13BCS-00020-001

CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Informática

Publicado el Jueves 29 de Agosto de 2019

Resumen de noticias, reportes, alertas e indicadores de compromisos informados por CSIRT entre el jueves 22 y el miércoles 28 de Agosto.

Noticias

Publicado 26 agosto, 2019

Hackers atacaron sitio web de salud en India: robaron más de 6,8 millones de registros de pacientes y médicos

El atacante, que fue identificado por la firma americana FireEye como “fallensky519”, robó cerca de 6,8 millones de datos de pacientes y datos personales de médicos y sus credenciales de ese país desde un sitio web de atención de salud.

Enlace:

https://www.csirt.gob.cl/noticias/hackers-atacaron-sitio-web-de-salud-en-india-robaron-mas-de-68-millones-de-registros-de-pacientes-y-medicos/

Publicado 27 agosto, 2019

Agencia de ciberseguridad del Reino Unido urge a migrar antes de fin de año a la nueva versión de Python

El NCSC está promoviendo el cambio a la versión 3 de Python, reafirmando que “de continuar utilizando módulos no compatibles, están arriesgando la seguridad de su organización así como sus datos, ya que tarde o temprano aparecerán vulnerabilidades que nadie podrá reparar”

Enlace:

https://www.csirt.gob.cl/noticias/841/

8FFR-00024-001 CSIRT ADVIERTE DE SITIO BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00024-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Agosto de 2019
Última revisión	22 de Agosto 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 del **bancochile.cl,** 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/media/2019/08/8FFR-00024-001.pdf

https://www.csirt.gob.cl/alertas/8ffr-00024-001-csirt-advierte-de-sitio-bancario-fraudulento/

8FFR-00025-001 CSIRT ADVIERTE DE ACTIVACIÓN DE UN PORTAL DE FRAUDE BANCARIO

Alerta de seguridad informática	8FFR-00025-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Agosto de 2019
Última revisión	23 de Agosto 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 del **bancofalabella.cl,** 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/media/2019/08/8FFR-00025-001.pdf

https://www.csirt.gob.cl/alertas/8ffr-00025-001-csirt-advierte-de-activacion-de-un-portal-de-fraude-bancario/

8FFR-00026-001 CSIRT ADVIERTE DE 134 PORTALES QUE SUPLANTAN A SITIO BANCARIO

Alerta de seguridad informática	8FFR-00026-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Agosto de 2019
Última revisión	23 de Agosto de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de 134 portales fraudulentos asociados a una IP que suplantan el sitio web oficial del bancochile.cl los que podrían servir para robar credenciales de usuarios de esa entidad.

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

Enlace:

https://www.csirt.gob.cl/media/2019/08/8FFR-00026-001.pdf

https://www.csirt.gob.cl/alertas/8ffr-00026-001-csirt-advierte-de-134-portales-fraudulentos-que-suplantan-a-un-sitio-bancario/

8FFR-00027-001 CSIRT ADVIERTE DE PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00027-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Agosto de 2019
Última revisión	23 de Agosto 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 del bancoestado.cl 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/media/2019/08/8FFR-00027-001.pdf

https://www.csirt.gob.cl/alertas/8ffr-00027-001-csirt-advierte-de-sitio-bancario-fraudulento-utilizado-para-el-robo-de-credenciales/

8FFR-00028-001 CSIRT ADVIERTE DE 46 SITIOS FALSOS BANCARIOS ASOCIADOS A 3 IP'S

Alerta de seguridad informática	8FFR-00028-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Agosto de 2019
Última revisión	26 de Agosto de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de 46 portales fraudulentos asociados a 3 IP's que suplantan el sitio web oficial del bancochile.cl 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/media/2019/08/8FFR-00028-001.pdf

https://www.csirt.gob.cl/alertas/8ffr-00028-001-csirt-advierte-de-46-sitios-falsos-bancarios-asociados-a-3-ips/

8FFR-00029-001 CSIRT ADVIERTE DE PORTAL FRAUDULENTO QUE PODRÍA SERVIR PARA EL ROBO DE CREDENCIALES BANCARIAS

Alerta de seguridad informática	8FFR-00029-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Agosto de 2019
Última revisión	27 de Agosto de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento que suplanta el sitio web oficial del bancoestado.cl 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/media/2019/08/8FFR-00029-001.pdf

https://www.csirt.gob.cl/alertas/8ffr-00029-001/

8FFR-00030-001 CSIRT ADVIERTE DE LA ACTIVACIÓN DE SITIO BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00030-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Agosto de 2019
Última revisión	27 de Agosto 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 del bancochile.cl, 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/media/2019/08/8FFR-00030-001.pdf
https://www.csirt.gob.cl/alertas/8ffr-00030-001/

8FFR-00031-001 CSIRT ADVIERTE DE SITIO BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00031-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Agosto de 2019
Última revisión	29 de Agosto 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 del bancoestado.cl, 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/media/2019/08/8FFR-00031-001.pdf
https://www.csirt.gob.cl/alertas/8ffr-00031-001/

8FFR-00032-001 CSIRT ADVIERTE SITIO FRAUDULENTO QUE SUPLANTA AL SII

Alerta de seguridad informática	8FFR-00032-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Agosto de 2019
Última revisión	29 de Agosto de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de portal fraudulentos asociados a una IP que suplantan el sitio web oficial del Servicio de impuestos Internos los que podrían servir para robar credenciales de usuarios de esa entidad.

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

Enlace:

https://www.csirt.gob.cl/media/2019/08/8FFR-00032-001.pdf
https://www.csirt.gob.cl/alertas/8ffr-00032-001/

8FFR-00033-001 CSIRT ADVIERTE ACTIVACIÓN DE PORTAL FRAUDULENTO ASOCIADO A SITIO BANCARIO

Alerta de seguridad informática	8FFR-00033-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Agosto de 2019
Última revisión	29 de Agosto de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de portal fraudulentos asociados a una IP que suplantan el sitio web oficial del bancoestado.cl, los que podrían servir para robar credenciales de usuarios de esa entidad.

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

Enlace:

https://www.csirt.gob.cl/media/2019/08/8FFR-00033-001.pdf
https://www.csirt.gob.cl/alertas/8ffr-00033-001/

Alertas de Spam

1ASP-00010-001 CSIRT ADVIERTE DE CAMPAÑAS DE SPAM

Alerta de seguridad informática	1ASP-00010-001
Clase de alerta	Contenido Abusivo
Tipo de incidente	Spam
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Agosto de 2019
Última revisión	29 de Agosto de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado dos campañas de Spam que aprovecha la configuración automática del calendario de Google, que en realidad intentan engañar a los usuarios para seleccionar un hipervínculo adjunto que, al ser seleccionado redirecciona a sitios no confiables. Si el usuario ingresa al enlace, este se expone a ser víctima de un fraude, robo de información personal o posible malware.

La primera de las campañas comunica que sortea gratuitamente un iPhone Xs. La segunda, menciona que existe una oferta del día que tiene como regalo una tarjera de Amazon con US $700 (Dólares) para clientes leales. El regalo tiene un tiempo limitado de 12 horas para reclamado.

De la primera campaña no se pudieron obtener los índices de compromisos pues se encontraban desactivados los enlaces que direccionaban a los sitios supuestamente maliciosos. CSIRT presume que podrían volver a activarse. La segunda campaña está activa. De esta se pudieron identificar 4 dominios con 375 subdominios que tienen relación a la campaña de spam. Este ataque aprovecha la configuración automática del calendario de Google.

Enlace

https://www.csirt.gob.cl/media/2019/08/1ASP-00010-001.pdf
https://www.csirt.gob.cl/alertas/1asp-00010-001/

Alertas de Malware y Adware

2CMV-00026-001 CSIRT ADVIERTE DE SITIOS DE ADWARE

Alerta de seguridad informática	2CMV-00026-001
Clase de alerta	Código Malicioso
Tipo de incidente	Adware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Agosto de 2019
Última revisión	23 de Agosto de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado sitios relacionados con anuncios publicitarios no deseados (Adware). Este ataque de ingeniería social intenta persuadir a los usuarios para que seleccionen “permitir” en el mensaje que aparece en el navegador, lo que como consecuencia multiplicará el envío de anuncios no deseados directamente al equipo del afectado.

El anuncio puede ser activado al ingresar en algún sitio no confiable. El usuario será bombardeado de mensajes para ver contenidos o para descargar información.
También cabe la posibilidad que un usuario haya instalado algún software gratuito que contenga un Adware, por ejemplo, a través de una "Play Store" con aplicaciones (APK), ofreciendo anuncios no deseados. Dichas aplicaciones se hacen pasa por aplicaciones legítimas especialmente centrada en juegos y fotografías.

Enlace

https://www.csirt.gob.cl/media/2019/08/2CMV-00026-001.pdf
https://www.csirt.gob.cl/alertas/2cmv-00026-001-csirt-advierte-de-sitios-de-adware/

2CMV-00027-001 CSIRT IDENTIFICÓ SITIOS NACIONALES CLONADOS CON MALWARE ASOCIADO

Alerta de seguridad informática	2CMV-00027-001
Clase de alerta	Código Malicioso
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Agosto de 2019
Última revisión	29 de Agosto de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado sitios web nacionales clonados con malware asociado, a continuación se enumeran los sitios web y los IoC relacionado al archivo que inyecta el malware.

Enlace

https://www.csirt.gob.cl/media/2019/08/2CMV-00027-001.pdf
https://www.csirt.gob.cl/alertas/2cmv-00027-001/

Vulnerabilidades

9VSA-00039-001 CSIRT COMPARTE INFORMACIÓN SOBRE VULNERABILIDADES Y PARCHES ENTREGADAS POR CISCO

Alerta de seguridad informática	9VSA-00039-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	23 de agosto de 2019
Última revisión	23 de agosto de 2019

Vulnerabilidad

CVE-2019-1982	CVE-2019-1883
CVE-2019-1980	CVE-2019-12627
CVE-2019-1981	CVE-2019-12621
CVE-2019-1978	CVE-2019-1871
CVE-2019-9506	CVE-2019-1850
CVE-2019-12626	CVE-2019-1864

CVE-2019-1865	CVE-2019-1935
CVE-2019-1634	CVE-2019-12624
CVE-2019-1896	CVE-2019-12623
CVE-2019-1900	CVE-2019-1984
CVE-2019-1908	CVE-2019-12622
CVE-2019-1907	CVE-2019-1839
CVE-2019-1863	CVE-2019-1885
CVE-2019-1937	CVE-2019-12634
CVE-2019-1974	CVE-2019-1938
CVE-2019-1936	CVE-2019-1948

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por CISCO referente vulnerabilidades detectadas en varios de sus productos y sus respectivas actualizaciones para mitigar el riesgo.

Enlace

https://www.csirt.gob.cl/media/2019/08/9VSA-00039-001.pdf
https://www.csirt.gob.cl/vulnerabilidades/9vsa-00039-001/

Indicadores de Compromisos

Se comparte a continuación el listado de indicadores de compromisos que fueron detectados durante la pasada semana 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:

IP's	Causa Asociada
185.153.198.196	Scan
92.119.160.52	Scan
198.54.117.200	Malware
185.53.88.20	Scan
201.150.255.185	Scan
195.123.245.185	Scan
185.225.17.5	Scan
169.239.128.29	Scan
198.54.115.43	Scan
199.188.200.90	Scan
213.190.6.125	Scan
104.31.68.241	Scan
213.190.6.77	Scan
185.201.10.67	Scan
77.247.110.66	Scan
92.119.160.251	Scan
92.119.160.250	Scan

167.71.138.4	Scan
77.247.110.99	Scan
164.77.119.18	Scan
64.91.238.61	Scan
104.27.150.248	Scan
178.159.36.236	Scan
185.68.16.4	Scan
212.47.242.53	Scan
178.159.36.177	phishing
95.211.198.90	Scan
185.53.88.41	phishing
80.211.249.70	phishing
77.247.110.83	phishing
45.125.66.68	phishing
57.230.30.55	Scan
151.217.75.58	Scan
167.86.72.241	Scan
216.144.240.6	Scan
204.16.169.2	Scan
176.31.86.164	Scan
42.231.162.193	Scan
185.40.4.246	Scan

URL's Bloqueadas	Causas Asociadas
https[://]www[.]banconestado[.]com/imagenes/comun2009/en-linea-personas[.]php	phishing
http[://]www[.]personas-bancodechile[.]alertasviabcpe[.]com/persona/login/	phishing
Portalweb[.]live	phishing
http[://]www[.]sadhgeabe[.]com	phishing
https[://]pioimpaireddrivinguae[.]com	phishing
http[://]kfues[.]com	phishing
https[://]sopfdiseh[.]com	phishing
http[://]sopfdisstrack[.]com	phishing
https[://]soidiie[.]com	phishing
http[://]sopfdiss[.]com	phishing

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: 2019.08.30 16:06:44 -04'00'