03-09-2020 | Año 2 | N°61

Boletín de Seguridad Cibernética

Semana del 27 de agosto al 03 de Septiembre de 2020

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

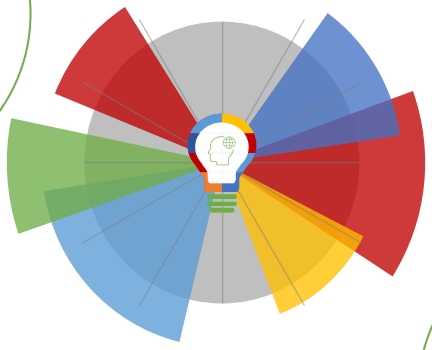
División de Redes y Seguridad Informática.
Gobierno de Chile

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Resumen de la semana en cifras

Body Hash
169
Sha 256
Asociadas a múltiples campañas de phishing son archivos que contienen malware

Se advirtieron
81
URLs
Asociadas a sitios fraudulentos y múltiples campañas de phishing y malware



Parches
1
para vulnerabilidades
Las mitigaciones son útiles para productos Cisco.

IPs
19
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 de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00659-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Agosto de 2020
Última revisión	27 de Agosto de 2020
Indicadores de compromiso	
URL	
prestamosaprobad0s-2020-cl-home[.]000webhostapp[.]com/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
145[.]14[.]144[.]23	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00659-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00659-01.pdf	

Imagen del sitio

CSIRT informa sobre portal que suplanta sitio bancario	
Alerta de seguridad cibernética	8FFR20-00660-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Agosto de 2020
Última revisión	27 de Agosto de 2020
Indicadores de compromiso	
URL	
www[.]bancoltau[.]club	
IP	
195[.]2[.]93[.]235	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00660-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00660-01.pdf	

Imagen del sitio

CSIRT advierte de web de suplantación bancaria	
Alerta de seguridad cibernética	8FFR20-00661-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Agosto de 2020
Última revisión	27 de Agosto de 2020
Indicadores de compromiso	
URL	
bancoestado-bancaporinternet[.]link/inicio/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
68[.]65[.]123[.]126	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00661-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00661-01.pdf	

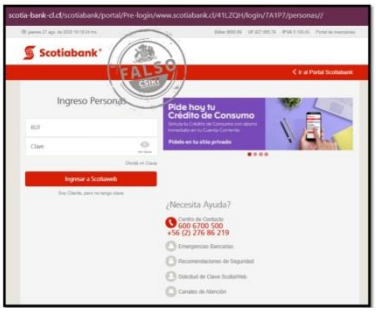
Imagen del sitio

CSIRT advierte de sitio que suplanta web bancaria	
Alerta de seguridad cibernética	8FFR20-00662-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Agosto de 2020
Última revisión	27 de Agosto de 2020
Indicadores de compromiso	
URL	
bancoestado-cl-chile-verificaciones[.]gq/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00662-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00662-01.pdf	

Imagen del sitio

CSIRT informa sobre portal de suplantación bancaria	
Alerta de seguridad cibernética	8FFR20-00663-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Agosto de 2020
Última revisión	27 de Agosto de 2020
Indicadores de compromiso	
URL	
free-netflix-account[.]cf	
IP	
185[.]27[.]134[.]252	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00663-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00663-01.pdf	

Imagen del sitio



CSIRT informe sobre portal de suplantación bancaria	
Alerta de seguridad cibernética	8FFR20-00664-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Agosto de 2020
Última revisión	28 de Agosto de 2020
Indicadores de compromiso	
URL	
scotia-bank-cl[.]cf	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00664-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00664-01.pdf	

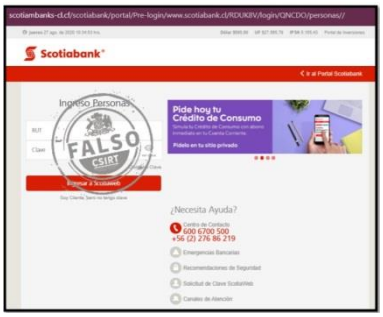
Imagen del sitio

CSIRT advierte de sitio de suplantación bancaria	
Alerta de seguridad cibernética	8FFR20-00665-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Agosto de 2020
Última revisión	28 de Agosto de 2020
Indicadores de compromiso	
URL	
scotiambanks-cl[.]ga	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00665-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00665-01.pdf	

Imagen del sitio

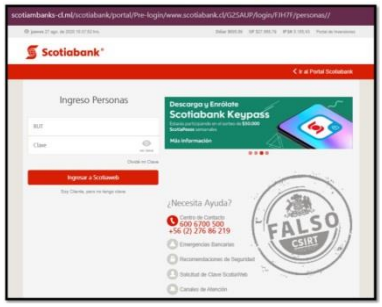
CSIRT advierte de web de suplantación bancaria	
Alerta de seguridad cibernética	8FFR20-00666-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Agosto de 2020
Última revisión	28 de Agosto de 2020
Indicadores de compromiso	
URL	
scotiambanks-cl[.]tk	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00666-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00666-01.pdf	

Imagen del sitio



CSIRT advierte de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00667-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Agosto de 2020
Última revisión	28 de Agosto de 2020
Indicadores de compromiso	
URL	
scotiambanks-cl[.]cf	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00667-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00667-01.pdf	

Imagen del sitio



CSIRT advierte de web de suplantación bancaria	
Alerta de seguridad cibernética	8FFR20-00668-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Agosto de 2020
Última revisión	28 de Agosto de 2020
Indicadores de compromiso	
URL	
scotiambanks-cl[.]ml	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00668-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00668-01.pdf	

Imagen del sitio

CSIRT advierte de sitio de suplantación de banco	
Alerta de seguridad cibernética	8FFR20-00669-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Agosto de 2020
Última revisión	28 de Agosto de 2020
Indicadores de compromiso	
URL	
bit[.]do/estadoverify	
zonasegura-bcestadocl[.]website/1598541857/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
198[.]187[.]29[.]193	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00669-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00669-01.pdf	

Imagen del sitio

CSIRT advierte de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00670-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Agosto de 2020
Última revisión	28 de Agosto de 2020
Indicadores de compromiso	
URL	
bancoestado-cl-chile-verificaciones[.]tk/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00670-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00670-01.pdf	

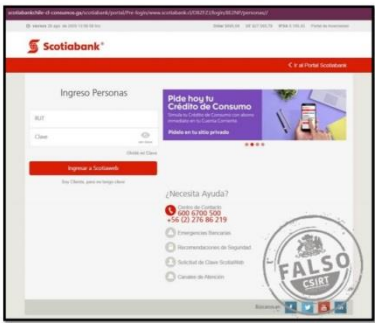
Imagen del sitio

CSIRT advierte de sitio de suplantación bancaria	
Alerta de seguridad cibernética	8FFR20-00671-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Agosto de 2020
Última revisión	28 de Agosto de 2020
Indicadores de compromiso	
URL	
bancoestado-cl-chile-verificaciones[.]cf/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00671-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00671-01.pdf	

Imagen del sitio

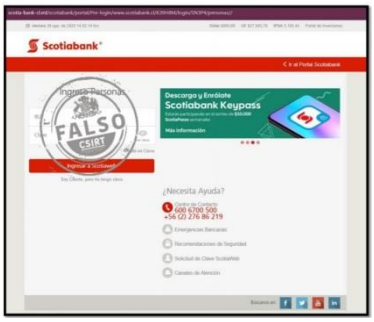
CSIRT advierte de sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00672-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Agosto de 2020
Última revisión	29 de Agosto de 2020
Indicadores de compromiso	
URL	
scotiabankchile-cl-consumos[.]cf	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00672-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00672-01.pdf	

Imagen del sitio



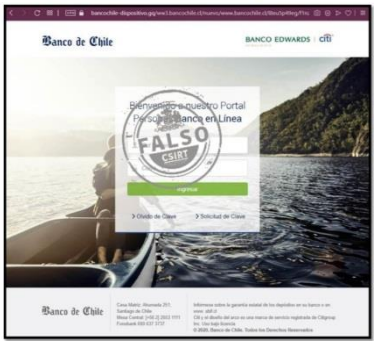
CSIRT informa sobre web de suplantación bancaria	
Alerta de seguridad cibernética	8FFR20-00673-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Agosto de 2020
Última revisión	29 de Agosto de 2020
Indicadores de compromiso	
URL	
scotiabankchile-cl-consumos[.]ga	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00673-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00673-01.pdf	

Imagen del sitio



CSIRT informa sobre portal de suplantación bancaria	
Alerta de seguridad cibernética	8FFR20-00674-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Agosto de 2020
Última revisión	29 de Agosto de 2020
Indicadores de compromiso	
URL	
scotia-bank-cl[.]ml	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00674-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00674-01.pdf	

Imagen del sitio



CSIRT advierte de falso sitio que suplanta a web bancaria	
Alerta de seguridad cibernética	8FFR20-00675-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Agosto de 2020
Última revisión	29 de Agosto de 2020
Indicadores de compromiso	
URL	
bancochile-dispositivo[.]gq	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00675-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00675-01.pdf	

Imagen del sitio

CSIRT advierte de sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00676-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Septiembre de 2020
Última revisión	01 de Septiembre de 2020
Indicadores de compromiso	
URL	
scotiabankchle[.]cf/scotiabank/portal/Pre-login/	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00676-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00676-01.pdf	

Imagen del sitio

CSIRT advierte de sitio de suplantación bancaria	
Alerta de seguridad cibernética	8FFR20-00677-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Septiembre de 2020
Última revisión	01 de Septiembre de 2020
Indicadores de compromiso	
URL	
scotiabankchle[.]gq/scotiabank/portal/Pre-login/	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00677-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00677-01.pdf	

Vulnerabilidades

CSIRT comparte vulnerabilidad obtenida de Cisco	
Alerta de seguridad cibernética	9VSA20-00293-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Septiembre de 2020
Última revisión	02 de Septiembre de 2020
CVE	
CVE-2020-3569	
Fabricante	
Cisco	
Productos afectados	
Todos los productos Cisco que ocupen alguna versión del software Cisco IOS XR, con una interfaz activa configurada para ruteo multicast y que reciba tráfico DVMRP.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00293-01/	
https://www.csirt.gob.cl/media/2020/09/9VSA20-00293-01.pdf	

Indicadores de Compromisos

Se comparte a continuación el listado de IPs que fueron detectadas durante la pasada semana por el Equipo del CSIRT intentando ejecutar escaneaos 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)

02ef5cd80f285c9986694cf33576f73f3c2968f919beee47115b2b4c1e9def6a	835d0910a541696111ecf4588e19a2c361e1ed6a61d2b680e1dd1cfcd85b4da9
032813fe4d6260828e500d070f8a2ce00c08f363bb933f7f786b00de5ddb67b5	863d1f9eb383c31bf64a088968c090cf84d15151c8e0f3948b1d849d9280d5be
03b03647dd601a8ca52b7b9ab214f1546ceaee498e740e371ceb935bc900ef09	8669cfa1c690396a1e41737827625e7204c547ff9d59fefa6b3dc2b96c9ff023
05d9e516aab30eaed79b81c313c01e1358ee30ecf522c2121ffe5c8d298a6817	86a1be50f3d7d3d3c76266d11b8ff15fc0b91d3f7d1ac71adeec6f4cf5b28528
066051dc77ae25b26c38a62c8bc13eee160fa32657231cbfb1611a2ce8a3445c	876448ff5aa74ac966c662a97c6fbf8f64cd57f9148bda620f9ca5d9589275f8
0838b43fe71b005d04ef6de838a55335adfaad67d3e5089cf7585d0e0be03e82	87c2af348d80f2d0818ac02a667eb6bf793d18324c43f4273572793db16085e2
08d6e7fcc2e2cc9338c3c7ab9a223c50909d15a1d1bc71f06c3e276800a47ab0	89456bf194ce7d9cfb66ba09352d1d0c22dee9324896c45b596588b563201ba1
115f9dae21f3c83258653e6a5949b5c50999f707876404f845ad434dfff2cbd2	8b6e6542b11a89f43268a5bbab76e9543c48c8ed35598096ff9422a6f854d234
11d1855e471ebfa4197e9a24201272d3b43c3d0155c767d9abbb12aadb09a694	8ba9c16815127ea0dd1d899dcff1569fc505d84f5efb0c3724fbba62691a5a60
11f958d598c4e1b0b0978b6e9d9ea6f5e1a8fa34f1af035d657f13b04bb128be	8cebeffd84d2ef6b8e9b93338651237815f6682d20e6a70eb6ea6dd9f4625435
130fa091d8cc924c8a70e7a03c2f3947d783b189a6a3842f14807bd72828535e	8e613687f31d459362fb1d307c495562b2a528f32b0b2f0b6a9fed1dadc0f3e3
154a18acd2486163682664e2c2aea63d14e5f466b6a861ffb5568b31a49e9cf7	8f33d7ea4a7ba61871627527e0d0ca62bf82f56d8a40448ced4087f3654fd8de
159298b9928775bbc5f69c4479e4382bc434afccd42071cb9e6e05934536553c	8f67c85dbe12ce4b30003c17104c069728f76d564430434c5830221045780144
1777a62fe7df40cf57e27aeba4a8c8c50dfc4b978a2ef0e383dc2a63fd6fbf8c	8fcdb657e7b619a1671c5992fb2e79d00e2b795af5a2463de945688377926201
1c3592ba34594ef1a243ca3fa4b97bd82f77705ae385481aeb68a81c09000e4b	90766fde5e407fe0ffbe4ed9f9b9f9b6eb0fdd8d3e694e418de7cd2e5aadab20
1c6b8a2ef41e241b403a8da6859e39f963b7062ce8a1a66afaae1f388a7febcf	9293848a589af567094cd2bdce0ee80f984253bfc03742c8784009050f881b36
21a41841b55f20580bfda66c767f0a1e396cbf0de3d9dcd2b9838ac3799714f8	93e68a462f76926f039cef0a76141a4d828653e473690e1e1780fee83e1a265d
2524d6a961f73fcdc4003d81f1cb7c590aaa34c8a113f7d9c9e18057411e0738	949d3f6f58c2bff76e4441feebd9ec14c3c958584b9e5ebb382fb980eae6e4e8
25abdb7dc1a29dfe13ce9b9474572abff423bb8d1eeaf7bf03d20952185000bb	94c64cf7370b83ff74104184726d5d860932a7cd6a1a4d392898d41484e9758c
27821a47a140cf4d8fba8d6651ffc790f9b4196e0f90cd22c9e3485f1386b1ca	964d170c22ca7564b27f8f395b9dd86dca266557cb85156a37e3813657ba0973
28e25acc247d5e664e763a22813a67f922751e72abc172372d701c9c724a90cc	996b00c7337136910e895da61bc5f795a6cc83df143672caeb72260f9e0ed2de
29b35e9721ae527050bd145fa7febb1620181a8aa4ad75845ed2283567571bb7	9a2ef8c338c7c6c6ba07a2395d6f0bcc376f1b6df6cb7ebdc96e8e87601f2670
2af5be188235899d26b5702b870f230186206861ea6aec2c29c198936775e303	9c91e32bb564fe98d85cdbf09467d2c2addc80b022c13fc4717af74f11e5556e
2b7e4e0d89f72c4027e5f59fbba3732843756fbd750ece6854cbfe6b7470af20	a7947986465546c3aca3b31bc07361e41e3e9d572585ed512d162a8be1cc5b6d
2ca29108b0e63e61cdb298c9ccd5064b364cac8fcffd4972481abed54e0ddfd1	a8a21ead3a5a000b8f2f4e1fdabf7009ad045e3a47dae99990e831e47dace6c7
2d49046fc064b91ca9ac6b885536752ac075d5f370afc9d43148a0d79c4cfa51	a9281fb1208914d2617e86c608a4b98cabf97d43afde5da01ef405bfe3e42d98
2f9adcc7c67376e00dde4d6f205bf986682cba2577e744bfddab1371e33c769a	abc5554f1af794e9a8ba5f31d2e9f771fbeb068eb9cc1ae54ad32f51c9ffe5fb
31b47d1e9862a24d4787ed9a10dc28f84e616a0a2b94a6a2fac44cde47d565a4	ada5d5a85c0e92e434eb4e09e80098ce790f760203cbaccdd9b95388ac6b7e21
33ebcfcf2a9cadcc5e5d8bc55e233a9fe1cc1e4be394464c7358d53f5a1af636	af710207f9ae5cb7ab1454b309faf5fb7ec3e8594f1a7034c9aa8564ac084cf7
34e358e5f5a27c3a11d3d24d9c2ce77ffd4287d4a27624e178523abab322280a	b1f67a18c51c0c2ad1702273a472dfabbd980f939f2d8b04b1a3a280d5d02443
3568c70e775ee5811a5b7e2469404ff40381661edfb5e3c269c431f4e0e77874	b5596ba3b944bc700fdd50f4164c02d645993998fb4249d6794231104 70c501c
358ed107c0ee5415d97b9bd9445a363ce135bbab29a12ae7daa028dd9e5514fe	b65aa82b120c9778dcd5c912d1cf7c3899c23f3b36d55856f28e783f5ce9bdb7
35c27e9f9d2ad8f424658af047fc11b16bf6bbf1d36ae26786287de135e77a0a	b8ccabde83c2922ad13986c7dee9e17f8c0b113c3d75c5f0abf305531e2abef8

3854a40447d291cd2fd1dbbacdbb1b3cea3b1a5d4ed3c9dde930e828573dcb17	be6db13663d7371c3c55ea4899e8651420b47ac10a24d080c0be848faa6189b0
3a433845664c3eb9b020309ea027eb1315e3f3efcd1ba1343198169011b4c9f2	bf27ad817e199bdd5adc27520bd69e639488e83dd869167e5d3442df1e9e4f1b
3c5ca617ed954bb26d37c378f6af82b49a887014a1e4932816ef7f803e3ca732	bf88bc70aadf8a2d5000fa16f683f0540733c8034ad611a896509f47d95fd976
3cac09e1d7db76e410618bdbb47ae900eaa2822ed673795566df74c40e64466d	c50c41a537a9d403e30b52b64b4543901f25fb3d5a3b23dd078d859a8e49bff7
405c07246bb15a22efe0a182e7d4a305a47143a05d614724e664216833542c79	c5150498d85f37076366cb75c223d4c26b65ed7a7466ece0af3344c3e7189044
41944366953e90e2ac766eaabd79ffe7025801a5561368e1d9e382f9288c4d3d	c56202470ed30ddfdd640490fe05bbdfbc741543d58f33e14a702584fb752f1f
4227bfd44fb17b8ca12b101935d21584bfcea0900cb21ca9b046843c13302ca3	c741db44bb434a01cb739da0ba7df5ad5e396e7a3a5afcf79c11d071a5339b4b
450d39fc584c17f1c098b2450657577da632d6591e06a3ac0a7884cb82a09089	c7d43135ef0bca64a05155797f2da23750bbbf82d6700a0345e3153f2569ece0
46311c56735daaa51d8a66e1083b0a7e9c481284ce049527d40b15584da4e44e	c8593c3cdcd06782a31b0ea47aadc95e1adaf94ef97f90f6f5832d3512998ff5
469ac8a418f2dbb4e433d022cc757fe2ddb270878b4c7ab13ebf4f8a316c30e6	c89f378b13772515bb6877e0911f8cc20089a6a0134919f51a96a90a20722358
46c9b8459b323f282b67b7d0758493871ec65dabe811966a8d5defd25d860a5e	c8a03988e9c6e10231ff77b69c6e05c1086137547a1afcb77684b2261133c647
48be4f36de2d5ea66cbd3771f9bcef4e135042d6c48278b029e4c81baca59e40	cc903d861cab466b9b294590eeb754bdd87345ef6c5e780e0a9edda184578857
49b0709d22536eb3ddbf6b3468a63cb48491a014a7895436ceed6e3749888f5e	ccb68c28786d4c0f1a0206942a333afa24df6c13d0ee87ee170373e25790a2b3
4b29413aa72ff561fd947dc960551620689f88f16374c70101f64355d5586bf0	cd60dfdb49c85d438bbccbe45f1a36fc63112986cb4b101adfedb218f755d70b
4ce9df1e1264045ad777d99c61dddefe4fef6126a7fd8af26fddb734798a13c2	cdda83dacfd4df53a2d3f69dbadd021280b774cb52cd9cdadab432d8b33445bd
4d9c498ea23d508747ea31f1e2e91d939466b5d4eb6f5d42c318d993a126bec6	ce28a590d073b5a16ea79f625fc76c9066761a9fb633a21b4112163537910 46a
50c99a8c87e058a5014d571e6c88924d68e4288b438a78f66e424e26c51854b2	cf7c5c9932e84c5e7b4581ed4ab33d064f13bac0d2cf382eb274c72730bebf5e
55568557ef7932bdc075a93a999f9f0661f65f2188e57071ee48109650a32ee5	d27dd6bc62a7a144b980a08fa423ede7050a711dd0b48bdea98dca9918beb03c
55675c3ae80a0285d40309b105ef21b18e91676944b6c9db5653d0c9c575c6e1	d35cab9f4802e9c8b6c7411ff662238c96d503898aff61a765f3f8949709bbd7
56104a9e473ce1e37bb91ba141ba0b88a92e310e6d084c3db7dfd5bd0c71dd0b	d626392670f46bce0b566365be6e6bfef4fa0a0d21e52f593c21522fdee4d6b2
569a7d28d6d93e5fa505d0d61c6c4d34ab1434b4aaefe24d2ff54992d7fdc7b8	d7db49d46500e27b9b41dfc477ff5bbeea95a7cc1dfbed007c8af3cb01eed77e
570247981c6c548f87e70c05c004ca61ed127a972ddee406fac05b811a9d3341	d8419b48de488430efb5c7e0cc5483cba6ad43e27d166447cc37eaee019e202e
5766acffa3c66b956594558c7a4e8047f2cd3a85a639833a4fa3cd0afb3af511	d9e36a8e86f9e2b3cbe50c855545956d453aa525e09054818792659d8d9865c8
57acfc3aa4a6971016d73d91eb986ac18344bdc56a6b7ecdd5bbc045d04f75cb	dbe26fdd06b44960348b6413a87d6de6227e3f7bd67af08a57ec8c3eb35e6c87
59d2fe350de6d5a8e7812752db8aac8720354bc02d9f245016c8c8ca0ebfadc1	dd2d287a890a8e4dd284ff9ae71fd2c5811987acf1b42bca8dd12ac2cda9e202
5a39b64f351708e72ad56acbd1067970f2a17194dabd5eecdf3dfa44b7e2dece	e0697a7fb940a64bd2d83be1a1aa165adbe9d4a17f1d4c04cae13129ffe132bd
5bf845e70cde6a5112d1aec081e98995bc8494ce31682762bad07ec7c92a2889	e12977f6f0fbea8d2906b68d1dd3cb3d96d0c9580dec5511df4e62efb128be62
5da8641af0443860606e234da7b5ea3bced3827ed38f612afdfe5a180a374ee2	e1fe084dc36faee91808c5a09e21d09c5ad2031142751576cc1259e99844e246
5f6d826b32b5b3fa5a3eb0346ccd94042e0ac9b22340f515557882cd1de63c73	e9149eb49ae80c9b0ee866edb0481d589602c94342ea3f13c1eb6c1a751b2324
5f878288e6e1b79f0646d9a72b1fc6cc7cd904797f3c3cf13914ce0d49b0b21f	ea0166846a9854c37b48fcf2e496ff1ab18420b7537f8cbdaaf0489fbbc77a71
613b5390c9730a4cc28e78503e23cdc3fdf46f27f1ed9fcade224d5123331c92	ec1e659237ab236777d1d1dd5d5ba44bb09afec4acfd9eae136805dac0f9cb70
6249bb48d251f321bcacba5f13d625f82913f17bb22178dcfd0e445f41c7e273	ed9cb7b72c98557788c22d2f07c0c40b5e51c9a8a91c6a4b43d06eed20c7ad2a
625fb24b0d1fb53f2bbd10bbfcf7f752bca0d497275a10f8b307afe08748baff	edbc823090374983bc1af9bd53a2ce3b02039d99afd8b0ed29e121202eae920e
660baf31937efc802ffc09397e319b3404dd242281144d98604d7b689db83b11	efec1393393c4f4655ebc3b8a18a05ff216b462c2ad207777c37680321269498
697931f83507d2cbc800d1964f6e1fe4a5b31dd3124e20063cb846b4a8181020	f0f0ab7a04453d0254724613cfca62b5ec613b5af5b11183af648ad8a558a47c
6c11c295ca138decdc721470c867b1e45723acba612bfdd37a226cbe2b200b45	f982a511c13d6871b6e5274a5706a17110508cd6aff15525b61817609a4257cb
6f0b5cd72bd26cb6f643da4ae44722b917e3f9ba614e2242401660c6ebe23655	faf1bc224c559ee645998e3e2e934e04cc04a48be6bda76b03445ca20a92c3ed
72898d5db856d5107d6da2b6bef3edb138aa1a464f99ba4768d2ee55697098f5	fc2c979f533e79f45f858febf1103743fc092cc5882960c399a2d7764a067fc1
72c44eace723309b8b2706abf65df470aa630607d4ccc423fe68c7c896c04b89	fd18d4dd7f49cc50513089885552f63976fe52368a8f80e1215a17a7345463e1
7376b4a154eb73e11fa0b124f4dcb685e2557503a5b6c50a13f4223125757394	feb1f6b1c4eb87944ab748cd361b96cc5b59bcb5006df792f5d5c4b2def633f8
73906ffaf4e05f5fec65308473dd8d22808806dc12fee04b1cd6c0df82ce69d0	09fe3fdbea7c4614855237eb2a19b1efa3d204591a11eb2d0b2a34c4f30d9da9
77c90077fd50fc3c9450dba377e5833840baca792e34af9d0bce8fe40ea270fa	0e46c07eeabe6829beb260251ed62eb4724d318954cb3ead3eb8bb8133f4f2bc
7b20c42eabfcb75c62ba2730d3e92e4fb4b6b8b025039d6a80f23462aa755027	3209a985960e1272ea8f886f8096b103577aa5aa041150ee14c5445ad82cedac
7cbf2adb28ac387eb17d82a6d7b3c81056c87f43396a7f40b778688c16528194	ca35b7fab0b94484f4865d1804251255d5a5778567715d70496a11e76d26aeba
7d843782853790c18855b93602b2c260cbe9542216c6ed95aebcdb2f1c41be4e	db0f02e7fe6714d6e101c8441b4b31e20929fd6cda45a6df3ab425341218b14d
7e0d6fc8bc7a69d5e27e2130c83b434512af52a5337145098c2426f62abf97ee	e4023c3ed629d16ec28bf13929b329b798cbc0cc05aafa2abf04045d9209eae4

7f1fe8748f260ff27f08ebf04ccedd2cb34a45a95f9dba3d0e0c36cf6c8cb252	e71e6d04f1065ef25ec0c07652439fbd663c1113afd6314690a1b0d2c6dcae87
7f686e839b9a238cdcc244ff0dffc85135f88dc7ac49bc09aba46a1481e52cc3	4d27b24408ccaed59ba5977e7e7309fc42fc9964bc4e3d4cd3ac363f1b539454
80920c14b4f64ef5834a704586c5133f12a331fa562219b16dcfec0c4af4aa87	b15af175de8cf5d1a9527f047643f5039a1506dee07822e6d73746fc60d67dad
818856325a3aaaf54865c43c6efbfbe60605e3e10d7ec5b5936471479bae050e	67d62b54619a4b53ddaebbacf6b88f623933cfe54340797a92c3012b65b8a11b
c8613cbe02f1e23ab87fcce103efa89cc8da78705c42ca373fa45f3d213b9f5a	

Archivos reportados (se recomienda mantener monitoreo)

153.153.67.31	157.7.218.241
184.95.40.234	181.211.39.118
153.153.66.24	72.52.184.156
103.148.85.24	69.89.28.227
69.64.67.199	200.105.166.165
211.13.204.70	51.195.21.184
192.185.67.41	119.2.43.162
185.222.57.80	201.76.49.195
192.185.59.4	84.205.254.49
74.208.160.241	154.0.166.36
118.70.177.62	192.185.60.19
186.15.226.14	200.147.35.78
45.232.16.3	98.142.235.175
168.234.50.3	107.6.16.119
62.171.190.234	119.47.118.39
62.141.37.114	41.168.2.24
192.185.146.119	192.185.143.4
162.144.150.204	182.16.156.253
103.70.62.133	43.229.86.7
192.185.146.82	189.126.112.24
192.185.51.110	103.15.48.14
202.139.238.241	188.130.162.100
192.185.145.119	64.64.10.218
202.4.96.94	162.213.253.84
118.98.75.71	62.149.157.214
59.106.33.116	62.149.157.206
112.213.92.40	93.174.123.137
112.213.92.70	192.185.144.91
120.72.119.27	59.106.171.40
173.212.232.194	52.214.185.48
162.144.201.136	62.149.157.210
158.69.184.123	64.22.104.113
103.247.8.181	41.223.192.18
222.255.235.87	207.180.200.146
192.185.45.163	192.81.129.195
103.247.9.47	213.180.89.149
121.254.168.204	212.174.74.2
66.96.184.9	203.160.60.220
192.185.146.97	174.136.29.115
197.211.212.80	196.200.16.23
209.95.56.247	103.76.228.139

197.211.212.99	190.5.10.29
98.142.233.70	203.124.41.30
192.185.151.58	196.6.233.230
192.185.45.43	200.6.225.45
103.28.38.40	103.28.38.233
192.185.186.5	210.172.192.21
203.128.6.125	103.94.220.248
197.221.52.212	95.65.9.19
153.138.237.27	103.23.20.233
131.153.50.170	183.81.158.163
41.76.0.123	94.100.6.16
5.160.71.152	64.136.55.15
192.185.49.40	91.223.162.21
98.142.235.168	203.90.226.196
109.105.60.2	40.92.20.74
192.185.149.101	41.89.36.2
66.96.184.1	187.84.239.20
207.248.63.91	196.15.235.90
185.145.97.151	186.189.234.20
207.38.82.50	23.83.215.42
113.23.215.180	177.70.124.124
81.19.149.129	213.159.30.161
216.157.33.76	154.73.84.9
182.71.244.126	45.11.19.191
203.152.107.75	69.63.70.199
62.12.150.104	203.160.242.138
202.43.45.113	40.92.10.100
186.46.43.163	40.92.42.65
62.149.158.120	128.199.22.174
154.0.173.36	142.93.218.187
200.147.35.72	142.93.213.160
69.89.23.89	128.199.22.15
70.40.196.235	95.111.255.154
202.59.89.60	153.153.67.30
192.185.198.13	216.198.226.94
192.185.145.18	202.84.44.77
81.21.76.54	203.128.3.19
206.152.134.66	109.237.142.241
200.45.1.137	104.148.61.170
202.134.99.174	92.223.93.162
192.185.149.62	139.59.89.144
192.185.65.13	104.148.61.175
192.185.192.34	104.148.61.165
144.208.64.39	104.148.61.168
69.89.22.91	104.148.61.178
192.185.45.95	103.146.234.10
192.185.143.31	104.148.61.171
65.99.252.241	104.148.61.173
173.212.242.213	37.48.85.221

Correo electrónico (se recomienda mantener monitoreo)	
accounts@himraj.in	kepsdpml@oel.or.id
admin@victoryeng.co.za	kmohan@sail-steel.com
administrativo@fitoformulalab.com.br	kos@hcg.gr
adualdobobbiesi@cernet.com.ar	kvnm02@vnmail.kymco.com
agmajid@omnigroup.com.pk	liliana.benalcazar@17d01.mspz9.gob.ec
akash.maharjan@smarttel.com.np	ljnikolic@bkosa.edu.rs
almoxarifado.filialar@almad.com.br	lkchau@bvpharma.com.vn
ammar.khan@apag.com.pk	luziane@jamengenharia.com.br
ashish.garg@obeetee.com	m.ameer@noon.com.pk
ashish@techindiawide.biz	m.tavakoli@tabiatco.ir
atin@e.pthunga.com	sergiobianchini@arnet.com.ar
ationashe@concretemasters.co.zw	shoaibahmed@masoodtextile.com.pk
awais.amir@profarm.com.pk	siven@ymscc.co.za
bau@bureckbau.at	skovde@ljusexperten.se
bids@maverickmillwork.com	sta.tax@sta.co.id
bitutu.nyambane@kirdi.go.ke	stephen.mutangadura@sgmusoni.co.zw
bkadirov@gilanconstruction.com	stores@daimeislk.com
bongsiwe@dnet.co.sz	studio1@rongtulipvtltd.com
caotuan@ybm.com.vn	sumon.ahamed@fsl.com.bd
carlos.lopez@honda.com.gt	supervisor.tdasps@grupohon.com
chaish@hongshinbuilders.com.sg	sureshus@secokomos.co.kr
cirebon_rpt2@suryadonasin.com	susi.rahmawati@dls.co.id
comercial@hospitaldasacacias.com.br	tahir.mushtaq@toyota-islamabad.com
comercial@hospitaljardins.com.br	tanin.asil@meghnabangladesh.com
comercial@hospitalstaclara.com.br	tarun.s@bg-groups.com
contacteuppy@eup-energy.com.vn	m.waheed@ificonsultants.com
contato@clipperturismo.com.br	mail@asfhousingscheme.com
css.del@znsgroup.in	makarand.mehendale@obeetee.com
cutting@denimasia.com.bd	makhdoom@kissanengg.com.pk
danish.imtiaz@kiamotors-macca.com	mandisa@neighbiz.co.za
diannepaul@compassnet.co.nz	mandy@ammtrstarcargo.com
diepltn@techtrol.com.vn	marketing@totalsolutions.co.tz
dladla@iburst.co.za	maruume@ip.mirai.ne.jp
dp.rh@ciamarro.com.br	maryaye@centurytel.net
ecoecoagro@uvigo.es	mectbc@juno.com
edmondsiebert@vodamail.co.za	mizan@unitedinsurance.com.bd
eduardomiretto@ri.com.ar	Monica@transorientgroup.com
eg.adminmanager@algoa.li	muh.ishak@skalasukses.id
eigyouka@yokoo-net.co.jp	mumbaihr@ampsindia.in
eitta@kamalenany.com	n.sultani@afghantelecom.af
electromacltda31@outlook.es	nages.ts@tucksun.com
estherobeng@centrepointgh.com	nagumo@shiba-ken.net
eyecareplus@cleworthbarinioptometrists.com.au	nakatani@maho.co.jp
ezequias.araujo@fulltimesolucoes.com.br	negishi@koyanokoumuten.co.jp
fabiana.stassi@ladisaristorazione.it	nikat@fintel.uz
fabio.pallaoro@rossinitrading.it	noel_iqc@pungkookid.com
facturas@elephant.mx	Noman@adam.com.pk
fbm@gtspringhilllampung.com	norlie@victorymaritime.com

fc@rhdevani.com	nv05@tthla.com
financeiro@ecobituqueiras.com.br	o.oke@westernlottoandbet.com
financeiro@rphospitalar.com.br	oanhntk@eup-energy.com.vn
tesoreria94procolombia@outlook.es	office@bronhill.com
thaesler@ksh-haustechnik.de	olimpio.vendas07@terra.com.br
thana@bisaim.com	operacionalsc@disktrans.com.br
thassia@kantoferramentaria.com.br	oskim@dbgroup.co.kr
tho@kyosekisangyo.co.jp	outbound@kbatur.com
tmakame@e-com.co.tz	pagos@hsbc.com.mx
training.ahu@iso-jo.com	pcp@ciamarro.com.br
unit@cwpolicing.co.za	pericotecnico@macgroupweb.com
ushan@intecssl.com	po@memoirehotelsresorts.com
ventas.apodaca1@elcastillorio.com.mx	portagemaputo@tracn4.co.mz
ventasferre1@ferrefama.com	ptorronics@vodamail.co.za
viceintendencia@junindelosandes.gov.ar	purchasing@pidman.com
vmendieta@autoridadempresas.gob.bo	quelcy.vasquez@cobankiat.com.ph
volquetes.kolpa@mceisa.com	raebarelioffice@bloom-india.com
vu@vantaiqueanh.vn	ragab@sunsnack.com
financeiro1@tadex.com.br	rajashekar.narayandas@rehlat.com
francisco.bezerra@abccrm.com.br	raquel.martins@medicalseer.com.br
g.merida@ocacall.com	reservas@altosdesantateresa.com
ga@armabali.com	responsabilemagazzino@cilsrl.it
gaurav.arora@magnusfm.in	rizkyningrum@e.pthunga.com
geral@mozsecurity.com	rocio.morales@17d06.mspz9.gob.ec
gerencia@conexaohome.com.br	romar@htsphils.com
gerleen@secunet.co.za	rongai.station@toshapetroleum.co.ke
global@bomtech.net	rotorua@greatlaketransport.co.nz
gm@zivavillas.com	royalties@baraodistribuidor.com.br
guntars.velbergs@meliorprojekts.lv	rpm@work.co.bw
henrique@salessa.com	rwh.mgr@ethicsgroups.in
hkajal@awcsoftware.net	s.canales@adepeshn.org
hoque@meghnabangladesh.com	sales@bachthang.com.vn
hr@hillockshotel.com	sales@pomco.ae
hradmin@cengkarenggolfclub.com	sales@tin-mx.com
htnkfin2@ovk.co.za	sales1.vn@artrend.com
iab.gtm4@biomedicaenlinea.com	sales2@isk.com.hk
imraanm@pulsegroup.co.za	samoranandos@simbisa.co.zw
info@5stripe.co.bw	saranya@morrisperlis.com
info@apicsglobal.com	sea.valare@amosconnect.com
info@bravointimo.gr	sergey.turcanu@bmw.md
info@emomo.top	tasnim.ahmed@clarichembd.com
info@hotelpapiros.com	tesoreria53procolombia@outlook.es
info@igsmd.de	yaser@agrizone.ae
info@msc.com	garyxu@icoolglobal.com
info@noedj.com	sokgim.lua@ikano.asia
info@patelpackaging.com	glenshan72wcpo@gmail.com
info@rugby-osaka.org	sales@tcfs.net.in
inv_railaybay@krabi-railaybay.com	Daniel-Wei@co.ac.uk
Jabeen@pizzaking.com.fj	accounts01@shipping.sinosteel.com

jaime@notariahopkins.com	patrhoyt29hejy@gmail.com
jcarlos@ureserra.ind.br	chris@admatehellas.gr
jeffry.lie@henanputihrai.com	trojlita384qiqyi@gmail.com
jia.yu@genolution1.com	wandaver2nygnx@gmail.com
john@dreykon.co.za	sawijama5qe@gmail.com
johncy@npmanila.com	klostocc091akiz@gmail.com
jtejada@ct.co.cr	medinaluca1kntiu@gmail.com
karachi@pasarigrp.com	fadecice330motoy@gmail.com
kdemir@riskmed.com.tr	itsupport.gopinath@newtoncsc.com
keith@texasskillet.com	fantjame060pee@gmail.com
michcons458nacyo@gmail.com	lacejoly2muua@gmail.com
fui.manak@mojaz.org	sales@mickmgmt.com

URL (se recomienda mantener monitoreo)

hxxps://sulselekspres[.]com/cgi-bin/6l0nyO/
hxxps://maulanarumifoundation[.]com/RumiFoundation/Q9etF/
hxxps://kelas[.]yec[.]co[.]id/srjns/B/
hxxp://caesarmoving[.]com/wp-content/9s/
hxxps://kinepremins[.]cl/wp-admin/6wr/
hxxp://dolphininsight[.]it/wp-includes/LVf/
hxxp://hdfilmkurdu[.]tk/fwecj/w5ghXyxtzp63449/
hxxp://retrocycle[.]cc/wp-content/Ulgocr0611/
hxxps://pc-a[.]co[.]th/wp-admin/3cu5a279445382/
hxxps://novavitta[.]com[.]br/site/sdxrk4616/
hxxp://miniessay[.]net/wp-includes/YhhuqdBFmjcZ/
hxxp://pemnas[.]ub[.]ac[.]id/wp-content/reUfk5i84877332/
hxxp://hdfilmkurdu[.]tk/fwecj/w5ghXyxtzp63449/
hxxp://retrocycle[.]cc/wp-content/Ulgocr0611/
hxxps://pc-a[.]co[.]th/wp-admin/3cu5a279445382/
hxxps://novavitta[.]com[.]br/site/sdxrk4616/
hxxp://miniessay[.]net/wp-includes/YhhuqdBFmjcZ/
hxxp://pemnas[.]ub[.]ac[.]id/wp-content/reUfk5i84877332/
hxxp://www[.]novachem[.]com[.]tr/wp-includes/file/HDSTwTon/
hxxp://www[.]novachem[.]com[.]tr/wp-includes/file/HDSTwTon/
hxxp://hdfilmkurdu[.]tk/fwecj/w5ghXyxtzp63449/
hxxp://retrocycle[.]cc/wp-content/Ulgocr0611/
hxxps://pc-a[.]co[.]th/wp-admin/3cu5a279445382/
hxxps://novavitta[.]com[.]br/site/sdxrk4616/
hxxp://miniessay[.]net/wp-includes/YhhuqdBFmjcZ/
hxxp://pemnas[.]ub[.]ac[.]id/wp-content/reUfk5i84877332/
hxxp://somosdrucken[.]com/upload/GGQL96W/

hxxp://www[.]vedigitize[.]com/wp-includes/l9K6YJ/
hxxp://www[.]sosyalben[.]org/hpKTnb/
hxxp://www[.]sutomoresmestaj[.]net/menu/E/
hxxp://www[.]traveltoharamain[.]com/cgi-bin/b/
hxxp://www[.]thinkdesign4u[.]com/css/Rtc1/
hxxps://www[.]mwk-bionik[.]de/fileadmin/vOJ/
hxxp://solution[.]seeedstudio[.]com/tag/FNLFibbOyHa/
hxxps://dangkyinternetviettel[.]shop/wp-admin/anSiIxw/
hxxps://firstresponsecpr[.]com/alfacgiapi/hNBmlles94w163/
hxxp://literadiocebu[.]com/vhvjt/aycx52bqm330139/
hxxp://latestmoviesbox[.]com/wp-includes/uwap2390/
hxxp://arya-co[.]com/wp-includes/lIaWADd/
hxxp://pizzaherbs[.]com[.]pk/pjqbq/XnPgtdPPN/
hxxp://www[.]riserproperty[.]com/wp-content/SMXB/
hxxp://laurenebohn[.]com/bGOHy/8qa07472/
hxxp://lezliedavis[.]com/swift/5TQW6sf32736/
hxxp://cityplanter[.]co[.]uk/zy0b9r0s/lTZlc101auo37/
hxxp://farooquie[.]com/wp-admin/da52f6268411/
hxxps://onejmd[.]com/wp-content/xmO/
hxxps://s1[.]finmsb[.]com/uc_autoscripts/AcpPvTthOX/
hxxp://www[.]novachem[.]com[.]tr/wp-includes/file/HDSTwTon/
hxxp://hdfilmkurdu[.]tk/fwecj/w5ghXyxtzp63449/
hxxp://retrocycle[.]cc/wp-content/Ulgocr0611/
hxxps://pc-a[.]co[.]th/wp-admin/3cu5a279445382/
hxxps://novavitta[.]com[.]br/site/sdxrk4616/
hxxp://miniessay[.]net/wp-includes/YhhuqdBFmjcZ/
hxxp://pemnas[.]ub[.]ac[.]id/wp-content/reUfk5i84877332/
hxxp://qstride[.]com/img/0/
hxxp://tskgear[.]com/wp-content/uploads/2015/06/pz/
hxxp://vermasiyaahi[.]com/cgi-bin/8/
hxxp://www[.]weblabor[.]com[.]br/avisos/QIU9/
hxxp://viniciusrangel[.]com/experimental/VIhMh1/
hxxp://westvac[.]com/wp-content/GOYx/
hxxps://viewall[.]eu/cgi-bin/SbhZP9X/

Recomendaciones y Buenas Prácticas

Recomendaciones generales de seguridad

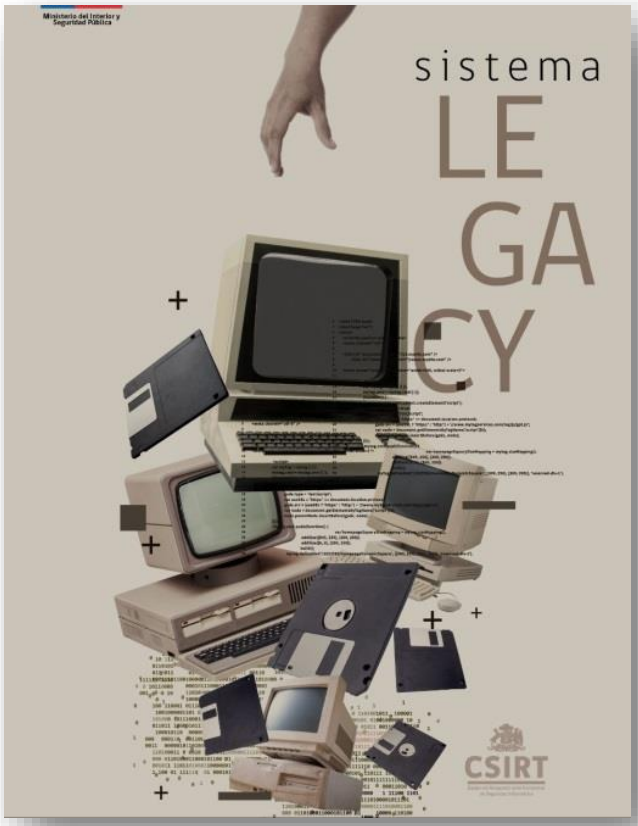
- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet
- 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.

Investigación

Sistemas Legacy

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la décimo sexta edición de su publicación sobre amenazas cibernéticas el que analiza los sistemas legacy. El artículo fue elaborado por Natalia Pérez y Paula Moraga, analistas de CSIRT.

Los sistemas legacy o sistemas heredados son soluciones computacionales en contextos tecnológicos ya superados, pero que siguen vinculados a activos críticos centrales en las organizaciones. En otros términos, son soluciones del pasado que representan un problema en retrospectiva. Este tipo de sistemas son un desafío para las organizaciones que los sostienen en el actual contexto global, dado que la disponibilidad de tecnologías depende de múltiples soluciones en una industria que, además avanza a un ritmo acelerado, donde los sistemas tecnológicos de épocas pasadas están destinados a la obsolescencia. El desafío de este artículo fue crear un acotado panorama de los sistemas legacy en nuestro ecosistema nacional, para lo cual se acompañan algunas tablas estadísticas que indican que tipo de software cuentan o carecen de soporte –en general-, y cuantos sistemas expuestos a internet estarían dentro de esta categoría.



Ver más en: https://www.csirt.gob.cl/reportes/an2-2020-16/

Actualidad

Cyberday es un evento que adquiere cada año más relevancia para el comercio y los consumidores en línea en nuestro país. Más de 500 marcas ofrecerán, por tres días, ofertas especiales e imperdibles en una actividad que no solo llama la atención de los clientes, sino también, de los cibercriminales. Los riesgos de ser víctimas de un ataque cibernético en este fecha aumentan, por eso, queremos que tomes algunas precauciones antes de visitar un sitio inseguro y realizar un click apresurado.

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.

- Francisco Brandan
- Matia Cornejo
- Ewald Hollstein

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.09.05 18:56:25 -04'00'