CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Informática

Publicado el Viernes 17 de Enero de 2020

Resumen de noticias, reportes, alertas e indicadores de compromisos informados por CSIRT entre el jueves 09 de y el miércoles 15 de Enero de 2020.

Falsificación de Registro o Identidad

8FFR20-00179-01 CSIRT ADVIERTE DE SIETE PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00179-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Enero de 2020
Última revisión	10 de Enero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de siete portales fraudulentos asociados a dos IP's que suplantan el sitio web oficial de Banco Scotiabank, el que podría servir para robar credenciales de usuarios de esa entidad.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://csirt.gob.cl/alertas/8ffr20-00179-01/

https://csirt.gob.cl/media/2020/01/8FFR20-00179-01.pdf

8FFR20-00180-01 CSIRT ADVIERTE DE PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR20-00180-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Enero de 2020
Última revisión	10 de Enero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial de Banco Santander, el que podría servir para robar credenciales de usuarios de esa entidad.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://csirt.gob.cl/alertas/8ffr20-00180-01/
https://csirt.gob.cl/media/2020/01/8FFR20-00180-01.pdf

8FFR20-00181-01 CSIRT ADVIERTE DE 12 PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00181-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Enero de 2020
Última revisión	14 de Enero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de 12 portales fraudulentos asociados a tres IP's que suplantan el sitio web oficial de Banco Scotiabank, los que podrían servir para robar credenciales de usuarios de esa entidad.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://csirt.gob.cl/alertas/8ffr20-00181-01/
https://csirt.gob.cl/media/2020/01/8FFR20-00181-01.pdf

8FFR20-00182-01 CSIRT ADVIERTE DE TRES PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00182-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Enero de 2020
Última revisión	15 de Enero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de tres portales fraudulentos asociados a tres IPs que suplantan el sitio web oficial de Banco Estado, los que podrían servir para robar credenciales de usuarios de esa entidad.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://csirt.gob.cl/alertas/8ffr20-00182-01/

https://csirt.gob.cl/media/2020/01/8FFR20-00182-01.pdf

Phishing

8FPH20-00091-01 CSIRT ADVIERTE DE PHISHING POR TANSFERENCIA DE FONDOS RETINADA

Alerta de seguridad informática	8FPH20-00091-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Enero de 2020
Última revisión	11 de Enero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing a través de un correo electrónico que intenta persuadir a los usuarios del Banco Scotiabank para seleccionar un hipervínculo que los direcciona a un sitio semejante al del Banco. Para ello, el atacante utiliza un mensaje indicando que existe una transferencia de fondos retenida y así convencer a la víctima de seleccionar el enlace.

Enlace:

https://csirt.gob.cl/alertas/8fph20-00091-01/

https://csirt.gob.cl/media/2020/01/8FPH20-00091-01.pdf

8FPH20-00092-01 CSIRT ADVIERTE DE PHISHING POR ACTUALIZACIÓN DE SERVIDORES

Alerta de seguridad informática	8FPH20-00092-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Enero de 2020
Última revisión	11 de Enero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing a través de un correo electrónico que intenta persuadir a los usuarios del Banco Estado.

El falso mensaje informa que se realizó un proceso de actualización de los servidores, sin embargo, la cuenta del usuario no se registró correctamente, motivo por el cual ésta fue bloqueada temporalmente. Para restablecer la cuenta, el usuario debe ingresar a un enlace que los atacantes han dispuesto en el cuerpo del correo. Al seleccionar el vínculo el usuario es dirigido a un sitio semejante al del Banco.

Enlace:

https://csirt.gob.cl/alertas/8fph20-00092-01/

https://csirt.gob.cl/media/2020/01/8FPH20-00092-01.pdf

Malware

2CMV20-00042-01 CSIRT ADVIERTE DE CAMPAÑA DE PHISHING CON MALWARE EMOTET

Alerta de seguridad informática	2CMV20-00042-01
Clase de alerta	Código Malicioso
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Enero de 2020
Última revisión	15 de Enero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de Phishing con malware Emotet.

La campaña consiste en el envío de un correo cuyo mensaje hace alusión a una factura que se adjunta en el documento, sin indicar otros detalles. El objetivo es incentivar al receptor del correo para que seleccione el enlace. Al hacerlo se realiza la descarga de un archivo doc, el que una vez abierto desencadena una infección del malware comunicándose con otras URLs y servidores comando y control.

Enlace:

https://csirt.gob.cl/alertas/2cmv20-00042-01/

https://csirt.gob.cl/media/2020/01/2CMV20-00042-01.pdf

Vulnerabilidades

9VSA20-00114-01 CSIRT COMPARTE ACTUALIZACIONES DE MOZILLA PARA FIREFOX Y FIREFOXESR

Alerta de seguridad informática	9VSA20-00114-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Enero de 2020
Última revisión	09 de Enero de 2020

Vulnerabilidad

CVE-2019-17016
CVE-2019-17017
CVE-2019-17018
CVE-2019-17019
CVE-2019-17015
CVE-2019-17020
CVE-2019-17021
CVE-2019-17022
CVE-2019-17023
CVE-2019-17024
CVE-2019-17025

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de Mozilla, referente a vulnerabilidades que afectan a sus exploradores Firefox y Firefox ESR, las cuales de ser explotadas, permitirían a un atacante remoto obtener información confidencial, inyectar código de forma remota, saltar ciertas restricciones de seguridad, entre otras cosas. En el contenido de este informe se encuentra la respectiva mitigación.

Enlace

https://csirt.gob.cl/vulnerabilidades/9vsa20-00114-01/
https://csirt.gob.cl/media/2020/01/9VSA20-00114-01.pdf

9VSA20-00115-01 CSIRT COMPARTE ACTUALIZACIONES DE FORTINET PARA ORTIOS Y FORTIAP-S/W2

Alerta de seguridad informática	9VSA20-00115-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de enero de 2020
Última revisión	09 de enero de 2020

Vulnerabilidad

CVE-2019-9494
CVE-2019-9495

CVE-2019-9496
CVE-2019-9497
CVE-2019-9498
CVE-2019-9499

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Fortinet referente a diversas vulnerabilidades que afectan a la implementación estandar de FortiOS y FortiAP-S/W2. El informe contiene la correspondiente mitigación.

Enlace

https://csirt.gob.cl/vulnerabilidades/9vsa20-00115-01/
https://csirt.gob.cl/media/2020/01/9VSA20-00115-01.pdf

9VSA20-00116-01 CSIRT COMPARTE ACTUALIZACIONES DE MOZILLA PARA FIREFOX Y FIREFOX ESR

Alerta de seguridad informática	9VSA20-00116-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de enero de 2020
Última revisión	07 de enero de 2020

Vulnerabilidad

CVE-2019-17026

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de Mozilla, referente a una vulnerabilidad que afecta a sus exploradores Firefox y Firefox ESR, la cual, de ser explotada, permitiría a un atacante remoto realizar la ejecución de código remoto sobre el sistema afectado. Esto junto a su respectiva mitigación.

Enlace

https://csirt.gob.cl/vulnerabilidades/9vsa20-00116-01/
https://csirt.gob.cl/media/2020/01/9VSA20-00116-01.pdf

9VSA20-00117-01 CSIRT COMPARTE ACTUALIZACIÓN DE PHPMYADMIN PARA MYSSQL

Alerta de seguridad informática	9VSA20-00117-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de enero de 2020
Última revisión	11 de enero de 2020

Vulnerabilidad

CVE-2020-5504

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de phpMyAdmin, referente a una vulnerabilidad que afecta a su herramienta de administración MySQL web, la cual de ser explotada, permitiría a un usuario no autorizado obtener el control completo de la base de datos. El informe contiene la respectiva mitigación de la vulnerabilidad.

Enlace

https://csirt.gob.cl/vulnerabilidades/9vsa20-00117-01/
https://csirt.gob.cl/media/2020/01/9VSA20-00117-01.pdf

9VSA20-00118-01 CSIRT COMPARTE ACTUALIZACIONES PARA IBM QRADAR

Alerta de seguridad informática	9VSA20-00118-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de enero de 2020
Última revisión	12 de enero de 2020

Vulnerabilidad

CVE-2019-4559

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de la fuente oficial de IBM, referente a una vulnerabilidad que afecta a su sistema SIEM, IBM QRadar, la cual permitiría a usuarios no autorizados obtener información sensible. El informe incluye la respectiva mitigación.

Enlace

https://csirt.gob.cl/vulnerabilidades/9vsa20-00118-01/
https://csirt.gob.cl/media/2020/01/9VSA20-00118-01.pdf

9VSA20-00119-01 CSIRT COMPARTE ACTUALIZACIÓN PARA MOZILLA THUNDERBIRD

Alerta de seguridad informática	9VSA20-00119-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de enero de 2020
Última revisión	13 de enero de 2020

Vulnerabilidad

CVE-2019-17015
CVE-2019-17016
CVE-2019-17017
CVE-2019-17021
CVE-2019-17022
CVE-2019-17024

CVE-2019-17026

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de Mozilla, referente a vulnerabilidades que afectan a Mozilla Thunderbird, las cuales de ser explotadas permitirían a un atacante remoto obtener información confidencial, inyectar código de forma remota, saltar ciertas restricciones de seguridad, entre otras cosas. Este informe incluye la respectiva mitigación.

Enlace

https://csirt.gob.cl/vulnerabilidades/9vsa20-00119-01/
https://csirt.gob.cl/media/2020/01/9VSA20-00119-01.pdf

9VSA20-00120-01 CSIRT COMPARTE ACTUALIZACIÓN PARA FORTINET FORTISIEM

Alerta de seguridad informática	9VSA20-00120-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de enero de 2020
Última revisión	13 de enero de 2020

Vulnerabilidad

CVE-2019-16153

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de Fortinet, referente a una vulnerabilidad que afecta a Fortinet FortiSIEM, la cual de ser explotada permitiría a un atacante remoto obtener credenciales embebidas en el sistema y comprometerlo completamente. Este informe incluye la respectiva mitigación.

Enlace

https://csirt.gob.cl/vulnerabilidades/9vsa20-00120-01/
https://csirt.gob.cl/media/2020/01/9VSA20-00120-01.pdf

9VSA20-00121-01 CSIRT COMPARTE ACTUALIZACIONES DE NGINX

Alerta de seguridad informática	9VSA20-00121-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de enero de 2020
Última revisión	14 de enero de 2020

Vulnerabilidad

CVE-2019-20372

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de Nginx, referente a una vulnerabilidad que afecta a su servidor web/proxy/mail, la cual

de ser explotada permitiría a un atacante remoto obtener acceso a páginas web no autorizadas. Este informe incluye la respectiva mitigación.

Enlace

https://csirt.gob.cl/vulnerabilidades/9vsa20-00121-01/
https://csirt.gob.cl/media/2020/01/9VSA20-00121-01.pdf

9VSA20-00122-01 CSIRT COMPARTE ACTUALIZACIONES ENTREGADAS POR MICROSOFT

Alerta de seguridad informática	9VSA20-00122-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de enero de 2020
Última revisión	15 de enero de 2020

Vulnerabilidad

CVE-2020-0601
CVE-2020-0607
CVE-2020-0608
CVE-2020-0615
CVE-2020-0622
CVE-2020-0637
CVE-2020-0639
CVE-2020-0643
CVE-2020-0647
CVE-2020-0650
CVE-2020-0651
CVE-2020-0652
CVE-2020-0653
CVE-2020-0654
CVE-2019-1491
CVE-2020-0602
CVE-2020-0603
CVE-2020-0605
CVE-2020-0606
CVE-2020-0609
CVE-2020-0610
CVE-2020-0611
CVE-2020-0612
CVE-2020-0613
CVE-2020-0614
CVE-2020-0616
CVE-2020-0617
CVE-2020-0620
CVE-2020-0621

CVE-2020-0623
CVE-2020-0624
CVE-2020-0625
CVE-2020-0626
CVE-2020-0627
CVE-2020-0628
CVE-2020-0629
CVE-2020-0630
CVE-2020-0631
CVE-2020-0632
CVE-2020-0633
CVE-2020-0634
CVE-2020-0635
CVE-2020-0636
CVE-2020-0638
CVE-2020-0640
CVE-2020-0641
CVE-2020-0642
CVE-2020-0644
CVE-2020-0646
CVE-2020-0656

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Microsoft en su reporte mensual de actualizaciones correspondiente a Enero de 2020, parchando 14 vulnerabilidades en sus softwares. Además se informa de 36 vulnerabilidades adicionales al reporte mensual.

Entre la información entregada por Microsoft, se destaca la vulnerabilidad CVE-2020-0601, ya que esta vulnerabilidad afecta a todas las máquinas que ejecutan sistemas operativos Windows 10 de 32 o 64 bits, incluidas las versiones de Windows Server 2016 y 2019. Esta vulnerabilidad permite que la validación del certificado de Elliptic Curve Cryptography (ECC) omita el almacén de confianza, permitiendo que el software no deseado o malicioso se disfrace como firmado auténticamente por una organización confiable. Esto podría engañar a los usuarios o frustrar los métodos de detección de malware, como los antivirus. Además, se podría emitir un certificado creado con fines malintencionados para un nombre de host que no lo autorizó, y un navegador que se base en Windows CryptoAPI no emitiría una advertencia, lo que permitiría a un atacante descifrar, modificar o inyectar datos en las conexiones del usuario sin detección.

Enlace

https://csirt.gob.cl/vulnerabilidades/9vsa20-00122-01/
https://csirt.gob.cl/media/2020/01/9VSA20-00122-01.pdf

9VSA20-00123-01 CSIRT COMPARTE ACTUALIZACIÓN ENTREGADA POR VMWARE PARA VMWARE TOOLS

Alerta de seguridad informática	9VSA20-00123-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de enero de 2020
Última revisión	15 de enero de 2020

Vulnerabilidad

CVE-2020-3941

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de VMware referente a una vulnerabilidad que afecta a VMware Tools, la cual de ser explotada permitiría a un atacante escalar privilegios en el sistema Windows VM afectado. Este informe incluye la respectiva mitigación.

Enlace

https://csirt.gob.cl/vulnerabilidades/9vsa20-00123-01/
https://csirt.gob.cl/media/2020/01/9VSA20-00123-01.pdf

Indicadores de Compromisos

Se comparte a continuación el listado de indicadores de compromisos que fueron detectados durante las pasadas dos semanas 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:

IoC	Motivo
162.208.50.75	Port Scan
117.4.139.56	Port Scan
58.229.119.103	Port Scan
180.148.5.217	Port Scan
113.161.167.11	Port Scan
143.215.247.68	Port Scan
163.172.240.196	Port Scan
60.199.133.71	Port Scan
185.153.199.242	Port Scan
140.240.36.179	DdoS
140.240.40.6	DdoS
171.107.12.206	DdoS
171.109.122.143	DdoS
18.209.163.113	Phishing

54.145.144.164	Phishing
107.151.148.2	Port Scan
185.53.88.110	Port Scan
120.243.59.211	DdoS
121.52.214.245	DdoS
122.238.94.242	DdoS
122.240.164.128	DdoS
125.67.65.51	DdoS
37.49.227.202	DdoS
45.136.109.221	DdoS
45.141.86.127	DdoS
45.141.86.132	DdoS
61.167.94.163	DdoS
222.212.16.203	DdoS
223.71.167.165	DdoS
223.89.163.193	DdoS
36.157.125.166	DdoS
36.43.236.13	DdoS
107.180.48.66	Phishing
185.216.140.252	DdoS
193.32.163.74	DdoS
218.0.6.74	DdoS
219.217.246.81	DdoS
221.234.236.214	DdoS
117.153.3.83	DdoS
117.182.132.8	DdoS
119.96.109.43	DdoS
120.228.221.87	DdoS
120.239.165.69	DdoS
106.6.171.74	DdoS
110.230.249.130	DdoS
111.18.44.228	DdoS
111.187.43.204	DdoS
117.151.42.147	DdoS
171.83.116.132	DdoS
175.1.15.37	DdoS
183.151.134.141	DdoS
183.221.76.132	DdoS
185.175.93.14	DdoS
37.46.114.17	DdoS
194.61.24.69	Port Scan

91.208.184.72	Port Scan
82.102.173.94	Port Scan
138.197.130.211	Port Scan
62.201.241.77	Port Scan
177.22.123.13	Port Scan
62.210.13.253	Port Scan
66.70.181.31	Port Scan
116.110.234.131	Port Scan
117.215.188.254	Port Scan
49.142.74.176	Port Scan
69.197.131.122	Port Scan
139.162.73.192	Port Scan
212.71.255.153	Port Scan
43.245.209.72	Port Scan
79.223.84.61	Port Scan
80.82.65.122	Port Scan
217.61.111.14	Port Scan
181.211.130.109	Emotet
41.169.20.147	Emotet
201.48.45.213	Port Scan
51.75.232.162	Port Scan
23.227.194.156	Port Scan
103.66.79.94	Port Scan
173.194.91.138	Port Scan
115.195.211.130	Port Scan
52.142.25.231	Port Scan
109.172.57.250	Port Scan
51.105.107.92	Port Scan
82.55.190.203	Port Scan
147.135.118.74	Port Scan
193.210.18.18	Port Scan
185.171.121.86	Port Scan
46.80.111.75	Port Scan
37.203.250.88	Port Scan
189.84.242.84	Port Scan
58.182.239.252	Port Scan
58.182.249.84	Port Scan
195.231.2.26	Port Scan
69.162.126.238	Port Scan
80.82.64.98	Port Scan
213.136.68.63	Port Scan

189.110.92.60	Port Scan
164.68.112.178	Port Scan
36.82.97.125	Port Scan
221.238.11.98	DdoS
125.46.86.42	DdoS
42.243.14.230	DdoS
210.73.80.131	DdoS
101.88.80.170	DdoS
119.39.18.128	DdoS
171.41.237.66	DdoS
122.96.50.81	DdoS
210.211.117.196	Port Scan
5.196.75.24	Port Scan
64.235.45.123	Port Scan
64.188.21.26	Port Scan
64.188.21.35	Port Scan
64.188.21.12	Port Scan
64.188.21.16	Port Scan
216.198.73.78	Port Scan
45.76.99.82	Port Scan
14.188.122.108	Port Scan
192.223.27.100	Port Scan
64.188.21.13	Port Scan
171.67.70.102	Port Scan
39.50.49.198	Port Scan
192.161.188.144	Port Scan
83.34.73.68	Port Scan
192.161.188.142	Port Scan
216.198.73.95	Port Scan
216.198.73.90	Port Scan
216.198.73.89	Port Scan
62.201.240.210	Port Scan
197.253.146.107	Port Scan
167.172.237.162	Port Scan
77.247.110.197	Port Scan
125.161.106.94	Port Scan
155.94.211.30	Port Scan
77.247.110.77	Port Scan
51.159.56.252	Port Scan
51.159.56.249	Port Scan
51.159.56.248	Port Scan

51.159.56.250	Port Scan
51.159.56.251	Port Scan
104.236.80.32	Port Scan
89.248.173.7	Port Scan
41.223.105.228	Port Scan
116.105.252.92	Port Scan
14.186.93.5	Port Scan
185.20.198.23	Port Scan
185.176.27.90	Port Scan
195.231.1.129	Port Scan
195.231.2.125	Port Scan
201.245.168.163	Port Scan
193.56.28.114	Port Scan
192.227.67.194	Port Scan
188.214.88.206	Port Scan
172.105.225.32	Port Scan
94.102.52.241	Port Scan
49.236.198.162	Port Scan
94.23.155.15	Port Scan
157.245.243.158	Port Scan
190.113.172.152	Port Scan
144.217.89.17	Port Scan
185.246.210.151	Port Scan
14.248.80.6	Port Scan
59.98.48.149	Port Scan
62.201.218.22	Port Scan
51.79.83.81	Port Scan
41.38.245.24	Port Scan
139.194.90.192	Port Scan
45.225.236.37	Port Scan
45.143.220.139	Port Scan
144.91.120.84	Port Scan
80.82.77.192	Port Scan
144.91.112.94	Port Scan
172.14.88.205	Port Scan
185.116.166.26	Port Scan
14.188.76.219	Port Scan
92.246.76.200	Port Scan
195.231.5.38	Port Scan
194.180.224.124	Port Scan
92.42.44.244	Port Scan

144.217.34.148	Port Scan
78.47.62.255	Port Scan
79.137.37.62	Port Scan
80.211.186.179	Port Scan
173.249.8.119	Phishing
163.172.9.40	Port Scan
31.14.40.200	Port Scan
51.159.0.190	Port Scan
102.140.197.193	Port Scan
163.172.200.81	Port Scan
165.22.122.240	Port Scan
185.106.96.150	Cryptocurrency
78.47.123.168	Cryptocurrency
185.53.179.8	Cryptocurrency
78.47.118.115	Cryptocurrency
78.47.121.215	Cryptocurrency
1.235.72.112	Port Scan
202.60.94.196	Port Scan
175.158.43.245	Port Scan
104.194.11.10	Port Scan

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.

- Nicolás Fernández - https://www.linkedin.com/in/nicolas-fernandez-6415b377/
- Jacob Salazar - https://www.linkedin.com/in/jacob-alexis-salazar-ramirez-6870725b/

Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java, entre otras)
- 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

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.01.17 16:20:02 -03'00'