Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

30-04-2021 | Año 3 | N°95

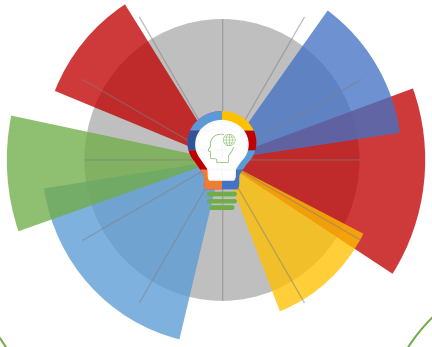
Boletín de Seguridad Cibernética

Semana del 23 al 29 de abril de 2021

La semana en cifras

Hash
46
SHA
Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron
7
URL
Asociadas a sitios fraudulentos y campañas de phishing



Parches
150
para vulnerabilidades
Las mitigaciones son útiles para productos de Google, Citrix, Microsoft, Oracle, Red Hat y Apple.

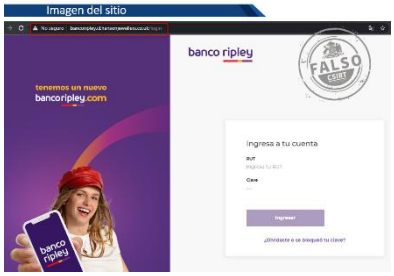
IP
38
Informadas
Listado de IP advertidas en múltiples campañas de phishing y de malware.

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

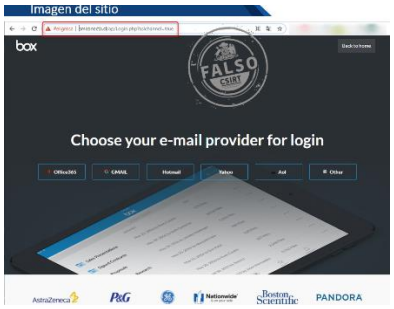
Contenido

Sitios fraudulentos 2
Phishing 4
Vulnerabilidades 5
IoC Malware 10
Actualidad 14
Muro de la Fama 18

Sitios fraudulentos



CSIRT alerta por sitio que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FFR21-00939-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de abril de 2021
Última revisión	26 de abril de 2021
Indicadores de compromiso	
URL sitio falso	
http://www.bancoripley.cl.hansonjewellers.co[.]uk/login	
IP	
[35.242.131.169]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00939-01/	
https://www.csirt.gob.cl/media/2021/04/8FFR21-00939-01.pdf	



CSIRT alerta por sitio que suplanta varios portales de correo electrónico	
Alerta de seguridad cibernética	8FFR21-00940-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de abril de 2021
Última revisión	28 de abril de 2021
Indicadores de compromiso	
URL sitio falso	
https://smconecta[.]cl/ap/Login.php?sslchannel=true	
IP	
[18.222.62.89]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00940-01/	
https://www.csirt.gob.cl/media/2021/04/8FFR21-00940-01.pdf	

CSIRT alerta por sitio fraudulento que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FFR21-00941-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de abril de 2021
Última revisión	29 de abril de 2021
Indicadores de compromiso	
URL sitio falso	
https://rlplay.prixmaelec[.]com/login	
IP	
[186.64.116.25]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00941-01/	
https://www.csirt.gob.cl/media/2021/04/8FFR21-00941-01.pdf	

Phishing

CSIRT alerta por phishing con email que suplanta a Netflix	
Alerta de seguridad cibernética	8FPH21-00395-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de abril de 2021
Última revisión	26 de abril de 2021
Indicadores de compromiso	
URL sitio redirección	
http://chechu.mandril.avnam[.]net/wp-content/plugins/preferred-languages/inc/PPPTTXXXMMMMLLLHHTHTTAA.html	
URL sitio falso	
https://directnewz[.]com/.well-known/INGODWETRUST/5080d8e13c72e6080f7f943359ab44b4/	
IP	
[192.185.35.200]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00395-01/	
https://www.csirt.gob.cl/media/2021/04/8FPH21-00395-01.pdf	

CSIRT alerta por phishing con falso email que suplanta a Netflix	
Alerta de seguridad cibernética	8FPH21-00396-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de abril de 2021
Última revisión	28 de abril de 2021
Indicadores de compromiso	
URL sitio redirección	
http://chechu.mandril.avnam[.]net/wp-content/plugins/preferred-languages/inc/LINKKHOOPOODECODEMOMP.html	
URL sitio falso	
https://stunnerciti[.]com/.well-known/INGODWETRUST/f1afd614784a5bd5b2993e152ce08134/	
IP	
[162.215.240.200]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00396-01/	
https://www.csirt.gob.cl/media/2021/04/8FPH21-00396-01.pdf	

Vulnerabilidades

CSIRT alerta de vulnerabilidades en Microsoft Edge	
Alerta de seguridad cibernética	9VSA21-00428-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	23 de abril de 2021
Última revisión	23 de abril de 2021

CVE	
CVE-2021-21222	CVE-2021-21225
CVE-2021-21223	CVE-2021-21226
CVE-2021-21224	

Fabricante
Microsoft
Productos afectados
Microsoft Edge, versiones de la 79.0.309.71 a la 90.0.818.39.
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00428-01
https://www.csirt.gob.cl/media/2021/04/9VSA21-00428-01.pdf

CSIRT alerta ante vulnerabilidades en varios productos Oracle	
Alerta de seguridad cibernética	9VSA21-00429-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de abril de 2021
Última revisión	23 de abril de 2021

CVE		
CVE-2020-24750	CVE-2020-17527	CVE-2020-8203
CVE-2020-11979	CVE-2020-25649	CVE-2020-1971
CVE-2020-5421	CVE-2020-11987	CVE-2020-27218
CVE-2020-13954	CVE-2021-22112	CVE-2020-8203
CVE-2020-13871	CVE-2019-10086	CVE-2020-17521
CVE-2020-24750	CVE-2020-11987	CVE-2020-11022
CVE-2020-28052	CVE-2020-28052	CVE-2019-12423
CVE-2020-11612	CVE-2020-10188	CVE-2020-1927
CVE-2019-0228	CVE-2020-24750	CVE-2020-27193
CVE-2019-3900		CVE-2020-11022

Fabricante
Oracle
Productos afectados
Oracle Communications Calendar Server: 8.0
Oracle Communications Unified Inventory Management 7.3.4 a 7.4.1.
Oracle Communications Design Studio: 7.4.2.
Oracle Communications Messaging Server: 8.1.
Oracle Communications Performance Intelligence Center Software: 10.4.0.3

Oracle Communications Performance Intelligence Center Software: 10.4.0.2 Oracle Communications Interactive Session Recorder: 6.3, 6.4 Oracle Communications Application Session Controller: 3.9m0p3 Oracle Communications MetaSolv Solution: 6.3.0, 6.3.1 Oracle Communications Contacts Server: 8.0 Oracle Communications Session Router: cz8.2, cz8.3, cz8.4 Oracle Communications Session Border Controller: cz8.2, cz8.3, cz8.4 Oracle Enterprise Communications Broker: PCz3.1, PCz3.2, PCZ3.3 Oracle Enterprise Session Border Controller: cz8.2, cz8.3, cz8.4 Oracle Communications Subscriber-Aware Load Balancer: cz8.2, cz8.3, cz8.4 Oracle Communications Converged Application Server Service Controller: 6.2 Oracle Communications Services Gatekeeper: 6.0, 6.1, 7.0 Oracle Commerce Guided Search: 11.3.2 Oracle Commerce Merchandising: 11.3.0, 11.3.1, 11.3.2 Oracle SD-WAN Edge: 8.2, 9.0. Oracle SD-WAN Aware: 8.2
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00429-01
https://www.csirt.gob.cl/media/2021/04/9VSA21-00429-01.pdf

CSIRT alerta de vulnerabilidades en Google Chrome		
Alerta de seguridad cibernética	9VSA21-00430-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	27 de abril de 2021	
Última revisión	27 de abril de 2021	
CVE		
CVE-2021-21227 CVE-2021-21232 CVE-2021-21233	CVE-2021-21228 CVE-2021-21229 CVE-2021-21230	CVE-2021-21231 CVE pendiente
Fabricante		
Google		
Productos afectados		
Google Chrome		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00430-01		
https://www.csirt.gob.cl/media/2021/04/9VSA21-00430-01.pdf		

CSIRT advierte de vulnerabilidades en productos de Apple	
Alerta de seguridad cibernética	9VSA21-00431-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de abril de 2021
Última revisión	27 de abril de 2021

CVE

CVE-2020-27942	CVE-2021-1825	CVE-2021-1860
CVE-2020-3838	CVE-2021-1826	CVE-2021-1864
CVE-2020-7463	CVE-2021-1828	CVE-2021-1865
CVE-2020-8037	CVE-2021-1830	CVE-2021-1867
CVE-2020-8285	CVE-2021-1831	CVE-2021-1868
CVE-2020-8286	CVE-2021-1832	CVE-2021-1872
CVE-2021-1739	CVE-2021-1834	CVE-2021-1873
CVE-2021-1740	CVE-2021-1835	CVE-2021-1874
CVE-2021-1784	CVE-2021-1836	CVE-2021-1875
CVE-2021-1797	CVE-2021-1837	CVE-2021-1876
CVE-2021-1805	CVE-2021-1839	CVE-2021-1877
CVE-2021-1806	CVE-2021-1840	CVE-2021-1878
CVE-2021-1807	CVE-2021-1843	CVE-2021-1881
CVE-2021-1808	CVE-2021-1846	CVE-2021-1882
CVE-2021-1809	CVE-2021-1847	CVE-2021-1883
CVE-2021-1810	CVE-2021-1848	CVE-2021-1884
CVE-2021-1811	CVE-2021-1849	CVE-2021-1885
CVE-2021-1813	CVE-2021-1851	CVE-2021-21300
CVE-2021-1815	CVE-2021-1852	CVE-2021-30652
CVE-2021-1816	CVE-2021-1853	CVE-2021-30653
CVE-2021-1817	CVE-2021-1854	CVE-2021-30656
CVE-2021-1820	CVE-2021-1857	CVE-2021-30659
CVE-2021-1822	CVE-2021-1858	CVE-2021-30660
CVE-2021-1824		CVE-2021-30661

Fabricante

Apple

Productos afectados

Apple Safari 14.0 a 14.0.3-15610.4.3.1.7.
macOS 10.14 18A391 a 11.2.3 20D91.
iOS 14.5
iPadOS 14.5
Xcode 12.5
iCloud for Windows 12.3

Enlaces para revisar el informe:

https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00431-01
https://www.csirt.gob.cl/media/2021/04/9VSA21-00431-01.pdf

CSIRT alerta por vulnerabilidad crítica en Citrix ShareFile	
Alerta de seguridad cibernética	9VSA21-00432-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	28 de abril de 2021
Última revisión	28 de abril de 2021
CVE	
CVE-2021-22891	
Fabricante	
Citrix	
Productos afectados	
Citrix ShareFile, versiones 5.7 anteriores a la 5.7.3, 5.8 anteriores a la 5.8.3, 5.9 anteriores a la 5.9.3, 5.10 anteriores a la 5.10.1 y 5.11 anteriores a la 5.11.18.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00432-01	
https://www.csirt.gob.cl/media/2021/04/9VSA21-00432-01.pdf	

CSIRT advierte de vulnerabilidades en varios productos de Red Hat		
Alerta de seguridad cibernética	9VSA21-00433-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	29 de abril de 2021	
Última revisión	29 de abril de 2021	
CVE		
CVE-2021-20305	CVE-2020-27779	CVE-2020-25678
CVE-2019-3884	CVE-2020-28362	CVE-2021-3139
CVE-2020-6829	CVE-2021-3121	CVE-2020-12723
CVE-2020-8566	CVE-2021-3449	CVE-2021-23961
CVE-2020-12400	CVE-2021-3450	CVE-2021-23994
CVE-2020-12403	CVE-2021-20225	CVE-2021-23995
CVE-2020-14372	CVE-2021-20233	CVE-2021-23998
CVE-2020-15157	CVE-2021-20305	CVE-2021-23999
CVE-2020-25632	CVE-2020-25648	CVE-2021-24002
CVE-2020-25647	CVE-2020-25692	CVE-2021-29945
CVE-2020-25658	CVE-2021-3449	CVE-2021-29946
CVE-2020-27749	CVE-2021-3450	CVE-2021-29948
Fabricante		
Red Hat		
Productos afectados		
thunderbird (Red Hat package): 78.3.1-1.el7_9 al 78.9.1-1.el7_9 Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for ARM 64 8 aarch64		

Red Hat Enterprise Linux Server 7 x86_64 Red Hat Enterprise Linux Desktop 7 Red Hat Enterprise Linux Workstation 7 Red Hat Enterprise Linux for IBM z Systems 7 s390x Red Hat Enterprise Linux for Power, little endian 7 ppc64le Red Hat Enterprise Linux for Power little endian Extended Update Support 8.1 Red Hat Enterprise Linux for x86_64 – Extended Update Support: 8.1 Red Hat Enterprise Linux Server – Update Services for SAP Solutions: 8.1 Red Hat Enterprise Linux Server (for IBM Power LE) – Update Services for SAP Solutions: 8.1 Red Hat OpenShift Container Platform 4.3 a 4.6 para RHEL 8 x86_64 Red Hat OpenShift Container Platform for Power 4.3 a 4.6 para RHEL 8 ppc64le Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.3 a 4.6 para RHEL 8 s390x Red Hat Ceph Storage MON 4 for RHEL 8 x86_64 Red Hat Ceph Storage MON 4 for RHEL 7 x86_64 Red Hat Ceph Storage OSD 4 for RHEL 8 x86_64 Red Hat Ceph Storage OSD 4 for RHEL 7 x86_64 Red Hat Ceph Storage for Power 4 for RHEL 7 y 8 ppc64le Red Hat Ceph Storage MON for Power 4 for RHEL 7 y 8 ppc64le Red Hat Ceph Storage OSD for Power 4 for RHEL 7 y 8 ppc64le Red Hat Ceph Storage for IBM z Systems 4 s390x Red Hat Ceph Storage MON for IBM z Systems 4 s390x Red Hat Ceph Storage OSD for IBM z Systems 4 s390x
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00433-01
https://www.csirt.gob.cl/media/2021/04/9VSA21-00433-01.pdf

IoC Malware

A continuación, se comparten los Indicadores de Compromiso (IoC) que fueron detectados durante la semana pasada por el Equipo del CSIRT. Recomendamos a administradores y usuarios bloquear los hash publicados en este informe y mantener el monitoreo sobre el resto de los IoC.

Hash de archivos maliciosos	Documento web
0432d7d30283a74a01e466fd289f35040c30e48b29e73e149b3374d6e07f752c	2CMV21-00173-01
048518f8b11aa405bde1b4c8d71e9537b1a7200a5c816fa4fb451476c93e18b0	2CMV21-00173-01
07b1bddd60ba94eb9b1d304d068d39ca3e8ce1d190accea08102f32551839cfb	2CMV21-00173-01
0b5172660a81c31765d166bcae95cf648bfbfca599a8adadcf504c1a1ff973b6	2CMV21-00173-01
0ba92d397ba717cead88c29be8935dc04917e248504d8c16b6b44a02920aff56	2CMV21-00173-01
0e13f3fd36b3add7f3e7221975469ad8e7a625d9c4be5b7ba81d75dc5576b8d1	2CMV21-00173-01
0edb8c8d9ff0709677aca64cc723b82302d244cfb9dc69129674aa417d495321	2CMV21-00173-01
11ec8c695558777665276c406b5c435fa87ef81912dd18d4f82629589f36c74b	2CMV21-00173-01
1730da6bbda8300eca3cc4ebd072fbeba77dc964e86af7c672dd02f4034dcc74	2CMV21-00173-01
17fe063619c08c97dd6ebaa9e4e47df51852a2873e2a13f0260620add41b34d4	2CMV21-00173-01
1cb3b34388e2d48113df87ebbda683117d978fc4ce1f17cb5c1d09ddf353edee	2CMV21-00173-01
270094a04bd98204e670de290b23650f21749695cc370cb0eb18f26f05e98eef	2CMV21-00173-01
2c21d8f271d81bd393a2a509e154b254bf5064ba9e4d95be860a9bdf1c0fd5b6	2CMV21-00173-01
2cf709ace0280783623acbc9fb826c931a647c3305fc1e1a1c3f9411638d386e	2CMV21-00173-01
2e682bc8983776309a853f887f16dc5ea3fb9c61519c67f3262757d2ca747b47	2CMV21-00173-01
3a0f55d13641d30db8dcde1abc0120c0ded4c35d6fb907bdfbcedeeb29b4aeb3	2CMV21-00173-01
42c36caf58671da2a6e90667cd25855f4f85c8ab9ced1f12a493a6d0da8271e8	2CMV21-00173-01
4549d011b949eb75c36b49772f47368ccfe9931a021fd434850dc45a56458c2c	2CMV21-00173-01
45812edf47ba8b8d20db1674bd19f38ca5459d125602b8c5ec3aea2dfc9ff328	2CMV21-00173-01
45baf56d201786cc94c817345e7afafe75e9815700bce36799971cd76983fdae	2CMV21-00173-01
4d632467af35b152b404bad6ccb8298ff8860500bdaee9e6a87b192e3d7b1383	2CMV21-00173-01
4e49a6eaacc7abbb0a5fe51657d2fb986a0f392118d593dc4a59fb3fe8db6bee	2CMV21-00173-01
514de68ddc8a32c2a8a62fdd0bf2a494c6120a2da46b15a20724fca4499847e8	2CMV21-00173-01
5d7deb44ec0daaac2216e4ab7a1034033e0c0818c12f5d7332278c094ac3a029	2CMV21-00173-01
676edb4d46cdcd7c680e3fd3975d787ac4a3e5c704fe1cecc0ab13735bf32b26	2CMV21-00173-01
7813058478aa477d0e397f275ee6f31877c8059bec82f0dbb48160af799c77e8	2CMV21-00173-01
78855573c8fd546b70baf202cfdc65a9f0f9da0d8170dfa5689ee618f7613130	2CMV21-00173-01
7b6e793102058d786cd54fcdaa3633a91083e5b3d358c95e7d17e199723894a2	2CMV21-00173-01
80da74ac91a4cb0bcd7af65334fe67d09d495e9c1eba52ee8383dcfe2107fcf2	2CMV21-00173-01
8d3d3d54ee6d432a075e9d21d959404accdc25d44baa25e6cf17fce34b8bee82	2CMV21-00173-01

8f47f3a107ba22caf91ca8019baabd6d2d46bf9b6ce79f0d34ae98c31624083a	2CMV21-00173-01
96ee0d500aa147d71bc99c27b5e4fb534c3e120bf2d165907ca4612f8023cc9f	2CMV21-00173-01
9ac24a51135efe8b707fad83090bba020b67df7da026a3805025480bcb0d8040	2CMV21-00173-01
9ddea1c5a5c08a83a3b2a7282b1b651a984e0e7ca7dea1c1085bf2a1fc77c994	2CMV21-00173-01
a9bc6403435e0f077bd24f94ef0a100ed114b588513f474450605e38523b1920	2CMV21-00173-01
b4b18b1a1c8b6d7d979d93897d1b710fc81d4309b3e3a07ea757d1ce95428357	2CMV21-00173-01
c0ded1fae7b9bc0422ae464c86d6cc2e64d7536a3f660d91c521ca52db6d0d21	2CMV21-00173-01
c60bb0ef48e4a7ed7f414bf7a4678a4adaa83e8fcbccb7607f5b3b98f29c2d18	2CMV21-00173-01
d0527be82e7950e363f7030e931be288c4222019e5f3876a98d6b021feb185ee	2CMV21-00173-01
d745b4373a1db12c38d23c946abce152bf064cd74ed7efd67fcc17e179816240	2CMV21-00173-01
e06b9da757791b7ed2b58617bdad9ec542f91cbeb74b817f25b1a4d569a3d08e	2CMV21-00173-01
e9c102eeb57bd3cb741238b0328a8eeb0f441493ae96a8c791cb5e087bebe558	2CMV21-00173-01
eadfd82f1ccb229f3bb5bf229e04de7a36156e8799a04a9c5d31c60de7c6f217	2CMV21-00173-01
f8da473ee2c2398e5574c79d35b4d195598fa22418b3aba36e245bcb11bc5c51	2CMV21-00173-01
fa084536ab457ebff57cf069faa57fe1a3d69076a628427793d5706c67af26cd	2CMV21-00173-01
fe62cb2dd8dc13f7c15e84d090a6d112d6f84845129182fd3ca0154b560d98f2	2CMV21-00173-01

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
157.90.50.57	Hetzner Online GmbH	2CMV21-00173-01
45.143.147.194	Hyonix LLC	2CMV21-00173-01
50.210.204.193	COMCAST-7922	2CMV21-00173-01
81.144.138.194	British Telecommunications PLC	2CMV21-00173-01
87.125.174.245	Vodafone Spain	2CMV21-00173-01
103.138.109.241	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP	2CMV21-00173-01
103.151.122.244	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP	2CMV21-00173-01
103.245.209.226	HK Kwaifong Group Limited	2CMV21-00173-01
128.199.152.121	DIGITALOCEAN-ASN	2CMV21-00173-01
190.210.196.123	NSS S.A.	2CMV21-00173-01
195.140.213.222	Hydra Communications Ltd	2CMV21-00173-01
198.244.135.246	OVH SAS	2CMV21-00173-01
103.145.252.28	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP	2CMV21-00173-01
138.117.148.93	SOC. COMERCIAL WIRENET CHILE LTDA.	2CMV21-00173-01

138.68.65.174	DIGITALOCEAN-ASN	2CMV21-00173-01
143.198.55.51	DIGITALOCEAN-ASN	2CMV21-00173-01
181.30.31.36	Telecom Argentina S.A	2CMV21-00173-01
185.222.57.142	RootLayer Web Services Ltd.	2CMV21-00173-01
185.222.57.90	RootLayer Web Services Ltd	2CMV21-00173-01
185.6.88.18	Siportal Srl	2CMV21-00173-01
187.39.254.56	CLARO S.A	2CMV21-00173-01
199.250.200.47	IMH-IAD	2CMV21-00173-01
31.210.20.195	Des Capital B.V.	2CMV21-00173-01
31.210.20.199	Des Capital B.V.	2CMV21-00173-01
45.137.22.120	RootLayer Web Services Ltd	2CMV21-00173-01
45.137.22.133	RootLayer Web Services Ltd.	2CMV21-00173-01
51.79.14.27	OVH SAS	2CMV21-00173-01
64.188.20.247	ASN-QUADRANET-GLOBAL	2CMV21-00173-01
68.183.10.90	DIGITALOCEAN-ASN	2CMV21-00173-01
77.247.110.43	ABC Consultancy	2CMV21-00173-01
82.142.14.233	Free SAS	2CMV21-00173-01
84.38.133.6	DataClub S.A.	2CMV21-00173-01
88.198.112.68	Hetzner Online GmbH	2CMV21-00173-01

Correos electrónicos de donde son enviados los archivos adjunto con malware.

Dirección	Documento web
abdullah-jallad@veniciaco.com	2CMV21-00173-01
ramon.huidobro@gmail.com	2CMV21-00173-01
a.varghese@fugro.com	2CMV21-00173-01
accounts@ccmarine.in	2CMV21-00173-01
angelyim@chargeurs-pcc.com	2CMV21-00173-01
AP@nestle.com	2CMV21-00173-01
ctelesca@amnistreasury.ch	2CMV21-00173-01
docusign@capitolcitystorage.com	2CMV21-00173-01
docusign@johngallison.com	2CMV21-00173-01
gvu@un.org	2CMV21-00173-01
info@basarimuhendislik.com	2CMV21-00173-01
info@erapres.com.tr	2CMV21-00173-01
info@gac.com	2CMV21-00173-01
info@hvcontratistas.com.pe	2CMV21-00173-01
koukharsky@koukharsky.com.ar	2CMV21-00173-01

marina.a@scorpiosmykonos.com	2CMV21-00173-01
marlene@heliosemalharia.com	2CMV21-00173-01
nsakiya@sinopec.com	2CMV21-00173-01
ops@csdvlp.com.sg	2CMV21-00173-01
p_jamei@godakhtar.co.ir	2CMV21-00173-01
purchase.pmgroup@mail.ru	2CMV21-00173-01
purchasing@springmarine.com	2CMV21-00173-01
ross.kohlbeck@amerhart.com	2CMV21-00173-01
sahajdeep.khanuja111.sk9@gmail.com	2CMV21-00173-01
sales@amalgamuae.com	2CMV21-00173-01
sales1@agiindustries.com	2CMV21-00173-01
sanjeev.shukla@bioayurveda.in	2CMV21-00173-01
sghanavati@mpc.ir	2CMV21-00173-01
sherif.elgendy@adesgroup.com	2CMV21-00173-01
sherly@zbqishuai.cn	2CMV21-00173-01
siddharth.kharat@kwe.com	2CMV21-00173-01
ssparks@hemsaw.com	2CMV21-00173-01
Teresa.Fuentes@gmail.com	2CMV21-00173-01
test@sferalegal.com	2CMV21-00173-01

Actualidad

Superintendencia de Casinos de Juego publica normativa en ciberseguridad junto al CSIRT de Gobierno

En una reunión encabezada por el Subsecretario del Interior, Juan Francisco Galli en el Palacio de La Moneda, junto con la Superintendenta de Casinos de Juego (SCJ), Vivien Villagrán, se llevó a cabo esta mañana la firma de la Normativa para la Gestión de la Ciberseguridad, con los lineamientos que deben seguir las operadoras y concesionarias de casinos de juego, entidades fiscalizadas por la SCJ.

Pueden ver más fotografías y encontrar toda la información sobre la firma de esta normativa, aquí: https://www.csirt.gob.cl/noticias/superintendencia-de-casinos-de-juego-publica-normativa-en-ciberseguridad-junto-al-csirt-de-gobierno/.

Ciberconsejos para evitar caer en estafas este Día de la Madre

El Día de la Madre es una de las jornadas de más estafas en el ciberespacio. Por eso decidimos compartir las principales precauciones que debemos recordar al comprar en línea: csirt.gob.cl/recomendaciones/ciberconsejos-el-bitcoin-y-las-estafas-que-lo-rodean/.

CSIRT de Gobierno presenta su novena edición de la revista CiberSucesos, con la inteligencia artificial como tema central

El número de abril de CiberSucesos trata sobre distintas implicancias que trae el desarrollo de la inteligencia artificial para la ciberseguridad, tanto en la promesa que representa para reforzar la defensa de nuestros sistemas, como en la amenaza que significa para volver los ciberataques más fáciles de masificar y de dificultar su detección.

Lea y descargue la revista completa aquí: https://www.csirt.gob.cl/recomendaciones/cibersucesos-no-9/ .

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.

- Sang Min Sin
- Joshua Provoste
- José Gregorio Flores Blanco
- Fernando Lagos
- MR. H
- Jorge Muñoz

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.04.30 12:44:36 -04'00'