17-06-2020 | Año 1 | N°50

Boletín de Seguridad Cibernética

Semana del 11 al 18 de junio 2020

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

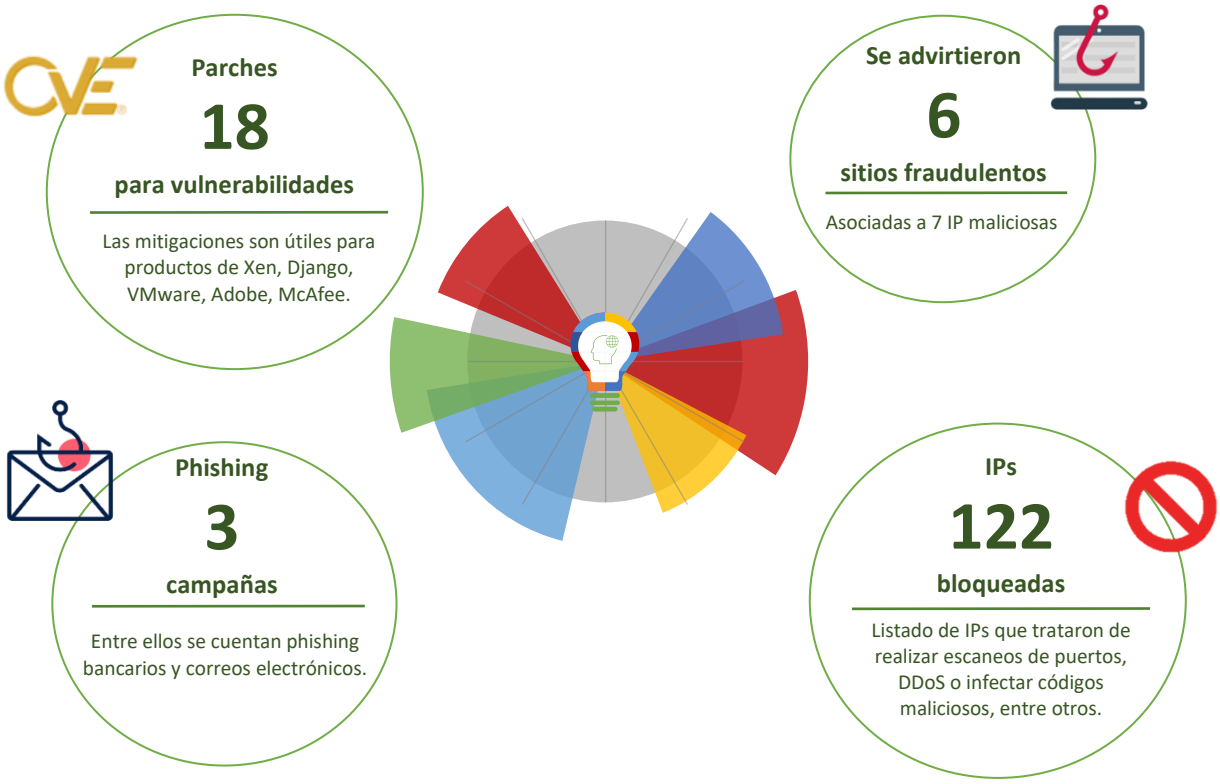
División de Redes y Seguridad Informática.

Gobierno de Chile

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

Resumen de la semana en cifras



*Los datos recopilados corresponden a información publicada en diferentes secciones del sitio web https://www.csirt.gob.cl

Contenido

Sitios fraudulentos

Imagen del sitio

CSIRT advierte la activación de un sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00446-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de Junio de 2020
Última revisión	12 de Junio de 2020
Indicadores de compromiso	
URL	
hxxp://acceso.bancochile.online/	
IP	
37.120.144.0/20	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00446-01/	
https://www.csirt.gob.cl/media/2020/06/8FFR20-00446-01.pdf	

Imágenes del sitio

CSIRT advierte de dos sitios bancarios fraudulentos	
Alerta de seguridad cibernética	8FFR20-00447-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Junio de 2020
Última revisión	15 de Junio de 2020
Indicadores de compromiso	
URL	
https[:]//hostalrestauranteentalara[.]com	
https[:]//frdscd[.]online/accessweb/bancochile-web/persona/login/index[.]php	
IP	
68[.]65[.]123[.]121	
199[.]188[.]206[.]170	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00447-01/	
https://www.csirt.gob.cl/media/2020/06/8FFR20-00447-01.pdf	

Imagen del sitio

CSIRT advierte de un portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00448-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Junio de 2020
Última revisión	15 de Junio de 2020
Indicadores de compromiso	
URL	
http[:]//acceso.bancochlie[.]online/	
IP	
157.245.255.18	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00448-01/	
https://www.csirt.gob.cl/media/2020/06/8FFR20-00448-01.pdf	

Imagen del sitio

CSIRT informa de un sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00449-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Junio de 2020
Última revisión	15 de Junio de 2020
Indicadores de compromiso	
URL	
http[:]//bancoestasdo[.]com/1592248262/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
139.99.155.233	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00449-01/	
https://www.csirt.gob.cl/media/2020/06/8FFR20-00449-01.pdf	

Imagen del sitio

CSIRT advierte de una página bancaria fraudulenta	
Alerta de seguridad cibernética	8FFR20-00450-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Junio de 2020
Última revisión	15 de Junio de 2020
Indicadores de compromiso	
URL	
http[:]//banacoestados-cl[.]website/RQ3HJ42/1KYQ45B/bancapersonal[.]html	
IP	
198.54.126.77	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00450-01/	
https://www.csirt.gob.cl/media/2020/06/8FFR20-00450-01.pdf	

Imagen del sitio

CSIRT informa sobre portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00451-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Junio de 2020
Última revisión	16 de Junio de 2020
Indicadores de compromiso	
URL	
http[:]//bancoestasdo[.]com/1592356933/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
139.99.155.233	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00451-01/	
https://www.csirt.gob.cl/media/2020/06/8FFR20-00451-01.pdf	

Phishing

Imagen del mensaje

CSIRT advierte phishing por caducidad de tarjeta de coordenadas	
Alerta de seguridad cibernética	8FPH20-00244-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Junio de 2020
Última revisión	11 de Junio de 2020
Indicadores de compromiso	
URL	
hxxps://bit[.]ly/2XQgvE8	
hxxp://cifras[.]cl/es/	
http://bancamovilseguro.tonohost.com/imagenes/comun2008/banca-en-linea-personas.html	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00244-01/	
https://www.csirt.gob.cl/media/2020/06/8FPH20-00244-01.pdf	

Imagen del mensaje

CSIRT advierte smishing que ofrece hielera de cerveza	
Alerta de seguridad cibernética	8FPH20-00245-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Junio de 2020
Última revisión	11 de Junio de 2020
Indicadores de compromiso	
URL	
hxxps://heineken.regalo[.]top/	
IP	
[91.221.70.106]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00245-01/	
https://www.csirt.gob.cl/media/2020/06/8FPH20-00245-01.pdf	

Imagen del mensaje

CSIRT advierte phishing por expiración en versión de cuenta de correo	
Alerta de seguridad cibernética	8FPH20-00246-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Junio de 2020
Última revisión	17 de Junio de 2020
Indicadores de compromiso	
URL	
https[:]//outlook1200[.]wixsite[.]com/gracias	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00246-01/	
https://www.csirt.gob.cl/media/2020/06/8FPH20-00246-01.pdf	

Vulnerabilidades

CSIRT comparte vulnerabilidad y mitigación liberada por Django para desarrollo web	
Alerta de seguridad cibernética	9VSA20-00242-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Junio de 2020
Última revisión	11 de Junio de 2020
CVE	
CVE-2020-13254 -CVE-2020-13596	
Fabricante	
Django	
Producto afectado	
Django rama maestra. Django versión 3.1 (En estado alpha). Django versión 3.0. Django versión 2.2.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00242-01/	
https://www.csirt.gob.cl/media/2020/06/9VSA20-00242-01.pdf	

CSIRT comparte vulnerabilidad y mitigación liberada por Xen	
Alerta de seguridad cibernética	9VSA20-00243-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Junio de 2020
Última revisión	11 de Junio de 2020
CVE	
CVE-2020-0543	
Fabricante	
Xen	
Producto afectado	
Todos los sistemas con arquitectura x86 de Intel que utilicen Xen son vulnerables. No se ha comprobado que otras arquitecturas y otros procesadores (como ADM) sean vulnerables.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00243-01/	
https://www.csirt.gob.cl/media/2020/06/9VSA20-00243-01.pdf	

CSIRT advierte vulnerabilidades y mitigaciones de VMware para ESXi, Workstation, Fusion y Horizon Client	
Alerta de seguridad cibernética	9VSA20-00244-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de Junio de 2020
Última revisión	12 de Junio de 2020
CVE	
CVE-2020-3960 - CVE-2020-3961	
Fabricante	
VMware	
Producto afectado	
VMware vSphere ESXi versiones 6.7 y 6.5. VMware Workstation Pro/Player versión 15.x. VMware Fusion Pro/Fusion versión 11.x.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00244-01/	
https://www.csirt.gob.cl/media/2020/06/9VSA20-00244-01.pdf	

CSIRT comparte vulnerabilidades y mitigaciones liberadas por Adobe para sus productos	
Alerta de seguridad cibernética	9VSA20-00245-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Junio de 2020
Última revisión	15 de Junio de 2020
CVE	
CVE-2020-9633 - CVE-2020-9634 - CVE-2020-9635 CVE-2020-9636 - CVE-2020-9643 - CVE-2020-9644 CVE-2020-9645 - CVE-2020-9647 - CVE-2020-9648 CVE-2020-9651	
Fabricante	
Adobe	
Producto afectado	
Flash Player para Escritorio versión 32.0.0.371 y anteriores en Windows, macOS y Linux. Flash Player para Google Chrome versión 32.0.0.371 y anteriores en Windows, macOS, Linux y Chrome OS. Flash Player para Microsoft Edge e Internet Explorer 11 versión 32.0.0.330 y anteriores en Windows 10 y 8.1.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00245-01/	
https://www.csirt.gob.cl/media/2020/06/9VSA20-00245-01.pdf	

CSIRT advierte tres vulnerabilidades y comparte mitigaciones liberadas por McAfee para VirusScanEnterprise	
Alerta de seguridad cibernética	9VSA20-00246-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Junio de 2020
Última revisión	16 de Junio de 2020
CVE	
CVE-2019-3585 - CVE-2019-3588 CVE-2020-7280	
Fabricante	
McAfee	
Producto afectado	
VirusScan Enterprise parche 14, versión 8.7 y anteriores.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00246-01/	
https://www.csirt.gob.cl/media/2020/06/9VSA20-00246-01.pdf	

Indicadores de Compromisos

Se comparte a continuación el listado de IPs que fueron detectadas 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	IoC	Motivo
185.153.199.201	Port Scan	185.53.88.182	Port Scan
80.82.65.40	Port Scan	45.143.220.134	Port Scan
80.82.65.60	Port Scan	103.141.136.52	Port Scan
185.39.10.54	Port Scan	103.99.2.12	Port Scan
93.174.93.68	Port Scan	167.99.228.233	Port Scan
185.39.10.25	Port Scan	5.182.210.16	Port Scan
185.153.199.201	Port Scan	45.143.220.119	Port Scan
80.82.64.105	Port Scan	161.97.66.235	Port Scan
185.39.10.14	Port Scan	103.145.12.163	Port Scan
89.248.168.62	Port Scan	141.98.10.172	Port Scan
94.102.49.104	Port Scan	45.143.220.151	Port Scan
80.82.77.214	Port Scan	104.194.11.173	Port Scan
83.97.20.232	Port Scan	185.153.180.250	Port Scan
54.39.131.174	Port Scan	199.201.110.206	Port Scan
5.39.19.236	Port Scan	103.35.65.54	Port Scan
157.52.193.85	Port Scan	45.143.223.148	Port Scan
157.52.193.121	Port Scan	191.101.22.206	Port Scan
81.218.45.141	Port Scan	80.82.77.41	Port Scan
162.241.50.117	Port Scan	5.182.210.100	Port Scan
45.143.220.242	Port Scan	45.143.220.240	Port Scan
190.47.236.83	Malware	163.172.9.67	Port Scan
128.199.37.230	Port Scan	185.156.73.42	Port Scan
80.82.77.193	Port Scan	92.63.197.70	Port Scan
115.68.188.134	Port Scan	131.108.162.24	Port Scan
141.98.10.172	Port Scan	192.241.229.239	Port Scan
186.10.92.114	Malware	5.180.211.107	Port Scan
103.15.135.140	Port Scan	5.180.211.73	Port Scan
79.137.20.20	Port Scan	85.204.116.139	Malware
195.22.26.248	Malware	205.185.124.79	Port Scan
88.198.62.227	Malware	157.230.112.195	Port Scan
167.71.74.183	Port Scan	212.129.18.55	Port Scan
64.225.28.124	Port Scan	125.62.85.63	Port Scan
157.245.34.59	Port Scan	79.124.62.250	Port Scan
178.128.204.172	Port Scan	79.124.62.118	Port Scan

173.212.225.214	Port Scan	185.200.118.42	Port Scan
196.74.172.204	Port Scan	185.53.88.197	Port Scan
37.49.224.187	Port Scan	186.10.92.114	Malware
157.52.193.92	Port Scan	79.124.62.118	Port Scan
159.89.226.247	Port Scan	89.248.172.196	Port Scan
185.39.11.48	Port Scan	185.153.180.251	Port Scan
51.195.161.211	Port Scan	185.53.88.9	Port Scan
45.143.220.114	Port Scan	37.49.230.102	Port Scan
185.200.34.176	Port Scan	93.115.29.49	Port Scan
104.168.219.181	Port Scan	185.200.118.83	Port Scan
82.221.128.73	Port Scan	185.39.11.56	Port Scan
180..180.144.63	Port Scan	185.176.27.2	Port Scan
84.54.150.211	Port Scan	77.247.110.103	Port Scan
185.200.34.176	Port Scan	134.122.107.65	Port Scan
45.148.10.115	Port Scan	178.128.107.249	Port Scan
185.53.88.189	Port Scan	77.247.108.15	Port Scan
37.139.1.149	Port Scan	104.17.244.81	Malware
185.153.180.250	Port Scan	104.16.173.80	Malware
93.174.93.45	Port Scan	35.231.151.7	Malware
198.199.94.181	Port Scan	180.214.238.174	Port Scan
192.241.194.171	Port Scan	45.148.10.94	Port Scan
103.117.172.206	Malware	162.241.46.0	Port Scan
185.39.10.47	Port Scan	128.14.181.158	Port Scan
89.248.174.201	Port Scan	194.61.27.241	Port Scan
185.39.10.45	Port Scan	89.248.172.85	Port Scan
185.39.11.32	Port Scan	23.237.44.162	Port Scan
89.248.160.178	Port Scan	51.161.12.231	Port Scan

Recomendaciones y Buenas Prácticas

Recomendaciones generales de seguridad

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet
- Prestar atención en los detalles de los mensajes o redes sociales
- 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.
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
- Visualizar los sitios web que se ingresen sean los oficiales.

Investigación

Emotet. Limpieza de equipos y servidores

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la octava edición de su publicación sobre amenazas cibernéticas el que analiza la amenaza de Emotet y su limpieza. Este artículo que fue elaborado en conjunto por Paula Moraga Montero, Carlos Silva Caffi y Natalia Pérez Muñoz, todos analistas de nivel 2 de CSIRT.

Emotet nació como un troyano bancario polimórfico, que en la actualidad, funciona como descargador de otros troyanos bancarios. Desde el 2014 hasta la fecha, ha experimento cambios en su estructura modular, probando ser uno de los más eficientes, destructivos y costosos programas maliciosos del mundo. Este artículo fue elaborado para apreciar la dimensión general de la amenaza en su segunda fase de infección y servir como apoyo a la solución de su impacto.

Ver en: https://www.csirt.gob.cl/reportes/an2-2020-08/

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.

- Cristián Caris
  Twitter: @MrCaris1
- Felipe Bravo
  Twitter: @fbravoalliende
- Diego Arias
  Twitter: @Deariasc