@popsmile.com.tw
daniela@contrifiad.ec	ops1@rosemoore.co.in
Rafael.matos@botelhomesquita.adv.br	eng.mhd-alhalwani@future-electric.co
credi-nissan@legaxxi.com	rfouilloux@vannichile.cl
margarita.cenci@betco.com.pa	godlisteneliona@norplan.co.tz
elsie@daisec.co.za	fiscal.filial1@hbbcontabilidade.com.br
carlos.schmidt@fribal.com.br	gislene.noleto@amecconstrutora.com.br
carteracali@yupi.com.co	matheusl@colomboagroindustria.com.br
ventas@apinter.com.ar	adm@timejardimdasperdizes.com.br
comercial@suplayinc.com	lina@krishibidgroup.com
wesley.santos@galvorada.com	vanzari2@citgrup.ro
junpen_y@srikrungbroker.co.th	comptabilite@hotel-madrague.com
16gbb4@polmil.sp.gov.br	oscarchicharro@duoharinero.com
cotacao@gruponutricare.com.br	mail@dide.mes.sch.gr
vendas1@colomarti.com.br	roy@digitaladvertisershub.com
anag.coggiola@ptb.provincia.biella.it	proiecte@primariacurteadearges.ro
inbound.isb@amllogistics.com	valerie.lozano@montgiscard.com
compras1@solabcientifica.com.br	marija.spasovska@investnorthmacedonia.gov.mk
anderson@sampaiotem.com.br	manuel.martins@costasoliveira.com
rafael@tbi.com.br	rosa.pombo@apeci.org.pt
admvo.ph@legaxxi.com	vasanth.k@tigerlogistics.in
muhasebe@guveclokantasi.com	

Actualidad

Ciberguía de mediación parental

Navegar por internet e ingresar a las distintas apps puede ser muy atractivo para los niños, sin importar su edad. Pero es importante que los padres conozcan qué hacen los menores o con quiénes conversan, de manera que tengan una vida virtual saludable. El CSIRT junto con el Ministerio de Educación, se unieron para contribuir en esta tarea y ser un apoyo para los padres.

Ver más: https://www.csirt.gob.cl/recomendaciones/ciberguia-de-mediacion-parental/

Investigaciones

Costos ocultos de Seguridad de Endpoint: ¿Qué hacer para evitarlos?

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la edición n° 20 de su publicación sobre Análisis de Amenazas Cibernéticas. El artículo que presentamos en esta nueva edición, elaborado por Pía Salas y Juan Pablo Arias, ambos de Fortinet, analiza los costos menos visibles en el uso de la seguridad de endpoints, un problema que, de acuerdo a las estadísticas con se apoyan los autores, la mayoría de los CISOs asumen que puede ocurrir dentro de una organización. En el centro de esta investigación, los autores proponen una arquitectura de referencia para crear un ecosistema de protección integrada para el endpoint, el que considera mecanismos de seguridad, accesos seguros y segmentación de la red. Para ello comparte seis casos de uso en los que brevemente describen esta arquitectura y como se debe utilizar para proteger el punto final, la red y los datos.

Ver más: https://www.csirt.gob.cl/reportes/an2-2020-20/

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.

- Carlos Ramos
- Alfonso Moreno
- María Paulina Gubelin
- Anger Pulido

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.10.30 17:07:49 -03'00'