13BCS-00027-001

CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Informática

Publicado el Jueves 24 de Octubre de 2019

Resumen de noticias, reportes, alertas e indicadores de compromisos informados por CSIRT entre el jueves 24 de octubre y el miércoles 06 de Noviembre.

Falsificación de Registro o Identidad

8FFR-00098-001 CSIRT ADVIERTE ACTIVACIÓN DE SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR-00098-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Octubre de 2019
Última revisión	25 de Octubre de 2019

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/8ffr-00098-001/

https://www.csirt.gob.cl/media/2019/10/8FFR-00098-001.pdf

8FFR-00099-001 CSIRT ADVIERTE DE WEB FRAUDULENTA PARA ROBO DE CREDENCIALES

Alerta de seguridad informática	8FFR-00099-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Octubre de 2019
Última revisión	24 de Octubre de 2019

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/8ffr-00099-001/
https://www.csirt.gob.cl/media/2019/10/8FFR-00099-001.pdf

8FFR-00100-001 CSIRT ADVIERTE SOBRE SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR-00100-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Octubre de 2019
Última revisión	28 de Octubre de 2019

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/8ffr-00100-001/
https://www.csirt.gob.cl/media/2019/10/8FFR-00100-001.pdf

8FFR-00101-001 CSIRT ADVIERTE DE SITIO WEB FRAUDULENTO DE INSPECCIÓN DEL TRABAJO

Alerta de seguridad informática	8FFR-00101-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Octubre de 2019
Última revisión	30 de Octubre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que se hace pasar por el sitio oficial de la Dirección del Trabajo.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios del servicio y a la entidad aludida.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00101-001/
https://www.csirt.gob.cl/media/2019/10/8FFR-00101-001.pdf

8FFR-00102-001 CSIRT ADVIERTE SOBRE SITIO BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00102-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Noviembre de 2019
Última revisión	04 de Noviembre de 2019

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/8ffr-00102-001/
https://www.csirt.gob.cl/media/2019/11/8FFR-00102-001.pdf

8FFR-00103-001 CSIRT ADVIERTE DE SITIO FRAUDULENTO PARA ROBO DE CREDENCIALES BANCARIAS

Alerta de seguridad informática	8FFR-00103-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Noviembre de 2019
Última revisión	05 de Noviembre de 2019

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/8ffr-00103-001/
https://www.csirt.gob.cl/media/2019/11/8FFR-00103-001.pdf

8FFR-00104-001 CSIRT ADVIERTE DE ACTIVACIÓN DE PORTAL BANCARIA FRAUDULENTO

Alerta de seguridad informática	8FFR-00104-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Noviembre de 2019
Última revisión	05 de Noviembre de 2019

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/8ffr-00108-001/
https://www.csirt.gob.cl/media/2019/11/8FFR-00104-001.pdf

8FPH-00069-001 CSIRT ADVIERTE DE PHISHING EN SUPUESTA CUENTA DE ZIMBRA

Alerta de seguridad informática	8FPH-00069-001
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Octubre de 2019
Última revisión	24 de Octubre de 2019

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 indicando que existe una actividad inusual en su cuenta de correo de la plataforma Zimbra. El atacante utiliza datos falsos para persuadir al usuario para que seleccione un enlace, siendo direccionado desde éste hasta un sitio que le solicitara su usuario y contraseñas de correo. De esta forma los estafadores capturan las credenciales de la persona.

Enlace

https://www.csirt.gob.cl/alertas/8fph-00069-001/
https://www.csirt.gob.cl/media/2019/10/8FPH-00069-001.pdf

8FPH-00070-001 CSIRT ADVIERTE DE PHISHING BANCARIO POR CUENTA SUSPENDIDA

Alerta de seguridad informática	8FPH-00070-001
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Noviembre de 2019
Última revisión	02 de Noviembre de 2019

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 del Banco Estado. El correo indica a la persona que lo recibe que, de acuerdo al Banco, la cuenta arroja un error, lo que el sistema entiende como “cuenta suspendida”. La razón sería un supuesto proceso de validación de identidad pendiente por parte del usuario, acción que los estafadores facilitan de realizar a través de un enlace en el correo. Cuando la víctima ingresa al vínculo, se expone al robo de sus credenciales desde un sitio semejando al del Banco.

Enlace

https://www.csirt.gob.cl/alertas/8fph-00070-001/
https://www.csirt.gob.cl/media/2019/11/8FPH-00070-001.pdf

8FPH-00071-001 CSIRT ADVIERTE DE PHISHING EN CORREOS INSTITUCIONALES

Alerta de seguridad informática	8FPH-00071-001

Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Noviembre de 2019
Última revisión	02 de Noviembre de 2019

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 usuarios de instituciones de Gobierno. El correo indica que los mensajes entrantes han sido suspendidos ya que la cuenta del usuario no ha sido verificada por Microsoft. Los estafadores disponibilizan un enlace para restablecer la cuenta. Las personas que ingresan al vínculo se exponen al robo de sus credenciales desde un sitio semejando al Outlook.

Enlace

https://www.csirt.gob.cl/alertas/8fph-00071-001/
https://www.csirt.gob.cl/media/2019/11/8FPH-00071-001.pdf

Alertas de Malware

2CMV-00035-001 CSIRT ADVIERTE DE MALWARE EN FALSO CORREO DE TESORERÍA

Alerta de seguridad informática	2CMV-00035-001
Clase de alerta	Fraude
Tipo de incidente	Phishing - Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Octubre de 2019
Última revisión	23 de Octubre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing con malware asociado, a través de un correo electrónico que supuestamente proviene de la Tesorería General de la Republica. Los criminales buscan engañar a los usuarios advirtiéndoles sobre una supuesta liquidación tributaria impaga. A la potencial víctima se le ofrece la posibilidad de descargar desde un enlace el informe generado por el Servicio de Impuesto Internos. Al seleccionar el hipervínculo se inicia el proceso para la descarga del archivo malicioso. Junto a este informe se adjuntan indicadores de compromiso.

Enlace

https://www.csirt.gob.cl/alertas/2cmv-00035-001/
https://www.csirt.gob.cl/media/2019/10/2CMV-00035-001.pdf

2CMV-00036-001 CSIRT ADVIERTE DE MALWARE EN CORREO DE EMPRESA COURIER

Alerta de seguridad informática	2CMV-00036-001

Clase de alerta	Fraude
Tipo de incidente	Phishing - Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Octubre de 2019
Última revisión	25 de Octubre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing con malware asociado, a través de un correo electrónico que supuestamente proviene de la Empresa de Courier Nacional e Internacional Chilexpress. Los cibercriminales buscan engañar a los usuarios informándoles sobre la existencia de un paquete en sus depósitos, adjuntando un código de seguimiento. Lo anterior busca incitar a las víctimas para realizar un seguimiento del supuesto pedido a través del enlace. Al seleccionar el hipervínculo, la víctima es redireccionada automáticamente hasta descargar el archivo malicioso e infectarse con un malware bancario. Se adjuntan los indicadores de compromisos.

Enlace

https://www.csirt.gob.cl/alertas/2cmv-00036-001/
https://www.csirt.gob.cl/media/2019/10/2CMV-00036-001.pdf

2CMV-00037-001 CSIRT ADVIERTE DE MALWARE ASOCIADOS A CORREOS CON INFORMACIÓN TRIBUTARIA Y FACTURAS

Alerta de seguridad informática	2CMV-00037-001
Clase de alerta	Fraude
Tipo de incidente	Phishing - Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de Octubre de 2019
Última revisión	31 de Octubre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha detectado la activación de campañas de phishing con malware asociado, a través de correos electrónicos que suplantan a la Tesorería General de la Republica y a la empresa de telecomunicaciones ENTEL.

En los dos casos el delincuente busca engañar a los usuarios para que estos seleccionen el enlace indicado para infectarse del Malware Bancario. En el caso de la Tesorería General de la Republica existen dos correos circulando. Uno ínsita al usuario para que descargue un Informe tributario que se encontraría impago. El segundo correo informa que se realizó una transferencia electrónica de Fondos (TEF) y trata de persuadir al usuario para que descargue el archivo de transferencia. En relación a la empresa ENTEL en el correo se informa al usuario que tiene una factura correspondiente al tráfico móvil del mes de Mayo, invitando al usuario para visualizar o cancelar la factura.

Enlace

https://www.csirt.gob.cl/alertas/2cmv-00037-001/
https://www.csirt.gob.cl/media/2019/10/2CMV-00037-001.pdf

2CMV-00038-001 CSIRT ADVIERTE DE MALWARE EN CORREO SOBRE SUPUESTO PROCESO JUDICIAL

Alerta de seguridad informática	2CMV-00038-001

Clase de alerta	Fraude
Tipo de incidente	Phishing - Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Noviembre de 2019
Última revisión	06 de Noviembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha detectado una campaña de phishing con malware asociado, a través de un correo electrónico suplantando al Ministerio de Justicia y Derechos Humanos. Los estafadores buscan engañar a los usuarios advirtiéndoles que existe un proceso criminal en su nombre y que tienen un plazo de 48 horas para recurrir en su defensa. A la potencial víctima se le ofrece la posibilidad de descargar desde un enlace en el correo, una copia del proceso judicial. Al seleccionar el hipervínculo, la víctima es direccionada automáticamente hasta página donde se descarga el archivo malicioso.

Enlace

https://www.csirt.gob.cl/alertas/2cmv-00038-001/
https://www.csirt.gob.cl/media/2019/11/2CMV-00038-001.pdf

Vulnerabilidades

9VSA-00074-001 CSIRT COMPARTE ACTUALIZACIONES DE MOZILLA PARA SU NAVEGADOR DE FIREFOX Y FIREFOX ESR

Alerta de seguridad informática	9VSA-00074-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	24 de octubre de 2019
Última revisión	24 de octubre de 2019

Vulnerabilidad

CVE-2019-17000	CVE-2019-11758	CVE-2019-11759
CVE-2019-11765	CVE-2019-11763	CVE-2019-11760
CVE-2018-6156	CVE-2019-11762	CVE-2019-11761
CVE-2019-17001	CVE-2019-11757	CVE-2019-11764
CVE-2019-1700	CVE-2019-15903	

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Mozilla correspondiente a diferentes vulnerabilidades que afectan a su navegador Firefox y Firefox ESR.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00074-001/
https://www.csirt.gob.cl/media/2019/10/9VSA-00074-001.pdf

9VSA-00075-001 CSIRT COMPARTE ACTUALIZACIONES PARA GOOGLE CHROME

Alerta de seguridad informática	9VSA-00075-001

Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de octubre de 2019
Última revisión	24 de octubre de 2019

Vulnerabilidad

CVE-2019-13699	CVE-2019-13706	CVE-2019-13713
CVE-2019-13700	CVE-2019-13707	CVE-2019-13714
CVE-2019-13701	CVE-2019-13708	CVE-2019-13715
CVE-2019-13702	CVE-2019-13709	CVE-2019-13716
CVE-2019-13703	CVE-2019-13710	CVE-2019-13718
CVE-2019-13704	CVE-2019-13711	
CVE-2019-13705	CVE-2019-15903	

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Google, referente a vulnerabilidades en Google Chrome, junto a sus respectivas formas de mitigarlas.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00075-001/
https://www.csirt.gob.cl/media/2019/10/9VSA-00075-001.pdf

9VSA-00076-001 CSIRT COMPARTE ACTUALIZACIONES PARA VMWARE

Alerta de seguridad informática	9VSA-00076-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de octubre de 2019
Última revisión	27 de octubre de 2019

Vulnerabilidad

CVE-2019-5537
CVE-2019-5538

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por VMware, referente a vulnerabilidades en VMware vCenter Server Appliance, junto a sus respectivas formas de mitigarlas.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00076-001/
https://www.csirt.gob.cl/media/2019/10/9VSA-00076-001.pdf

9VSA-00077-001 CSIRT COMPARTE ACTUALIZACIONES PARA PHP7

Alerta de seguridad informática	9VSA-00077-001

Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de octubre de 2019
Última revisión	28 de octubre de 2019

Vulnerabilidad
CVE-2019-11043

Resumen
El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información obtenida de diferentes fuentes, referente a una vulnerabilidad en PHP7 al ser utilizado en NGINX o PHP-FPM, junto a su respectiva forma de mitigarla.

Enlace
https://www.csirt.gob.cl/vulnerabilidades/9vsa-00077-001/
https://www.csirt.gob.cl/media/2019/10/9VSA-00077-001.pdf

9VSA-00078-001 CSIRT COMPARTE ACTUALIZACIONES PARA PRODUCTOS IBM

Alerta de seguridad informática	9VSA-00078-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de octubre de 2019
Última revisión	29 de octubre de 2019

Vulnerabilidad
CVE-2019-4394

Resumen
El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por IBM, referente a una vulnerabilidad en sus productos, junto a su respectiva forma de mitigarla.

Enlace
https://www.csirt.gob.cl/vulnerabilidades/9vsa-00078-001/
https://www.csirt.gob.cl/media/2019/10/9VSA-00078-001.docx.pdf

9VSA-00079-001 CSIRT COMPARTE ACTUALIZACIONES DE APPLE PARA WATCHOS, SAFARI, IOS, IPADOS, MACOS CATALINA Y TVOS.

Alerta de seguridad informática	9VSA-00074-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de octubre de 2019
Última revisión	30 de octubre de 2019

Vulnerabilidad

CVE-2017-7152	CVE-2019-8764	CVE-2019-8802
CVE-2018-12152	CVE-2019-8765	CVE-2019-8803
CVE-2018-12153	CVE-2019-8766	CVE-2019-8804
CVE-2018-12154	CVE-2019-8767	CVE-2019-8805
CVE-2019-8509	CVE-2019-8775	CVE-2019-8807
CVE-2019-8706	CVE-2019-8782	CVE-2019-8808
CVE-2019-8708	CVE-2019-8783	CVE-2019-8811
CVE-2019-8715	CVE-2019-8784	CVE-2019-8812
CVE-2019-8716	CVE-2019-8785	CVE-2019-8813
CVE-2019-8736	CVE-2019-8786	CVE-2019-8814
CVE-2019-8737	CVE-2019-8787	CVE-2019-8815
CVE-2019-8743	CVE-2019-8788	CVE-2019-8816
CVE-2019-8744	CVE-2019-8789	CVE-2019-8817
CVE-2019-8747	CVE-2019-8793	CVE-2019-8819
CVE-2019-8749	CVE-2019-8794	CVE-2019-8820
CVE-2019-8750	CVE-2019-8795	CVE-2019-8821
CVE-2019-8756	CVE-2019-8797	CVE-2019-8822
CVE-2019-8759	CVE-2019-8798	CVE-2019-8823
CVE-2019-8761	CVE-2019-8801	

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Apple correspondiente a múltiples vulnerabilidades en watchOS, Safari, iOS, iPadOS, macOS Catalina y tvOS.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00078-001-2/
https://www.csirt.gob.cl/media/2019/10/9VSA-00079-001.pdf

9VSA-00080-001 CSIRT COMPARTE ACTUALIZACIONES PARA GOOGLE CHROME

Alerta de seguridad informática	9VSA-00080-001

Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de noviembre de 2019
Última revisión	01 de noviembre de 2019

Vulnerabilidad

CVE-2019-13720
CVE-2019-13721

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Google, referente a vulnerabilidades en su explorador Google Chrome, junto a su respectiva forma de mitigarlas.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00080-001/
https://www.csirt.gob.cl/media/2019/11/9VSA-00080-001-1.pdf

9VSA-00081-001 CSIRT COMPARTE ACTUALIZACIONES PARA JETBRAINS TOOLBOX

Alerta de seguridad informática	9VSA-00081-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de noviembre de 2019
Última revisión	04 de noviembre de 2019

Vulnerabilidad

CVE-2019-18368

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida del sitio oficial de JetBrains, referente a una vulnerabilidad que afecta a su herramienta de trabajo JetBrains ToolBox, la cual, si es explotada, puede resultar en elevación de privilegios sin autorización. Esto junto a su respectiva actualización para mitigar el riesgo.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00081-001/
https://www.csirt.gob.cl/media/2019/11/9VSA-00081-001.pdf

REPORTE SOBRE ATAQUES CIBERNÉTICOS DURANTE EL FIN DE SEMANA ENTRE EL 19 Y 20 DE OCTUBRE DE 2019

Resumen Ejecutivo

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, detectó tráfico anómalo en la red de conectividad del Estado y en los sitios web de gobierno que visualiza a través de sus plataformas. Esta anomalía fue detectada entre los días sábado 19, domingo 20 y lunes 21 de octubre de 2019.

El siguiente documento resume los eventos y ataques ocurridos durante esos días. CSIRT pudo identificar diferentes fuentes de ataques, siendo la gran mayoría internacionales, y otros nacionales. En este último caso, CSIRT pudo confirmar que existió concertación por parte de grupos nacionales para la perpetración de actividad maliciosa.

Enlace

https://www.csirt.gob.cl/reportes/10cnd-00024-001/
https://www.csirt.gob.cl/media/2019/10/10CND-00024-001.pdf

REPORTE SOBRE ATAQUES CIBERNÉTICOS ENTRE LOS DÍAS 21 Y 25 DE OCTUBRE DE 2019

Resumen Ejecutivo

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, detectó tráfico anómalo en la red de conectividad del Estado y en los sitios web de gobierno y otros sitios públicos que visualiza a través de sus plataformas. Esta anomalía fue detectada entre los días lunes 21 y viernes 25 de octubre de 2019. El siguiente documento resume los eventos y ataques ocurridos durante esos días.

Enlace

https://www.csirt.gob.cl/reportes/10cnd-00026-002/
https://www.csirt.gob.cl/media/2019/10/10CND-00026-002-1.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
51.89.251.196	Port Scan
77.247.108.125	Port Scan
112.175.126.18	Port Scan
188.165.219.27	Port Scan
198.50.183.35	Port Scan
162.244.80.38	Port Scan
37.49.227.109	Port Scan
159.203.201.239	Port Scan

31.13.114.124	Port Scan
185.172.110.222	Port Scan
37.49.227.109	Port Scan
190.47.113.147	Port Scan
138.99.224.159	DdoS
167.86.71.238	Port Scan
144.91.76.115	Port Scan
176.107.133.164	Port Scan
144.91.76.115	Port Scan
45.143.220.21	Port Scan
138.201.232.60	Port Scan
172.105.25.41	Hacking
211.44.226.158	Port Scan
112.175.127.179	Port Scan
112.175.124.2	Port Scan
217.182.196.164	Port Scan
62.210.177.9	Port Scan
51.15.27.103	Port Scan
177.67.82.218	DdoS
177.67.82.210	DdoS
194.99.104.35	Port Scan
89.248-.169.17	Port Scan
194.99.104.35	Port Scan
162.244.80.228	Port Scan
37.49.231.123	Port Scan
185.53.88.72	Port Scan
198.74.53.233	Port Scan
159.203.193.41	Port Scan
49.45.28.6	Port Scan
193.201.224.199	Port Scan
172.105.151.161	Port Scan
89.248.174.206	Port Scan
92.118.37.95	Port Scan
188.240.220.58	Port Scan
173.44.55.155	DdoS
5.254.74.2	Port Scan
159.203.201.236	Port Scan
95.213.242.138	Port Scan
31.184.218.239	Port Scan
83.97.20.47	Port Scan
77.247.108.119	Port Scan
185.209.0.83	Port Scan
88.208.3.143	Port Scan
185.209.0.58	Port Scan

185.209.0.31	Port Scan
45.14.15.139	Malware
45.147.196.226	Malware
185.219.81.207	Malware
185.224.134.37	Malware
185.224.134.46	Malware
185.231.68.218	Malware
185.231.69.131	Malware
185.231.69.96	Malware
185.235.131.48	Malware
185.92.148.117	Malware
134.175.45.187	Hacking
112.29.140.222	Hacking
45.14.12.155	Malware
45.14.12.156	Malware
45.14.12.157	Malware
45.14.12.158	Malware
45.147.196.227	Malware
45.132.104.237	Malware
45.132.104.238	Malware
45.132.104.239	Malware
185.92.148.118	Malware
185.92.148.119	Malware
185.92.148.120	Malware
185.92.148.125	Malware
185.92.148.128	Malware
45.132.104.240	Malware
45.132.104.241	Malware
45.132.104.242	Malware
45.132.104.243	Malware
45.14.15.134	Malware
45.14.15.136	Malware
45.14.15.137	Malware
183.110.242.142	Port Scan
112.175.124.8	Port Scan
156.96.113.149	Port Scan
14.160.93.230	Malware
35.239.45.46	DdoS
37.49.231.154	Port Scan
170.254.228.100	Port Scan
212.89.132.246	Port Scan
107.189.11.50	Port Scan
193.124.187.24	Port Scan
81.22.45.20	Port Scan

185.153.198.150	Port Scan
77.247.108.119	Port Scan
185.209.0.58	Port Scan
185.209.0.84	Port Scan
51.91.212.79	Port Scan
201.218.136.177	DdoS
107.167.244.67	DdoS
198.203.28.43	DdoS
92.118.160.45	Port Scan
188.208.143.118	Port Scan
193.56.28.78	Port Scan
172.105.226.84	Port Scan
80.66.85.2	Port Scan
62.210.188.203	Port Scan
46.182.6.38	Port Scan
90.118.161.49	Port Scan
62.210.188.230	Port Scan
45.143.220.14	Port Scan
137.74.157.89	Port Scan
158.69.58.42	Port Scan
62.210.162.128	Port Scan
80.66.85.2	Port Scan
138.246.253.248	Port Scan
149.28.69.84	Port Scan
159.203.201.222	Port Scan
37.49.231.143	Port Scan
37.49.231.158	Port Scan
66.115.173.74	Port Scan
51.91.212.81	Port Scan
159.203.197.5	Port Scan
81.176.228.2	Port Scan
152.78.189.211	Port Scan
62.210.90.221	Port Scan
159.203.201.9	Port Scan
159.203.193.253	Port Scan
159.203.201.185	Port Scan
201.219.234.227	DdoS
141.125.82.105	DdoS
209.90.63.86	DdoS
203.199.89.124	DdoS
173.249.35.163	DdoS
58.82.214.233	DdoS
159.138.3.119	DdoS
37.229.122.18	DdoS

159.138.21.170	DdoS
119.192.195.83	DdoS
159.138.5.222	DdoS
103.77.11.98	Port Scan
159.203.193.36	Port Scan
185.176.27.34	Port Scan
185.176.27.86	Port Scan
45.136.110.16	Port Scan
72.52.104.74	Port Scan
159.203.201.55	Port Scan
107.6.151.194	Port Scan
45.143.220.17	Port Scan
107.189.10.171	Port Scan
45.143.221.6	Port Scan
82.76.44.175	Hacking
94.177.183.28	Malware
69.163.33.84	Malware
159.203.201.242	Port Scan
185.153.198.230	Port Scan
159.203.201.39	Port Scan
107.189.10.171	Port Scan
142.11.195.229	Port Scan
164.68.104.74	Port Scan
160.153.129.229	Phishing
159.203.201.125	Port Scan
181.75.77.180	DdoS
186.156.191.119	DdoS
190.160.9.168	DdoS
201.239.191.55	DdoS
200.112.253.148	DdoS
190.162.243.14	DdoS
200.74.101.83	DdoS
190.161.219.237	DdoS
190.101.205.217	DdoS
190.46.59.103	DdoS
185.53.91.150	Port Scan
159.203.201.172	Port Scan
185.216.32.170	Port Scan
37.200.64.50	Port Scan
37.200.64.51	Port Scan
185.176.27.102	Port Scan
185.176.27.38	Port Scan
192.99.10.122	Port Scan
185.176.27.30	Port Scan

193.32.163.72	Port Scan
185.176.27.46	Port Scan
77.247.110.161	Port Scan
124.6.158.62	Port Scan
141.98.80.204	Port Scan
185.176.27.26	Port Scan
185.175.93.3	Port Scan
151.80.36.188	Port Scan
159.203.201.165	Port Scan
178.218.24.178	Port Scan
185.176.27.14	Port Scan
103.141.138.133	Port Scan
185.246.128.135	Port Scan
159.203.201.183	Port Scan
107.189.10.180	Port Scan
210.245.83.158	Port Scan
185.112.248.29	Port Scan
158.69.58.46	Port Scan
158.69.58.35	Port Scan
159.203.197.18	Port Scan
131.108.136.130	Port Scan
62.173.149.65	Port Scan
45.82.153.34	Port Scan
45.82.153.42	Port Scan
45.82.153.35	Port Scan
45.136.109.252	Port Scan
159.203.197.25	Port Scan
200.9.99.55	Port Scan
159.203.201.249	Port Scan
103.133.104.167	Port Scan
43.245.241.245	Port Scan
185.153.199.102	Port Scan
89.249.73.130	Port Scan
185.153.199.106	Port Scan
93.174.93.218	Port Scan
77.247.110.144	Port Scan
185.176.27.190	Port Scan
103.89.90.230	Port Scan
185.176.27.194	Port Scan
190.8.119.66	Port Scan
92.53.65.136	Port Scan
209.95.50.119	DdoS
194.28.172.81	DdoS
99.248.27.81	Hacking

176.58.73.105	Port Scan
77.247.108.236	Port Scan
81.22.45.133	Port Scan
211.150.70.18	Port Scan
193.29.15.60	Port Scan
92.119.160.247	Port Scan
88.214.26.74	Port Scan
80.82.77.139	Port Scan
92.53.65.123	Port Scan
92.53.65.201	Port Scan
193.32.163.71	Port Scan
172.105.89.161	Port Scan
92.53.65.196	Port Scan
49.146.5.130	Port Scan
43.254.52.188	Port Scan
92.53.65.184	Port Scan
92.53.65.131	Port Scan
178.128.114.248	Port Scan
80.82.77.33	Port Scan
91.206.15.161	Port Scan
172.104.242.173	Port Scan
205.185.115.72	Port Scan
92.53.65.82	Port Scan
188.246.226.71	Port Scan
92.53.65.129	Port Scan
92.53.65.200	Port Scan
71.6.232.5	Port Scan
192.115.165.2	Port Scan
92.53.65.128	Port Scan
192.115.165.3	Port Scan
45.82.153.132	Port Scan
82.102.173.67	Port Scan
45.33.5.240	Port Scan
192.115.165.5	Port Scan
192.115.165.4	Port Scan
185.175.93.22	Port Scan
88.214.26.53	Port Scan
157.245.81.162	Port Scan
74.82.47.55	Port Scan
134.209.224.40	Port Scan
162.241.129.247	Port Scan
212.129.24.77	Port Scan
184.105.247.238	Port Scan
69.61.38.136	Port Scan

61.51.116.74	Port Scan
193.188.22.193	Port Scan
117.160.138.79	Port Scan
139.59.123.163	Port Scan
92.119.160.60	Port Scan
206.189.177.133	Port Scan
74.82.47.10	Port Scan
159.203.201.86	Port Scan
107.189.11.150	Port Scan
5.188.86.22	Port Scan
159.203.201.226	Port Scan
190.22.182.175	DdoS
159.203.201.128	Port Scan
61.177.172.128	Port Scan
185.16.37.186	Hacking
159.203.201.46	Port Scan
91.126.88.98	Port Scan
5.189.142.120	Port Scan
5.9.29.43	Port Scan
89.248.169.95	Port Scan
185.53.91.35	Port Scan
99.248.27.81	Port Scan
176.58.73.105	Port Scan
77.247.108.236	Port Scan
81.22.45.133	Port Scan
211.150.70.18	Port Scan
193.29.15.60	Port Scan
92.119.160.247	Port Scan
88.214.26.74	Port Scan
80.82.77.139	Port Scan
92.53.65.123	Port Scan
92.53.65.201	Port Scan
193.32.163.71	Port Scan
172.105.89.161	Port Scan
92.53.65.196	Port Scan
49.146.5.130	Port Scan
43.254.52.188	Port Scan
92.53.65.184	Port Scan
92.53.65.131	Port Scan
178.128.114.248	Port Scan
80.82.77.33	Port Scan
91.206.15.161	Port Scan
172.104.242.173	Port Scan
205.185.115.72	Port Scan

92.53.65.82	Port Scan
188.246.226.71	Port Scan
92.53.65.129	Port Scan
92.53.65.200	Port Scan
71.6.232.5	Port Scan
192.115.165.2	Port Scan
92.53.65.128	Port Scan
192.115.165.3	Port Scan
45.82.153.132	Port Scan
82.102.173.67	Port Scan
45.33.5.240	Port Scan
192.115.165.5	Port Scan
192.115.165.4	Port Scan
185.175.93.22	Port Scan
88.214.26.53	Port Scan
157.245.81.162	Port Scan
74.82.47.55	Port Scan
134.209.224.40	Port Scan
162.241.129.247	Port Scan
212.129.24.77	Port Scan
184.105.247.238	Port Scan
69.61.38.136	Port Scan
61.51.116.74	Port Scan
193.188.22.193	Port Scan
117.160.138.79	Port Scan
139.59.123.163	Port Scan
92.119.160.60	Port Scan
206.189.177.133	Port Scan
74.82.47.10	Port Scan
159.203.201.86	Port Scan
107.189.11.150	Malware
5.188.86.22	Port Scan
159.203.201.226	Port Scan
159.203.201.128	Port Scan
61.177.172.128	Port Scan
185.16.37.186	Hacking
159.203.201.46	Port Scan
91.126.88.98	Port Scan
5.189.142.120	Port Scan
5.9.29.43	Port Scan
185.53.91.35	Port Scan
89.248.169.95	Port Scan
176.113.74.30	Port Scan
103.125.116.20	Port Scan

77.247.110.36	Port Scan
128.14.181.98	Port Scan
193.32.163.44	Port Scan
149.56.179.249	Port Scan
193.32.163.106	Port Scan
185.176.27.118	Port Scan
185.200.118.68	Port Scan
157.245.83.211	Port Scan
159.203.193.42	Port Scan
46.105.132.32	Port Scan
81.22.45.17	Port Scan
51.255.74.98	Port Scan
104.234.247.64	Port Scan
167.99.38.73	Port Scan
185.95.14.230	Port Scan
89.248.174.193	Port Scan
51.77.192.7	Port Scan
101.227.169.106	Port Scan
157.230.57.112	Port Scan
180.163.8.123	Port Scan
139.162.215.46	Port Scan
172.105.17.166	Port Scan
118.70.113.1	Port Scan
213.166.71.228	Port Scan
103.206.219.66	Port Scan
159.203.197.148	Port Scan
159.203.201.25	Port Scan
36.27.209.179	Port Scan
111.53.76.186	Port Scan
139.99.179.179	Port Scan
51.83.138.91	Port Scan
139.59.170.231	Port Scan
31.132.225.136	Port Scan
159.203.197.175	Port Scan
98.153.101.132	Port Scan
185.93.180.130	Port Scan
195.37.190.84	Port Scan
62.210.17.74	Port Scan
62.210.18.16	Port Scan
178.79.147.205	Port Scan
159.203.201.60	Port Scan
193.32.163.112	Port Scan
159.203.201.79	Port Scan
185.175.93.78	Port Scan

80.82.78.33	Port Scan
51.89.185.101	Port Scan
51.83.138.91	Port Scan
45.136.109.228	Port Scan
77.247.110.54	Port Scan
112.121.163.11	Port Scan
77.247.110.81	Port Scan
88.214.26.102	Port Scan
219.235.84.15	Port Scan
185.200.118.88	Port Scan
45.79.152.7	Port Scan
81.22.45.100	Port Scan
45.79.195.211	Port Scan
157.245.49.227	Port Scan
185.164.136.243	Port Scan
163.172.6.239	Port Scan
45.143.220.18	Port Scan
159.203.193.250	Port Scan
45.119.240.68	Port Scan
45.143.220.52	Port Scan
158.69.58.34	Port Scan
190.210.45.137	Port Scan
66.220.151.253	Port Scan
185.39.146.215	Port Scan
207.150.245.254	Port Scan
203.158.221.169	Hacking
118.25.42.134	Hacking
5.135.67.229	Port Scan
77.247.108.56	Port Scan
77.247.110.25	Port Scan
159.203.201.221	Port Scan
45.136.109.174	Port Scan
45.136.109.87	Port Scan
159.203.201.122	Port Scan
185.200.118.44	Port Scan
125.62.85.63	Port Scan
185.176.27.162	Port Scan
159.203.201.139	Port Scan
62.173.154.12	Port Scan
176.32.34.86	Port Scan
185.219.133.125	Port Scan
142.44.236.5	Port Scan
185.176.221.238	Port Scan
216.243.31.2	Port Scan

51.15.6.193	Port Scan
119.147.213.103	Port Scan
123.135.127.85	Port Scan
78.47.53.190	Port Scan
175.193.68.12	Hacking
128.14.133.58	Hacking
5.181.233.166	Port Scan
172.104.65.140	Port Scan
62.210.89.152	Port Scan
159.203.197.28	Port Scan
106.52.246.97	Hacking
159.203.197.28	Port Scan
98.153.101.132	Port Scan
159.203.197.30	Port Scan
185.132.249.244	Port Scan
159.203.201.140	Port Scan
88.9.177.147	Port Scan
221.1.223.150	Port Scan
37.120.152.214	Port Scan
45.143.221.11	Hacking
45.143.220.16	Hacking
37.43.230.8	Port Scan
42.143.220.55	Port Scan
45.143.221.11	Port Scan
158.69.58.46	Port Scan
23.83.129.219	Port Scan
46.246.122.10	Port Scan
137.74.213.137	Port Scan
159.203.201.119	Port Scan
54.38.67.145	Port Scan
60.191.82.92	Port Scan
195.231.9.176	Port Scan
195.231.0.186	Port Scan
195.231.1.162	Port Scan
92.119.160.67	Port Scan
195.231.1.123	Port Scan
62.138.6.39	Port Scan
195.3.146.88	Port Scan
105.27.197.94	DDoS
191.241.235.24	DDoS
129.146.181.251	DDoS
51.158.123.35	DDoS
51.158.98.121	DDoS
124.172.232.57	DDoS

200.31.16.202	DDoS
183.111.26.15	DDoS
177.6.234.194	DDoS
183.111.25.67	DDoS
159.203.201.0/24	Port Scan
45.133.180.162	DDoS
35.247.253.206	Malware
193.124.94.218	Malware
178.211.56.22	Malware
185.182.57.52	Malware
24.206.17.102	Malware
173.34.90.245	Malware
5.100.251.106	Malware
109.176.117.11	Malware
159.203.193.240	Port Scan
112.175.92.57	Malware
113.114.117.122	Malware
117.239.241.2	Malware
119.18.230.253	Malware
128.200.115.228	Malware
137.139.135.151	Malware
14.140.116.172	Malware
181.39.135.126	Malware
186.169.2.237	Malware
195.158.234.60	Malware
197.211.212.59	Malware
21.252.107.198	Malware
210.137.6.37	Malware
218.255.24.226	Malware
221.138.17.152	Malware
26.165.218.44	Malware
47.206.4.145	Malware
70.224.36.194	Malware
81.94.192.10	Malware
81.94.192.147	Malware
84.49.242.125	Malware
97.90.44.200	Malware
45.129.96.9	Malware
195.123.238.51	Malware
195.123.213.19	Malware
185.92.74.215	Malware
95.174.67.250	Hacking
185.209.0.90	Hacking
92.63.194.56	Port Scan

142.44.243.161	Port Scan
82.119.102.242	Port Scan
185.175.93.104	Port Scan
159.203.197.170	Port Scan
194.28.112.49	Port Scan
192.229.179.46	Port Scan
192.229.133.139	Port Scan
139.162.221.245	Port Scan
37.49.231.104	Port Scan

URL	Motivo
https[://]www.bancoestadoocl.xyz/imagenes/comun2009/en-linea-personas.php	Phishing
https[://]www[.]baancoestado[.]xyz/	Phishing
https[://]www.bancoeestadocl[.]xyz	Phishing
http://109.176.117.11/362611986ed4/page	Malware
http://109.176.117.11:8000/	Malware
http://109.176.117.11:8080/362611986ed4/page	Malware
http://5.100.251.106:52057	Malware
http://5.100.251.106:443/64.exe	Malware
https://esancendoc.esan.edu.pe/	Malware

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

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.

- Hugo Miranda Vera - https://www.linkedin.com/in/hugo-miranda-vera-1a972149/
- Camilo Mix Vásquez - https://www.linkedin.com/in/lixah/

Campaña

El CSIRT quiere promover una campaña para no confundirse con el bombardeo de información falsa que circula en redes sociales. El llamado es, ANTES DE VIRALIZAR, VERIFICAR. La información falsa puede generar confusión, llevarnos a tomar decisiones erradas o generar conflictos.

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.11.08 12:26:16 -03'00'