13BCS-00030-001

CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Informática

Publicado el Viernes 29 de Noviembre de 2019

Resumen de noticias, reportes, alertas e indicadores de compromisos informados por CSIRT entre el jueves 21 y el miércoles 27 de Noviembre.

Falsificación de Registro o Identidad

8FFR-00118-001 CSIRT ADVIERTE DE UN SITIO BANCARIO CLONADO PARA ROBAR CREDENCIALES

Alerta de seguridad informática	8FFR-00118-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Noviembre de 2019
Última revisión	22 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 Falabella, 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-00118-001/

https://www.csirt.gob.cl/media/2019/11/8FFR-00118-001.pdf

8FFR-00119-001 CSIRT advierte de dos sitios bancarios fraudulentos

Alerta de seguridad informática	8FFR-00119-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Noviembre de 2019
Última revisión	22 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/9vsa-00118-001/
https://www.csirt.gob.cl/media/2019/11/8FFR-00119-001.pdf

8FFR-00120-001 CSIRT ADVIERTE SOBRE ACTIVACIÓN DE 4 PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR-00120-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Noviembre de 2019
Última revisión	23 de Noviembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de cuatro portales bancarios fraudulentos asociados a una IP que suplantan el sitio web oficial de Banco de Chile, lo que podría servir para el robo de 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-00120-001/
https://www.csirt.gob.cl/media/2019/11/8FFR-00120-001.pdf

8FFR-00121-001 CSIRT ADVIERTE DE 3 NUEVOS SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR-00121-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Noviembre de 2019
Última revisión	23 de Noviembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de 3 portales bancarios fraudulentos asociados a 3 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 comercial aludida.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00121-001/
https://www.csirt.gob.cl/media/2019/11/8FFR-00121-001.pdf

8FFR-00124-001 CSIRT ADVIERTE CUATRO WEBS BANCARIAS FRAUDULENTAS PARA ROBO DE CREDENCIALES

Alerta de seguridad informática	8FFR-00124-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Noviembre de 2019
Última revisión	24 de Noviembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de cuatro portales fraudulentos asociados a una IP que suplanta el sitio web oficial 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/8ffr-00124-001/
https://www.csirt.gob.cl/media/2019/11/8FFR-00124-001.pdf

8FFR-00125-001 CSIRT ADVIERTE DE TRES PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR-00125-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Noviembre de 2019
Última revisión	24 de Noviembre de 2019

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/8ffr-00125-001/
https://www.csirt.gob.cl/media/2019/11/8FFR-00125-001.pdf

8FFR-00126-001 CSIRT ADVIERTE ACTIVACIÓN DE DOS 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	25 de Noviembre de 2019
Última revisión	25 de Noviembre 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 clonan 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-00126-001/
https://www.csirt.gob.cl/media/2019/11/8FFR-00126-001.pdf

8FFR-00127-001 CSIRT ADVIERTE DE LA ACTIVACIÓN DE SITIO WEB BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00127-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Noviembre de 2019
Última revisión	25 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 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/8ffr-00127-001/
https://www.csirt.gob.cl/media/2019/11/8FFR-00127-001.pdf

8FFR-00128-001 CSIRT ADVIERTE SUPLANTANCIÓN DE SITIO DE OPERADOR DE TARJETAS DE CRÉDITO

Alerta de seguridad informática	8FFR-00128-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Noviembre de 2019
Última revisión	27 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 CMR Falabella, 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-00128-001/
https://www.csirt.gob.cl/media/2019/11/8FFR-00128-001.pdf

9VSA-00088-001 CSIRT ADVIERTE VULNERABILIDAD EN DISPOSITIVOS ANDROID Y GOOGLE

Alerta de seguridad informática	9VSA-00088-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	21 de noviembre de 2019
Última revisión	21 de noviembre de 2019

Vulnerabilidad

CVE-2019-2234

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de diferentes fuentes, referente a una vulnerabilidad que afecta a la cámara de los dispositivos móviles utilizados para Android y Google. De ser explotada la vulnerabilidad, puede resultar en el uso no autorizado de la cámara para, entre otros, robar datos de los usuarios. El informe también incluye las respectivas actualizaciones para mitigar el riesgo.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00087-001-2/
https://www.csirt.gob.cl/media/2019/11/9VSA-00088-001.pdf

9VSA-00089-001 CSIRT COMPARTE ACTUALIZACIONES PARA APP MÓVIL DE OUTLOOK

Alerta de seguridad informática	9VSA-00089-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de noviembre de 2019
Última revisión	22 de noviembre de 2019

Vulnerabilidad

CVE-2019-1460

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida del sitio oficial de Microsoft, referente a una vulnerabilidad que afecta a su aplicación móvil de mensajería, Outlook, la cual, si es explotada, puede resultar en un ataque de tipo spoofing (suplantación de usuario). Este informe incluye la respectiva actualización para mitigar el riesgo.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00089-001/
https://www.csirt.gob.cl/media/2019/11/9VSA-00089-001.pdf

9VSA-00090-001 CSIRT COMPARTE ACTUALIZACIONES PARA MONITOR DHCP DE FORTIGUARD

Alerta de seguridad informática	9VSA-00090-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de noviembre de 2019
Última revisión	25 de noviembre de 2019

Vulnerabilidad

CVE-2019-6697

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida del sitio oficial de FortiGuard referente a una vulnerabilidad que afecta a su herramienta de monitoreo DHCP, la cual, si es explotada, puede resultar en ataques remotos de tipo XSS persistente (Stored Cross-site Scripting). El informe contiene información sobre las actualizaciones para mitigar el riesgo.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00090-001/
https://www.csirt.gob.cl/media/2019/11/9VSA-00090-001.pdf

9VSA-00091-001 CSIRT COMPARTE ACTUALIZACIONES PARA MCAFEE CLIENT PROXY (MCP)

Alerta de seguridad informática	9VSA-00090-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de noviembre de 2019
Última revisión	25 de noviembre de 2019

Vulnerabilidad

CVE-2019-6697

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida del sitio oficial de McAfee referente a una vulnerabilidad que afecta a su herramienta McAfee Client Proxy (MCP) en el sistema operativo Windows, la cual, si es explotada, puede resultar en la evasión local de autenticación. Este informe incluye la respectiva actualización para mitigar el riesgo.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00091-001/
https://www.csirt.gob.cl/media/2019/11/9VSA-00091-001.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:

IoC	Motivo
77[.]247[.]109[.]49	Port Scan
37[.]49[.]231[.]146	Port Scan
207[.]180[.]250[.]173	Port Scan
104[.]40[.]149[.]33	Port Scan
207[.]180[.]193[.]225	Port Scan
200[.]19[.]156[.]22	Port Scan
71[.]6[.]200[.]207	Port Scan
133[.]34[.]149[.]5	Port Scan
62[.]210[.]10[.]244	Port Scan
5[.]35[.]213[.]20	Port Scan
191[.]253[.]65[.]70	Port Scan
178[.]128[.]214[.]153	Port Scan
185[.]219[.]133[.]163	Port Scan
80[.]82[.]78[.]211	Port Scan
85[.]195[.]230[.]179	Port Scan
103[.]76[.]85[.]136	Hacking
89[.]238[.]178[.]206	Port Scan
155[.]138[.]216[.]87	Port Scan
83[.]110[.]94[.]169	Port Scan
113[.]203[.]250[.]145	Port Scan
45[.]94[.]149[.]132	Port Scan
103[.]116[.]12[.]234	Port Scan
185[.]95[.]132[.]186	Port Scan
93[.]55[.]130[.]87	Port Scan
92[.]184[.]97[.]63	Port Scan
92[.]223[.]236[.]214	Port Scan
80[.]250[.]8[.]204	Port Scan
213[.]165[.]37[.]154	Port Scan
85[.]42[.]52[.]66	Port Scan
85[.]43[.]254[.]97	Port Scan
213[.]137[.]43[.]14	Port Scan
185[.]122[.]225[.]18	Port Scan
185[.]232[.]130[.]102	Port Scan

92[.]247[.]88[.]94	Port Scan
113[.]36[.]78[.]181	Port Scan
116[.]109[.]81[.]249	Port Scan
93[.]57[.]241[.]217	Port Scan
139[.]255[.]116[.]236	Port Scan
105[.]22[.]39[.]178	Port Scan
89[.]207[.]110[.]243	Port Scan
92[.]63[.]196[.]3	Hacking
115[.]23[.]172[.]24	Port Scan
151[.]106[.]59[.]214	Port Scan
175[.]126[.]145[.]10	Hacking
182[.]50[.]132[.]70	Hacking
208[.]93[.]152[.]17	Port Scan
89[.]39[.]107[.]197	DDoS
51[.]75[.]79[.]176	Port Scan
159[.]203[.]197[.]22	Port Scan
45[.]11[.]0[.]133	Port Scan
104[.]244[.]75[.]179	Port Scan
185[.]207[.]37[.]166	Port Scan
119[.]73[.]204[.]206	Port Scan
208[.]112[.]75[.]204	Port Scan
37[.]49[.]231[.]129	Port Scan
96[.]44[.]139[.]178	Port Scan
138[.]99[.]216[.]221	Port Scan
46[.]166[.]187[.]141	Port Scan
193[.]32[.]161[.]123	Hacking
23[.]228[.]96[.]18	Hacking
109[.]70[.]100[.]26	DDoS
185[.]220[.]101[.]72	DDoS
199[.]249[.]230[.]72	DDoS
199[.]249[.]230[.]78	DDoS
51[.]158[.]184[.]28	DDoS
104[.]244[.]79[.]222	DDoS
176[.]119[.]28[.]25	DDoS
159[.]203[.]193[.]44	Port Scan
144[.]91[.]88[.]63	Port Scan
159[.]203[.]193[.]249	Port Scan
201[.]214[.]220[.]58	Port Scan
159[.]203[.]197[.]8	Port Scan
185[.]176[.]27[.]42	Port Scan
45[.]134[.]179[.]20	Port Scan
45[.]134[.]179[.]15	Port Scan

2[.]56[.]8[.]17	Port Scan
107[.]174[.]170[.]101	Port Scan
167[.]71[.]11[.]215	Port Scan
23[.]228[.]73[.]183	Port Scan
23[.]228[.]73[.]171	Port Scan
185[.]89[.]102[.]8	Port Scan
129[.]28[.]174[.]228	Hacking
91[.]121[.]76[.]175	Hacking
69[.]30[.]200[.]178	Port Scan
115[.]23[.]172[.]24	Port Scan
185[.]153[.]197[.]149	Port Scan
159[.]203[.]193[.]241	Port Scan
80[.]82[.]65[.]90	Port Scan
45[.]134[.]179[.]10	Port Scan
91[.]93[.]172[.]59	Port Scan
46[.]166[.]187[.]159	Port Scan
123[.]51[.]152[.]54	Port Scan
182[.]55[.]136[.]224	Port Scan
186[.]222[.]57[.]22	Port Scan
103[.]26[.]221[.]244	Port Scan
112[.]133[.]251[.]51	Port Scan
46[.]161[.]27[.]122	Port Scan
163[.]172[.]7[.]18	Port Scan
176[.]107[.]130[.]109	Port Scan
5[.]26[.]57[.]119	Port Scan
39[.]109[.]181[.]160	Port Scan
45[.]11[.]19[.]111	Port Scan
80[.]123[.]55[.]236	Port Scan
86[.]125[.]136[.]112	Port Scan
92[.]63[.]194[.]91	Port Scan
105[.]227[.]162[.]172	Port Scan
212[.]83[.]149[.]96	Port Scan
45[.]143[.]220[.]46	Port Scan
92[.]63[.]194[.]81	Port Scan
128[.]14[.]156[.]186	Port Scan
37[.]49[.]230[.]17	Port Scan
185[.]164[.]72[.]139	Port Scan
62[.]210[.]28[.]186	Port Scan
117[.]254[.]60[.]49	Port Scan
138[.]68[.]219[.]40	Port Scan
47[.]75[.]123[.]162	Port Scan
207[.]180[.]200[.]99	Port Scan

5[.]189[.]170[.]207	Port Scan
144[.]91[.]80[.]182	Port Scan
207[.]180[.]201[.]204	Malware
198[.]134[.]112[.]244	Malware
198[.]134[.]112[.]241	Malware
208[.]83[.]223[.]34	Malware
193[.]23[.]244[.]244	Malware
131[.]188[.]40[.]189	Malware
69[.]162[.]92[.]86	Port Scan
74[.]91[.]113[.]136	Port Scan
178[.]32[.]217[.]124	Port Scan
185[.]176[.]27[.]242	Port Scan
64[.]76[.]136[.]2	Port Scan
134[.]119[.]194[.]102	Port Scan

URL	Motivo
http[://]glovalcoin[.]site	Phishing
http[://]www[.]gigalan[.]pe	Phishing
https[://]qrcoach[.]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: 2019.11.29 16:58:33 -03'00'