CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

31-12-2020 | Año 2 | N°78

Boletín de Seguridad Cibernética

Semana del 24 al 30 de Diciembre de 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

136

Sha 256

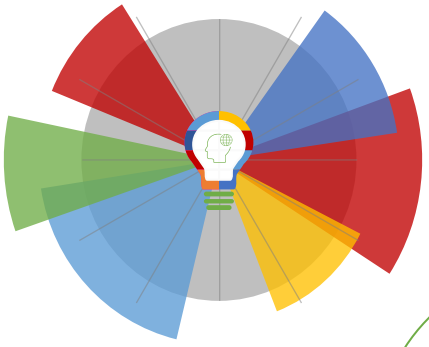
Asociadas a múltiples campañas de phishing son archivos que contienen malware

Se advirtieron

9

URLs

Asociadas a sitios fraudulentos y campañas de phishing



Parches

9

para vulnerabilidades

Las mitigaciones son útiles para productos Windows, Nagios Core, OpenJPEG y SolarWinds.

IPs

296

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 informa de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00859-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Diciembre de 2020
Última revisión	24 de Diciembre de 2020
Indicadores de compromiso	
URL	
https[:]//zorg[.]cl/auth/?platform=hootsuite	
IP	
[186.64.117.135]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00859-01/	
https://www.csirt.gob.cl/media/2020/12/8FFR20-00859-01-1.pdf	

CSIRT informa sitio fraudulento de herramienta de software	
Alerta de seguridad cibernética	8FFR20-00860-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Diciembre de 2020
Última revisión	28 de Diciembre de 2020
Indicadores de compromiso	
URL	
hxxps://escuelasantapatricia[.]cl/view/accessms/	
IP	
[54.224.202.63]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00860-01/	
https://www.csirt.gob.cl/media/2020/12/8FFR20-00860-01.pdf	

CSIRT advierte sitio web de software falso	
Alerta de seguridad cibernética	8FFR20-00861-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Diciembre de 2020
Última revisión	28 de Diciembre de 2020
Indicadores de compromiso	
URL	
hxxps://www.dispensariosur[.]cl/fast/office-3D8/index.html	
IP	
[170.84.209.80]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00861-01/	
https://www.csirt.gob.cl/media/2020/12/8FFR20-00861-01.pdf	

CSIRT advierte sitio falso de gestor de información	
Alerta de seguridad cibernética	8FFR20-00862-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Diciembre de 2020
Última revisión	30 de Diciembre de 2020
Indicadores de compromiso	
URL	
https[:]//templatee.sfo2.digitaloceanspaces[.]com/outlook/index.html	
IP	
138[.]68.32.225	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00862-01/	
https://www.csirt.gob.cl/media/2020/12/8FFR20-00862-01.pdf	

CSIRT informa página fraudulenta de software	
Alerta de seguridad cibernética	8FFR20-00863-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Diciembre de 2020
Última revisión	30 de Diciembre de 2020
Indicadores de compromiso	
URL	
https[:]//now.skype-for-windows[.]casa/	
IP	
159[.]69.158.6	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00863-01/	
https://www.csirt.gob.cl/media/2020/12/8FFR20-00863-01.pdf	

Phishing

CSIRT advierte phishing por suspensión de cuenta en sitio de streaming	
Alerta de seguridad cibernética	8FPH20-00345-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Diciembre de 2020
Última revisión	28 de Diciembre de 2020
Indicadores de compromiso	
URL	
hxxps://jeandescardtshtpmmh[.]com/LIFELIFEISGOODOOO	
hxxps://jeandescardtshtpmmh[.]com/LIFELIFEISGOODOOO/1ae67da1107e057f084290ebc9b5c726/	
IP	
[209.239.115.22]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00345-01/	
https://www.csirt.gob.cl/media/2020/12/8FPH20-00345-01.pdf	

CSIRT informa phishing de SúperClave inactiva	
Alerta de seguridad cibernética	8FPH20-00346-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Diciembre de 2020
Última revisión	28 de Diciembre de 2020
Indicadores de compromiso	
URL	
https[:]//santander.personascl.online/	
https[:]//santander.personascl[.]online/1609167424/index.asp	
IP	
[108.166.219.79]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00346-01/	
https://www.csirt.gob.cl/media/2020/12/8FPH20-00346-01.pdf	

Vulnerabilidades

CSIRT comparte vulnerabilidad obtenida por SolarWinds	
Alerta de seguridad cibernética	9VSA20-00346-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Diciembre de 2020
Última revisión	28 de Diciembre de 2020
CVE	
CVE-2020-10148	
Fabricante	
SolarWinds	
Productos afectados	
Solarwinds Orion Platform, versiones de la 2016.1 a la 2020.2.1 HF 1.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00346-01/	
https://www.csirt.gob.cl/media/2020/12/9VSA20-00346-01.pdf	

CSIRT advierte vulnerabilidad de Windows	
Alerta de seguridad cibernética	9VSA20-00347-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Diciembre de 2020
Última revisión	28 de Diciembre de 2020
CVE	
CVE-2020-17008	
Fabricante	
Microsoft	
Productos afectados	
Windows 8.1, 10 20H2, 10 1507 a 2004, 10 Gold, 10 Mobile, RT 8.1. Windows Server 2021 a 2019 2004.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00347-01/	
https://www.csirt.gob.cl/media/2020/12/9VSA20-00347-01-1.pdf	

CSIRT comparte vulnerabilidad en Nagios Core	
Alerta de seguridad cibernética	9VSA20-00348-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Diciembre de 2020
Última revisión	29 de Diciembre de 2020
CVE	
CVE-2020-35269	
Fabricante	
Nagios Enterprise	
Productos afectados	
Nagios Core 4.2.4.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00348-01/	
https://www.csirt.gob.cl/media/2020/12/9VSA20-00348-01-1.pdf	

CSIRT comparte mitigaciones obtenidas de OpenJPEG	
Alerta de seguridad cibernética	9VSA20-00349-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Diciembre de 2020
Última revisión	30 de Diciembre de 2020
CVE	
CVE-2020-15389 - CVE-2020-27814 - CVE-2020-27824 CVE-2020-27841 - CVE-2020-27844 - CVE-2020-27845	
Fabricante	
OpenJPEG	
Productos afectados	
OpenJPEG 2.3.0 y 2.3.1.	
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	

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

28072983ab85c6c066ed45307c69fcd92a0b85ba4c396458e798f3e2fdba61cb	66dee1c531293e20e26da0ffd7b7d4825876218dc4a90d537af904966fbb7db5
f87d4f9335a5a19b22703050482c4916fb6928d471e6f80ba87653b5fae074aa	6a14b0c30175c029ffd20001912c51cd6a7084240acef0ab1139cfadec64b5a1
a05b6385e22aa09aec239128decf022b6622b2633891c376c109305b4a5d9c9b	6a1b1d5d2ea4ef8860f4d1eebe713415a715edbcb8cb7ef683196936f229a75f
205f89b7d1f123f76320ecb1a84ee7ac1a76e29c26bbbc3bf60294f98f016298	6a4dd3c63086d87ed26f08be92f5b8480def89ab6ad5a8ea53e2e9b7446dc281
0e8460001cf94892343e766fe05019c40b1224bd7581a7ede6a63e9ca438b537	6ae13a12baaf1966a1b672ec45aaff934ef60f13fcd6d0df780ca587955ae5af
c7d457f1e15140629eb77774723557553593753e8653d3ac07759bf66f8ed481	6cac8ca3a3bdd0f3b37b7c5b108d5b18c35bff691923bb1d02edae43ee3df6e5
ceaa5de6774e28cd884c142f20d5f405546d6b609f9651a3f7e49f3f47e547a4	6f513e7300aec90543fdc0ef13377b05ed0a0ad346ae59112eb3753bd4664f08
cccff0ce9643649ac6833c840a8b181e6322e7e694495f143f9f354e0060fb96	7222fdbb77f25f6e668f4e34f0da752b0668ff12ee4aee442d6d89ecafc94ff9
47be3d6b42cbfb40e8087dcab2296b6f5dd577324ca38b63892139164e91e754	73b437a148519cb7133db064b5a00d9d6aee625dc8660c9f47e14d183a4d903e
a61add91d1ec99ec85463137cdefd5a4f56e2bc5885b00b4fdb840347ed6ab4e	75e6fc7e5c98a20bc64f7944d2bead6901f575fe20135e9aafe210ee2e1e2c49
e8672abb918f9c3e55cdf3c1038b3f73f5b4a785e49974456ef6295b32a6cbfc	76d6dd30e047aa598db2926e1869c1798d23c7486b2392d5190f795ce1382ab2
3e53c7421a59330c78325d05bf49fb8e5d021f5bcff335b45ab668c33bbf6722	76e27d48c88ccce543ebffbdac4248c8f1c03a3925357d3f5c24c4fc431e84fe
c4555949d96950deabb746149a655725781dee1c2d889192c7705463f456af3e	7774622dc1658a5afb589b6661582fe5e20672ed2e0ea808e3c22a91b0bb0e40
9715eea2416d772d16991d73e709d6a8b12eefb48de19eb700b5111bda1039e2	7a8d6629bfca211542bdee56f999f7cfd7589907c51c4ee05023e62716c8166f
5bce5c7c72915bde490ec837d14eaa3ed3303aac144b3b8b880182dce94d3f21	7f975c35b98c82e158e6689e3a8d6c5da6a640ba0f279256f3c01927e7476fbb
46800a3f95b5a20f39dd52907133678058ddb0fb79595508d76ef76917d77c32	812748f39fac8a866cc1196cc3947efc5ae8f9534246ddc828b78dd3ae7bbfa8
35b6316194a6cbc26240c81d7c2059d49155ba961f0892c6b193bbd6454d6576	865d58e3f55f2d1f7f7c0102845db1fef2d1d373dd3fabcc822d91c643a60a62
26c09e11e1095a1905a5e68fad4e91bb1594b4d43291ee750f4aa442f427d28b	869758da2cc6797c1a802611835c989d2f2748e077fc52903e02af0ae85f5d21
23e2c17ed7cfca4d041f2d164af07528f424dde00663eea69431dfb8727d12a1	86fb0903fe795c1851fc44939538d6261847b179c00ea2bf42a6dd8e0b0a553f
01872d93ed7dfca12babcf201094cd64772eae0dad212076fb52d685c48c1b8c	89711c3c9a120e6483c1622822d9517de2d8e3ac0ce012313d4ba593b4451428
097234279d3321c5af9e943ee4171b8b30258cc924fa909d3219fc21f69aa4e6	89a8df31e44c3c4df1a68681f376de9c8605608c7631037d8a1def1c60f15aa6
0bdd6592592d4be7ed904ddb4df6aaaa06e1f1116795e936aa51751e59c8f02c	8bd6dc7cca5e5865fe6a94156af1b4e58fa8439fc643e14afaa10c589db62bc3
0c9071269b7c2589b55d954425e231f04028d0d700e12c52567e75fc8669f0f2	8da9ca91829d11ad66643ab399180103b46cfe4c10397464d66aca0b7ddf2e84
0d90ca158eabbf8ebd00e4093c2ccbd118833f31c3c6902dc7cc079b6ad27560	976a60526e50d7a62932fa7aed3e8447dee3dff9777db299a6f4eaa831bc246f
118f33c9a3de922579f1aa3ad43f85e40ed10edc7ef6c881b667db675ff09dcd	9d159aa160fa9b07240a5947643de6a0381c15f6e27fa78a56f4f538c7a166cb
13f1c66896a1c40f53f90c4132994a55c9363a7044989a67b6ad42a8965f69ea	9e1444d10f2e3d6c07194182ec9afcaae4c1aef54be2c38b6dd4895ab9af634b
157e5cedd249bd2acba754752129a0fefbf2302fdd884a705cc30b734a4477c5	a268e9e152c260a0e80431aa8d6df187d9f24a1b6be71328ea14320436083f51
1606071be859711221c84c4474770c76cc9bd5bfd6e9289f1518926f7103c80e	a2c9b31097a16489dce2a8875a69f29b752afd8c0ebfee1991dfb23fb8c3f73d
1635b4d5da68b732b2c3250465a1068a415199342c1e2bef0ac276419cd804ae	a5bc4cb5b6e9fb3faac1ba6e45d987757ab2bbb0266710f1302c0de9382f2162
19dee3df18f9767d4dd14ee1c3ed05a893f7ba7592926caea0284cafeb4326ef	a7e8faacd84aabcb2ca33e0485636a66813233fcedb031bc97ee91a35354922e
1b508e81f2b5ce3f8a8cc52d01b8d3fcad27135341c17e3d26a04adce2017bc5	abff62bfa148c0606f2b0f545934c0ddaf4b00cc13c5f3c051a22f8d53b089ee
1c40fedf88ae71176dfb3bac67ea4bb5e4bdab5d7ec11413847d39486af28672	acbe714eb0a6893954ce2d0c7cf9453c7770f2d6e9d3f8fc267c1b6f865aa972
211a5a88e567052b7c19efddb1373a599203746bccd37e0707283689b249b053	ad0151c5113107d864f25a6d5c6f33cdb5c38af7c392a43c83b84e9b2753d0de
2120a84c53879148f19185e854d0f2bd564bab0c71b4d11e89ff8a2b923f540a	b07ef3318f6bcd869a115219403c874d5755c0993f2e62c40c6fd47f1110c1b0
22899e83cb30db524679f0e8385d3fb02c24480e7388e84acf100bc7f1641bb3	b4ce0900f2c0d6d99075edf48d95f3bc52c5599e328590495a27720bf183f25a
26eaeed81c06cdcb31127bb193787c4fac6e77fda2c26b984b00ea10f153450b	b6c180997faa973727315dbab5056d940fb185e0be73ab57ce3d81933f11f10d

278f1cbb7bfff54ea0597e2de43545619795407c63dbaf34e6dfd3800897347f	b8a869d6957329c83a3203d74c14f0ee2f0848782eac8ad17256ae15dce4cae5
2976819cc0f99eda7e02837e7b96b6e8b39f8298db2dc48df1d60cfd182cd844	ba9c801c087d58002e00029bd3c5042aad383ada79b3830eba10484549576b5d
2bbbeffa2565ba4f4f6bbf4642dafa81da8a947b7de6d78591399f8a131c9632	baa34a96181ff5e02ba132304415e8878a13ef640501db136dae73e64d3361e4
2dce743bff251b08928ac30202169bc840074ff20f64fa614447fe0e7dac5986	be2287f06352c21f4412b81411c76a2e3c23bc99bfd67a39549574e6f0143ec5
2f87f9dfc21b3bf28e05b410fae3b5e7c8c1aff9f754f5e14a14aeec884aeac4	bf4b1333c169b4c3b653e8df33d6b3b8ef7b73f6461f4b9b9f20642e3d7c5574
2fe65afe2ee9a4272a0354a47a5380ead7214578c07b6181808143f1f0047ea2	c071499cd020fb03f6713bb36679cb3881d2fe9f8e501e5de846c472f2fd0ebe
325a9b75ee1145a597756e7289b5e40d52160ecbd43fdda5d0f9adf1888ae854	c46d5ee8a0329733bb9de38eb76403a53c1a97988d8e9b1e8f0a28b0ecea0530
34161448e8f0b6c4f0ff3904628cf8cdb1f4f4794ddc79b0cda765b490619e4d	c554df69e42c1b14f29537e5a8414ac455b70eb2fd203588fe4de13a0b2bcc5c
34193a09b87ec1ddb0eeb0bef1296cef50961ff44f74655870b6894b7ec22871	c6333efba033ab3aa174d7b6254aa11c1b7c56ae806599e8b9361bf603477a09
3606e042b0d2e8fd2827d872f4805cfa9e71b409ed658535d3db40f5fc7ed0cb	c8b49c2292e087f722d2422f84d52d6850ce69b6cf230ee27f2b2e82d4df7cdd
36193b38a4cc6ba4dd680ac68e9caf27653b9b9fac1b65563e89c23a969f12e8	c8ecacd276697e3812669b243a54ef1e7415f87479438efc5c27cdbe0312af99
36669e2c21769cf9e843dc75027c11e3fa43c28e86a310ca7303c273993e0692	c97f960703675966e7a0a8e6cb48f66e954aa9b40c307db9c4965075b3c553cc
38bbd83de3da247dd96f8f463e73ebc76a9165bb783fc85432714e863675d87f	cb857fa1a6f145590d9ce05fca3f6906d5831286e54540052e77625786f28f15
38f93023bb5df97d8d74fd362fc71e4ab8cfec3ad712871c32bd360fa8267272	cfde1fb313a0ce73984e005f1ad21bf37d6e0052b474500a8550c552d00eb16b
39e24a73656d38c94f1c4abc67b93be532659af2fa07966c372424780e54cb24	d08bca9f926920b2f85e5b7bec30f872cd48615f0ab552f727f9cae055fab628
3c2ed9471901c2a6ecb559a6af4a9ae579b9e6e93ffd08595f002d8b0ea1afd9	d1b055f730d56fef75cd826b96c669e9aa16832079dfa132b8a1e4ef76e2351f
3c5a0e1906eb2a02dc597a235c6ba9b3faccc526ef1aa3b2f34f462257ff7261	d5a23fc9d1f83490847cc316f8ddb71465b3308de54f891473d6e75fe691210d
407d56f25106b346313d71ef109309b3124baa949838fd1d91dbd8dcf8e73054	d740fd613b61bfa7c6fb730568257d6b499db6401e6cd9b3ffb7005403b3e21e
4239d149bdc65c62946a2bffabc81bcc602baf67a1d402b898c4c036073d627b	d7580e2470858a8fb6d5b4c8023fdeb779c7755814f4ba49f92a19d5d7bc3041
43334e0c4050101786c3f6d932a7ee3c1556497e2e29b6c8dc30165ab79b1e8f	d985c0b0119ddd4d947409506642c4ded6ce2533b32d3a4147422417ee979a4c
4768978578650362b2a6dad282e9a7de5e2632542a41a9ede152c3261d5656dd	dcb7872fbcfd5c4d82665480c0e8995b991d25272fbd21eaf39d7b376421fb95
5084cd90d8e8ed3863d9b3c12027d26bbd061cd0f39901611ba27ea79cd8bec3	dd2fb6306e8f3dc2849a641608ae41a0a339a1b522cf120a47fa7b2d825e21dc
5269b1802b227eb87862817d6b4ae3b74a316d2212ca808f64bbbf1c67b5216d	dfd22de90a282954d8b1ae5462bb4df06c777293d6326b46037a99b43ad47c0a
529b95c3c3fe28fdfb9e0db464ceae55e8a51c9c8458d014adc29344ff81b2b3	e0906cd11e8ed41199e6bfdc6d61f43a692a2824fe8eeaefe044b9c8bd81625d
5424a9ebc15b5294dbe17c36e54e1282d8eb2a86792b3cb3381bba14a746ff2d	e9a7000b6216e1cdd6280e0d3b11b52bfa0cfc1a49f3eb8488ebb26b6f0852c5
55554b1b627075ce4dbdbf6b5e98865d100ebb8d8184374368d56a637cd29dad	ebb494890c3756f3bd2d17fe15fea7443671ce48c7d22821b6f0e73920ab061b
555c247789f6210fd2f84f448e878932060fc1e75d187ac60d6f13e67607875e	ed417d96112ec1f055fea100fc8f57c3aba8748983cba7f2ea562cbd0be6cb10
55fbac965c3f9270efded083fc5cd5c0bc8f26f8610a33084dc6aed452f530c7	f087744977f77b9662829bc12bde6d8fd085441f9f646469e12fb9f34cbe9251
59a3bfb08605427811b6548c99a92bca56bb3d0d9c33e2c06705721194d7d518	f2c230749a5834a704880ec2b4b5ebb472798ef740b78d97ce9cd37d918fcf51
5e29f85770da8d5b6a53c9a18f74a6027657b44901a55361dcde94c646978eab	f7216d4aa975655eb5d58c7aa71e446cb222cc19b696390ff2eb5c5a820c07ac
610af38d736288484e1ee11f5b0deb8cb6a36640750ee80a9ce15de63bfd181f	fad898ec89cc81bacf8a7edea7f43a0a4304e4bb40221c447893f21f969e8ed6
fc5f218a335827dae3d47a83de79fbe3bf8e3da9308f22edf5d9a17c8d1ee1ff	fbfe3a9773578c2f99e7a96c45bd44b4fed5bb5c6bf310fdb1d14d158f584a38

Correos electrónicos de donde son enviados los archivos adjunto con malware

stores@baywatchresort.in
info@sino-imports.com
vijaykpillai@lifecarehll.com
firecare@kidanet.net.fj
cytemym@infonegocio.com
teomaninaner@hotmail.com
advising.service@hsbc.com
info@mclhk.xyz
ungkwangmedtech@gmail.com

cruiz@conaipd.gob.sv
gmiranda@conaipd.gob.sv
spares@angelicoussisgroup.com
info@taixingmachinery.com
jdiaz@conaipd.gob.sv
SRS0=sVH0fn=GB=duwellinc.com=jnix@yourhostingaccount.com
junalcasquejo@asisisafety.com
dem.grammateia@hcg.gr
hilton@telecam.net
aster@targetethiopia.com
mustafa.halim@mail.com
naveed.bhutta@globalpharmaceuticalspk.com
ricardo.martinezb@bbcconsultores.cl
l.fortunato@commercialistisalerno.it
charlotte@svt.es
gicuta.marcu@primariabacau.ro
SRS0=9y9hb6=GC=aaafrt.com=cs1@eigbox.net
l46manager@e-npw.com
Finance@stesalitltd.com
SRS0=zYkDfK=GC=grancarenc.com=cjohnson@eigbox.net
sekpo@africaonline.com.gh
royarzun@institutosantiago.cl
lloyd.f@melodica.ae
rda@itatiles.it
shj@metrofiresystems.com
d.durando@mdsonline.it
kgolden@metrocomm.com
leo.romero@maulme.com.ec
cristian.olvera@transmana.com
shahinur@pnl-bd.com
SRS0=vPWluh=GC=weutilities.com=k.smith@eigbox.net
junaid.qadir@sharmeengroup.com
SRS0=vatnm0=GC=geneshifters.com=sukh@eigbox.net
segreteria@fedeanto.it
boldbury@katconstruction.net
cristi@marpet.ro
es@brenhampark.com
urbanistica@pec.comune.gragnanotrebbiense.pc.it

office@ruempel-max.at
commerciale@fllimilani.com
azizulhaq@stormfiber.com
megel@wenlen.com
k-ueno@nitto-cs.co.jp
khalid@labbik.om
shimada-hideyuki@maruo-co.com
calidad@chocolatescodeland.com.ar
info@officinacastagna.it
psefcik@centrapartners.com
safety@auglaizeseniorservices.com
Rodrigo@blendpub.com
cnareport@i-claims.net
SRS0=1mY6Is=GC=greenetnso.org=jkey@eigbox.net
cancunt2salidas@mobo.com.mx
lana.dzodzo@full-point.rs
SRS0=SaCP9O=GC=dhabicontracting.com=mubasher.h@eigbox.net
harold@hdcordyandassociates.com
perez@prestointl.ae
jbleiweis@vir3-ing.si
SRS0=D39P6C=GC=gsilab.com=sfaulkner@eigbox.net
salesanalyst@burlingtonphils.com
friedrich@alsterhyp.de
grant@metrocommunityservices.net
didier.izabel@axys-finance.com
p.latulippe@hydrauliquesrive-sud.com
yemliha.avcu@gresmax.com.tr
finance@rockwallpowersports.com
shijithkj.acct@darwish.net.qa
SRS0=Gc1JuV=GC=jetonsuae.com=athif@yourhostingaccount.com
info@fifthworld-inc.com
larrinaga@abogadoslarrinaga.com
mauricio.milanes@chronusoil.com
carlosfer@higuerasa.com
atiwari@accindiaonline.com
franz.eversheim@highlevelgroup.eu
laura@studiopresolana.com
suksan_w@globaltel.co.th

SRS0=rlYGgg=GC=aqd-algawdah.com=purchases@eigbox.net
drivingschool.mlp@saboomaruti.in
m.mameshi@mammutteleca.com
sales@protred.co.ke
mjuez@decimas.es
puran.katariya@ecity.esselgroup.com
info@vebko.ir
farellano@soluglobikon.mx
jd@bielmeier-und-partner.de
yoshida.k@sumimoto.jp
testa@amazonfoods.ae
alexandra@familieraschle.ch
geral@registoinicial.pt
santuarioaparecida@diocesesa.org.br
dzenan.omanovic@cip.gov.ba
annamossi@disegnoceramica.com
h-ito@nitto-cs.co.jp
office@malerei-bharth.at
heng@itusaha.com
marquiscstore@lakecountrycoop.ca
k-kuroda@cas-co.jp
louis.premel@votreagent.fr
coordinador@cubatoptravel.com
alondrah@compassat.com.mx
info@inotech.com.tr
info@vakgaragezuid.nl
sadia.abbas@mail.pakgulf.com
khalid.masood@gerrys.com.pk
st@ultima.de
principal.c7@falconhousegs.com
SRS0=x3NwPo=GC=dhabicontracting.com=christina.c@eigbox.net
ambrosius@insignia.com.na
SRS0=MBnNIA=GC=transportesbega.com=fernando@eigbox.net
SRS0=/ZPNoQ=GC=gsilab.com=spoole@eigbox.net
gjones@metromealsonwheels.net
jofel-p.jimeno@empleyado.com
moonjun.lee@gmc-korea.co.kr
SRS0=rEKq5h=GC=almaceneshatuey.com=compras@yourhostingaccount.com

operation@chandford.in
SRS0=0JKns4=GC=sawarigroup.com=mousa@eigbox.net
a.pantaloni@globalservicescoop.it
info@miangeni.co.ke
jbr.spv@sap-express.com
khalid.aziz@gerrys.com.pk
alperucur@aksular.com.tr
cargoey.isb@gerrysdnata.com.pk
consents@housecallsmma.com
carlomilani@fllimilani.com
likizoguide@journeystravelclub.com
SRS0=+gYT1r=GB=triadschool.com=dan.conrad@eigbox.net
01020176af941119-7b2a5453-03e4-4dfd-beac-c97476d3ac59-000000@eu-west-1.amazonses.com
import1@daehangloballogistics.co.id
info@pead.ps
SRS0=hIuPQw=GB=greenwoodmachine.net=Kristin@eigbox.net
riyanto@dian-heavylift.com
marcos.perez@key.com.mx
ka-taniguchi@morinaga-net.co.jp
ahsan@afroze.com
henrique.peixoto@onincorporadora.com.br
val_branch@comglasco.com
sano@itsuwa-home.jp
prajasa@prajasacompany.com
SRS0=Pgmx0J=GB=eriksen-email.com=diane@eigbox.net
lahore@globalpharmaceuticalspk.com
secretary.hrg@travelways-egypt.com
admin@farhaxerox.com
p.okojabhole@medplusng.com
baky.ullah@hpchemicalsltd.com
cecilia.mendes@saojoaodedeus.pt
keech@itusaha.com
drivingschool@saboomaruti.in
h.h.x.1999@docomo.ne.jp
fd1@mpt.co.id
financecbe@genie-toys.com
ruben.cintora@huimilpan.gob.mx
SRS0=SqQpMd=GB=drshirin.com=jon@eigbox.net

os-kneginec-gornji@vz.t-com.hr
f.bianchi@ivgroma.it
giuseppe.pedone@fidimed.eu
SRS0=YuVtlj=GB=weutilities.com=k.smith@eigbox.net
khairul.alam@pnl-bd.com
ezawa@jimbodenki.co.jp
wirat_c@ultraengineering.co.th
takamatsu@nitto-cs.co.jp
lcopa@salta.gov.ar
sri.karno@dynaplast.co.id
raheel.asif@tandhint.com
faleconosco@unimedregistro.com.br
SRS0=tDlV69=GB=bividvietnam.com=dung.huynhcong@eigbox.net
contador.general@medicalpharma.com.sv
comercial@aqua.es
vlinares@hostnews.com.ar
abarcenas@centrodedistribucionget.com
rentas@salta.gov.ar
SRS0=BjK/aH=GB=mullenmotors.com=service@eigbox.net
SRS0=9a4jBB=GB=dhabicontracting.com=christina.c@eigbox.net

Direcciones IP de servidor SMTP donde es enviado el correo malicioso

101.53.155.82	62.149.158.134
46.183.221.10	189.126.112.2
185.222.57.251	66.96.185.7
113.20.90.118	62.149.157.210
185.239.242.41	62.149.158.119
185.222.57.137	91.185.198.250
190.120.4.24	94.107.201.197
65.254.253.37	94.177.208.112
45.56.85.142	94.177.208.130
84.205.254.49	189.126.112.162
168.243.48.34	189.126.112.163
69.73.181.38	189.126.112.164
131.255.194.243	189.126.112.165
210.56.11.43	189.126.112.166
80.88.94.22	189.126.112.167
68.178.252.102	189.126.112.168

79.62.191.82	192.185.145.100
188.241.113.120	192.185.145.178
162.144.195.178	192.185.146.130
54.188.53.74	192.185.148.204
202.146.193.141	195.140.156.231
74.202.142.113	199.193.207.173
86.96.131.226	199.193.207.188
62.149.156.165	213.158.164.196
173.201.192.106	101.99.66.95
189.126.112.10	103.120.176.72
66.96.188.1	103.13.29.223
189.126.112.76	103.213.115.34
173.231.200.225	103.31.132.106
200.58.121.160	103.4.66.106
200.115.37.29	116.90.163.172
77.245.145.67	124.29.202.132
189.126.112.159	125.206.175.70
195.114.26.37	144.208.127.58
159.69.106.183	146.20.161.112
62.149.158.146	148.251.12.109
189.126.112.161	158.255.47.192
66.96.184.8	162.144.158.98
62.149.157.209	162.250.191.48
77.245.152.18	178.208.4.148
120.50.30.27	182.50.132.194
201.76.49.122	184.106.54.76
201.76.49.127	184.154.30.186
201.76.49.124	185.125.77.111
62.149.156.108	185.128.81.119
66.96.184.2	189.126.112.3
103.227.62.244	189.126.112.77
77.245.152.28	189.126.112.8
66.96.184.6	189.126.112.9
211.13.204.74	190.0.161.202
185.64.24.112	190.61.219.211
163.172.83.68	191.96.107.217
193.137.75.241	192.185.143.39
66.96.189.4	192.185.149.77

162.255.118.216	192.185.196.18
66.96.190.8	192.185.45.2
189.126.112.5	192.185.47.129
201.76.49.126	192.203.239.81
201.76.49.241	195.29.150.135
82.223.103.184	198.154.250.18
81.19.149.132	200.45.111.119
150.95.29.49	200.73.116.8
64.69.218.88	201.20.9.92
210.172.223.65	201.76.49.123
131.72.236.72	201.76.49.128
46.43.66.107	201.76.49.129
189.126.112.74	201.76.49.242
189.126.112.4	201.76.49.243
195.8.209.17	201.76.49.244
198.57.162.62	201.76.49.246
65.254.253.144	201.76.49.247
189.126.112.157	201.76.49.248
173.236.35.242	202.46.200.102
66.96.186.5	202.69.33.243
51.161.35.216	202.69.36.36
84.232.181.45	202.77.104.104
210.133.167.2	203.160.57.20
167.250.5.44	206.221.182.77
189.126.112.160	209.195.1.90
195.222.50.170	210.129.49.174
175.107.198.120	210.131.0.52
66.96.188.10	210.131.4.98
211.13.204.72	210.131.4.99
64.235.40.28	211.13.204.68
173.201.193.232	211.13.204.70
189.126.112.158	212.114.52.49
162.214.70.141	212.34.194.142
66.96.184.9	212.85.196.25
192.190.84.36	213.133.103.20
173.201.192.237	219.99.208.167
66.96.187.9	45.151.248.63
148.251.15.247	45.84.191.188

173.201.192.236	51.75.130.83
66.84.9.24	54.240.2.49
62.149.156.164	62.146.106.30
187.248.46.197	63.249.18.13
62.149.157.204	64.15.147.113
189.126.112.6	65.254.253.43
66.34.138.227	65.254.254.66
115.166.150.132	66.96.186.7
173.201.192.105	66.96.187.6
66.96.190.1	66.96.188.2
189.126.112.7	66.96.188.3
74.208.4.194	66.96.189.1
134.119.228.97	66.96.190.2
94.127.7.164	66.96.190.4
95.130.52.38	80.67.18.29

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	
212.70.149.54	138.0.255.22
212.70.149.85	45.165.213.133
195.39.133.158	45.181.31.103
141.98.80.87	190.109.43.210
5.188.206.204	190.105.217.204
199.192.16.253	45.179.112.124
78.128.113.68	45.181.31.103
103.156.92.189	45.224.160.129
193.56.28.190	45.179.112.124
41.83.218.103	191.243.32.4
94.74.172.243	191.53.193.141
94.74.191.192	191.53.238.201
45.181.31.113	177.36.40.106
191.53.198.243	103.87.46.192
31.170.61.137	45.181.31.1
193.242.194.219	103.53.113.51
191.240.116.120	103.87.205.15
177.52.68.75	191.53.220.183
189.50.146.168	177.154.238.86
177.184.245.112	77.45.85.15
170.246.207.132	5.190.81.78
45.6.27.221	45.179.191.195
131.108.160.183	45.227.98.141
191.240.116.70	45.225.49.196
210.16.88.179	45.165.214.111
103.133.109.40	45.160.138.192
103.25.134.184	45.165.214.111
168.205.195.20	45.160.138.192
45.230.80.52	189.89.212.72

191.53.52.109	212.70.149.85
191.53.208.139	212.70.149.54
189.91.4.179	177.154.226.44
191.240.112.238	31.170.53.48
191.53.221.239	193.56.28.190
177.200.64.152	45.165.213.25
51.81.170.75	92.222.241.68
177.21.199.78	177.154.226.62
45.7.225.204	

Actualidad

Ciberconsejos para proteger y cuidar nuestros datos

Para adivinar la contraseña de un usuario o sitio web se requiere de mucho tiempo. Para evitar esto, los ciberdelincuentes han desarrollado herramientas que aceleran este proceso y así obtener la información que necesitan para cometer algún fraude o estafa.

Ver más: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-proteger-y-cuidar-nuestros-datos/

Investigación

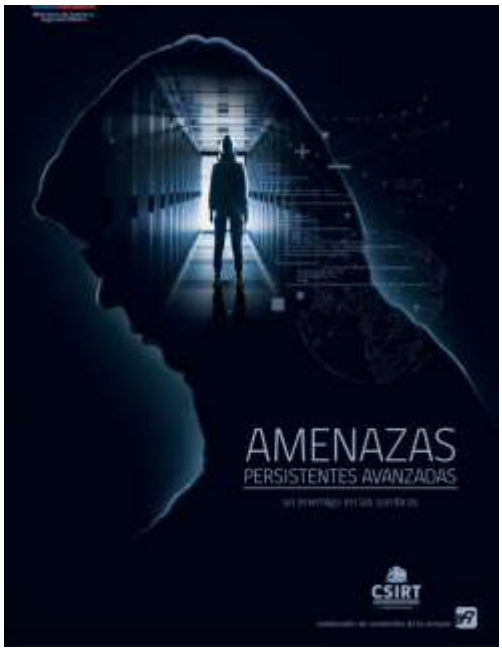
Amenazas Persistentes Avanzadas: Un enemigo en las sombras

La actual edición 26 de Análisis de Amenazas Cibernéticas estuvo liderado por Juan Roa Salinas, quien junto a su equipo nos entrega una mirada de un enemigo en las sombras: Las Amenazas Persistentes, Juan Roa, quien actualmente se desempeña como Gerente de Ciberseguridad y Defensa en Redbanc.

En el transcurso de la presente investigación —Amenazas Persistentes Avanzadas (APT): un enemigo en las sombras—, el autor y su equipo explican qué es una APT y cómo se diferencian de otros tipos de amenazas más comúnmente enfrentadas por los sistemas informáticos en el día a día.

La inmersión continúa con una detallada explicación de las características y principales objetivos de un APT, para luego explicar los distintos pasos que requiere, en general, implementar una operación de tipo APT: la preparación y el acceso inicial, expansión, persistencia y Asset Targeting, exfiltración y limpieza.

Asimismo, describen los principales grupos APT y cierra con las principales conclusiones y consejos para evitar en el mayor grado posible ser víctimas de las operaciones de uno de estos poderosos grupos.



Ver más: https://www.csirt.gob.cl/reportes/amenazas-persistentes-avanzadas-un-enemigo-en-las-sombras/

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.

- Claudio Valderrama
- Fernando Cid

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.01.05 07:22:41 -03'00'