13BCS-00017-001

CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Informática

Publicado el Jueves 08 de Agosto de 2019

Resumen de noticias, reportes, alertas e indicadores de compromisos informados por CSIRT entre el jueves 01 y el miércoles 07 de Agosto.

Noticias

Publicado 7 agosto, 2019

Ransomware que Atacó a Escuelas en Louisiana, Ahora se Extiende a Hospitales.

El atacante, que no ha sido identificado aún, logró infiltrar un malware a la red el pasado 19 de mayo.

Enlace:

https://www.csirt.gob.cl/noticias/ransomware-que-ataco-a-escuelas-en-louisiana-ahora-se-extiende-a-hospitales/

Publicado 7 agosto, 2019

Localidad del Estado de Florida Perdió 700 mil Dólares por Ataque de spear Phishing

Los criminales se hicieron pasar por una compañía de construcción que prestaba servicios a la ciudad y lograron burlar la ciberseguridad para personal del staff transfiriera el dinero a una cuenta en un portal bancario fraudulento.

Enlace:

https://www.csirt.gob.cl/noticias/localidad-del-estado-de-florida-perdio-700-mil-dolares-por-ataque-de-spear-phishing/

Falsificación de Registro o Identidad

8FFR-00010-001 CSIRT ADVIERTE SOBRE FALSIFICACIÓN DE SITIO BANCARIO

Alerta de seguridad informática	8FFR-00010-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	31 de Julio de 2019
Última revisión	31 de Julio de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de portales fraudulentos que suplantan el sitio web oficial del **BANCOESTADO.CL** con el objetivo de obtener las credenciales de potenciales víctimas. Algunos de los sitios incluso cuentan con certificados que les permiten tener el candado para brindar la sensación de seguridad a los usuarios que puedan ser víctimas del fraude.

Lo anterior constituye una falsificación de la marca institucional con fines de fraude hacia los usuarios y/o clientes de la entidad afectada.

Enlace:

https://www.csirt.gob.cl/media/2019/08/8FFR-00010-001.pdf

8FFR-00010-002 CSIRT ACTUALIZA INFORMACIÓN SOBRE FALSIFICACIÓN DE SITIO BANCARIO

Alerta de seguridad informática	8FFR-00010-002
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	31 de Julio de 2019
Última revisión	07 de Agosto de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha actualizado la información sobre la activación de portales fraudulentos que suplantan el sitio web oficial del BANCOESTADO.CL que se informó el 31 de julio pasado, y que tenían como objetivo obtener las credenciales de potenciales víctimas. Algunos de los sitios incluso cuentan con certificados que les permiten tener el candado para brindar la sensación de seguridad a los usuarios que puedan ser víctimas del fraude.

Lo anterior constituye una falsificación de la marca institucional con fines de fraude hacia los usuarios y/o clientes de la entidad afectada.

CSIRT quiere informar que los dominios informados en su oportunidad fueron neutralizados antes de que pudieran ser utilizados por los atacantes.

Enlace:

https://www.csirt.gob.cl/media/2019/08/8FFR-00010-002.pdf

8FPH-00052-001 CSIRT ADVIERTE DE PHISHING POR REEMBOLSO

Alerta de seguridad informática	8FPH-00052-001
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Agosto de 2019
Última revisión	05 de Agosto 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 que intenta engañar a los usuarios indicando que tienen un rembolso de $587,58 Dólares en un sistema llamado Latino Tax. Los usuarios que pueden tener curiosidad podrían intentar ingresar al enlace y entregar sus credenciales en un sitio semejante al Sistema Impuesto Interno.

Enlace

https://www.csirt.gob.cl/media/2019/08/8FPH-00052-001.pdf

8FPH-00053-001 CSIRT ADVIERTE SOBRE PHISHING BANCARIO QUE SOLICITA SINCRONIZAR DISPOSITIVO CON SERVICIO WEB

Alerta de seguridad informática	8FPH-00053-001
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Agosto de 2019
Última revisión	05 de Agosto 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 que intenta engañar a los usuarios del Banco Scotibank, solicitando con urgencia sincronizar su dispositivo para ingresar a la cuenta de ScotiaWeb y así optar a los beneficios que tiene como afiliado. El correo también advierte de un plazo máximo de 48 horas para realizar el procedimiento, de lo contrario la cuenta será bloqueada. Si el usuario ingresa al enlace se expone a que el atacante rober sus credenciales desde un sitio semejante al del Banco.

Enlace

https://www.csirt.gob.cl/media/2019/08/8FPH-00053-001.pdf

8FPH-00054-001 CSIRT ADVIERTE DE PHISHING BANCARIO POR ACTUALIZACIÓN DE DIGIPASS

Alerta de seguridad informática	8FPH-00054-002
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Agosto de 2019
Última revisión	08 de Agosto de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), con la colaboración de usuarios de redes sociales, ha identificado una campaña de phishing a través de un correo electrónico que intenta persuadir a los usuarios del Banco Chile, solicitando a quienes pudieran recibir el correo que sincronicen su dispositivo DigiPass ya que existe un error, el cual se solucionaría con la sincronización, indicando que esta acción es "obligatoria", de lo contrario la cuenta podría ser bloqueada por temas de seguridad. Si el usuario ingresa al enlace se expone a que el atacante robe sus credenciales desde un sitio semejante al del Banco.

Enlace

https://www.csirt.gob.cl/media/2019/08/8FPH-00054-001.pdf

Alertas de Malware

2CMV-00024-001 CSIRT ADVIERTE DE PHISHING MALWARE EN SUPUESTO CORREO DE TESORERÍA

Alerta de seguridad informática	2CMV-00024-001
Clase de alerta	Fraude
Tipo de incidente	Phishing - Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Agosto de 2019
Última revisión	08 de Agosto 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 delincuentes buscan engañar a los usuarios advirtiéndoles que existe una obligación tributaria que se encuentra impaga. Para visualizar el informe generado por el Servicio Impuesto Interno, un usuario debe descargar el enlace adjunto en el correo electrónico. Al ser ejecutado desencadena la infección del malware.

Enlace

https://www.csirt.gob.cl/media/2019/08/2CMV-00024-001.pdf

Vulnerabilidades

9VSA-00027-001 CSIRT COMPARTE INFORMACIÓN DE ACTUALIZACIÓN EN VMWARE

Alerta de seguridad informática	9VSA-00027-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	2 de agosto de 2019
Última revisión	2 de agosto de 2019

Vulnerabilidad

CVE-2019-5521
CVE-2019-5684

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por VMWare referente a 2 vulnerabilidades presente en 3 de sus productos VMware Fusion, VMware Workstation y VMware ESXi.

Enlace

https://www.csirt.gob.cl/media/2019/08/9VSA-00027-001.pdf

9VSA-00028-001 CSIRT COMPARTE INFORMACIÓN SOBRE ACTUALIZACIONES EN DJANGO

Alerta de seguridad informática	9VSA-00028-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de Agosto de 2019
Última revisión	3 de Agosto de 2019

Vulnerabilidad

CVE-2019-14232
CVE-2019-14233
CVE-2019-14234
CVE-2019-14235

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Django (Framework de desarrollo web de código abierto) referente a múltiples vulnerabilidades que afectan a distintas versiones del software.

Enlace

https://www.csirt.gob.cl/media/2019/08/9VSA-00028-001.pdf

9VSA-00029-001 CSIRT COMPARTE INFORME SOBRE ACTUALIZACIÓN PARA DHCP DE WINDOWS 10

Alerta de seguridad informática	9VSA-00029-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de Agosto de 2019
Última revisión	3 de Agosto de 2019

Vulnerabilidad

CVE-2019-0547

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Microsoft referente a una vulnerabilidad detectada en el cliente DHCP de Windows 10.

Enlace

https://www.csirt.gob.cl/media/2019/08/9VSA-00029-001.pdf

9VSA-00030-001 CSIRT COMPARTE INFORMACIÓN DE ACTUALIZACIONES EN NVIDIA GPU DISPLAY DRIVER

Alerta de seguridad informática	9VSA-00030-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de Agosto de 2019
Última revisión	7 de Agosto de 2019

Vulnerabilidad

CVE-2019-5683
CVE-2019-5684
CVE-2019-5685
CVE-2019-5686
CVE-2019-5687

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por NVIDIA referente a una actualización para NVIDIA GPU Display Driver, para mitigar 5 vulnerabilidades que pueden permitir ejecución de código local, denegación de servicios o elevación de privilegios.

Enlace

https://www.csirt.gob.cl/media/2019/08/9VSA-00030-001.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 Bloqueadas	Causa Asociada
103[.]117[.]172[.]206	Malware
103[.]117[.]232[.]198	Malware
103[.]207[.]1[.]44	Malware
103[.]84[.]238[.]3	Malware
107[.]172[.]143[.]241	Malware
107[.]173[.]42[.]177	Malware
125[.]99[.]253[.]34	Malware
131[.]0[.]142[.]120	Malware
131[.]196[.]184[.]141	Malware
131[.]255[.]82[.]24	Malware
138[.]121[.]24[.]78	Malware
144[.]217[.]12[.]34	Malware
146[.]196[.]122[.]152	Malware
146[.]196[.]122[.]167	Malware
162[.]247[.]155[.]131	Malware
164[.]132[.]138[.]134	Malware
168[.]227[.]229[.]112	Malware
168[.]235[.]102[.]16	Malware
177[.]103[.]240[.]149	Malware
177[.]52[.]79[.]29	Malware
177[.]8[.]172[.]86	Malware
180[.]250[.]197[.]188	Malware
181[.]115[.]168[.]69	Malware
181[.]129[.]140[.]140	Malware
181[.]129[.]49[.]98	Malware
181[.]129[.]93[.]226	Malware
185[.]180[.]197[.]38	Malware
185[.]202[.]174[.]72	Malware
185[.]251[.]38[.]35	Malware
186[.]183[.]199[.]114	Malware
186[.]42[.]186[.]202	Malware
186[.]42[.]226[.]46	Malware
187[.]58[.]56[.]26	Malware
189[.]80[.]134[.]122	Malware

190[.]152[.]4[.]210	Malware
190[.]154[.]203[.]218	Malware
191[.]37[.]181[.]152	Malware
192[.]227[.]232[.]26	Malware
192[.]243[.]101[.]232	Malware
195[.]123[.]246[.]69	Malware
202[.]4[.]169[.]178	Malware
23[.]94[.]93[.]106	Malware
36[.]89[.]85[.]103	Malware
45[.]237[.]240[.]178	Malware
5[.]253[.]63[.]112	Malware
51[.]254[.]69[.]233	Malware
103[.]231[.]146[.]242	Ataque
151[.]61[.]68[.]155	Ataque
52[.]73[.]169[.]169	Scan
82[.]102[.]23[.]6	Scan
62[.]210[.]178[.]28	Scan
42[.]231[.]162[.]195	Ataque
42[.]231[.]162[.]202	Ataque
94[.]102[.]50[.]96	Scan
140[.]143[.]69[.]109	Scan
36[.]92[.]9[.]106	Scan
129[.]204[.]8[.]185	Scan
59[.]125[.]179[.]244	Scan
212[.]64[.]25[.]196	Scan
58[.]242[.]233[.]108	Scan
203[.]113[.]174[.]104	Malware
223[.]26[.]48[.]131	Malware
121[.]188[.]88[.]70	Malware
114[.]67[.]77[.]4	Malware
118[.]25[.]91[.]209	Malware
111[.]230[.]229[.]231	Malware
82[.]208[.]67[.]230	Malware
107[.]148[.]196[.]129	Malware
36[.]92[.]68[.]55	Malware
118[.]25[.]111[.]38	Malware
107[.]170[.]198[.]115	Scan
176[.]107[.]131[.]213	Scan
107[.]170[.]200[.]63	Scan
104[.]46[.]42[.]254	Scan
110[.]164[.]184[.]95	Ataque
119[.]3[.]89[.]47	Ataque

140[.]143[.]243[.]190	Ataque
122[.]116[.]68[.]107	Ataque
129[.]28[.]171[.]221	Ataque
49[.]4[.]65[.]223	Ataque
124[.]156[.]182[.]203	Ataque
94[.]102[.]50[.]96	Ataque
115[.]78[.]65[.]235	Ataque
118[.]25[.]105[.]88	Ataque
195[.]229[.]223[.]114	Ataque
118[.]25[.]73[.]12	Ataque
182[.]61[.]106[.]24	Ataque
49[.]234[.]29[.]162	Ataque
118[.]24[.]182[.]72	Ataque
41[.]188[.]66[.]164	Ataque
139[.]155[.]110[.]62	Ataque
49[.]234[.]29[.]162	Malware
213[.]32[.]9[.]157	Malware
185[.]245[.]43[.]102	Malware
107[.]170[.]204[.]68	Malware
23[.]27[.]127[.]13	Malware
118[.]24[.]4[.]204	Malware
119[.]29[.]157[.]216	Malware
190[.]5[.]135[.]121	Malware
114[.]116[.]116[.]99	Malware
200[.]24[.]255[.]244	Malware
118[.]163[.]243[.]74	Malware
181[.]170[.]121[.]9	Malware
94[.]191[.]71[.]240	Malware
122[.]142[.]17[.]11	Ataque
58[.]153[.]157[.]245	Ataque
185[.]98[.]208[.]101	Ataque
132[.]232[.]6[.]93	Malware
123[.]207[.]170[.]219	Malware
80[.]82[.]78[.]57	Malware
123[.]207[.]170[.]219	Scan
195[.]88[.]184[.][.]186	Scan
222[.]161[.]17[.]58	Scan
138[.]99[.]6[.]169	Scan
31[.]163[.]192[.]230	Scan
112[.]213[.]117[.]209	Scan
132[.]232[.]88[.]125	Scan
182[.]61[.]109[.]185	Scan

146[.]0[.]75[.]34	Malware
104[.]152[.]52[.]26	Scan
179[.]43[.]143[.]149	Scan
185[.]232[.]67[.]121	Scan
202[.]75[.]216[.]136	Scan
54[.]39[.]105[.]194	Ataque
185[.]244[.]25[.]180	Ataque
118[.]193[.]31[.]181	Ataque
107[.]170[.]204[.]68	Ataque
82[.]102[.]23[.]6	Ataque
107[.]170[.]237[.]129	Ataque
163[.]172[.]82[.]142	Ataque
185[.]12[.]177[.]134	Ataque
104[.]152[.]52[.]26	Ataque
167[.]179[.]76[.]246	Ataque
120[.]52[.]152[.]18	Ataque
193[.]32[.]163[.]123	Ataque
77[.]247[.]108[.]175	Ataque
185[.]56[.]81[.]41	Ataque
107[.]170[.]202[.]91	Ataque
211[.]8[.]50[.]230	Scan
80[.]211[.]251[.]205	Scan
77[.]247[.]110[.]37	Scan
77[.]247[.]110[.]30	Scan
77[.]247[.]110[.]29	Scan
77[.]247[.]110[.]31	Scan
77[.]247[.]110[.]32	Scan
192[.]31[.]80[.]30	Malware
185[.]175[.]93[.]14	Scan
80[.]82[.]77[.]20	Scan
163[.]172[.]82[.]142	Scan
120[.]52[.]152[.]18	Scan
185[.]94[.]111[.]1	Scan
209[.]24[.]1[.]4	Scan
81[.]169[.]188[.]158	Scan
158[.]69[.]58[.]48	Scan
92[.]118[.]161[.]49	Scan
196[.]52[.]43[.]92	Scan
151[.]1[.]48[.]2	Scan

URL's Bloqueadas	Causa Asociada
https://bncostado[.]xyz/imagenes/comun2009/en-linea-personas[.]php	phishing
http://mie[.]crypto-crypto[.]site/	Malware
http://dsntu[.]top/	Malware
http://elienne[.]net/	Malware
http://amnsns[.]com/	Malware
http://mmasl[.]com/s1[.]exe	Malware
http://calacs-laurentides[.]com/s1[.]exe	Malware
http://homeunix[.]com	Malware
http://mine[.]nu	Malware
http://game-server[.]cc	Malware
http://scrapping[.]cc	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: 2019.08.08 16:59:01 -04'00'