13BCS20-00051-01

CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Cibernética

Publicado el Viernes 23 de Abril de 2020

Resumen de noticias, reportes, alertas e indicadores de compromisos informados por CSIRT entre el jueves 16 de Abril y el miércoles 22 de Abril de 2020.

Falsificación de Registro o Identidad

8FFR20-00338-01 CSIRT ADVIERTE 582 DOMINIOS CON PROMOCIONES FALSAS

Alerta de seguridad cibernética	8FFR20-00338-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Abril de 2020
Última revisión	16 de Abril de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha detectado 582 dominios fraudulentos asociados a 10 IPs.

Los dominios potencialmente maliciosos exhiben anuncios o promociones falsas. Los atacantes, usurpando la imagen de Google, tratan de persuadir a las personas para que completen una encuesta alojada en los sitios fraudulentos. El mensaje indica que al responder la encuesta las personas podrían obtener un regalo. Terminada la encuesta, se solicitada algunos antecedentes personales, y en algunos casos, datos de las tarjetas de crédito.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr20-00338-01/

https://www.csirt.gob.cl/media/2020/04/8FFR20-00338-01.pdf

8FFR20-00339-01 CSIRT ADVIERTE DE UN PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad cibernética	8FFR20-00339-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Abril de 2020
Última revisión	16 de Abril 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 la tarjeta cencosud, 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/8ffr20-00339-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00339-01.pdf

8FFR20-00340-01 CSIRT ADVIERTE DE TRES SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad cibernética	8FFR20-00340-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Abril de 2020
Última revisión	16 de Abril 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/8ffr20-00340-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00340-01.pdf

8FFR20-00341-01 CSIRT INFORMA DE TRES PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad cibernética	8FFR20-00341-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Abril de 2020
Última revisión	16 de Abril 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 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/8ffr20-00341-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00341-01.pdf

8FFR20-00342-01 CSIRT ADVIERTE SOBRE DOS PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad cibernética	8FFR20-00342-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Abril de 2020
Última revisión	16 de Abril 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, 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/8ffr20-00342-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00342-01.pdf

8FFR20-00343-01 CSIRT ADVIERTE DE CINCO SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad cibernética	8FFR20-00343-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Abril de 2020
Última revisión	16 de Abril de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de cinco portales fraudulentos asociados a un IP que suplantan 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/8ffr20-00343-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00343-01.pdf

8FFR20-00344-01 CSIRT ADVIERTE ACTIVACIÓN DE UN SITIO BANCARIO FRAUDULENTO

Alerta de seguridad cibernética	8FFR20-00344-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Abril de 2020
Última revisión	17 de Abril 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/8ffr20-00344-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00344-01.pdf

8FFR20-00345-01 CSIRT ADVIERTE SOBRE PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad cibernética	8FFR20-00345-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Abril de 2020
Última revisión	17 de Abril 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 una web oficial para los Bancos de Chile, Edwards y CrediChile, 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/8ffr20-00345-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00345-01.pdf

8FFR20-00346-01 CSIRT ADVIERTE SITIO DE STREAMING FRAUDULENTO

Alerta de seguridad cibernética	8FFR20-00346-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Abril de 2020
Última revisión	18 de Abril 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 servicio de streaming Disney+, el que podría servir para robar credenciales de suscriptores de ese servicio.

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/8ffr20-00346-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00346-01.pdf

8FFR20-00347-01 CSIRT ADVIERTE DE UN SITIO BANCARIO FRAUDULENTO

Alerta de seguridad cibernética	8FFR20-00347-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Abril de 2020
Última revisión	18 de Abril 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/8ffr20-00347-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00347-01.pdf

8FFR20-00348-01 CSIRT ADVIERTE DE UN PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad cibernética	8FFR20-00348-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Abril de 2020
Última revisión	15 de Abril 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/8ffr20-00348-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00348-01.pdf

8FFR20-00349-01 CSIRT INFORMA DE DOS SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad cibernética	8FFR20-00349-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Abril de 2020
Última revisión	18 de Abril 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, 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/8ffr20-00349-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00349-01.pdf

8FFR20-00350-01 CSIRT ADVIERTE DE DOS PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad cibernética	8FFR20-00350-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Abril de 2020
Última revisión	18 de Abril 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 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/8ffr20-00350-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00350-01.pdf

8FFR20-00351-01 CSIRT ADVIERTE DE UN SITIO BANCARIO FRAUDULENTO

Alerta de seguridad cibernética	8FFR20-00351-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Abril de 2020
Última revisión	21 de Abril de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulentos asociados a dos IPs que suplantan 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/8ffr20-00351-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00351-01.pdf

8FFR20-00352-01 CSIRT INFORMA DE UN PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad cibernética	8FFR20-00352-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Abril de 2020
Última revisión	21 de Abril 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/8ffr20-00352-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00352-01.pdf

8FFR20-00353-01 CSIRT ADVIERTE DE UN SITIO BANCARIO FRAUDULENTO

Alerta de seguridad cibernética	8FFR20-00353-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Abril de 2020
Última revisión	21 de Abril 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/8ffr20-00353-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00353-01.pdf

8FFR20-00354-01 CSIRT ADVIERTE DE TRES SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad cibernética	8FFR20-00354-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Abril de 2020
Última revisión	22 de Abril 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, 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/8ffr20-00354-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00354-01.pdf

8FFR20-00355-01 CSIRT ADVIERTE DE DOS SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad cibernética	8FFR20-00355-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Abril de 2020
Última revisión	22 de Abril 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, 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/8ffr20-00355-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00355-01.pdf

8FFR20-00356-01 CSIRT ADVIERTE DE UN SITIO BANCARIO FRAUDULENTO

Alerta de seguridad cibernética	8FFR20-00356-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Abril de 2020
Última revisión	22 de Abril 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, 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/8ffr20-00356-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00356-01.pdf

8FPH20-00181-01 CSIRT ADVIERTE PHISHING POR MANTENIMIENTO DE SERVICIOS

Alerta de seguridad cibernética	8FPH20-00181-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Abril de 2020
Última revisión	16 de Abril de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), advierte sobre una campaña de phishing que se está difundiendo a través de un correo electrónico supuestamente proveniente del Banco Estado. El atacante intenta persuadir a quien recibe el mensaje, de utilizar un enlace ubicado en el cuerpo del correo. El mensaje informa sobre un error que perjudica al cliente. El error se descubrió al realizar un supuesto mantenimiento en los servicios del banco, como Caja Vecina y ServiEstado. Producto de esta situación, y argumentando seguir una supuesta normativa de seguridad, se indica a la persona que se procedió al bloqueo de su cuenta, la que se puede desbloquear al verificar su información bancaria a través de un enlace. Si la persona utiliza el enlace disponible, será dirigida a un sitio web semejante al del banco, donde se expondrá al robo de sus credenciales.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00181-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00181-01.pdf

8FPH20-00182-01 CSIRT ADVIERTE PHISHING POR INCONVENIENTE EN DISPOSITIVO DE SEGURIDAD

Alerta de seguridad cibernética	8FPH20-00182-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Abril de 2020
Última revisión	17 de Abril de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), advierte sobre una campaña de phishing que se está difundiendo a través de un correo electrónico, que aparenta provenir del Banco Scotiabank. El mensaje intenta persuadir a las personas para utilizar un enlace malicioso adjunto en el cuerpo del correo.

Quien recibe el correo es informado sobre la detección de un inconveniente con su dispositivo de seguridad, por lo que se requiere su sincronización de forma inmediata. El mensaje advierte de un tiempo límite para realizar la acción -48 horas desde recibido el correo- de lo contrario la cuenta podría ser bloqueada, lo que podría generar presión en la decisión de la víctima para ingresar a los enlaces disponibles en el correo para realizar la gestión de sincronizar el dispositivo.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00182-01/

https://www.csirt.gob.cl/media/2020/04/8FPH20-00182-01.pdf

8FPH20-00183-01 CSIRT ADVIERTE DE PHISHING SOBRE FALSO PREMIO DE LOTERÍA INTERNACIONAL

Alerta de seguridad cibernética	8FPH20-00183-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Abril de 2020
Última revisión	17 de Abril de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), advierte sobre una campaña de phishing que se está difundiendo a través de un correo electrónico que proviene de una organización supuestamente denominada Departamento de la Oferta Mundial de Promociones de Lotería la que actúa junto a una popular Lotería de EEUU. El mensaje busca generar una respuesta de quien lo recibe a una casilla enmascarada entregada por el remitente.

El mensaje del correo informa a la víctima que fue ganador de la lotería realizada el pasado 28 de marzo y distribuye premios para familias e individuos afectados para sobrevivir a la pandemia de Covid-19. Para cobrar el premio de 500 mil dólares americanos, el receptor debe responder el correo indicando los números ganadores. La cantidad de dinero expresada en palabras tiene un error, pues el monto escrito es “cincocientos mil”, lo que podría suponer el uso de un traductor en la elaboración del mensaje. La narrativa es a veces extraña y reiterativa, por ejemplo, al mencionar la fecha en que fue realizado el sorteo, indicada al principio y final de un breve párrafo.

El correo se recibe desde la casilla jewellann.harry[@]caricom[.]org, pero al enviar la respuesta, ésta es enviada al correo “bwann1977[@]gmail[.]com”.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00183-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00183-01.pdf

8FPH20-00184-01 CSIRT ADVIERTE PHISHING INTERNACIONAL DE 5 SUPERMERCADOS, UNO CHILENO

Alerta de seguridad cibernética	8FPH20-00184-01

Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de Abril de 2020
Última revisión	19 de Abril de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, advierte sobre una campaña de phishing que se está difundiendo en diferentes países a través de WhatsApp, el que supuestamente proveniente de cinco Supermercados, entre ellos Líder de Chile, Éxito de Ecuador, SuperSeis de Paraguay, SuperMaxi-MegaMaxi de Colombia y la cadena internacional Tesco, con base en Reino Unido.

En el caso del supermercado Líder y Líder Express de Chile, los atacantes tratan de persuadir a las personas para utilizar el enlace disponible en el cuerpo del mensaje. El mensaje informa que durante el período que dura la cuarentena, supermercados Líder y Líder Express regalarán 1.000 cupones de $100.000 pesos y disponibilizan un enlace para obtener el cupón. Si una persona utiliza el enlace es derivada a una encuesta. Una vez que responde la encuesta debe reenviar el mensaje de WhatsApp. Posteriormente se le solicitan un correo y clave y finalmente una tarjeta de crédito.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00184-01/

https://www.csirt.gob.cl/media/2020/04/8FPH20-00184-01.pdf

8FPH20-00185-01 CSIRT ADVIERTE DE PHISHING BANCARIO CON FALSO BONO FAMILIAR COVID-19

Alerta de seguridad cibernética	8FPH20-00185-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de Abril de 2020
Última revisión	20 de Abril de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), advierte sobre una campaña de phishing que se está difundiendo a través de un correo electrónico supuestamente proviene del Banco Estado. El atacante intenta persuadir a las personas de utilizar algunos de los enlaces ubicados en el cuerpo del correo. El mensaje informa sobre la existencia de un Bono de Ayuda Familia Covid-19, cuyo monto asciende a los $80.000 (ochenta mil pesos). Para consultar si las personas son beneficiarias de este falso bono, los atacantes solicitan consultar uno de los enlaces disponibles en el correo. Si la persona utiliza el enlace, será dirigida a un sitio falso del banco, donde se expone al robo de sus credenciales.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00185-01/

https://www.csirt.gob.cl/media/2020/04/8FPH20-00185-01.pdf

8FPH20-00186-01 CSIRT ADVIERTE DE PHISHING POR CUENTA CADUCADA DE SERVICIO DE CORREO

Alerta de seguridad cibernética	8FPH20-00186-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de Abril de 2020
Última revisión	20 de Abril de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, ha identificado una campaña de phishing a través de del correo electrónico supuestamente proveniente del servicio de correo electrónico Outlook. El atacante busca que las personas ingresen a un enlace fraudulento ubicado en el cuerpo del correo.

El mensaje informa a quienes los reciben que la cuenta de Outlook ha caducado, por lo que requiere el cambio de la contraseña para evitar problemas en su próximo inicio de sesión. El mensaje indica que existe un límite de 24 horas desde la recepción del aviso para realizar la acción, de lo contrario, la cuenta será inmediatamente bloqueada. Si la persona utiliza el enlace será dirigida a un sitio falso del correo corporativo donde se le solicitará su nombre de usuario y contraseña, exponiéndose así a la vulneración de sus credenciales.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00186-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00186-01.pdf

8FPH20-00187-01 CSIRT advierte de campaña de phishing de sextorsión

Alerta de seguridad cibernética	8FPH20-00187-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de Abril de 2020
Última revisión	20 de Abril de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, ha identificado una campaña de sextorsión a través de del correo electrónico. El atacante busca que la víctima deposite dinero en bitcoins a una cuenta adjunta en el cuerpo del correo.

El mensaje informa a quien lo recibe que el atacante logró obtener acceso a la pantalla y cámara web de la víctima a través de un malware que se encuentra en el equipo. El mensaje continua y señala que la víctima habría sido grabada mientras visitaba un sitio para adultos, lo cual tiene registrado en un video obtenido con su propia cámara web. El demanda un pago de 1.000 dólares en Bitcoins para no divulgar el video o de lo contrario enviara la información a los contactos de la víctima. Para dar la apariencia de que la información es real, se adjunta una contraseña que fue robada al usuario. Esa información puede ser real y correspondería a claves obtenidas producto de masivas exfiltraciones de datos de empresas ocurridos en años anteriores, como Canva, Lindkedln, PDL, entre otros. Sin embargo, es falso que el atacante tenga la información que señala.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00187-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00187-01.pdf

8FPH20-00188-01 CSIRT ADVIERTE PHISHING PARA RECLUTAR TRABAJADORES EN SUPERMERCADO

Alerta de seguridad cibernética	8FPH20-00188-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de Abril de 2020
Última revisión	20 de Abril de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, advierte sobre una campaña de phishing supuestamente proveniente de la cadena de supermercados Jumbo. Los atacantes buscan persuadir a las personas para utilizar un enlace, a través del cual solicitan información personal y comercial de sus víctimas. El mensaje informa a quienes lo reciben que la cadena de supermercados Jumbo está reclutando trabajadores para el próximo mes de mayo, explotando la incertidumbre económica y social por el aumento del desempleo producto de la crisis sanitaria. Los cibercriminales realizan una entrevista virtual que consiste en responder un formulario donde recolectan información personal y comercial de la víctima. Si una persona utiliza el enlace se expone a la pérdida de información y a posibles perjuicios económicos.

CSIRT hace un llamado al cuidado extremo de los trabajadores que estén desempleados y a las personas que sean convocadas por este phishing o similares, a denunciar y evitar caer víctima de este fraude. Así mismo, llama al comercio y a los empleadores, para que informen de la usurpación de sus marcas y el cuidado de su reputación, y actuar para la revocación de los dominios fraudulentos que no solo les perjudican a ellos, sino a la comunidad en general.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00188-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00188-01.pdf

8FPH20-00189-01 CSIRT ADVIERTE DE PHISHING BANCARIO POR BLOQUEO DE CUENTA

Alerta de seguridad cibernética	8FPH20-00189-01
Clase de alerta	Fraude

Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de Abril de 2020
Última revisión	20 de Abril de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), advierte sobre una campaña de phishing que se está difundiendo a través de un correo electrónico supuestamente proviene del Banco Scotiabank. Los atacantes buscan persuadir a sus víctimas para utilizar un enlace adjunto en el correo y entregar información personal y bancaria.

El mensaje del correo informa que se detectó un error de afiliación en la banca en línea. El texto utilizado es un tanto confuso al plantear cual sería el error. El mensaje continúa señalando que por seguridad se procedió al bloqueo de la cuenta de manera temporal hasta que no termine su registro correcto. Los motivos del bloqueo podrían ser el registro de datos personales, el acceso a su cuenta a través de diferentes lugares, o falta activar de la clave 3.0 y superclave. El atacante disponibiliza un enlace para realizar la supuesta activación. Si una persona selecciona el enlace, será dirigida a un sitio web semejante al del banco, donde se expondrá al robo de sus credenciales.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00189-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00189-01.pdf

8FPH20-00190-01 CSIRT ADVIERTE SMISHING BANCARIO POR USO DE DISPOSITIVO NO FRECUENTE

Alerta de seguridad cibernética	8FPH20-00190-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Abril de 2020
Última revisión	14 de Abril de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, ha identificado una campaña de Smishing, que se está difundiendo a través de mensaje de texto falso que aparenta provenir de Banco Estado. La campaña busca persuadir a quienes reciben el mensaje para utilizar el enlace fraudulento adjunto. El mensaje informa que se detectó un dispositivo no frecuente –se desprende que para realizar alguna operación bancaria del cliente- y para evitar que la cuenta sea suspendida, se deben verificar sus datos con el enlace adjunto. Si la persona utiliza el enlace, será dirigido a una web bancaria fraudulenta que imita a la del Banco Estado, donde se expondrá al robo de sus credenciales.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00190-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00190-01.pdf

8FPH20-0191-01 CSIRT ADVIERTE DE PHISHING BANCARIO CON OFERTA EN PAGO DE CONTRIBUCIONES

Alerta de seguridad cibernética	8FPH20-00191-01
Clase de alerta	Fraude

Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Abril de 2020
Última revisión	22 de Abril de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), advierte sobre una campaña de phishing que se está difundiendo a través de un correo electrónico supuestamente proveniente del Banco Security. El atacante trata de persuadir a quien lo recibe de utilizar un enlace adjunto en el cuerpo del correo electrónico. El correo tiene dos mensajes. El primero de ellos ofrece el pago de contribuciones en 4 o 6 cuotas utilizando la tarjeta One, con la posibilidad de participar en un sorteo de 3 premios de "devolución de pago" con un tope máximo de $500.000 (quinientos mil pesos). El segundo mensaje es una advertencia producto de la contingencia por la expansión del contagio del Covid-19 y las medidas adoptadas por la autoridad, razón por la cual los clientes podrían verse impedidos del uso de la tarjeta One porque el comercio podría encontrarse cerrado. Junto con lamentar la situación, el correo dispone de un botón de validación, se entiende, de la promoción anterior. Si una persona utiliza el botón de enlace será dirigida a un sitio falso del banco, donde se expone al robo de sus credenciales.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-0191-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00191-01.pdf

8FPH20-00192-01 CSIRT ADVIERTE DE PHISHING EN FALSA CUENTA DE CORREO

Alerta de seguridad cibernética	8FPH20-00192-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Abril de 2020
Última revisión	22 de Abril de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, ha identificado una campaña de phishing a través de del correo electrónico proveniente de una supuesta agencia de vigilancia de correo electrónico. El atacante intenta persuadir a su víctima para utilizar un enlace y acceder a la fachada de una cuenta de correo falsa. El mensaje informa que debe actualizar la cuenta de correo ya que existen 10 correos entrantes en curso. Si la persona utiliza el enlace será dirigida a un sitio falso del correo corporativo donde se le solicitará su nombre de usuario, contraseña y correo electrónico, exponiéndose así a la vulneración de sus credenciales.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00192-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00192-01.pdf

8FPH20-00193-01 CSIRT ADVIERTE SMISHING BANCARIO POR USO DE DISPOSITIVO NO FRECUENTE

Alerta de seguridad cibernética	8FPH20-00193-01
Clase de alerta	Fraude

Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Abril de 2020
Última revisión	23 de Abril de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, ha identificado una campaña de Smishing, que se está difundiendo a través de mensaje de texto falso que aparenta provenir de Banco Estado. La campaña busca persuadir a quienes reciben el mensaje para utilizar el enlace fraudulento adjunto. El mensaje informa que se detectó un dispositivo no frecuente –se desprende que para realizar alguna operación bancaria del cliente- y para evitar que la cuenta sea suspendida, se deben verificar sus datos con el enlace adjunto. Si la persona utiliza el enlace, será dirigido a una web bancaria fraudulenta que imita a la del Banco Estado, donde se expondrá al robo de sus credenciales.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00193-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00193-01.pd

Vulnerabilidades

9VSA20-00180-01 CSIRT COMPARTE ACTUALIZACIONES LIBERADAS POR GOOGLE PARA CHROME

Alerta de seguridad cibernética	9VSA20-00180-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Abril de 2020
Última revisión	16 de Abril de 2020

Vulnerabilidad

CVE-2020-6457

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Google referente a vulnerabilidad que afecta al explorador Google Chrome. El presente informe incluye la respectiva medida de mitigación.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00180-01/
https://www.csirt.gob.cl/media/2020/04/9VSA20-00180-01.pdf

9VSA20-00181-01 CSIRT COMPARTE ACTUALIZACIONES PARA PHP

Alerta de seguridad cibernética	9VSA20-00181-01
Clase de alerta	Vulnerabilidad

Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Abril de 2020
Última revisión	16 de Abril de 2020

Vulnerabilidad

CVE-2020-7067

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por PHP referente a vulnerabilidad que afecta al lenguaje de programación. El presente informe incluye la respectiva medida de mitigación.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00181-01/
https://www.csirt.gob.cl/media/2020/04/9VSA20-00181-01.pdf

9VSA20-00182-01 CSIRT COMPARTE ACTUALIZACIONES PARA SERVIDOR DE BASE DE DATOS ORACLE

Alerta de seguridad cibernética	9VSA20-00182-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Abril de 2020
Última revisión	17 de Abril de 2020

Vulnerabilidad

CVE-2020-2734
CVE-2020-2514
CVE-2016-7103
CVE-2019-2853
CVE-2020-2737
CVE-2019-17563
CVE-2016-10251
CVE-2020-2735

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Oracle referente a múltiples vulnerabilidades que afectan al servidor de base de datos Oracle. El presente informe incluye la respectiva medida de mitigación.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00182-01/
https://www.csirt.gob.cl/media/2020/04/9VSA20-00182-01.pdf

9VSA20-00183-01 CSIRT COMPARTE ACTUALIZACIÓN LIBERADAS POR CISCO PARA SUS PRODUCTOS

Alerta de seguridad cibernética	9VSA20-00183-01

Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de Abril de 2020
Última revisión	20 de Abril de 2020

Vulnerabilidad

CVE-2020-3260
CVE-2020-3177
CVE-2020-3162
CVE-2020-3261
CVE-2020-3194
CVE-2020-3262
CVE-2020-3273
CVE-2020-3161
CVE-2020-1421
CVE-2020-3239
CVE-2020-3240
CVE-2020-3243
CVE-2020-3247
CVE-2020-3248
CVE-2020-3249
CVE-2020-3250
CVE-2020-3251
CVE-2020-3252

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Cisco referente a vulnerabilidades que afectan a sus productos. El presente informe incluye las respectivas medidas de mitigación.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00183-01/
https://www.csirt.gob.cl/media/2020/04/9VSA20-00183-01.pdf

9VSA20-00184-01 CSIRT COMPARTE ACTUALIZACIONES ENTREGADAS POR OPENSSL

Alerta de seguridad cibernética	9VSA20-00184-01
Clase de alerta	Vulnerabilidad

Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Abril de 2020
Última revisión	21 de Abril de 2020

Vulnerabilidad

CVE-2020-1967

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por OpenSSL referente a vulnerabilidad que afecta a la disponibilidad de su servicio de conexión remota. El presente informe incluye la respectiva medida de mitigación.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00184-01/
https://www.csirt.gob.cl/media/2020/04/9VSA20-00184-01.pdf

9VSA20-00185-01 CSIRT COMPARTE ACTUALIZACIONES LIBERADAS POR GOOGLE PARA CHROME

Alerta de seguridad cibernética	9VSA20-00185-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Abril de 2020
Última revisión	22 de Abril de 2020

Vulnerabilidad

CVE-2020-6458

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Google referente a múltiples vulnerabilidades que afectan al explorador Google Chrome. El presente informe incluye la respectiva medida de mitigación.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00185-01/
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00185-01/

9VSA20-00186-01 CSIRT COMPARTE ACTUALIZACIONES DE JOOMLA PARA SU GESTOR DE CONTENIDOS

Alerta de seguridad cibernética	9VSA20-00186-01
Clase de alerta	Vulnerabilidad

Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Abril de 2020
Última revisión	22 de Abril de 2020

Vulnerabilidad

CVE-2020-11889

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Joomla referente a vulnerabilidades que afectan al gestor de contenidos. El presente informe incluye la respectiva medida de mitigación.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00186-01/
https://www.csirt.gob.cl/media/2020/04/9VSA20-00186-01.pdf

9VSA20-00134-02 CSIRT COMPARTE ACTUALIZACIONES PARA TEAMVIEWER

Alerta de seguridad cibernética	9VSA20-00134-02
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Abril de 2020
Última revisión	22 de Abril de 2020

Vulnerabilidad

CVE-2019-18998

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por TeamViewer referente a vulnerabilidad que afecta a su sistema de encriptación de credenciales. El presente informe incluye la respectiva medida de mitigación.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00134-02/
https://www.csirt.gob.cl/media/2020/04/9VSA20-00134-02.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
104.238.58.136	DDoS

209.131.133.206	Port Scan
209.131.133.222	Port Scan
199.7.52.211	Port Scan
199.7.52.212	Port Scan
209.131.133.208	Port Scan
209.131.133.202	Port Scan
199.7.52.223	Port Scan
141.101.101.72	Port Scan
108.179.232.162	Phishing
45.143.220.134	Port Scan
156.96.155.61	Port Scan
103.133.109.41	Port Scan
133.18.198.206	Port Scan
163.172.9.28	Port Scan
102.129.224.132	Port Scan
79.124.8.95	Port Scan
23.227.199.30	Port Scan
192.3.255.136	Hacking
104.219.248.46	Phishing
51.68.45.193	Phishing
141.98.10.33	Port Scan
77.247.109.87	Port Scan
172.93.101.247	Port Scan
140.238.249.115	Port Scan
77.247.109.72	Port Scan
45.143.220.146	Port Scan
185.53.88.103	Port Scan
51.91.48.18	Port Scan
103.145.12.75	Port Scan
15.165.76.150	Port Scan
102.129.224.180	Port Scan
185.176.27.62	Port Scan
50.7.206.2	DDoS
138.197.154.79	DDoS
173.249.45.143	Port Scan
192.34.57.157	Port Scan
167.172.132.243	DDoS
23.133.64.110	Port Scan
185.53.88.180	Port Scan
51.89.67.61	Port Scan
103.145.12.80	Port Scan

172.96.161.26	Port Scan
80.211.251.5	Port Scan
183.105.143.129	Port Scan
185.181.209.58	Port Scan
45.143.220.13	Port Scan
88.218.17.172	Port Scan
92.118.234.242	Port Scan
128.14.180.90	Port Scan
54.39.104.201	Port Scan
209.141.59.153	Port Scan
77.247.109.101	Port Scan
1.54.43.9	Port Scan
199.119.65.45	Port Scan
180.252.165.171	Port Scan
205.185.113.69	Port Scan
193.142.146.40	Port Scan
92.118.37.55	Port Scan
51.89.235.111	Port Scan
45.143.220.146	Port Scan
134.73.232.213	Port Scan
134.73.232.206	Port Scan
134.73.232.202	Port Scan
134.73.232.211	Port Scan
134.73.232.205	Port Scan
188.165.195.65	Port Scan
192.119.70.58	Phishing
205.185.216.10	Phishing
192.241.200.167	Port Scan
181.143.56.243	Port Scan
198.50.138.177	Port Scan
71.6.232.6	Port Scan
14.164.48.150	Port Scan
183.89.120.167	Port Scan
46.234.125.89	Port Scan
87.236.212.197	Port Scan
185.232.65.36	Port Scan
195.154.199.139	Port Scan
103.68.1.178	Port Scan
95.91.33.17	DDoS
136.143.190.226	DDoS
92.220.10.100	DDoS

185.227.82.50	Port Scan
157.245.168.11	Port Scan
103.238.68.3	Port Scan
51.15.85.14	Port Scan
222.252.17.159	Port Scan
192.241.235.230	Port Scan
185.200.118.75	Port Scan
198.16.74.146	Port Scan
178.32.92.81	Port Scan
197.202.13.3	Port Scan
161.35.101.82	Port Scan
103.199.68.92	Port Scan
103.199.68.188	Port Scan
185.233.149.104	Port Scan
159.89.33.57	Port Scan
198.98.60.10	Port Scan
40.112.132.56	Port Scan
122.53.122.163	Port Scan
35.228.13.240	Port Scan
45.149.206.194	Port Scan
119.160.118.150	Port Scan
171.67.71.98	Port Scan
94.102.50.136	Port Scan
80.211.131.110	Port Scan
140.238.246.171	Port Scan
139.28.235.244	Port Scan
89.248.167.191	Port Scan
216.244.66.248	Port Scan
49.51.8.188	Port Scan
71.6.147.254	Port Scan
46.229.168.154	Port Scan
134.209.106.28	Port Scan
94.102.50.137	Port Scan
62.171.186.15	Port Scan
140.238.248.52	Port Scan
5.135.47.97	DDoS
192.241.203.41	Port Scan
195.231.8.227	Port Scan
63.250.32.85	Port Scan
89.248.172.123	Port Scan
185.153.197.75	Port Scan

185.153.199.229	Port Scan
185.153.197.27	Port Scan
185.153.199.243	Port Scan
213.5.65.23	Port Scan
103.145.12.54	Port Scan
83.97.20.31	Port Scan
192.241.205.78	Port Scan
217.61.20.147	Port Scan
192.241.203.202	Port Scan
41.242.22.29	Port Scan
41.242.22.22	Port Scan
41.242.22.21	Port Scan
41.242.22.19	Port Scan
41.242.22.25	Port Scan
41.242.22.26	Port Scan
41.242.22.28	Port Scan
41.242.22.18	Port Scan
41.242.22.31	Port Scan
41.242.22.23	Port Scan
41.242.22.27	Port Scan
41.242.22.17	Port Scan
41.242.22.16	Port Scan
41.242.22.30	Port Scan
41.242.22.24	Port Scan
41.242.22.20	Port Scan
193.124.221.184	Port Scan
107.175.33.16	Malware
139.162.126.103	Port Scan
78.40.108.197	Port Scan
45.125.65.74	Port Scan
213.202.225.47	Port Scan
198.98.48.78	Port Scan
195.62.32.178	Port Scan
198.98.48.78	Port Scan
198.50.234.163	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.