CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Informática

Publicado el Viernes 21 de Febrero de 2020

Resumen de noticias, reportes, alertas e indicadores de compromisos informados por CSIRT entre el jueves 13 de Febrero y el miércoles 19 de Febrero de 2020.

Falsificación de Registro o Identidad

8FFR20-00215-01 CSIRT ADVIERTE DE SITIO BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR20-00215-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de febrero de 2020
Última revisión	13 de febrero 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 de Chile, 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://www.csirt.gob.cl/alertas/8ffr20-00215-01/

https://www.csirt.gob.cl/media/2020/02/8FFR20-00215-01.pdf

8FFR20-0216-01 CSIRT ADVIERTE DE 7 SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00216-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Febrero de 2020
Última revisión	13 de Febrero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de siete portales fraudulentos asociados a una IP 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://www.csirt.gob.cl/alertas/8ffr20-0216-01/
https://www.csirt.gob.cl/media/2020/02/8FFR20-00216-01.pdf

8FFR20-00217-01 CSIRT ADVIERTE 2 PÁGINAS BANCARIAS FRAUDULENTAS

Alerta de seguridad informática	8FFR20-00217-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Febrero de 2020
Última revisión	13 de Febrero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de dos portales fraudulentos asociados a una IP que suplanta el sitio web oficial de Banco Estado, 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://www.csirt.gob.cl/alertas/8ffr20-00217-01/
https://www.csirt.gob.cl/media/2020/02/8FF20R-00217-01.pdf

8FFR20-00218-01 CSIRT ADVIERTE DE SITIO BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR20-00218-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Febrero de 2020
Última revisión	16 de Febrero 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 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://www.csirt.gob.cl/alertas/8ffr20-00218-01/
https://www.csirt.gob.cl/media/2020/02/8FFR20-00218-01.pdf

8FFR20-00219-01 CSIRT ALERTA DE PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR20-00219-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Febrero de 2020
Última revisión	16 de Febrero 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 Itau, 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://www.csirt.gob.cl/alertas/8ffr20-00219-01/
https://www.csirt.gob.cl/media/2020/02/8FFR20-00219-01.pdf

8FFR20-00220-01 CSIRT ADVIERTE DE TRES SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00220-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Febrero de 2020
Última revisión	18 de Febrero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) ha identificado la activación de tres portales fraudulentos asociados a dos IP que suplantan el sitio web oficial del 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://www.csirt.gob.cl/alertas/8ffr20-00220-01/
https://www.csirt.gob.cl/media/2020/02/8FFR20-00220-01.pdf

8FFR20-00221-01 CSIRT ADVIERTE PÁGINA BANCARIA FRAUDULENTA

Alerta de seguridad informática	8FFR20-00221-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Febrero de 2020
Última revisión	18 de Febrero 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 del Banco Security, 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://www.csirt.gob.cl/alertas/8ffr20-00221-01/
https://www.csirt.gob.cl/media/2020/02/8FFR20-00221-01.pdf

8FFR20-00222-01 CSIRT ADVIERTE DE 2 PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-0022-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de febrero de 2020
Última revisión	19 de febrero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de dos portales fraudulentos asociados a dos IP que suplantan el sitio web oficial del Banco Estado, 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://www.csirt.gob.cl/alertas/8ffr20-00222-01/
https://www.csirt.gob.cl/media/2020/02/8FFR20-00222-01.pdf

Phishing

8FPH20-00112-01 CSIRT ADVIERTE DE PHISHING POR SATURACIÓN DE CUENTA

Alerta de seguridad informática	8FPH20-00112-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Febrero de 2020
Última revisión	13 de Febrero 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 supuestamente de un proveedor de servicio de correo.

El mensaje informa a la víctima que ha excedido el tamaño del buzón y no podrá enviar o recibir correos. El atacante ofrece como solución actualizar la cuenta y de esta forma aumentar el tamaño de la cuenta. Además indica que si no lo realiza dentro de tres próximos días se cerrará la cuenta permanentemente. Al seleccionar el vínculo para actualizar la cuenta, la víctima es dirigida a un sitio donde le solicitan su correo, su usuario y contraseña.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00112-01/
https://www.csirt.gob.cl/media/2020/02/8FPH20-00112-01.pdf

8FPH20-00113-01 CSIRT ADVIERTE PHISING DE SEXTORTION

Alerta de seguridad informática	8FPH20-00113-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Febrero de 2020
Última revisión	14 de Febrero 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 extorsionar a un usuario.

El mensaje informa a la víctima que un atacante ha logrado acceder a su sistema y a las cuentas del usuario. La intromisión, perpetrada hace meses atrás, se habría producido cuando la víctima supuestamente visitó un sitio para adultos, oportunidad en la cual el equipo fue infectado con un malware. Este malware habría permitido al atacante acceder a la pantalla, cámara, micrófono, correspondencia y a los contactos del usuario afectado. El atacante amenaza al usuario indicándole que compartirá un video comprometedor de la víctima a sus contactos. Para evitar esta situación, la víctima debe transferir $594 dólares a la dirección de bitcoin del hacker.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00113-01/

https://www.csirt.gob.cl/media/2020/02/8FPH20-00113-01.pdf

8FPH20-00114-01 CSIRT ADVIERTE PHISHING SOBRE CADUCIDAD DE CUENTA DE CORREO

Alerta de seguridad informática	8FPH20-00114-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Febrero de 2020
Última revisión	17 de febrero 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.

El mensaje informa a la víctima que su cuenta de correo caducará dentro de dos días, el atacante ofrece como solución iniciar sesión y confirmar la dirección del correo para continuar usándola. Para ello, disponibiliza un hipervínculo ubicado en el cuerpo del correo. Al seleccionar el enlace, el usuario es derivado a un sitio donde le solicitará los datos.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00114-01/

https://www.csirt.gob.cl/media/2020/02/8FPH20-00114-01.pdf

8FPH20-00115-01 CSIRT ADVIERTE PHISHING POR INCONVENIENTES EN EL PAGO

Alerta de seguridad informática	8FPH20-00115-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Febrero de 2020
Última revisión	17 de Febrero 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 cuyo mensaje intenta engañar a los usuarios que tienen contratado el servicio de Netflix.

El correo indica que existe un inconveniente con la información de pago. La modalidad de estafa en este caso es ofrecer varias alternativas al usuario, desde ir a un centro de ayudas, contactarse con la empresa, ofrece un nuevo intento o ingresar a la nueva forma de pago. Cada alternativa lleva a la víctima hacia un enlace que se asemeja al de Netflix. En ese sitio se solicita a las víctimas los datos de sus cuentas y luego los datos de la tarjeta de crédito.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00115-01/
https://www.csirt.gob.cl/media/2020/02/8FPH20-00115-01.pdf

Vulnerabilidades

9VSA20-00140-01 CSIRTCOMPARTE ACTUALIZACIONES DE MOZILLA PARA THUNDERBIRD

Alerta de seguridad informática	9VSA20-00140-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Febrero de 2020
Última revisión	13 de Febrero de 2020

Vulnerabilidad

CVE-2020-6792
CVE-2020-6793
CVE-2020-6794
CVE-2020-6795
CVE-2020-6797
CVE-2020-6798
CVE-2020-6800

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de Mozilla, referente a múltiples vulnerabilidades que afectan a cliente de correo Mozilla

Thunderbird. De ser explotadas, estas permitirían a un atacante causar denegación de servicios, obtener información sensible y hasta comprometer completamente al sistema vulnerable. Este informe incluye la respectiva mitigación.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00140-01/
https://www.csirt.gob.cl/media/2020/02/9VSA20-00140-01.pdf

9VSA20-00141-01 CSIRT COMPARTE ACTUALIZACIONES DE MICROSOFT

Alerta de seguridad informática	9VSA20-00141-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de febrero de 2020
Última revisión	13 de febrero de 2020

Vulnerabilidad

CVE-2020-0618
CVE-2020-0696
CVE-2020-0736
CVE-2020-0658
CVE-2020-0697
CVE-2020-0744
CVE-2020-0675
CVE-2020-0698
CVE-2020-0746
CVE-2020-0676
CVE-2020-0705
CVE-2020-0748
CVE-2020-0677
CVE-2020-0706
CVE-2020-0755
CVE-2020-0689
CVE-2020-0714
CVE-2020-0756
CVE-2020-0693
CVE-2020-0716
CVE-2020-0759
CVE-2020-0694
CVE-2020-0717
CVE-2020-0695
CVE-2020-0728

Reportados adicionalmente:

CVE-2020-0655
CVE-2020-0691

CVE-2020-0732
CVE-2020-0657
CVE-2020-0692
CVE-2020-0733
CVE-2020-0659
CVE-2020-0701
CVE-2020-0734
CVE-2020-0660
CVE-2020-0702
CVE-2020-0735
CVE-2020-0661
CVE-2020-0703
CVE-2020-0737
CVE-2020-0662
CVE-2020-0704
CVE-2020-0738
CVE-2020-0663
CVE-2020-0707
CVE-2020-0739
CVE-2020-0665
CVE-2020-0708
CVE-2020-0740
CVE-2020-0666
CVE-2020-0709
CVE-2020-0741
CVE-2020-0667
CVE-2020-0710
CVE-2020-0742
CVE-2020-0668
CVE-2020-0711
CVE-2020-0743
CVE-2020-0669
CVE-2020-0712
CVE-2020-0745
CVE-2020-0670
CVE-2020-0713
CVE-2020-0747
CVE-2020-0671
CVE-2020-0715
CVE-2020-0749
CVE-2020-0672
CVE-2020-0719
CVE-2020-0750
CVE-2020-0673
CVE-2020-0720

CVE-2020-0751
CVE-2020-0674
CVE-2020-0721
CVE-2020-0752
CVE-2020-0678
CVE-2020-0722
CVE-2020-0753
CVE-2020-0679
CVE-2020-0723
CVE-2020-0754
CVE-2020-0680
CVE-2020-0724
CVE-2020-0757
CVE-2020-0681
CVE-2020-0725
CVE-2020-0767
CVE-2020-0682
CVE-2020-0726
CVE-2020-0792
CVE-2020-0683
CVE-2020-0727
CVE-2020-0817
CVE-2020-0685
CVE-2020-0729
CVE-2020-0818
CVE-2020-0686
CVE-2020-0730
CVE-2020-0688
CVE-2020-0731

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de TeamViewer, referente a una vulnerabilidad que afecta su sistema de encriptación de contraseñas, la cual de ser explotada permitiría a un atacante local obtener las credenciales utilizadas en la aplicación. Este informe incluye la respectiva mitigación.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00141-001/
https://www.csirt.gob.cl/media/2020/02/9VSA20-00141-01.pdf

9VSA20-00142-01 CSIRT COMPARTE ACTUALIZACIONES DE GITLAB

Alerta de seguridad informática	9VSA20-00142-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de febrero de 2020
Última revisión	14 de febrero de 2020

Vulnerabilidad

CVE-2020-8795

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de GitLab, referente a una vulnerabilidad que afecta a su característica para compartir grupos, la cual, de ser explotada, permitiría a un atacante remoto acceder a proyectos de terceros sin autorización. Este informe incluye la respectiva mitigación.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00142-01/
https://www.csirt.gob.cl/media/2020/02/9VSA20-00142-01.pdf

9VSA20-00143-01 CSIRT COMPARTE ACTUALIZACIÓN PARA ANDROID

Alerta de seguridad informática	9VSA20-00143-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de febrero de 2020
Última revisión	17 de febrero de 2020

Vulnerabilidad

CVE-2020-0005
CVE-2020-0014
CVE-2020-0015
CVE-2020-0017
CVE-2020-0018
CVE-2020-0020
CVE-2020-0021
CVE-2020-0022
CVE-2020-0023
CVE-2020-0026
CVE-2020-0027
CVE-2020-0028
CVE-2020-0030
CVE-2019-2200

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de Google, referente a vulnerabilidades que afectan al sistema operativo Android, las cuales de ser explotadas permitirían a un atacante realizar ataques de denegación de servicios, obtener acceso a información sensible, escalar privilegios en el sistema y hasta comprometer completamente al sistema vulnerable. Este informe incluye la respectiva mitigación.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00143-01/
https://www.csirt.gob.cl/media/2020/02/9VSA20-00143-01.pdf

9VSA20-00144-01 CSIRT COMPARTE ACTUALIZACIÓN PARA DOTA 2

Alerta de seguridad informática	9VSA20-00144-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de febrero de 2020
Última revisión	19 de febrero de 2020

Vulnerabilidad

CVE-2020-9005

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de múltiples fuentes, referente a una vulnerabilidad que afecta al videojuego DOTA 2 de Valve, la cual de ser explotada, permitiría a un atacante realizar ataques de denegación de servicios y ejecución de código remoto. Este informe incluye la respectiva mitigación.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00144-01/
https://www.csirt.gob.cl/media/2020/02/9VSA20-00144-01.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
8.209.76.143	Malware
160.153.129.213	Malware
8.209.76.143	Malware
8.209.76.143	Malware
162.159.134.233	Malware
208.113.152.109	Phishing

45.77.229.248	SQLi Attempt
162.243.128.105	Port Scan
162.243.130.197	Port Scan
50.116.17.183	Port Scan
103.231.161.78	Port Scan
103.231.161.77	Port Scan
103.231.161.72	Port Scan
103.231.161.73	Port Scan
103.231.161.75	Port Scan
103.231.161.79	Port Scan
103.231.161.76	Port Scan
103.231.161.74	Port Scan
162.243.131.210	Port Scan
123.253.88.55	Port Scan
68.183.170.114	Port Scan
198.199.119.98	Port Scan
162.243.131.167	Port Scan
103.133.109.107	Port Scan
185.168.227.238	Port Scan
162.243.128.251	Port Scan
1.162.144.24	Port Scan
189.50.252.238	Port Scan
220.92.153.250	Port Scan
220.142.162.25	Port Scan
162.243.130.163	Port Scan
162.243.128.177	Port Scan
185.150.190.103	Port Scan
192.241.224.172	Port Scan
162.243.130.125	Port Scan
162.243.128.167	Port Scan
162.243.130.183	Port Scan
103.122.14.40	Port Scan
192.241.237.6	Port Scan
192.241.231.98	Port Scan
162.243.130.175	Port Scan
84.13.204.238	Port Scan
162.243.129.58	Port Scan
162.243.128.69	Port Scan
122.155.6.206	Port Scan
185.123.101.128	Port Scan
45.79.28.132	Port Scan

117.4.115.55	Port Scan
14.170.220.203	Port Scan
85.103.62.106	Port Scan
27.73.88.226	Port Scan
113.160.82.166	Port Scan
171.236.48.115	Port Scan
113.212.112.4	Port Scan
184.82.25.206	Port Scan
49.145.205.78	Port Scan
14.188.169.249	Port Scan
101.108.122.118	Port Scan
58.186.14.22	Port Scan
116.97.214.42	Port Scan
118.173.204.221	Port Scan
14.181.33.62	Port Scan
14.176.200.233	Port Scan
37.194.225.63	Port Scan
49.68.246.198	Port Scan
78.108.184.198	Malware
162.243.128.36	Port Scan
192.241.232.227	Port Scan
192.241.234.109	Port Scan
162.243.130.26	Port Scan
162.243.131.9	Port Scan
162.243.130.121	Port Scan
195.154.28.229	Port Scan
79.122.53.88	Port Scan
223.146.37.224	Port Scan
1.162.144.25	Port Scan
1.162.144.56	Port Scan
1.168.117.60	Port Scan
36.226.177.68	Port Scan
36.228.26.89	Port Scan
113.22.166.86	Port Scan
1.172.55.129	Port Scan
118.71.213.249	Port Scan
2.132.212.236	Port Scan
36.229.252.38	Port Scan
220.141.52.11	Port Scan
118.68.33.131	Port Scan
112.72.79.3	Port Scan

42.118.148.73	Port Scan
113.22.170.10	Port Scan
47.254.213.81	Port Scan
183.80.22.226	Port Scan
180.93.14.162	Port Scan
77.247.110.88	Port Scan
162.243.129.215	Port Scan
192.241.236.248	Port Scan
162.243.129.180	Port Scan
192.241.239.251	Port Scan
162.243.130.40	Port Scan
162.243.128.43	Port Scan
210.137.6.37	Port Scan
217.117.4.110	Port Scan
192.241.238.64	Port Scan
218.255.24.226	Port Scan
162.243.131.78	Port Scan
221.138.17.152	Port Scan
26.165.218.44	Port Scan
47.206.4.145	Port Scan
70.224.36.194	Port Scan
81.94.192.10	Port Scan
81.94.192.147	Port Scan
84.49.242.125	Port Scan
97.90.44.200	Port Scan
14.207.152.122	Port Scan
80.211.91.172	Port Scan
80.82.78.100	Port Scan
45.148.10.179	Port Scan
54.37.200.119	Port Scan
185.222.58.133	Port Scan
194.34.134.207	Port Scan
1.172.55.129	Port Scan
162.243.130.86	Port Scan
162.243.131.186	Port Scan
162.243.131.22	Port Scan
192.241.237.175	Port Scan
192.241.231.118	SSH Attempt
125.160.17.32	SSH Attempt
139.162.122.110	SSH Attempt
182.253.70.89	SSH Attempt

195.88.142.204	SSH Attempt
101.109.115.27	SSH Attempt
122.54.175.202	SSH Attempt
137.74.53.155	SSH Attempt
209.141.35.177	SSH Attempt
14.171.191.243	SSH Attempt
36.89.135.79	SSH Attempt
157.245.104.96	SSH Attempt
45.55.23.144	SSH Attempt
164.52.24.164	SSH Attempt
189.195.41.134	SSH Attempt
197.231.70.60	SSH Attempt
219.93.106.33	SSH Attempt
45.148.10.91	SSH Attempt
51.38.36.84	SSH Attempt
5.13.34.133	SSH Attempt
60.251.229.67	SSH Attempt
75.127.13.67	SSH Attempt
65.49.20.66	SSH Attempt
79.27.235.172	SSH Attempt
81.136.255.20	SSH Attempt
92.118.27.202	SSH Attempt
82.64.140.9	SSH Attempt
95.156.31.74	SSH Attempt
115.112.61.220	SSH Attempt
84.92.39.93	SSH Attempt
103.56.207.117	SSH Attempt
31.165.11.9	SSH Attempt
103.72.8.7	SSH Attempt
165.22.93.239	IP_Src_session
192.241.220.35	UDP_Src_session
162.243.135.103	Port Scan
192.241.224.81	Port Scan
192.241.235.86	Port Scan
192.241.223.106	Port Scan
185.53.88.126	Port Scan
162.243.135.115	Port Scan
162.243.130.198	Port Scan
192.241.224.81	Port Scan
192.241.220.215	Port Scan
162.243.133.91	Port Scan

70.36.103.235	Port Scan
140.238.225.206	Port Scan
178.173.203.159	Port Scan
92.118.234.202	Port Scan
172.81.129.216	Port Scan
5.145.86.46	Port Scan
79.112.194.149	Port Scan
86.123.36.217	Port Scan
162.243.132.6	Port Scan
162.243.134.201	Port Scan
192.241.203.139	Port Scan
192.241.208.65	Port Scan
192.241.219.25	Port Scan
192.241.222.28	Port Scan
198.199.105.231	Port Scan
210.186.147.107	Port Scan
218.212.42.143	Port Scan
86.98.86.126	Port Scan
162.243.132.159	Port Scan
192.241.232.88	Port Scan
14.254.87.160	Port Scan
192.241.238.183	Port Scan
23.237.55.10	Port Scan
162.243.129.51	Port Scan
162.243.132.7	Port Scan
162.243.132.157	Port Scan
27.77.77.148	Port Scan
162.243.132.165	Port Scan
162.243.134.225	Port Scan
192.241.213.129	Port Scan
45.143.221.47	Port Scan
192.241.219.143	Port Scan
156.218.229.248	Port Scan
193.31.40.36	Port Scan
192.241.198.105	Port Scan
193.31.40.37	Port Scan
45.143.220.200	Port Scan
192.241.223.231	Port Scan
192.241.238.152	Port Scan
77.247.110.39	Port Scan
192.241.237.102	Port Scan

192.241.210.125	Port Scan
162.243.134.64	Port Scan
192.241.211.113	Port Scan
192.241.238.229	Port Scan
192.241.237.187	Port Scan
162.243.135.71	Port Scan
198.199.105.154	Port Scan
192.241.224.19	Port Scan
192.241.208.144	Port Scan
192.241.227.177	Port Scan
192.241.233.208	Port Scan
162.243.130.234	Port Scan
192.241.231.174	Port Scan
192.241.133.191	Malware
43.255.30.111	Malware
103.108.195.89	Malware
143.92.56.10	Malware
186.10.66.139	Malware
192.241.223.140	Port Scan
192.241.227.88	Port Scan
125.104.198.245	Port Scan
125.104.205.200	Port Scan
115.214.203.114	Port Scan
183.152.216.128	Port Scan
125.122.215.57	Port Scan
162.243.136.76	Port Scan
162.243.136.41	Port Scan
51.159.30.47	Port Scan
62.171.142.207	Port Scan
162.243.135.221	Port Scan
162.243.135.9	Port Scan
36.91.107.125	Port Scan
162.243.134.169	Port Scan
103.88.129.71	Port Scan
172.104.241.110	Port Scan
221.140.57.201	Port Scan
192.241.213.146	Port Scan
198.199.117.93	Port Scan
192.64.112.32	Port Scan
31.14.40.94	Port Scan
162.243.133.176	Port Scan

114.34.72.141	Port Scan
162.243.134.111	Port Scan
111.241.199.110	Port Scan
118.163.41.12	Port Scan
88.232.5.11	Port Scan
174.138.183.59	Port Scan
188.217.238.230	Port Scan
36.232.69.137	Port Scan
114.40.188.138	Port Scan
78.47.123.172	Malware
78.47.121.243	Malware
199.231.85.124	Malware
78.47.121.241	Malware
45.9.148.125	Malware
5.9.163.18	Malware
107.191.99.95	Malware
107.191.99.221	Malware
45.9.148.129	Malware
45.9.148.117	Malware
94.130.193.148	Malware
94.130.193.147	Malware
94.130.193.146	Malware
94.130.165.87	Malware
5.9.163.19	Malware
212.83.146.233	Malware
68.183.89.155	Phishing
134.209.145.156	Phishing
45.152.6.58	Port Scan
94.1.138.47	Port Scan
105.157.228.40	Port Scan
162.243.133.57	Port Scan
162.243.133.95	Port Scan
162.243.134.131	Port Scan
162.243.135.167	Port Scan
187.93.145.58	Port Scan
192.241.211.106	Port Scan
192.241.234.246	Port Scan
199.59.242.153	Phishing
159.203.95.247	Phishing
36.170.14.2	DdoS
49.212.131.155	Port Scan

203.143.72.235	Phishing
198.199.113.198	Port Scan
186.67.71.53	Phishing
192.241.238.205	Port Scan
192.241.212.205	Port Scan
192.241.210.186	Port Scan
192.241.239.192	Port Scan
168.235.111.4	Port Scan
139.162.31.12	Port Scan
162.243.134.90	Port Scan
162.243.135.126	Port Scan
188.227.84.88	Port Scan
192.241.208.234	Port Scan
192.241.237.8	Port Scan
162.243.131.223	Port Scan
162.243.132.128	Port Scan
162.243.136.131	Port Scan
192.241.226.10	Port Scan
192.241.235.57	Port Scan
192.241.237.209	Port Scan
185.164.72.112	DdoS
192.241.238.11	Port Scan
192.241.238.154	Port Scan
192.241.238.210	Port Scan
192.241.238.245	Port Scan
192.241.239.123	Port Scan
162.243.134.66	Port Scan
162.243.136.51	Port Scan
162.243.133.116	Port Scan
192.241.225.221	Port Scan
192.241.209.7	Port Scan
192.241.235.87	Port Scan
162.243.134.66	Port Scan
193.142.146.53	Port Scan
192.241.227.213	Port Scan
192.241.225.162	Port Scan
162.243.133.233	Port Scan
192.241.221.16	Port Scan
111.121.77.153	DdoS
120.230.164.64	DdoS
124.89.78.169	DdoS

222.212.13.68	DdoS
59.42.39.51	DdoS
202.96.102.244	DdoS
27.153.71.211	DdoS
111.163.118.2	DdoS
125.73.104.191	DdoS
60.180.195.206	DdoS
206.189.74.166	Port Scan
92.249.44.4	Phishing
165.22.223.114	Phishing
51.253.85.168	Port Scan
74.63.223.110	Port Scan
162.243.131.97	Port Scan
162.243.131.200	Port Scan
192.241.239.179	Port Scan
192.241.220.151	Port Scan
192.241.212.239	Port Scan
185.244.39.76	Port Scan
162.243.136.15	Port Scan
45.56.77.175	Malware
185.103.156.5	Malware
46.182.5.20	Malware
195.22.26.248	Malware
195.110.43.159	Malware
204.11.56.48	Malware
196.245.247.17	Malware
103.27.61.222	SQLi Attempt
194.180.225.18	Port Scan
80.82.78.100	Port Scan
89.248.160.150	Port Scan
94.102.56.215	Port Scan
103.129.15.197	Port Scan
162.243.129.103	Port Scan
182.19.219.33	Port Scan
185.199.226.3	Port Scan
185.92.72.2	Port Scan
192.241.208.238	Port Scan
192.241.213.8	Port Scan
192.241.218.67	Port Scan
192.241.219.171	Port Scan
192.241.221.160	Port Scan

192.241.234.212	Port Scan
192.241.236.41	Port Scan
194.26.29.130	Port Scan
194.61.27.240	Port Scan
196.29.168.46	Port Scan
198.199.93.122	Port Scan
192.241.235.30	Port Scan
37.120.155.26	Port Scan
51.15.35.71	Port Scan
89.248.171.97	Port Scan
162.243.133.77	Port Scan
192.241.221.42	Port Scan
103.239.74.75	Malware
103.214.140.139	Malware
162.243.132.92	Port Scan
192.241.206.58	Port Scan
192.241.208.9	Port Scan
192.241.220.192	Port Scan
192.241.220.83	Port Scan

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: 2020.02.20 17:34:04 -03'00'