Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

05-02-2021 | Año 3 | N°83

Boletín de Seguridad Cibernética

Semana del 28 de Enero
al 03 de Febrero de 2021

Resumen de la semana en cifras

Hash

31

Sha

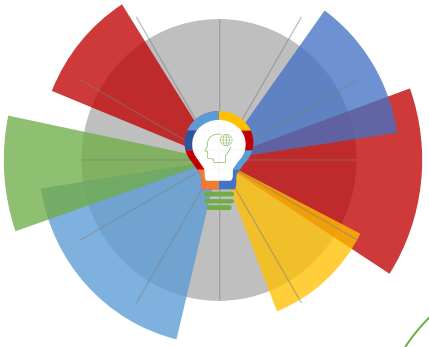
Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron

32

URLs

Asociadas a sitios fraudulentos y campañas de phishing



Parches

70

para vulnerabilidades

Las mitigaciones son útiles para productos Mozilla, Apache, Apple y Google.

IPs

27

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 advierte página bancaria fraudulenta	
Alerta de seguridad cibernética	8FFR21-00885-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Febrero de 2021
Última revisión	02 de Febrero de 2021
Indicadores de compromiso	
URL sitio falso	
http[:]//axentisgroup[.]com/rudy/www.bancoestado.cl/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[185.98.131.140]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00885-01/	
https://www.csirt.gob.cl/media/2021/02/8FFR21-00885-01.pdf	

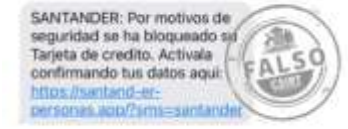
CSIRT informa suplantación de página de supermercado	
Alerta de seguridad cibernética	8FFR21-00886-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Febrero de 2021
Última revisión	02 de Febrero de 2021
Indicadores de compromiso	
URL sitio falso	
https[:]//abitobd[.]com/wp-admin/css/colors/coffee/Login.walmart/	
IP	
[43.245.118.2]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00886-01/	
https://www.csirt.gob.cl/media/2021/02/8FFR21-00886-01.pdf	

Phishing

CSIRT informa phishing de supuesta cuenta de correo caducada	
Alerta de seguridad cibernética	8FPH21-00363-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Febrero de 2021
Última revisión	02 de Febrero de 2021
Indicadores de compromiso	
URL sitio falso	
https[:]//2eeca221b8.nxcli[.]net/zm/Zimbra2020/vrfy/index.html	
IP	
8.29.155.208	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00363-01/	
https://www.csirt.gob.cl/media/2021/02/8FPH21-00363-01.pdf	

CSIRT advierte phishing de cuenta bloqueada	
Alerta de seguridad cibernética	8FPH21-00364-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Febrero de 2021
Última revisión	02 de Febrero de 2021
Indicadores de compromiso	
URL redirección	
https://appp-chile-cl.xyz/	
URL sitio falso	
https[:]//banco-santander.cl-xh[.]buzz/1612290173/index.asp	
IP	
[108.166.219.79]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00364-01/	
https://www.csirt.gob.cl/media/2021/02/8FPH21-00364-01.pdf	

Imagen del mensaje



CSIRT informa smishing sobre tarjeta bancaria dada de baja	
Alerta de seguridad cibernética	8FPH21-00365-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Febrero de 2021
Última revisión	03 de Febrero de 2021
Indicadores de compromiso	
URL redirección	
https[:]//santader-er-personas[.]app/?sms=santander	
URL sitio falso	
https[:]//banco-santa-nder-personas[.]app/1612372059/personas/index.asp	
IP	
198.54.119.112	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00365-01/	
https://www.csirt.gob.cl/media/2021/02/8FPH21-00365-01.pdf	

Malware

CSIRT informa correo con malware con supuesto pedido	
Alerta de seguridad cibernética	2CMV21-00142-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Enero de 2021
Última revisión	29 de Enero de 2021
Indicadores de compromiso	
SHA256	
097ADDEC05B08FE749C14F84FC5DCCE1F8673236CA871537C2E1E86872D468E9	
AEB3387852A76C1DA329CE66251B3005B1E2C7005E900BBAFA37BB923B5FEC34	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv21-00142-01/	
https://www.csirt.gob.cl/media/2021/01/2CMV21-00142-01.pdf	

CSIRT advierte campaña de malware con documentos originales	
Alerta de seguridad cibernética	2CMV21-00143-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Enero de 2021
Última revisión	29 de Enero de 2021
Indicadores de compromiso	
SHA256	
C69277659668C7A9EE3A21A8CB9871383910F5A7F024BDA97A04A4DCA6E85F8F	
3F9A4C4C4816AF6384F00D3864ED82C3E89DE730A8C57F84D445A4C7E1C93E9F	
98B97D4433C9C5D5D03E3F50C88675C69C25E6DDBB9369E8DB37D9DD7B9182E0	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv21-00143-01/	
https://www.csirt.gob.cl/media/2021/01/2CMV21-00143-01-1.pdf	

Vulnerabilidades

CSIRT comparte vulnerabilidades entregadas por Mozilla	
Alerta de seguridad cibernética	9VSA21-00379-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Enero de 2021
Última revisión	29 de Enero de 2021
CVE	
CVE-2021-23953 - CVE-2021-23954 - CVE-2021-23955 CVE-2021-23964 - CVE-2021-23965	
Fabricante	
Mozilla	
Productos afectados	
Mozilla Thunderbird, versiones anteriores a la 78.7. Firefox ESR, versiones anteriores a la 78.7. Firefox, versiones anteriores a la 85.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00379-01/	
https://www.csirt.gob.cl/media/2021/01/9VSA21-00379-01.pdf	

CSIRT comparte mitigaciones obtenidas de Apache	
Alerta de seguridad cibernética	9VSA21-00380-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Febrero de 2021
Última revisión	02 de Febrero de 2021
CVE	
CVE-2020-17523	
Fabricante	
Apache	
Productos afectados	
Apache Shiro, versiones de la 1.0.0. a la 1.7.0.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00380-01/	
https://www.csirt.gob.cl/media/2021/02/9VSA21-00380-01-1.pdf	

CSIRT comparte vulnerabilidades entregadas por Apple	
Alerta de seguridad cibernética	9VSA21-00381-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Febrero de 2021
Última revisión	02 de Febrero de 2021
CVE	
CVE-2021-1761 - CVE-2020-29614	
CVE-2021-1793	
CVE-2021-1737	
CVE-2021-1738	
CVE-2021-1744	
CVE-2021-1779	
CVE-2021-1757	
CVE-2021-1764	
CVE-2021-1750	
CVE-2020-29633	
CVE-2021-1771	
CVE-2021-1762	
CVE-2021-1763	
CVE-2021-1774	
CVE-2021-1767	
CVE-2021-1745	
CVE-2021-1753	
CVE-2021-1768	
CVE-2021-1751	
CVE-2020-27938	
CVE-2021-1769	
CVE-2021-1788	
CVE-2021-1765	
CVE-2021-1801	
CVE-2021-1789	
CVE-2021-1799	
CVE-2021-1777	
CVE-2021-1754	
CVE-2021-1797	
CVE-2021-1790	
CVE-2020-27945	
CVE-2021-1760	
CVE-2021-1747	
CVE-2021-1776	
CVE-2021-1759	
CVE-2021-1772	
CVE-2021-1792	
CVE-2021-1787	
CVE-2021-1786	
CVE-2020-27937	
CVE-2021-1802	

CVE-2021-1791 CVE-2021-1775 CVE-2021-1746 CVE-2020-29608 CVE-2021-1758 CVE-2021-1783 CVE-2021-1741 CVE-2021-1743 CVE-2021-1773 CVE-2021-1778 CVE-2021-1736 CVE-2021-1785 CVE-2021-1766 CVE-2021-1818 CVE-2021-1742 CVE-2020-27904
Fabricante
Apple
Productos afectados
macOS, versiones de la 10.15 a la 11.1.
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00381-01/
https://www.csirt.gob.cl/media/2021/02/9VSA21-00381-01.pdf

CSIRT comparte vulnerabilidades entregadas por Google	
Alerta de seguridad cibernética	9VSA21-00382-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Febrero de 2021
Última revisión	03 de Febrero de 2021
CVE	
CVE-2021-21142 - CVE-2021-21143 - CVE-2021-21144 CVE-2021-21145 - CVE-2021-21146 - CVE-2021-21147	
Fabricante	
Google	
Productos afectados	
Google Chrome, versiones de la 88.0.4324.0 a la 88.0.4324.145.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00382-01/	
https://www.csirt.gob.cl/media/2021/02/9VSA21-00382-01.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
26dc56dbddfa9bc6579031c4452ea30adf1894300347df4830b2291f9c176b94	Emotet	2CMV21-00140-01
b75d63fb633426e9fed2a5b18cd707161159b218fc06d6fb24e9bc56cb1890d8	Emotet	2CMV21-00140-01
925c378d40a9316392ebcafd83d74e9148741afa2f88e67c76b1f9bca8365423	Emotet	2CMV21-00140-01
1bb9591f1ed79d19e77dd9e9b0c05ee37aa36c317e93e1d275df2a801c05afe6	Emotet	2CMV21-00140-01
6520b87b306eadc88a7f1846db167cfe940dfc99343b028b74b138a8e4fcd08d	Emotet	2CMV21-00140-01
cecc57d7c797376b102ef29707158e2c22b94a1fe4f5e2c3dd0a11c538e90067	Emotet	2CMV21-00140-01
dc8ec4182f98572ae5ccb3034bf68da48ab28a3af56ef6bee1ca45f0a411aab6	Troyano - Wacatac - Kryptik	2CMV21-00141-01
129165b361ece5ef2ebc04fb39a2db75641220aa5a36cfbd90f7a7a6008812c9	Troyano - Wacatac - Kryptik	2CMV21-00141-01
1de689d729d11f0eb641347eda45fa729b70a2d039d6d85a4fcd79cc9835d0e1	Troyano - Wacatac - Kryptik	2CMV21-00141-01
1f2b5d967f14dfe7b2a744b2376a890b9e586a7fc4f7060e6003b277a66b68d4	Troyano - Wacatac - Kryptik	2CMV21-00141-01
26428f267b9bbca4016b30cae2dae4c4200add270040acb0eac3b02a607ed5d3	Troyano - Wacatac - Kryptik	2CMV21-00141-01
4ae0fec166b7ed50c172514bab9eb935efd6c30f72f1697e02457ef5ec39c881	Troyano - Wacatac - Kryptik	2CMV21-00141-01
4fbfffd8a3f3b7b3f0d8610890cba130b4968861a829b949d10b9fc2b9b65b36	Troyano - Wacatac - Kryptik	2CMV21-00141-01
56fac445faa088c47a6a6cd8f753fad8052b66562cfe2f5d8c4d1cd9dd4e0c64	Troyano - Wacatac - Kryptik	2CMV21-00141-01
5b49a5c0c5948f944b9c80773dd2e6958b320ed31934f265b509570563a89545	Troyano - Wacatac - Kryptik	2CMV21-00141-01
8515d5936ba536faa1e8ee0eca7cadc4273ef71ee18d72b2fc6de21b1b876a06	Troyano - Wacatac - Kryptik	2CMV21-00141-01
91d996d33439e0cc710f21affd607abc5ed82b740ed1089945f377eb235e6bd2	Troyano - Wacatac - Kryptik	2CMV21-00141-01
9358ed1c3f181a599e186eb610d24bd26b33d94ef849a423f190db4ffbdaa505	Troyano - Wacatac - Kryptik	2CMV21-00141-01
94fd646e7c729e5069a778f2379e864324d0f5fae7a51e3114b61817b09bdf8c	Troyano - Wacatac - Kryptik	2CMV21-00141-01
ae855736b9ccc3393214d9d42f9f8dcc79057c146e190b2502f5c6110bee77fc	Troyano - Wacatac - Kryptik	2CMV21-00141-01
b7c294024533d26e01ab2f5b2e90dcca4021c365160b34b416722b1c804072df	Troyano - Wacatac - Kryptik	2CMV21-00141-01
b9ece958582c9cd5ee96f5223167da22f54e6acde01fc08202944c7723f572b8	Troyano - Wacatac - Kryptik	2CMV21-00141-01
c68e339f2c9e1ea93cc9f57e85913a7d26b3ce9c2cf73af7dc1080fa8d0ae313	Troyano - Wacatac - Kryptik	2CMV21-00141-01
d576e87d9532edb6d9ccd4a4003d25175309e00bcf98840270e3c62a1e54e087	Troyano - Wacatac - Kryptik	2CMV21-00141-01
e6bd284f6c69d282ef8ed24d2d350e30e8a30d7c093d5fb170efa6e05bf933bf	Troyano - Wacatac - Kryptik	2CMV21-00141-01
f9fb0b379ac50ed83a28f7b3b911928b53f5e231f4f69296c5cd68b3e121c3dd	Troyano - Wacatac - Kryptik	2CMV21-00141-01

Correo electrónico dese son enviados los archivos	Tipo de Malware	Documento web
linhai@cn-noc.com	Emotet	2CMV21-00140-01
singvar@idrc-uganda.org	Emotet	2CMV21-00140-01
contact@ennovia.fr	Emotet	2CMV21-00140-01
inadlogistics.india@siemens.com	Emotet	2CMV21-00140-01
ChristopherClark@tengco.com	Emotet	2CMV21-00140-01
admin@xjxglobal.biz	Emotet	2CMV21-00140-01
SALEM.ALSHAMMARI@HAILCEMENT.COM	Troyano - Wacatac - Kryptik	2CMV21-00141-01
accounts@sgbl.com	Troyano - Wacatac - Kryptik	2CMV21-00141-01
info@247blindco.co.uk	Troyano - Wacatac - Kryptik	2CMV21-00141-01
rud-division@alkuhaimi.com	Troyano - Wacatac - Kryptik	2CMV21-00141-01
satis3@hidrodinc.com.tr	Troyano - Wacatac - Kryptik	2CMV21-00141-01
liuyangcheng@sinopharm.com	Troyano - Wacatac - Kryptik	2CMV21-00141-01
excord@asbury.com	Troyano - Wacatac - Kryptik	2CMV21-00141-01
sunny@chinahighlights.com	Troyano - Wacatac - Kryptik	2CMV21-00141-01
aDora.Tan@ttelectronics.com	Troyano - Wacatac - Kryptik	2CMV21-00141-01
d.garzarodriguez@alceda.com.mx	Troyano - Wacatac - Kryptik	2CMV21-00141-01
sales@progate.top	Troyano - Wacatac - Kryptik	2CMV21-00141-01
s.zennaro@omn.it	Troyano - Wacatac - Kryptik	2CMV21-00141-01
takemura@atlas-ltd.co.jp	Troyano - Wacatac - Kryptik	2CMV21-00141-01
Michele.Kester@bin-dasmal.ae	Troyano - Wacatac - Kryptik	2CMV21-00141-01
jconway@bdiworldwide.com	Troyano - Wacatac - Kryptik	2CMV21-00141-01
info@novagraf.top	Troyano - Wacatac - Kryptik	2CMV21-00141-01
xue_martin@gmail.com	Troyano - Wacatac - Kryptik	2CMV21-00141-01

URL
https://dropmb.com/files/3c09e20bddde6610c69ad85e797956f8.lovingtherid
http://becharnise.ir/temp/fre.php
http://tunedinblog.com/wp-includes/tempz.scr
http://cy.kl-re.com/power/bo/boobov.exe
http://193.239.147.103/base/9158412CBF14FB744AFA9F0D01F6CDF2.html
http://193.239.147.103/base/ED373B21DE74B174904C90C4F88850ED.html
http://cy.kl-re.com/power/oma/omamsa.exe
http://power/oma/omamsa.exe
http://tsdyupbckfaruzevimkx.dns.army/upkdoc/winlog.exe
http://zangaa.com/kaka/kaka1/fre.php
http://www.carrerco.com/bf3/?rH=k6AgYuMujeRW6N8gz5kkxbRfnT27DAvtDUNPhia+8i+Ep+mtg2WMbUxNw9Hm5v9U4NA=&Sx=5ja0c8rh
http://www.madebazar.com/bf3/?rH=Tkl32Nv9K9tXGi3SsfVFE6F0oUsrdzP8S5Qe0lxfUgQfTtTMANPf0bfyFBjX8Bo+l/Q=&Sx=5ja0c8rh
http://www.treycorbies.com/bf3/?rH=X3ySjUI5lkKg38MSCABSSqcU4kqTdzK46ni1Gbu3qWE1JVCaNGX8G17gWGT/YoKAbbI=&Sx=5ja0c8rh
http://www.excellencepi.com/bf3/?rH=K1cqXq6/Eug/TFn4Yn8dj0P/G2IXbjDq688jSsgdVbjeXRYDCtMByGrbC7epnVCpV6I=&Sx=5ja0c8rh
http://www.midnightsunhi.com/bf3/?rH=hxSy7dk+3cNA8HtDrozJ8q0KjfwbZf/2w2GU+6cBS6nMKaJ3UWW2m/wYUCSdKAh350g=&Sx=5ja0c8rh
http://www.tadalafil.website/bf3/?rH=A4iu9AEkEQaaI73cLWMUXvaY7i9AXVG/TdX+0E0usbohvYzlbLzighGeU3VJmWPcB0c=&Sx=5ja0c8rh
http://www.uk-calculation.net/bf3/?rH=SkdgG+2KTGDyXF1kaIHnvk8giHrNZd7tOkVavIJbRIqjJkm3oII9WMaCDvEslhcY6to=&Sx=5ja0c8rh
http://www.whereiswillgroup.com/bf3/?rH=7BrySp0bt6P1cJQcjr9LzAm/RXM1jDTJmCJD8mFsin5iR3rNxecJXafkW021enY5O4c=&Sx=5ja0c8rh
http://www.4week-keto-results.com/bf3/?rH=VNaNEuZ0lugK+Bf0ZPKDbNNgorG7szaAgbpX85loS5selOvSLaSfz14wZPWi+7ZaF8c=&Sx=5ja0c8rh
http://www.making50masks.com/bf3/?rH=TEZYcqlSYgZz0a32Xwqbk5/9+MM7H1sLTaewnJXJEf7Gh2ye4gVad+4AROi0WdKdj5w=&Sx=5ja0c8rh
http://www.datespot.info/rhg/?MFQLRV=xa96DJFgJj11zsj1O+4kkvozqshwYpIuqNem/hP/3g+1v2X+I2EqJvwcmELBtLDVBQw=&jHX06=EDKPpD8
http://www.alisengun.com/rhg/?MFQLRV=RlwVi5te47mkYmkSeRjeBSmTsDalKOD9epLZaNWfA/5+0i+W7CrXJgToxrO5eGXbiKo=&jHX06=EDKPpD8
http://movement2020.ddns.net/
http://richardgere.mywire.org/
http://168.119.250.13/index.php

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	Tipo Malware	Documento web
185.222.58.104	RootLayer Web Services Ltd.	Emotet	2CMV21-00140-01
37.49.225.202	Estro Web Services Private Limited	Emotet	2CMV21-00140-01
45.147.229.210	combahton GmbH	Emotet	2CMV21-00140-01
37.49.225.141	Estro Web Services Private Limited	Emotet	2CMV21-00140-01
84.252.95.45	Istanbuldc Veri Merkezi Ltd Sti	Emotet	2CMV21-00140-01
103.50.163.234	PDR	Troyano - Wacatac - Kryptik	2CMV21-00141-01
185.174.103.171	QuadraNet Enterprises LLC	Troyano - Wacatac - Kryptik	2CMV21-00141-01
167.71.171.94	DigitalOcean, LLC	Troyano - Wacatac - Kryptik	2CMV21-00141-01
95.211.208.50	LeaseWeb Netherlands B.V.	Troyano - Wacatac - Kryptik	2CMV21-00141-01
193.56.29.31	Web Hosted Group Ltd	Troyano - Wacatac - Kryptik	2CMV21-00141-01
84.38.133.173	DataClub S.A.	Troyano - Wacatac - Kryptik	2CMV21-00141-01
66.154.111.232	Total Server Solutions L.L.C.	Troyano - Wacatac - Kryptik	2CMV21-00141-01
185.209.22.45	TORAT Private Enterprise	Troyano - Wacatac - Kryptik	2CMV21-00141-01
190.103.224.9	Red Intercable Digital S.A.	Troyano - Wacatac - Kryptik	2CMV21-00141-01
134.119.177.108	Host Europe GmbH	Troyano - Wacatac - Kryptik	2CMV21-00141-01
134.119.181.221	Host Europe GmbH	Troyano - Wacatac - Kryptik	2CMV21-00141-01
197.155.141.129	IKATELNET	Troyano - Wacatac - Kryptik	2CMV21-00141-01
142.4.2.6	Unified Layer	Troyano - Wacatac - Kryptik	2CMV21-00141-01
45.133.203.125	Internet It Company Inc	Troyano - Wacatac - Kryptik	2CMV21-00141-01
192.255.166.96	Hostwinds LLC.	Troyano - Wacatac - Kryptik	2CMV21-00141-01
103.11.189.204	Vodien Internet Solutions Pte Ltd	Troyano - Wacatac - Kryptik	2CMV21-00141-01
69.73.168.158	NETWORK TRANSIT HOLDINGS LLC	Troyano - Wacatac - Kryptik	2CMV21-00141-01

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
45.142.120.55	Anton Mamaev
141.98.80.102	NForce Entertainment B.V.
87.246.7.226	Internet Hosting LTD

Actualidad

Ciberconsejos de verano para navegar seguros en redes sociales

Llegó la época de verano y comenzamos a relajarnos y a descansar de un año intenso y diferente. Pero hay algunas personas que no se toman vacaciones y aprovechan este tiempo para cometer estafas y delitos, y en el ciberespacio esto también ocurre. Las redes sociales son un canal por el que los delincuentes también cometen sus fraudes.

Ver más: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-estar-seguros-en-redes-sociales/

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.

- Consuelo Cabrera
- Claudio Valderrama
- Nicolás Lobos
- Mariana Rodríguez

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.02.05 16:44:29 -03'00'