13BCS20-00041-01

CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Informática

Publicado el Viernes 06 de Febrero de 2020

Resumen de noticias, reportes, alertas e indicadores de compromisos informados por CSIRT entre el jueves 05 de Febrero y el miércoles 12 de Febrero de 2020.

Falsificación de Registro o Identidad

8FFR20-00207-01 CSIRT ADVIERTE DE SITIO BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR20-00207-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de febrero de 2020
Última revisión	05 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 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/8ffr20-00207-01/

https://www.csirt.gob.cl/media/2020/02/8FFR20-00207-01.pdf

8FFR20-00208-01 CSIRT ADVIERTE DE DOS PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00208-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Febrero de 2020
Última revisión	05 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 IPs que suplantan el sitio web oficial de Banco Estado, los cuales 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://www.csirt.gob.cl/alertas/8ffr20-00208-01/
https://www.csirt.gob.cl/media/2020/02/8FFR20-00208-01.pdf

8FFR20-00209-01 CSIRT ALERTA SOBRE SITIO BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR20-00209-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Febrero de 2020
Última revisión	07 de Febrero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha ientificado la activación de un portal fraudulento asociado 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/8ffr20-00209-01/
https://www.csirt.gob.cl/media/2020/02/8FFR20-00209-01.pdf

8FFR20-00210-01 CSIRT ALERTA SOBRE TRES SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00210-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Febrero de 2020
Última revisión	07 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 tres IPs 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/8ffr20-00210-01/

https://www.csirt.gob.cl/media/2020/02/8FFR20-00210-01.pdf

8FFR20-00211-01 CSIRT ADVIERTE DE PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR20-00211-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Febrero de 2020
Última revisión	08 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 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/8ffr20-00211-01/

https://www.csirt.gob.cl/media/2020/02/8FFR20-00211-01.pdf

8FFR20-00212-01 CSIRT ADVIERTE DE DOS SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00212-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Febrero de 2020
Última revisión	08 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 IPs que suplantan el sitio web oficial de Banco de Chile, los cuales 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://www.csirt.gob.cl/alertas/8ffr20-00212-01/
https://www.csirt.gob.cl/media/2020/02/8FFR20-00212-01.pdf

8FFR20-00213-01 CSIRT ADVIERTE DE 4 SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00213-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Febrero de 2020
Última revisión	11 de Febrero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) ha identificado la activación de cuatro portales fraudulentos asociados a una IP que suplanta 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/8ffr20-00213-01/
https://www.csirt.gob.cl/media/2020/02/8FFR20-00213-01.pdf

8FFR20-00214-01 CSIRT ADVIERTE DE 2 PÁGINAS BANCARIAS FRAUDULENTAS

Alerta de seguridad informática	8FFR20-00214-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de febrero de 2020
Última revisión	11 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 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/8ffr20-00214-01/
https://www.csirt.gob.cl/media/2020/02/8FFR20-00214-01.pdf

Malware

2CMV20-00048-01 CSIRT ADVIERTE DE MALWARE A TRAVÉS DE CORREO QUE AVISA DE CUENTA IMPAGA

Alerta de seguridad informática	2CMV20-00048-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Febrero de 2020
Última revisión	10 de Febrero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de malware que indica que posee mora en un pago (no indicando cual entidad).

En el mensaje del correo se visualiza una imagen de la supuesta cuenta impaga, al hacer click en el adjunto, se descarga un malware el cual se ejecuta en el equipo víctima infectándolo con Emotet.

Enlace:

https://www.csirt.gob.cl/alertas/2cmv20-00048-01/
https://www.csirt.gob.cl/media/2020/02/2CMV20-00048-01.pdf

2CMV20-00049-01 CSIRT ADVIERTE DE MALWARE POR OBLIGACIONES DE DEUDAS

Alerta de seguridad informática	2CMV20-00049-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Febrero de 2020
Última revisión	11 de Febrero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de malware a través de un correo electrónico que utiliza el nombre de la Tesorería General de la República. El mensaje del correo indica que existen obligaciones de deuda producto de una liquidación tributaria que se encuentra impaga.

En el mensaje se agrega un enlace que, una vez seleccionado, descarga un archivo ZIP. Al descomprimir el archivo se obtiene otro archivo con extensión ejecutable MSI. Al ser ejecutado, se realiza un proceso falso de instalación, pero en realidad se gatilla un script que descarga el malware.

Enlace:

https://www.csirt.gob.cl/alertas/2cmv20-00049-01/
https://www.csirt.gob.cl/media/2020/02/2CMV20-00049-01.pdf

2CMV20-00050-01 CSIRT ADVIERTE DE MALWARE EN CORREO DE FÁBRICA INTERNACIONAL

Alerta de seguridad informática	2CMV20-00050-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de Febrero de 2020
Última revisión	12 de Febrero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de malware global de fabricantes de moldes.

El mensaje del correo en inglés, incita que se abra el archivo adjunto para poder revisar una lista de productos ofrecidos al usuario que recibe este correo.

En el mensaje se adjunta un archivo comprimido, al momento de abrir el ejecutable que se encuentra dentro del archivo ZIP se activa el malware.

Enlace:

https://www.csirt.gob.cl/alertas/2cmv20-00050-01/
https://www.csirt.gob.cl/media/2020/02/2CMV20-00050-01.pdf

8FPH20-00108-01 CSIRT ADVIERTE DE PHISHING BANCARIO POR SUSPENSIÓN DE CUENTA

Alerta de seguridad informática	8FPH20-00108-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Febrero de 2020
Última revisión	05 de Febrero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado dos campañas de phishing a través de correo electrónico supuestamente proveniente del Banco Estado. Un mensaje informa a la víctima sobre la suspensión de su cuenta, el otro mensaje informa sobre la deshabilitación de la cuenta. Con esto el atacante intenta persuadir al usuario para que seleccione el enlace que se encuentra en el cuerpo del correo, al seleccionar el vínculo la víctima es dirigida a un sitio semejante al del Banco donde se expone al robo de sus credenciales. Los dos mensajes redirigen al mismo sitio.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00108-01/
https://www.csirt.gob.cl/media/2020/02/8FPH20-00108-01.pdf

8FPH20-00109-01 CSIRT ALERTA DE PHISHING BANCARIO POR SUSPENSIÓN DE CUENTA

Alerta de seguridad informática	8FPH20-00109-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Febrero de 2020
Última revisión	06 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 proveniente del Banco Estado.

El mensaje informa a la víctima sobre la suspensión de la cuenta producto de la no verificación de identidad. El atacante intenta persuadir al usuario para que seleccione el enlace que se encuentra en el cuerpo del correo, indicando que al ingresar podrá reestablecer el acceso a la cuenta. Al seleccionar el vínculo la víctima es dirigida a un sitio semejante al del Banco donde se expone al robo de sus credenciales.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00109-01/
https://www.csirt.gob.cl/media/2020/02/8FPH20-00109-01.pdf

8FPH20-00110-01 CSIRT ALERTA DE PHISHING POR RETENCIÓN DE PRODUCTOS

Alerta de seguridad informática	8FPH20-00110-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Febrero de 2020
Última revisión	07 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 proveniente de DHL.

El mensaje en inglés informa a la víctima que su paquete fue devuelto a la oficina de DHL por el no pago del costo de envío. El atacante intenta persuadir al usuario para que seleccione el enlace que se encuentra en el cuerpo del correo, indicando que tiene un plazo de 72 horas para realizar el pago. Al seleccionar el vínculo, la víctima es dirigida a un sitio semejante al de DHL donde se expone al robo de sus datos personales y a los de su tarjeta de crédito.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00110-01/
https://www.csirt.gob.cl/media/2020/02/8FPH20-00110-01.pdf

8FPH20-00111-01 CSIRT ALERTA DE PHISHING BANCARIO POR RETENCIÓN DE FONDOS

Alerta de seguridad informática	8FPH20-00111-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Febrero de 2020
Última revisión	08 de Febrero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado campañas de phishing a través de un correo electrónico supuestamente proveniente del Banco Scotiabank.

El mensaje informa a la víctima que una transferencia a terceros fue rechazada. El atacante intenta persuadir al usuario para que seleccione el enlace que se encuentra en el cuerpo del correo, indicando que revise su estado de cuenta. Al seleccionar el vínculo la víctima es dirigida a un sitio semejante a la del Banco Scotiabank donde se expone al robo de sus datos personales.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00111-01/
https://www.csirt.gob.cl/media/2020/02/8FPH20-00111-01.pdf

Vulnerabilidades

9VSA20-00133-01 CSIRT COMPARTE ACTUALIZACIÓN PARA MARIADB

Alerta de seguridad informática	9VSA20-00133-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Febrero de 2020
Última revisión	05 de Febrero de 2020

Vulnerabilidad

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida del github de MariaDB, referente a una vulnerabilidad que afecta a su motor de base de datos, la cual de ser explotada permitiría a un atacante escalar privilegios en el sistema afectado. Este informe incluye la respectiva mitigación.

Resumen

CVE-2020-7221

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00133-01/
https://www.csirt.gob.cl/media/2020/02/9VSA20-00133-01.pdf

9VSA20-00134-01 CSIRT COMPARTE INFORMACIÓN PARA TEAMVIEWER

Alerta de seguridad informática	9VSA20-00134-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de febrero de 2020
Última revisión	05 de febrero de 2020

Vulnerabilidad

CVE-2019-18988

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/9vsa20-00134-01/
https://www.csirt.gob.cl/media/2020/02/9VSA20-00134-01.pdf

9VSA20-00135-01 CSIRT COMPARTE ACTUALIZACIÓN PARA GOOGLE CHROME

Alerta de seguridad informática	9VSA20-00135-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de febrero de 2020
Última revisión	06 de febrero de 2020

Vulnerabilidad

CVE-2019-18197
CVE-2019-19880
CVE-2019-19923
CVE-2019-19925
CVE-2019-19926
CVE-2020-6381
CVE-2020-6382
CVE-2020-6385
CVE-2020-6387
CVE-2020-6388
CVE-2020-6389
CVE-2020-6390
CVE-2020-6391
CVE-2020-6392
CVE-2020-6393
CVE-2020-6394
CVE-2020-6395
CVE-2020-6396
CVE-2020-6397
CVE-2020-6398
CVE-2020-6399
CVE-2020-6400
CVE-2020-6401
CVE-2020-6402
CVE-2020-6403
CVE-2020-6404
CVE-2020-6405
CVE-2020-6406
CVE-2020-6408
CVE-2020-6409
CVE-2020-6410
CVE-2020-6411
CVE-2020-6412
CVE-2020-6413
CVE-2020-6414
CVE-2020-6415

CVE-2020-6416
CVE-2020-6417

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de Google, referente a múltiples vulnerabilidades que afectan a su explorador de internet Google Chrome, la cuales de ser explotadas, permitirían a un atacante comprometer completamente al sistema vulnerable. Este informe incluye la respectiva mitigación.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00135-01/
https://www.csirt.gob.cl/media/2020/02/9VSA20-00135-01.pdf

9VSA20-00136-01 CSIRT COMPARTE ACTUALIZACIÓN PARA NODE.JS

Alerta de seguridad informática	9VSA20-00136-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de febrero de 2020
Última revisión	07 de febrero de 2020

Vulnerabilidad

CVE-2019-15604
CVE-2019-15605
CVE-2019-15606

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de múltiples fuentes, referente a vulnerabilidades que afectan Node.js, la cuales de ser explotadas, permitirían a un atacante realizar ataques de denegación de servicios, entre otros. Este informe incluye la respectiva mitigación.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00136-01/
https://www.csirt.gob.cl/media/2020/02/9VSA20-00136-01.pdf

9VSA20-00137-01 CSIRT COMPARTE ACTUALIZACIÓN PARA PRODUCTOS DE CISCO

Alerta de seguridad informática	9VSA20-00137-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de febrero de 2020
Última revisión	07 de febrero de 2020

Vulnerabilidad

CVE-2019-15253
CVE-2019-15972
CVE-2019-15993
CVE-2020-3110
CVE-2020-3111
CVE-2020-3117
CVE-2020-3118
CVE-2020-3119
CVE-2020-3120
CVE-2020-3147
CVE-2020-3149

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de Cisco, referente a diversas vulnerabilidades que afectan a sus productos. Este informe incluye la respectiva mitigación.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00137-01/
https://www.csirt.gob.cl/media/2020/02/9VSA-00137-01.pdf

9VSA20-00138-01 CSIRT COMPARTE ACTUALIZACIÓN PARA PHP

Alerta de seguridad informática	9VSA20-00138-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de febrero de 2020
Última revisión	10 de febrero de 2020

Vulnerabilidad

CVE-2020-7059
CVE-2020-7060

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de PHP, referente a múltiples vulnerabilidades la cuales de ser explotadas, permitirían a un atacante realizar ataques de denegación de servicios y acceder a información potencialmente sensible. Este informe incluye la respectiva mitigación.

Enlace
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00138-01/
https://www.csirt.gob.cl/media/2020/02/9VSA20-00138-01.pdf

9VSA20-00139-01 CSIRT COMPARTE ACTUALIZACIONES DE MOZILLA PARA FIREFOX

Alerta de seguridad informática	9VSA20-00139-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de febrero de 2020
Última revisión	12 de febrero de 2020

Vulnerabilidad
CVE-2020-6796
CVE-2020-6797
CVE-2020-6798
CVE-2020-6799
CVE-2020-6800
CVE-2020-6801

Resumen
El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de Mozilla, referente a múltiples vulnerabilidades que afectan a sus exploradores de internet, la cuales de ser explotadas, permitirían a un atacante comprometer completamente al sistema vulnerable. Este informe incluye la respectiva mitigación.

Enlace
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00139-01/
https://www.csirt.gob.cl/media/2020/02/9VSA20-00139-01.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
190.61.219.202	Malware
190.61.250.150	Malware
190.12.72.151	Malware
190.0.230.73	Malware
185.240.248.116	Malware
185.240.248.15	Malware

184.171.253.218	Malware
67.225.129.56	Malware
66.113.181.152	Malware
66.97.34.190	Malware
66.96.189.4	Malware
66.96.185.9	Malware
66.96.185.7	Malware
66.96.185.3	Malware
66.96.184.10	Malware
66.96.184.6	Malware
66.96.184.5	Malware
66.96.184.2	Malware
66.96.184.1	Malware
66.84.15.151	Malware
162.243.130.196	Port Scan
162.243.129.144	Port Scan
64.76.144.146	DDoS
64.225.15.75	Port Scan
180.232.99.45	Port Scan
46.246.63.215	Port Scan
183.80.224.78	Port Scan
42.113.22.246	Port Scan
139.59.6.236	Phishing
162.243.128.9	Port Scan
189.80.212.51	Port Scan
192.241.224.123	Port Scan
162.243.129.151	Port Scan
139.59.17.106	Phishing
139.59.9.22	Phishing
118.189.61.117	Port Scan
142.44.142.221	Port Scan
149.56.28.100	Port Scan
162.243.128.190	Port Scan
194.180.225.44	Port Scan
162.243.128.34	Port Scan
114.199.67.235	Port Scan
121.58.216.136	Port Scan
162.243.129.199	Port Scan
192.241.235.32	Port Scan
162.243.129.53	Port Scan
162.243.129.92	Port Scan

192.241.234.159	Port Scan
65.254.253.29	Malware
64.37.52.52	Malware
192.241.239.222	Port Scan
162.243.131.43	Port Scan
61.216.99.188	Malware
61.112.24.164	Malware
59.106.27.230	Malware
54.240.2.18	Malware
50.31.12.148	Malware
164.138.210.180	Malware
49.212.207.12	Malware
161.34.9.2	Malware
45.115.115.27	Malware
161.34.2.220	Malware
45.115.115.26	Malware
157.7.104.44	Malware
148.244.114.30	Malware
162.243.130.120	Port Scan
45.115.115.22	Malware
45.115.115.15	Malware
45.115.115.10	Malware
169.1.20.138	Malware
49.145.234.220	Port Scan
162.243.130.180	Port Scan
172.105.86.120	Port Scan
172.105.93.108	Port Scan
178.128.200.207	Port Scan
223.64.80.25	DDoS
60.222.105.193	DDoS
39.170.220.121	DDoS
117.32.129.38	DDoS
113.64.13.114	DDoS
106.58.26.11	DDoS
223.96.33.210	DDoS
118.112.115.174	DDoS
223.97.8.54	DDoS
149.56.28.100	Port Scan
92.118.160.57	Port Scan
74.82.47.44	Port Scan
210.146.152.179	Port Scan

200.150.69.26	Port Scan
162.241.95.113	Malware
200.73.28.35	Malware
186.64.116.185	Malware
186.64.117.235	Malware
199.195.254.80	DDoS
198.108.67.91	DDoS
198.108.67.81	DDoS
198.108.67.38	DDoS
197.37.16.82	DDoS
196.52.84.10	Port Scan
192.241.238.106	Port Scan
192.241.234.159	Port Scan
184.105.247.251	Port Scan
172.104.113.6	Port Scan
170.130.187.38	DDoS
170.106.37.63	DDoS
162.243.131.164	DDoS
198.143.158.85	DDoS
183.81.96.65	DDoS
183.80.22.226	Port Scan
180.93.14.162	Port Scan
112.72.79.3	Port Scan
42.118.148.73	Port Scan
113.22.170.10	Port Scan
104.248.66.120	Port Scan
162.243.130.27	Port Scan
118.71.213.249	Port Scan
118.68.33.131	Port Scan
113.22.166.86	Port Scan
80.21.75.143	Port Scan
129.213.72.224	Port Scan
42.113.68.92	Port Scan
72.94.160.71	Port Scan
42.114.197.185	Port Scan
162.243.128.161	Port Scan
192.241.231.154	Port Scan
176.32.34.181	Port Scan
162.243.131.188	Port Scan
162.243.128.104	Port Scan
58.182.5.218	Port Scan

162.243.130.176	Port Scan
51.15.156.14	Port Scan
222.164.168.169	Port Scan
198.199.114.89	Port Scan
192.241.239.247	Port Scan
77.247.109.96	Port Scan
162.243.131.133	Port Scan
77.247.109.98	Port Scan
162.243.131.202	Port Scan
188.213.25.232	Port Scan
185.156.73.60	Port Scan
162.243.129.36	Port Scan
192.241.239.204	Port Scan
162.243.128.37	Port Scan
181.114.224.13	Malware
45.115.115.9	Malware
178.17.171.99	Malware
45.115.115.7	Malware
173.243.136.65	Malware
162.241.138.37	Malware
45.115.115.5	Malware
161.34.20.178	Malware
161.34.14.216	Malware
158.199.161.242	Malware
45.56.110.58	Malware
34.192.122.33	Malware
147.135.54.119	Malware
143.202.160.203	Malware
132.247.16.103	Malware
129.205.241.4	Malware
123.30.133.92	Malware
27.254.87.146	Malware
121.83.254.141	Malware
119.245.151.191	Malware
23.83.209.12	Malware
119.245.189.66	Malware
116.202.87.46	Malware
111.221.43.203	Malware
103.254.210.173	Malware
103.254.84.150	Malware
103.241.181.154	Malware

103.110.83.71	Malware
103.74.54.6	Malware
103.15.48.141	Malware
99.198.125.118	Malware
162.243.128.11	Port Scan
162.243.128.20	Port Scan
162.243.128.204	Port Scan
162.243.128.214	Port Scan
162.243.129.138	Port Scan
162.243.129.239	Port Scan
162.243.129.93	Port Scan
162.243.129.94	Port Scan
162.243.130.179	Port Scan
80.82.77.189	Port Scan
49.45.28.164	Port Scan
77.247.108.92	Port Scan
90.220.36.206	Port Scan
104.244.76.133	Port Scan
138.68.230.63	Port Scan
162.243.129.159	Port Scan
188.213.25.232	Port Scan
192.241.234.17	Port Scan
222.127.119.140	Port Scan
162.243.129.233	Port Scan
162.243.128.147	Port Scan
192.241.227.209	Port Scan
192.16.48.200	Port Scan
192.241.209.216	Port Scan
162.243.131.173	Port Scan
192.241.239.175	Port Scan
192.241.239.71	Port Scan
125.25.31.107	Port Scan
45.79.25.214	Port Scan
37.49.226.117	Port Scan
212.129.18.55	Port Scan
194.180.225.19	Port Scan
183.81.96.65	Port Scan
178.128.200.121	Port Scan
139.162.138.126	Port Scan
192.241.239.108	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.

- Cristián Ovalle Núñez

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: 2020.02.14 11:35:49 -03'00'