02-07-2020 | Año 2 | N°52

Boletín de Seguridad Cibernética

Semana del 25 de junio al 01 de julio 2020

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

División de Redes y Seguridad Informática.

Gobierno de Chile

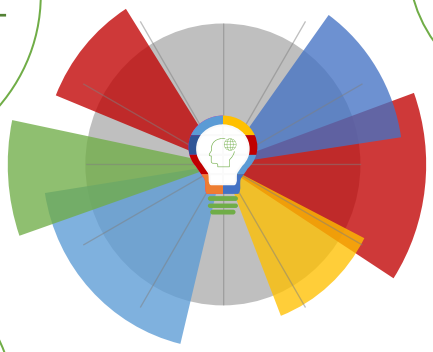
Ministerio del Interior y Seguridad Pública

Gobierno de Chile

Resumen de la semana en cifras

Parches
17
para vulnerabilidades
Las mitigaciones son útiles para productos VMware, Haxx, Delaware, Microsoft, Huawei y Mozilla.

Se advirtieron
12
sitios fraudulentos
Asociadas a 12 IP maliciosas



Phishing
3
campañas
Entre ellos se cuentan phishing bancarios y correos electrónicos.

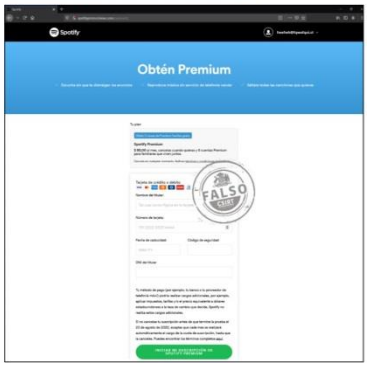
IPs
105
bloqueadas
Listado de IPs que trataron de realizar escaneos de puertos, DDoS o infectar códigos maliciosos, entre otros.

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

Contenido

Sitios fraudulentos

Imagen del sitio

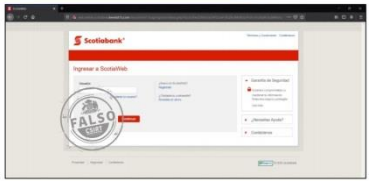


CSIRT advierte portal fraudulento de servicio de streaming	
Alerta de seguridad cibernética	8FFR20-00461-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Junio de 2020
Última revisión	25 de Junio de 2020
Indicadores de compromiso	
URL	
http[:]//spotifypromociones[.]com/usr/	
IP	
107.180.51.33	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00461-01/	
https://www.csirt.gob.cl/media/2020/06/8FFR20-00461-01.pdf	

Imagen del sitio

CSIRT advierte de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00462-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Junio de 2020
Última revisión	25 de Junio de 2020
Indicadores de compromiso	
URL	
https://sinatexcom.ir/Pensiones/www.bancoestado.cl/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
158.58.186.50	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00462-01/	
https://www.csirt.gob.cl/media/2020/06/8FFR20-00462-01.pdf	

Imagen del sitio



CSIRT advierte de sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00463-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Junio de 2020
Última revisión	25 de Junio de 2020
Indicadores de compromiso	
URL	
http[:]//web.online.scotiabnk.inverlat15[.]com/mxonlineV1/leap/signon/indexx[.]php?ID/ziiJRwd2XM3raUAPZzexPs8QfbOMb8DGPFxFoTKzfmjROLQWRxApGxaiwYtvxcKyhkhcCcb4oNSiQMnmcZNh6tYcjtczJvHfKDA5	
IP	
162.241.61.124	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00463-01/	
https://www.csirt.gob.cl/media/2020/06/8FFR20-00463-01.pdf	

Imagen del sitio

CSIRT advierte de sitio de streaming fraudulento	
Alerta de seguridad cibernética	8FFR20-00464-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Junio de 2020
Última revisión	25 de Junio de 2020
Indicadores de compromiso	
URL	
http[:]//sylvaniaduilawyer[.]com/Loguin/Netflix_Urochi/Netflix_Urochi/Home/login	
IP	
209.59.154.88	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00464-01/	
https://www.csirt.gob.cl/media/2020/06/8FFR20-00464-01.pdf	

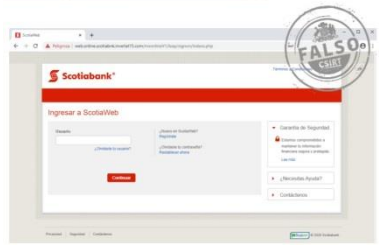
Imagen del sitio

CSIRT advierte de sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00465-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Junio de 2020
Última revisión	29 de Junio de 2020
Indicadores de compromiso	
URL	
hxxps://gharaviri.ir/Pension/www.bancoestado.cl/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
185.105.185.20	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00465-01/	
https://www.csirt.gob.cl/media/2020/06/8FFR20-00465-01.pdf	

Imagen del sitio

CSIRT advierte de un portal fraudulento bancario	
Alerta de seguridad cibernética	8FFR20-00466-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Junio de 2020
Última revisión	29 de Junio de 2020
Indicadores de compromiso	
URL	
https://www.hardworkerstudio.com/Avisos/www.bancoestado.cl/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
119.59.104.25	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00466-01/	
https://www.csirt.gob.cl/media/2020/06/8FFR20-00466-01.pdf	

Imagen del sitio



CSIRT informa sobre sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00467-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Junio de 2020
Última revisión	29 de Junio de 2020
Indicadores de compromiso	
URL	
hxxp://web.online.scotiabnk.inverlat15[.]com/mxonlineV1/leap/signon/indexx.php	
IP	
162.241.61.124	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00467-01/	
https://www.csirt.gob.cl/media/2020/06/8FFR20-00467-01.pdf	

Imagen del sitio

CSIRT advierte de una web que suplanta a sitio bancario	
Alerta de seguridad cibernética	8FFR20-00468-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Junio de 2020
Última revisión	29 de Junio de 2020
Indicadores de compromiso	
URL	
hxxp://157.245.64.118/acceso/personas/	
IP	
157.245.64.118	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00468-01/	
https://www.csirt.gob.cl/media/2020/06/8FFR20-00468-01.pdf	

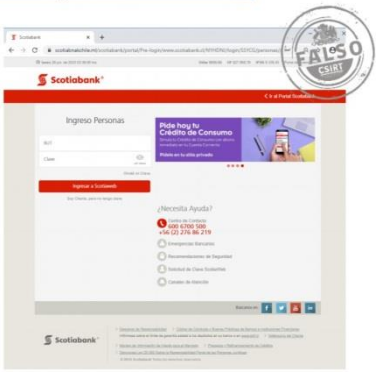
CSIRT advierte de sitio bancario para fraudes	
Alerta de seguridad cibernética	8FFR20-00469-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Junio de 2020
Última revisión	29 de Junio de 2020
Indicadores de compromiso	
URL	
hxxp://www-bancoestado.cl.wickedg[.]nl/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
185.56.146.196	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00469-01/	
https://www.csirt.gob.cl/media/2020/06/8FFR20-00469-01.pdf	

CSIRT informa de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00470-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Junio de 2020
Última revisión	29 de Junio de 2020
Indicadores de compromiso	
URL	
hxxps://movil-personas-estado-movil.000webhostapp[.]com/www.bancoestado.cl/imagenes/comun2008/banca-en-linea-personas.html	
IP	
145.14.144.8	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00470-01/	
https://www.csirt.gob.cl/media/2020/06/8FFR20-00470-01.pdf	

Imagen del sitio

CSIRT advierte de sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00471-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Junio de 2020
Última revisión	29 de Junio de 2020
Indicadores de compromiso	
URL	
hxxp://www.banc.oestado[.]live/comun2019/banca-en-linea-personas-session-1593411843-optimized-1593411843.html	
IP	
85.187.132.183	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00471-01/	
https://www.csirt.gob.cl/media/2020/06/8FFR20-00471-01.pdf	

Imagen del sitio



CSIRT informa portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00472-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Junio de 2020
Última revisión	29 de Junio de 2020
Indicadores de compromiso	
URL	
hxxps://scotiabnakchile[.]ml/scotiabank/portal/Pre-login/www.scotiabank.cl/NYHDNJ/login/SSYCG/personas//	
IP	
91.234.99.114	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00472-01/	
https://www.csirt.gob.cl/media/2020/06/8FFR20-00471-01.pdf	

Phishing

Imagen del mensaje

CSIRT advierte phishing en pago de beneficio Estatal	
Alerta de seguridad cibernética	8FPH20-00256-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Junio de 2020
Última revisión	26 de Junio de 2020
Indicadores de compromiso	
URL	
hxxp://wwwbancoestado[.]cl[.]diariooficialba[.]org/pagina/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
31.22.4.145	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00256-01/	
https://www.csirt.gob.cl/media/2020/06/8FPH20-00256-01.pdf	

Imagen del mensaje

CSIRT informa phishing con falso crédito aprobado por programa Covid-19	
Alerta de seguridad cibernética	8FPH20-00257-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Junio de 2020
Última revisión	27 de Junio de 2020
Indicadores de compromiso	
URL	
hxxps://bit[.]ly/31r5lYL?l=www[.]bancosecurity[.]cl	
hxxps://innovativeiteration[.]com/www[.]bancosecurity[.]cl/pagina/index[.]asp	
IP	
[67.205.103.117]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00257-01/	
https://www.csirt.gob.cl/media/2020/06/8FPH20-00257-01.pdf	

Imagen del mensaje

CSIRT advierte phishing bancario por supuesto crédito covid	
Alerta de seguridad cibernética	8FPH20-00259-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Julio de 2020
Última revisión	01 de Julio de 2020
Indicadores de compromiso	
URL	
hxxps://bit[.]ly/31r5lYL?l=www.bancosecurity.cl	
hxxps://acumensurgical[.]com/catalog/enviar.php?l=1963615076	
hxxps://www.spalvosspektras[.]lt/Creditos/www.bancosecurity.cl/	
IP	
[67.205.103.117]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00259-01/	
https://www.csirt.gob.cl/media/2020/07/8FPH20-00259-01.pdf	

*El archivo 8FPH20-00258-01 no está presente en el informe, debido a un error de correlación de número.

Vulnerabilidades

CSIRT advierte vulnerabilidades y mitigaciones liberadas por VMware	
Alerta de seguridad cibernética	9VSA20-00253-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Junio de 2020
Última revisión	26 de Junio de 2020
CVE	
CVE-2020-3962 - CVE-2020-3963 - CVE-2020-3964 CVE-2020-3965 - CVE-2020-3966 - CVE-2020-3967 CVE-2020-3968 - CVE-2020-3969 - CVE-2020-3970 CVE-2020-3971	
Fabricante	
VMware	
Productos afectados	
ESXi versión 7.0, 6.7 y 6.5. Fusion versión 11.x. Workstation versión 15.x. Cloud Foundation versión 4.x y 3.x.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00253-01/	
https://www.csirt.gob.cl/media/2020/06/9VSA20-00253-01.pdf	

CSIRT advierte vulnerabilidades y comparte mitigaciones obtenidas de Haxx para cURL	
Alerta de seguridad cibernética	9VSA20-00254-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de Junio de 2020
Última revisión	19 de Junio de 2020
CVE	
CVE-2020-8169 - CVE-2020-8177	
Fabricante	
Haxx	
Productos afectados	
Libcurl desde la versión 7.62.0 hasta la 7.70.0. cURL desde la versión 7.20.0 hasta la 7.70.0.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00254-01/	
https://www.csirt.gob.cl/media/2020/06/9VSA20-00254-01.pdf	

CSIRT advierte vulnerabilidad de protocolo NTP obtenido de la Universidad de Delaware	
Alerta de seguridad cibernética	9VSA20-00255-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Junio de 2020
Última revisión	26 de Junio de 2020
CVE	
CWE-401	
Fabricante	
Delaware	
Producto afectado	
Asociados que usen autenticación CMAC a través de los ntpd entre las versiones 4.2.8p11/4.3.97 y 4.2.8p14/4.3.100.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00255-01/	
https://www.csirt.gob.cl/media/2020/06/9VSA20-00255-01.pdf	

CSIRT comparte dos vulnerabilidades y mitigaciones obtenidas de Microsoft para Server y Windows 10	
Alerta de seguridad cibernética	9VSA20-00256-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Julio de 2020
Última revisión	01 de Julio de 2020
CVE	
CVE-2020-1425 - CVE-2020-1457	
Fabricante	
Microsoft	
Productos afectados	
Windows 10 Server	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00256-01/	
https://www.csirt.gob.cl/media/2020/07/9VSA20-00256-01.pdf	

CSIRT comparte mitigaciones liberadas por Huawei para dispositivos P30 y P30 Pro	
Alerta de seguridad cibernética	9VSA20-00257-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Julio de 2020
Última revisión	01 de Julio de 2020
CVE	
CVE-2020-1836	
Fabricante	
Huawei	
Producto afectado	
Huawei P30 versiones anteriores a la 10.1.0.160(C00E160R2P11). Huawei P30 Pro versiones anteriores a la 10.1.0.160(C00E160R2P8).	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00257-01/	
https://www.csirt.gob.cl/media/2020/07/9VSA20-00257-01.pdf	

CSIRT comparte una vulnerabilidad y mitigación obtenida de Mozilla para explorador web iOS	
Alerta de seguridad cibernética	9VSA20-00258-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Julio de 2020
Última revisión	01 de Julio de 2020
CVE	
CVE-2020-12414	
Fabricante	
Mozilla	
Producto afectado	
Huawei P30 versiones anteriores a la 10.1.0.160(C00E160R2P11). Huawei P30 Pro versiones anteriores a la 10.1.0.160(C00E160R2P8).	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00258-01/	
https://www.csirt.gob.cl/media/2020/07/9VSA20-00258-01.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
185.202.102.235	Port Scan	192.241.222.239	Port Scan
192.241.219.133	Port Scan	192.241.224.111	Port Scan
45.143.220.110	Port Scan	192.241.195.50	Port Scan
192.241.201.87	Port Scan	67.43.4.85	Port Scan
51.15.20.26	Port Scan	185.200.118.53	Port Scan
148.72.158.240	Port Scan	181.72.59.89	DDoS
192.241.234.142	Port Scan	173.252.100.25	Port Scan
5.2.78.43	Malware	117.34.127.40	Port Scan
192.241.236.184	Port Scan	45.148.121.43	Port Scan
192.241.234.58	Port Scan	37.49.230.247	Port Scan
188.173.246.76	Port Scan	207.180.231.54	Port Scan
211.222.16.89	Port Scan	192.241.227.138	Port Scan
192.241.233.249	Port Scan	192.241.224.122	Port Scan
192.241.236.149	Port Scan	192.241.229.141	Port Scan
192.241.234.238	Port Scan	192.241.229.60	Port Scan
192.241.225.64	Port Scan	192.241.229.77	Port Scan
161.97.74.222	Port Scan	192.241.227.222	Port Scan
192.241.224.96	Port Scan	223.26.31.221	Port Scan
192.241.227.246	Port Scan	192.241.217.216	Port Scan
199.127.63.79	Port Scan	68.183.229.108	Port Scan
192.241.224.235	Port Scan	192.241.230.12	Port Scan
45.143.220.32	Port Scan	192.241.219.143	Port Scan
192.241.214.44	Port Scan	192.241.227.29	Port Scan
103.145.12.176	Port Scan	45.58.138.178	Port Scan
80.82.64.106	Port Scan	45.143.220.130	Port Scan
31.13.115.129	Port Scan	185.200.118.67	Port Scan
31.13.115.130	Port Scan	199.231.184.43	Port Scan
31.13.115.134	Port Scan	185.183.96.217	Malware
23.111.137.194	Port Scan	45.148.10.67	Port Scan
104.128.65.63	Port Scan	157.52.193.114	Spam

202.101.173.147	Port Scan	212.129.47.91	Hacking
202.101.173.148	Port Scan	164.52.24.169	Hacking
128.14.180.218	Port Scan	199.191.50.188	Hacking
190.160.184.206	DDoS	185.200.118.45	Port Scan
209.159.158.85	Port Scan	192.241.228.14	Port Scan
192.241.211.133	Port Scan	94.102.51.75	Port Scan
192.241.230.227	Port Scan	192.241.230.178	Port Scan
192.241.230.216	Port Scan	156.96.128.162	Port Scan
45.143.220.115	Port Scan	51.15.20.26	Port Scan
192.241.225.122	Port Scan	51.159.88.179	Port Scan
192.241.224.106	Port Scan	192.241.228.205	Port Scan
192.241.219.195	Port Scan	61.19.54.165	Port Scan
49.238.142.29	Port Scan	192.241.214.170	Port Scan
192.241.192.224	Port Scan	190.217.1.149	Malware
45.91.225.107	Port Scan	192.241.219.218	Port Scan
192.241.212.152	Port Scan	104.131.58.148	Port Scan
62.210.188.206	Port Scan	159.203.124.114	Port Scan
178.128.162.208	Port Scan	62.210.89.207	Port Scan
192.241.222.5	Port Scan	192.241.193.188	Port Scan
192.241.225.212	Port Scan	37.49.224.26	Port Scan
192.241.227.241	Port Scan	45.143.220.74	Port Scan
192.241.222.45	Port Scan	192.241.217.150	Port Scan
185.56.81.52	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.

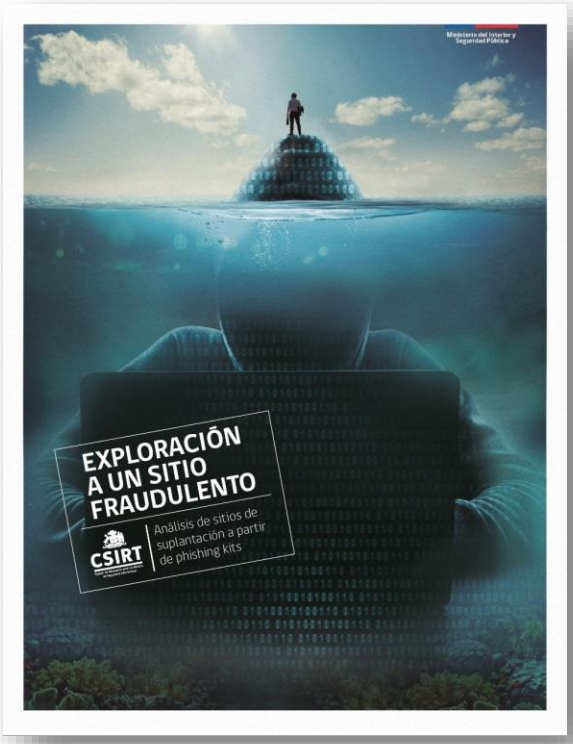
Investigación

Exploración a un sitio Fraudulento. Análisis de sitios de suplantación a partir de phishing kits

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la décima edición de su publicación sobre amenazas cibernéticas el que analiza los phishing kits utilizados para crear sitios de suplantación. Este artículo fue elaborado por Paula Moraga Montero, analista de nivel 2 de CSIRT.

La creación de sitios fraudulentos aumenta en correlación con los ataques de phishing, y con ello las víctimas, que no solo se pueden contar entre las personas que son dirigidas a los sitios fraudulentos, sino también entre las entidades que son suplantadas. Esta investigación trata de enfocarse en un elemento que es fundamental para facilitar el accionar de los cibercriminales: los phishing kits, o el conjunto de archivos que permiten que un sitio fraudulento pueda ser creado y operado. En este conjunto de archivos se encuentra el elemento que nutre un ataque de phishing.

Este trabajo hace referencia a la forma en que cibercriminales pueden obtener estos archivos y cómo se estructuran, así como de la simpleza para imitar lo elementos de un sitio web original. La investigación se completa con un análisis a dos phishing kit, para entender su composición y organización. Uno de ellos, es obtenido de un sitio con fines didácticos, el otro, corresponde a una muestra obtenida de un phishing real.



Ver en: https://www.csirt.gob.cl/reportes/an2-2020-10/

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.

- Claudio Miranda
  Linkedin:
  https://www.linkedin.com/in/claudio-alejandro-miranda-mu%C3%B1oz-56889144/
- Julián Palacios
  Linkedin:
  https://www.linkedin.com/in/julian-palacios-analista-prog/
- Camilo Orellana
  Linkedin:
  https://www.linkedin.com/in/camilo-esteban-orellana-diaz-403278a6/
- Jair Palma
  Linkedin: https://www.linkedin.com/in/jair-palma-vicenty-62038920/

CSIRT Gobierno de Chile