Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

28-05-2021 | Año 3 | N°99

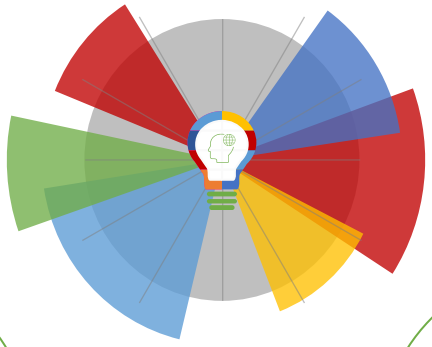
Boletín de Seguridad Cibernética

Semana del 20 al 27 de mayo de 2021

La semana en cifras

Hash
66
SHA
Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron
5
URL
Asociadas a sitios fraudulentos y campañas de phishing



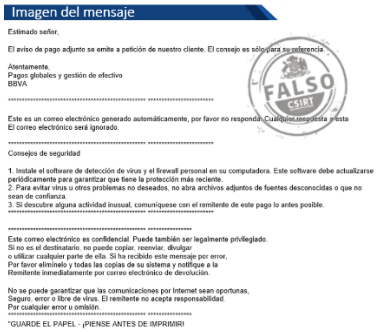
Parches
28
para vulnerabilidades
Las mitigaciones son útiles en productos de Red Hat, Ivanti, Trend Micro, VMware y SonicWall.

IP
56
Informadas
Listado de IP 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.

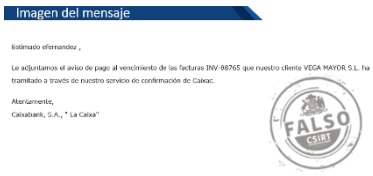
Contenido

Malware



CSIRT alerta por campaña de phishing que suplanta al banco BBVA	
Alerta de seguridad cibernética	2CMV21-00180-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de mayo de 2021
Última revisión	26 de mayo de 2021
Indicadores de compromiso	
SHA256	
F621E6EA86757329A4C5D9DC0465B3E7E850FD8CF2FB66CAAC8B3D5FF6FF475F F76BB6AA709B1AA421767E7861B85CE92C61C8BF0283614AA070C3B105FD751E	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00180-01/	
https://csirt.gob.cl/media/2021/05/2CMV21-00180-01.pdf	

CSIRT alerta por campaña de phishing que suplanta a Nestlé	
Alerta de seguridad cibernética	2CMV21-00181-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de mayo de 2021
Última revisión	26 de mayo de 2021
Indicadores de compromiso	
SHA256	
F621E6EA86757329A4C5D9DC0465B3E7E850FD8CF2FB66CAAC8B3D5FF6FF475F DA6C75EA9A77810C91F9376280A0C7C0A28D64AABEBA095B53B2C026BE24A41F	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00181-01/	
https://csirt.gob.cl/media/2021/05/2CMV21-00181-01.pdf	



CSIRT alerta por campaña de phishing que suplanta a La Caixa	
Alerta de seguridad cibernética	2CMV21-00182-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de mayo de 2021
Última revisión	27 de mayo de 2021
Indicadores de compromiso	
SHA256	
B8234FF9A19C19662B92000FE74B67E04970BBCD45E307CA45F51C4D8532739E 7693A7C44C28C716E3912663EFBE89E5DDF260E236BF3C7939DABD79D6D925F4	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00182-01/	
https://csirt.gob.cl/media/2021/05/2CMV21-00182-01.pdf	

CSIRT alerta por campaña de phishing que suplanta a la Tesorería General de la República	
Alerta de seguridad cibernética	2CMV21-00183-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de mayo de 2021
Última revisión	27 de mayo de 2021
Indicadores de compromiso	
SHA256	
d5fe97d4c738a779badb82fea8d5a3b6b4841dc5eea16e9580165956c6462db4 3b00ba098ef5d492c6a2cee50837e535cef3094e72705d35134ede26dbc1c351	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00183-01/	
https://csirt.gob.cl/media/2021/05/2CMV21-00183-01.pdf	

CSIRT alerta de campaña de phishing que suplanta a Dropbox	
Alerta de seguridad cibernética	2CMV21-00184-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de mayo de 2021
Última revisión	27 de mayo de 2021
Indicadores de compromiso	
SHA256	
05A62614830E67B22692B2504A6EC4BA5BE93EE3D757DA5A020FD12A657343B1	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00184-01/	
https://csirt.gob.cl/media/2021/05/2CMV21-00184-01.pdf	

CSIRT alerta por campaña de phishing que suplanta al banco HSBC	
Alerta de seguridad cibernética	2CMV21-00185-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de mayo de 2021
Última revisión	27 de mayo de 2021
Indicadores de compromiso	
SHA256	
2928734BB8B73D9B7C9DA9EE4BC8BE23C8F22D2FB8999A821AC23E0D716B543C D14FB279C5FA3A755EB6F9ADD867A8A7D293858D62C94EFB6A20BD5EEE35FC7F	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00185-01/	
https://csirt.gob.cl/media/2021/05/2CMV21-00185-01.pdf	

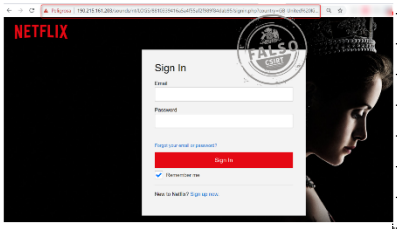
IoC Ataques de Fuerza Bruta

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), con el fin de suplantar un remitente original y así depositar correos con contenido o enlaces maliciosos en las bandejas de entrada de sus potenciales víctimas.

IP	Etiqueta de sistema autónomo	Documento web
45.227.253.116	Global Layer B.V.	4IIA21-00038-01
5.188.206.182	Krez 999 Eood	4IIA21-00038-01
85.93.20.10	&L Investment Ltd.	4IIA21-00038-01

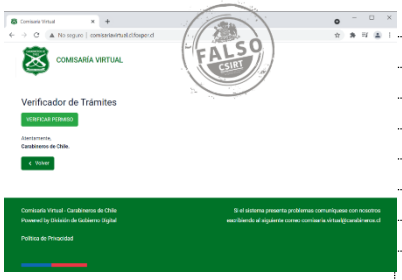
Sitios fraudulentos

Imagen del sitio



CSIRT alerta por sitio fraudulento que suplanta a Netflix	
Alerta de seguridad cibernética	8FFR21-00955-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de mayo de 2021
Última revisión	24 de mayo de 2021
Indicadores de compromiso	
URL sitio falso	
hXXp://190.215.161.203/sounds/nt/LOGS/8810339416a5a4f55af2f989f84dab95/signin.php?country=GB-United%20Kingdom&lang=en	
IP	
[190.215.161.203]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00955-01/	
https://www.csirt.gob.cl/media/2021/05/8FFR21-00955-01.pdf	

Imagen del sitio

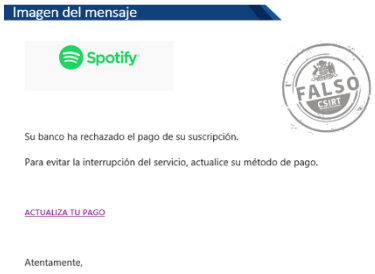


CSIRT alerta de sitio fraudulento que suplanta a la Comisaría Virtual de Carabineros	
Alerta de seguridad cibernética	8FFR21-00956-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de mayo de 2021
Última revisión	26 de mayo de 2021
Indicadores de compromiso	
URL sitio falso	
http://comisariavirtual.cl.foxper[.]cl/	
IP	
[184.171.242.173]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00956-01/	
https://www.csirt.gob.cl/media/2021/05/8FFR21-00956-01.pdf	

CSIRT alerta por sitio fraudulento que suplanta a Facebook	
Alerta de seguridad cibernética	8FFR21-00950-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de mayo de 2021
Última revisión	14 de mayo de 2021
Indicadores de compromiso	
URL sitio falso	
https://realestate-agent-290751038.steelwork[.]cl/	
IP	
[186.64.119.35]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00950-01/	
https://www.csirt.gob.cl/media/2021/05/8FFR21-00950-01.pdf	

CSIRT alerta por sitio fraudulento que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FFR21-00951-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de mayo de 2021
Última revisión	14 de mayo de 2021
Indicadores de compromiso	
URL sitio falso	
https://srv.proactivesolucioneslegales[.]cl/login	
IP	
[200.63.99.33]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00951-01/	
https://www.csirt.gob.cl/media/2021/05/8FFR21-00951-01.pdf	

Phishing



CSIRT alerta por sitio fraudulento que suplanta a Spotify	
Alerta de seguridad cibernética	8FPH21-00402-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de mayo de 2021
Última revisión	24 de mayo de 2021
Indicadores de compromiso	
URL sitio falso	
https://sodikmudjahid[.]com/Usario/Cuenta	
IP	
[202.52.147.113]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00402-01/	
https://www.csirt.gob.cl/media/2021/05/8FPH21-00402-01.pdf	

Vulnerabilidades

CSIRT advierte de vulnerabilidades en productos de Red Hat	
Alerta de seguridad cibernética	9VSA21-00446-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de mayo de 2021
Última revisión	24 de mayo de 2021

CVE

CVE-2015-8011	CVE-2020-28362	CVE-2021-3114
CVE-2020-15586	CVE-2020-35498	CVE-2021-3115
CVE-2020-16845	CVE-2021-20305	CVE-2021-3121
CVE-2020-25648	CVE-2021-21290	CVE-2021-31921
CVE-2020-25692	CVE-2021-21295	CVE-2021-3424
CVE-2020-27813	CVE-2021-25215	CVE-2021-3461
CVE-2020-27827	CVE-2021-30465	CVE-2021-3557

Fabricante

Red Hat

Productos afectados

Red Hat OpenShift Container Platform 4.7.12.
Red Hat OpenShift Container Platform 4.7 for RHEL 7 x86_64
Red Hat OpenShift Container Platform 4.7 for RHEL 8 x86_64
Red Hat OpenShift Container Platform for Power 4.7 for RHEL 8 ppc64le
Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.7 for RHEL 8 s390x
Red Hat Openshift Serverless 1 x86_64
Red Hat OpenShift Service Mesh 1.1 for RHEL 8 x86_64
Red Hat OpenShift Service Mesh for Power 1.1 for RHEL 8 ppc64le
Red Hat OpenShift Service Mesh for IBM Z 1.1 for RHEL 8 s390x
Red Hat Enterprise Linux Fast Datapath 7 x86_64
Red Hat Virtualization – Extended Update Support 4.2 for RHEL 7.6 x86_64
Red Hat Enterprise Linux Fast Datapath (for RHEL Server for IBM Power LE) 7 ppc64le
Red Hat Enterprise Linux Fast Datapath (for IBM z Systems) 7 s390x
Red Hat Single Sign-On Text-Only Advisories x86_64
Red Hat Single Sign-On 7.4 for RHEL 7 x86_64
Red Hat Single Sign-On 7.4.7 security update on RHEL 8
Red Hat Single Sign-On 7.4.7 security update on RHEL 6
Red Hat OpenShift GitOps 1.1 x86_64

Enlaces para revisar el informe:

https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00446-01
https://www.csirt.gob.cl/media/2021/05/9VSA21-00446-01.pdf

CSIRT advierte de vulnerabilidad en Pulse Connect Secure	
Alerta de seguridad cibernética	9VSA21-00447-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de mayo de 2021
Última revisión	25 de mayo de 2021
CVE	
CVE-2021-229088	
Fabricante	
Ivanti	
Productos afectados	
PCS 9.0Rx y 9.1Rx.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00447-01	
https://www.csirt.gob.cl/media/2021/05/9VSA21-00447-01.pdf	

CSIRT alerta de vulnerabilidades en Trend Micro Home Security Network		
Alerta de seguridad cibernética	9VSA21-00448-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	25 de mayo de 2021	
Última revisión	25 de mayo de 2021	
CVE		
CVE-2021-32457	CVE-2021-32458	CVE-2021-32459
Fabricante		
Trend Micro		
Productos afectados		
Trend Micro Home Network Security 6.1.567		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00448-01		
https://www.csirt.gob.cl/media/2021/05/9VSA21-00448-01.pdf		

CSIRT alerta de vulnerabilidad crítica en productos VMware	
Alerta de seguridad cibernética	9VSA21-00449-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de mayo de 2021
Última revisión	27 de mayo de 2021
CVE	
CVE-2021-21985	CVE-2021-21986
Fabricante	
VMware	
Productos afectados	
vCenter Server 6.5 a 7.0. Cloud Foundation (vCenter Server) 3.x, 4.x.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00449-01	
https://www.csirt.gob.cl/media/2021/05/9VSA21-00449-01.pdf	

CSIRT alerta de vulnerabilidad en SonicWall NSM On-Prem	
Alerta de seguridad cibernética	9VSA21-00450-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de mayo de 2021
Última revisión	27 de mayo de 2021
CVE	
CVE-2021-20026	
Fabricante	
SonicWall	
Productos afectados	
Sonicwall NSM On-Prem 2.2.0-R10 y anteriores.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00450-01	
https://www.csirt.gob.cl/media/2021/05/9VSA21-00450-01.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	Tipo de malware	Documento web
0bce8c45300761227cf1ce6e28145aa6e141b7d22fabdb4e4131b974853e0701	W32/Delf.DCB!tr	2CMV21-00186-01
11e1eb7dbb03308eab7be9f48aa2ee4ff4b4ab09988d20ab04366f7829cd440f	MSIL/GenKryptik.FFVH!tr	2CMV21-00186-01
2928734bb8b73d9b7c9da9ee4bc8be23c8f22d2fb8999a821ac23e0d716b543c	MSIL/Agent.AES!tr	2CMV21-00186-01
29bf642213921602445d34d9d6881d4d8b9e96da2589c8257307dc069bfc36e7	MSOffice/CVE_2017_11882.C!exploit	2CMV21-00186-01
5279d2643c676fbed810a0120bc8d3616bb85a47b2b09af945a54c5b921cefbb	PossibleThreat	2CMV21-00186-01
5b8c6441f5249adfa79fb11be31196b2bc6486160918f605c85cb737894f4f52	HTML/Phish.HP!tr	2CMV21-00186-01
65f25419f8b7d977644c9a8d21228be01a80627411e84d4ae9bc697135a155d6	HTML/Phishing.DOC!tr	2CMV21-00186-01
72080b88199e2e338aeed0965513ad8bbebc5efc67dd6591828da3255464d86f	MSIL/Kryptik.ABCL!tr	2CMV21-00186-01
782f81875dd8679b6b6385164239eea4de4a1c2353ab7941a640813fac2fa0e3	Malware_Generic.P0	2CMV21-00186-01
7d39bef9e7fd7e5f689a65c05567040238f6e390484d043534818d4ae2970b98	HTML/Phishing.AABE!tr	2CMV21-00186-01
7df726976fc7075640ed2b30d2d99ad80a8456657d2aab2d8e300ba1c6a03b8f	Malware_Generic.P0	2CMV21-00186-01
85e923630d654246e87c65aca8dcdfe98aa24638ab52cf3d040c9c361eb1d0eb	MSIL/Kryptik.ABCM!tr	2CMV21-00186-01
b7466ce4f6aa0473667dfdee3521452af75c1a541d51fae05ba71ef8da48dc90	MSIL/Kryptik.ABCL!tr	2CMV21-00186-01
b8b9fe6992bfa4e5604b5031895ee42096a1132c8b1d7b72e055251b1067dca3	MSIL/Kryptik.ABCM!tr	2CMV21-00186-01
d55be05b5dd111d22304305b4303c9496b2fcc0db25e12c8fc74ed84dbeace5a	Malware_Generic.P0	2CMV21-00186-01
db96240a6b30e174d07bea659113f961f96d18ab4083b5bd8b4fa064ad35ab62	MSIL/Kryptik.AAPN!tr	2CMV21-00186-01
dc14d3b61ed80f7655a29a9553e5b57cf7f3cfb29866fd643ac80b4fede5d166	HTML/Phish.BFN!tr	2CMV21-00186-01
fe27d7565eeb956fd7e25c0e9a4189db855851ad3e66bea34c88ee23b1d5de6e	JS/Agent.UBK!tr	2CMV21-00186-01
071a4606d681d058836106eb6e9eb180919b32b6ab776f73be3a14a729430d8e	Malware_Generic.P0	2CMV21-00186-01

0b16d8339ab7157817ec5312df186887fa147960673aae8795b9f4466de32dca	HTML/Fisher.296!tr	2CMV21-00186-01
15f5d677afee8420d1a64d37561b5b5277c205d4880b94c059a8630776dc0390	HTML/Fisher.296!tr	2CMV21-00186-01
186a6b4d8e375b46c07ab59265c360056bd9a319b6b25542984c2d54e79e9384	HTML/Fisher.296!tr	2CMV21-00186-01
2cdda40f85d3141dd47d4e4c0ec2548249f7e584b0335b8c8d7cddb209004dae	HTML/Fisher.296!tr	2CMV21-00186-01
3a7f2d0d405e3e17dde8bad93a092cf03f10fe7bba0230431a0b449a384dacc7	MSIL/Kryptik.ABCM!tr	2CMV21-00186-01
3f0fc274fa84a582bca0ec6beee4fd35e69bdfb46d62ea6226caaeffb7264556	HTML/Fisher.296!tr	2CMV21-00186-01
407369e411029512deda90479a6b89b609cf11991578a6ba278add3e5a68428b	HTML/Fisher.296!tr	2CMV21-00186-01
51a84d9c198418336152d4efceafe6dbd2d8919dcbf975bff3ae585257aaf42f	HTML/Fisher.296!tr	2CMV21-00186-01
63bde55db33b2d48dc14c6d17a14b5f6198a94adf7e69da297894ef010c72bda	HTML/Fisher.296!tr	2CMV21-00186-01
69d7f42bddec284a48ea4796b2ff010905b1f81c832aa1c7a9a2d9120b73d91a	HTML/Phish.1E81!tr	2CMV21-00186-01
6acc3c0a872083720558f67722e9b28decc0cba512904c6b77ace9860d845242	HTML/Phish.1E81!tr	2CMV21-00186-01
7269acdbad77ef1ab5c2795be42c03cf03132bf5480651b27e98eba1a480ea61	HTML/Phish.E6AD!tr	2CMV21-00186-01
887a3c6b8b84db5d0bb360036c46f57e402a7d36e8d0ea007529c8caf1585b8d	HTML/Fisher.296!tr	2CMV21-00186-01
89c04e91be884478bad8290cbd0ceb699dd27ed7249d22fd9d59c61d7b00eb8f	HTML/Phish.E6AD!tr	2CMV21-00186-01
8aa52e4095f5ae81b9f02b06717ee5d023ea8616edea10d2c11e42e1d0da9fce	MSIL/Kryptik.AAYL!tr	2CMV21-00186-01
8cd9494514730de3049c03e7950c29f94e7ac23667016911660bfacab0032a92	HTML/Fisher.296!tr	2CMV21-00186-01
924f1fd1a05a7b1c6b521b1358fc0203b9796dff3da1dc39eccce9b0825dc606	MSOffice/CVE_2018_0798!tr	2CMV21-00186-01
96353102062f43d5af97effcce1284436d54b6eadeb23ea1eb3dbd0a23732bc3	HTML/Fisher.296!tr	2CMV21-00186-01
a8bc13c69549a728a3ad0234a5d83903d41cd7bb1cd21ff583b6c970c86de6a2	HTML/Fisher.296!tr	2CMV21-00186-01
a9e8d7de3e94adfe57931aad3cff1c82948fc61ee3f3ab9846b229fb754f14e9	HTML/Phish.1E81!tr	2CMV21-00186-01
ad762b63ef8517ef9cc752ac120a9a9fe3d3e8717b0f32c09848d7b8789ec098	HTML/Fisher.296!tr	2CMV21-00186-01
adf5586c44136e67d2db92cbd05d75b8bb703707e8dee2642c8e5c6c26d65bc4	HTML/Fisher.296!tr	2CMV21-00186-01
ae3176e5f1989cb5c1249136a51fb3fb58f2dab8a816751de1005de782945118	Malicious_Behavior.SB	2CMV21-00186-01
b086e2c332a4fbdb392a85bac73fa9758f1b18a24d9f76f07d6c44e6f6778e79	W32/Noon!tr	2CMV21-00186-01
b0d763f47e40d7c81811432d29dc33943705d577caa97a076f616b509a87ff07	MSIL/GenKryptik.FFPM!tr	2CMV21-00186-01

bac5a50318a2a2c1c7637c67c1499f767252eb9dc55c1fbc36e9e6f24367c25b	HTML/Phish.1E81!tr	2CMV21-00186-01
bc08c54e6cf25dedadd3df9224ca958c054a11f64809a73b5d773a7d9fa8a406	HTML/Fisher.296!tr	2CMV21-00186-01
bd21b55e9f1f63ef4affaf68ecbf3ddef0d4b458f24a07e74195d5a60e67b934	PossibleThreat.PALLAS.H	2CMV21-00186-01
d4445b53f6e1fd80ba559faa95d041878659e0d3a8e76d1f64df0d6ce4f09be8	Riskware/Application	2CMV21-00186-01
dca092051ccfb3096fafb56ef4d6137d4bb0b5575096d8c70f8c3bf27e377c98	Malicious_Behavior.SB	2CMV21-00186-01
dd48f4342236d0418f1c4818d94fea9c2a9a7a7845bc9e5645098b996443510a	MSOffice/CVE_2017_11882.C!exploit	2CMV21-00186-01
e5d5f38eea18ac6a29c87d14fe3c7a1224df2eb070a9e7cd02e4b29e791e6657	HTML/Fisher.296!tr	2CMV21-00186-01
eb2aead159129b7972827dd55d2c347dbb6049315714952ce907cb24659a159b	MSIL/Kryptik.AAYL!tr	2CMV21-00186-01
eb88044b621fa8f8f7a23d744d37c93cf2520007bbee29078d198f85276f2190	MSIL/Kryptik.ABCL!tr	2CMV21-00186-01
f14df935d171fa4a3f5a5ee2aec95106bccf782277e98011e0819a251571e30d	MSIL/Kryptik.ABCL!tr	2CMV21-00186-01
fef7e38bd6deb8ef0dd46c840c7c4384ad387a777336982642ab6a912ac8a65a	HTML/Phish.1E81!tr	2CMV21-00186-01

Direcciones IP de servidor SMTP donde es enviado el correo malicioso: Recomendamos establecer cuarentena preventiva para estos indicadores de compromiso, previa evaluación del impacto en los servicios productivos. Una vez que sus plataformas de monitoreo no detecten actividad maliciosa, puede evaluar la posibilidad de liberar el bloqueo. Es importante considerar que podrían aparecer direcciones de IP de servicios Cloud reconocidos o amenazas mitigadas.

IP	Etiqueta de sistema autónomo	Documento web
193.253.98.8	LNREU656 La Reunion Bloc 1	2CMV21-00186-01
195.140.213.254	Hydra Communications Ltd	2CMV21-00186-01
157.230.17.237	DigitalOcean LLC	2CMV21-00186-01
43.225.47.32	HengTian Hong Kong Data Center ISP at HK ISP at HK	2CMV21-00186-01
187.182.170.192	CLARO S.A.	2CMV21-00186-01
103.140.250.169	Main Computer Trading Company Limited	2CMV21-00186-01
185.222.57.248	bd-rootlayer-1-mnt	2CMV21-00186-01
207.109.189.98	CenturyLink Communications LLC	2CMV21-00186-01
15.222.152.33	Amazon Technologies Inc.	2CMV21-00186-01
180.214.239.97	VietServer Services technology company limited	2CMV21-00186-01
175.195.182.119	Korea Telecom	2CMV21-00186-01
191.185.138.26	CLARO S.A.	2CMV21-00186-01
192.30.243.225	Majestic Hosting Solutions LLC	2CMV21-00186-01
199.193.204.182	Intermedia.net Inc.	2CMV21-00186-01

199.193.204.185	Intermedia.net Inc.	2CMV21-00186-01
199.193.204.188	Intermedia.net Inc.	2CMV21-00186-01
199.193.204.190	Intermedia.net Inc.	2CMV21-00186-01
199.193.204.183	Intermedia.net Inc.	2CMV21-00186-01
199.193.204.184	Intermedia.net Inc.	2CMV21-00186-01
199.193.204.189	Intermedia.net Inc.	2CMV21-00186-01
199.193.204.191	Intermedia.net Inc.	2CMV21-00186-01
199.193.204.187	Intermedia.net Inc.	2CMV21-00186-01
199.193.204.186	Intermedia.net Inc.	2CMV21-00186-01
212.5.52.58	KraKra AD	2CMV21-00186-01
143.198.112.111	DigitalOcean LLC	2CMV21-00186-01
188.166.175.7	digitalocean	2CMV21-00186-01
103.232.54.45	VietServer Services technology company limited	2CMV21-00186-01
120.50.8.164	TelNET Communication Ltd	2CMV21-00186-01
185.222.58.153	bd-rootlayer-1-mnt	2CMV21-00186-01
45.137.22.154	RootLayer Web Services Ltd.	2CMV21-00186-01
103.156.92.166	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP	2CMV21-00186-01
104.238.162.58	The Constant Company LLC	2CMV21-00186-01
92.187.1.12	Orange Spain Network	2CMV21-00186-01
195.133.40.125	Des Capital B.V.	2CMV21-00186-01
93.156.6.56	TeleCable	2CMV21-00186-01
222.117.185.51	Korea Telecom	2CMV21-00186-01
74.7.61.150	CBEYOND COMMUNICATIONS	2CMV21-00186-01
89.111.88.44	Telco Pro Services, a. s.	2CMV21-00186-01
40.92.41.87	Microsoft Corporation	2CMV21-00186-01
164.90.160.66	DigitalOcean LLC	2CMV21-00186-01
185.222.57.79	bd-rootlayer-1-mnt	2CMV21-00186-01
162.220.51.67	Express Web Systems Inc.	2CMV21-00186-01
173.88.167.203	Charter Communications Inc	2CMV21-00186-01
103.153.77.105	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP	2CMV21-00186-01
104.168.153.68	Hostwinds LLC.	2CMV21-00186-01
157.230.234.131	DigitalOcean LLC	2CMV21-00186-01
166.241.202.129	Service Provider Corporation	2CMV21-00186-01
185.222.57.165	bd-rootlayer-1-mnt	2CMV21-00186-01

Actualidad

CiberSucesos No. 10 | Nuestra vida en la nube

Decidir si migrar o no a la nube, y de qué forma, son preguntas a las que actualmente se enfrentan las organizaciones de todo nivel, entre empresas grandes, medianas y pequeñas, e incluso más, ahora en muchos casos también debe tomarse esa decisión en distintos órganos de la administración del Estado. Por esto, decidimos dedicar la décima edición de la revista CiberSucesos a la nube, sus oportunidades y amenazas desde una perspectiva de la ciberseguridad.

Pueden leerla aquí, en formato PDF: https://csirt.gob.cl/media/2021/05/CSIRT-MAYO-2021.pdf.

Ciberconsejos para comprar seguro este CyberDay 2021

Del lunes 31 de mayo al miércoles 2 de junio, la Cámara de Comercio de Santiago (CCS) celebra en todo el país un nuevo CyberDay, con 670 marcas adheridas. Para que las compras virtuales sean realizadas con seguridad, preparamos las siguientes recomendaciones junto a la CCS: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-comprar-seguro-este-cyberday-2021/.

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 de este.

- Fernando Lagos
- Sebastián Yuk-Lok Flores Chong
- Eduardo Jullian Fuentes
- Nicolás Alejandro Soto Ulloa
- Jessica del Carmen Escalona Angulo
- Andrés Basoalto Reyes
- Héctor Bignami Díaz
- Romel Rivas
- Bernardita Núñez Grado

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.05.28 12:36:37 -04'00'