13BCS-00023-001

CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Informática
Publicado el Jueves 19 de Septiembre de 2019

Resumen de noticias, reportes, alertas e indicadores de compromisos informados por CSIRT entre el jueves 12 y el miércoles 18 de Septiembre.

Falsificación de Registro o Identidad

8FFR-00057-001 CSIRT ADVIERTE DE 102 SITIOS BANCARIOS FRAUDULENTOS ASOCIADOS A IP

Alerta de seguridad informática	8FFR-00057-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Septiembre de 2019
Última revisión	13 de Septiembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de 102 portales fraudulentos asociados a una IP que suplantan el sitio web oficial del 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-00057-001/
https://www.csirt.gob.cl/media/2019/09/8FFR-00057-001.pdf

8FFR-00058-001 CSIRT ADVIERTE DE SITIO FRAUDULENTO BANCARIO

Alerta de seguridad informática	8FFR-00058-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Septiembre de 2019
Última revisión	13 de Septiembre 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 banco 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-00058-001/
https://www.csirt.gob.cl/media/2019/09/8FFR-00058-001.pdf

8FFR-00059-001 CSIRT ADVIERTE DE DOS SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR-00059-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Septiembre de 2019
Última revisión	13 de Septiembre 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 banco Itau, el que podría servir para robar credenciales de usuarios de esa entidad.
Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00059-001/
https://www.csirt.gob.cl/media/2019/09/8FFR-00059-001.pdf

8FFR-00060-001 CSIRT ADVIERTE DE PORTAL COMERCIAL FRAUDULENTO

Alerta de seguridad informática	8FFR-00060-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Septiembre de 2019
Última revisión	13 de Septiembre 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 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 comercial aludida.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00060-001/
https://www.csirt.gob.cl/media/2019/09/8FFR-00060-001.pdf

8FFR-00061-001 CSIRT ADVIERTE DE DOS PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR-00061-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Septiembre de 2019
Última revisión	16 de Septiembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de dos portales fraudulentos asociados a una IP que suplantan el sitio web oficial de Banco Estado, 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/alertas/8ffr-00061-001/
https://www.csirt.gob.cl/media/2019/09/8FFR-00061-001.pdf

8FFR-00062-001 CSIRT ADVIERTE DE UN SITIO BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00062-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Septiembre de 2019
Última revisión	16 de Septiembre 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-00062-001/

https://www.csirt.gob.cl/media/2019/09/8FFR-00062-001.pdf

8FFR-00063-001 CSIRT ADVIERTE DE 5 SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR-00061-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Septiembre de 2019
Última revisión	16 de Septiembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de cinco portales fraudulentos asociados a IPs que suplantan el sitio web oficial de Banco chile, 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/alertas/8ffr-00063-001/

https://www.csirt.gob.cl/media/2019/09/8FFR-00063-001.pdf

8FFR-00064-001 CSIRT ADVIERTE DE SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR-00064-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Septiembre de 2019
Última revisión	17 de Septiembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de portales fraudulentos asociados a IPs que suplantan el sitio web oficial de Banco Estado, lo 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-00064-001/

https://www.csirt.gob.cl/media/2019/09/8FFR-00064-001.pdf

8FFR-00065-001 CSIRT ADVIERTE DE UNA WEB BANCARIA FRAUDULENTA

Alerta de seguridad informática	8FFR-00065-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Septiembre de 2019
Última revisión	17 de Septiembre 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 internacional, 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-00065-001/

https://www.csirt.gob.cl/media/2019/09/8FFR-00065-001.pdf

Vulnerabilidades

9VSA-00049-001 CSIRT COMPARTE ACTUALIZACIONES PARA EXIM

Alerta de seguridad informática	9VSA-00049-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	12 de Septiembre de 2019
Última revisión	12 de Septiembre de 2019

Vulnerabilidad
CVE-2019-15846

Resumen
El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información obtenida de diferentes fuentes, referente a vulnerabilidades detectadas en el agente de transferencia de correos EXIM para Linux, junto a su respectiva actualización para mitigar el riesgo.

Enlace
https://www.csirt.gob.cl/vulnerabilidades/9vsa-00049-001/
https://www.csirt.gob.cl/media/2019/09/9VSA-00049-001.pdf

9VSA-00050-001 CSIRT COMPARTE ACTUALIZACIONES DE ADOBE FLASH PLAYER

Alerta de seguridad informática	9VSA-00050-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Septiembre de 2019
Última revisión	13 de Septiembre de 2019

Vulnerabilidad
CVE-2019-8069
CVE-2019-8070
Resumen
El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información obtenida de ADOBE, referente a vulnerabilidades detectadas en ADOBE Flash Player, cliente de ejecución de contenido multimedia y otros, junto a su respectivas actualizaciones.
Enlace
https://www.csirt.gob.cl/vulnerabilidades/9vsa-00050-001/
https://www.csirt.gob.cl/media/2019/09/9VSA-00050-001.pdf

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	Motivo
185[.]53[.]88[.]54	Scanning
167[.]86[.]114[.]134	Scanning
77[.]247[.]109[.]29	Scanning
159[.]203[.]193[.]246	Scanning
157[.]245[.]68[.]205	Scanning
157[.]245[.]68[.]199	Scanning
185[.]216[.]140[.]108	Scanning
157[.]245[.]68[.]205	Scanning
77[.]111[.]247[.]68	Scanning
64[.]235[.]37[.]103	Scanning
179[.]43[.]149[.]11	Vulnerabilidad
190[.]196[.]60[.]169	Scanning
186[.]10[.]136[.]78	Scanning
147[.]135[.]26[.]91	Phishing
157[.]245[.]110[.]23	Phishing
195[.]22[.]28[.]198	Malware
209[.]99[.]40[.]221	Malware
185[.]182[.]57[.]79	Vulnerabilidad
94[.]177[.]243[.]17	Scanning
37[.]120[.]152[.]186	Scanning
185[.]244[.]25[.]133	Scanning
37[.]49[.]231[.]132	Scanning
192[.]64[.]86[.]92	Scanning
5[.]9[.]137[.]105	Scanning
213[.]152[.]173[.]133	Scanning
212[.]83[.]148[.]254	Scanning
159[.]203[.]201[.]237	Scanning
77[.]247[.]110[.]215	Scanning
185[.]53[.]88[.]81	Scanning
185[.]244[.]25[.]203	Attack
162[.]242[.]150[.]89	Phishing
23[.]253[.]58[.]227	Phishing
77[.]247[.]110[.]196	Scanning
185[.]22[.]67[.]108	Malware
45[.]89[.]175[.]106	Scanning
190[.]119[.]180[.]226	Malware
203[.]150[.]19[.]63	Malware

190[.]3[.]183[.]19	Malware
71[.]244[.]60[.]230	Malware
45[.]79[.]130[.]89	Scanning
172[.]105[.]6[.]186	Scanning
95[.]171[.]222[.]186	Scanning
61[.]135[.]169[.]125	Scanning
80[.]211[.]246[.]118	Scanning
77[.]247[.]110[.]113	Scanning
192[.]99[.]30[.]200	Scanning
125[.]64[.]94[.]211	Scanning
157[.]245[.]72[.]214	Vulnerabilidad
208[.]100[.]26[.]229	Scanning
185[.]200[.]118[.]76	Scanning
159[.]203[.]193[.]49	Scanning
185[.]53[.]88[.]79	Scanning
212[.]83[.]137[.]50	Scanning
62[.]173[.]139[.]164	Scanning
169[.]239[.]182[.]217	Scanning
179[.]32[.]19[.]219	Scanning
177[.]246[.]193[.]139	Scanning
31[.]172[.]240[.]91	Scanning
152[.]169[.]236[.]172	Scanning
201[.]212[.]57[.]109	Scanning
222[.]214[.]218[.]192	Scanning
87[.]230[.]19[.]21	Scanning
46[.]105[.]131[.]87	Scanning
182[.]176[.]106[.]43	Scanning
83[.]29[.]180[.]97	Malware
181[.]36[.]42[.]205	Malware
200[.]21[.]90[.]6	Malware
123[.]168[.]4[.]66	Malware
151[.]80[.]142[.]33	Malware
159[.]65[.]241[.]220	Malware
43[.]229[.]62[.]186	Malware
190[.]1[.]37[.]125	Malware

URL	Motivo
www[.]lbancodlechileportalloginl[.]origene[.]co[.]in	Phishing
http://footballtimes[.]info	Malware
http://vegetableportfolio[.]com	Malware
http://windowsearchcache[.]com	Malware
http://electricalweb[.]org	Malware
http://upnpdiscover[.]org	Malware
http://www[.]lazymmfi[.]org/hiradc/lib/www[.]bancoestado	Phishing

https://www[.]stuevesiegel[.]com/assets/fpc/Activacion[.]php[.]cl	Phishing
https://www[.]itau[.]cl-wps2[.]xyz/	Phishing
www[.]itau[.]cl-wps1[.]xyz	Phishing
www[.]tarjetacencosud[.]cl-web[.]xyz/	Phishing
http://andr0ip[.]site/grow/imagenes/comun2008/banca-en-linea-personas[.]html	Phishing
https://www[.]bencostado[.]xyz/imagenes/comun2009/en-linea-personas[.]php	Phishing
http://trav3lcoin[.]net/single/imagenes/comun2008/banca-en-linea-personas[.]html	Phishing
todaynwescorp[.]com	Malware
http://li3ancocredichille[.]com/chile-personal/ingreso[.]html	Phishing
http://]3ancoocredichile[.]com/chile-personal/ingreso[.]html	Phishing
http://il3ancocredlchile[.]com/chile-personal/ingreso[.]html	Phishing
http://www[.]wwv-l3ancacredichille-cl[.]htlps-wwv-cmr-cl[.]com/personas-cl/ingreso[.]html	Phishing
http://jeitacave[.]org/ps004[.]jpg	Malware
http://141[.]98[.]216[.]130/1505132[.]jpg	Malware
http://141[.]98[.]216[.]130/1603232[.]jpg	Malware
http://141[.]98[.]216[.]130/1808132[.]jpg	Malware
http://141[.]98[.]216[.]130/pe[.]jpg	Malware
http://nw[.]brownsine[.]com/	Malware
http://141[.]98[.]216[.]130/1505164[.]jpg	Malware
http://zopso[.]org/	Malware
http://141[.]98[.]216[.]130/1808164[.]jpg	Malware
http://141[.]98[.]216[.]130/1603264[.]jpg	Malware
http://danangluxury[.]com/wp-content/uploads/KTgQsblu/	Malware
http://gcesab[.]com/wp-includes/customize/zUfJervuM/	Malware
http://autorepuestosdml[.]com/wp-content/CiloXIptI/	Malware
http://covergt[.]com/wordpress/geh7l30-xq85i1-558/	Malware
http://zhaoyouxiu[.]com/wp-includes/vxqo-84953w-5062/	Malware
http://rockstareats[.]com/wp-content/themes/NUOAajdJ/	Malware
http://inwil[.]com/wp-content/oyFhKHoe	Malware
http://inesmanila[.]com/cgi-bin/otxpnmxm-3okvb2-29756/	Malware
http://dateandoando[.]com/wp-includes/y0mcdp2zyq_lx14j2wh2-0551284557/	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

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.09.19 16:06:40 -03'00'