15-10-2020 | Año 2 | N°67

Boletín de Seguridad Cibernética

Semana del 08 al 14 de Octubre de 2020

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

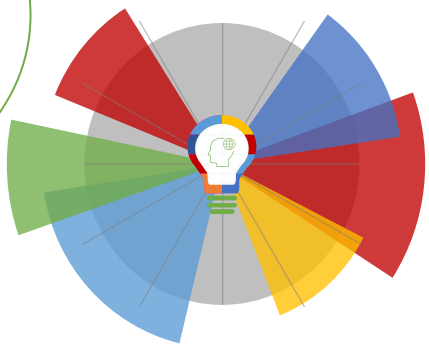
División de Redes y Seguridad Informática.
Gobierno de Chile

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Resumen de la semana en cifras

Hash
39
Sha 256
Asociadas a múltiples campañas de phishing son archivos que contienen malware

Se advirtieron
27
URLs
Asociadas a sitios fraudulentos y múltiples campañas de phishing y malware



Parches
88
para vulnerabilidades
Las mitigaciones son útiles para productos Cisco.

IPs
52
Informadas
Listado de IPs advertidas en múltiples campañas de phishing y de malware.

*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 informa de sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00789-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Octubre de 2020
Última revisión	08 de Octubre de 2020
Indicadores de compromiso	
URL	
porthealthpharmasave[.]com/www[.]bancoestado[.]cl/pagina/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
199[.]27[.]180[.]181	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00789-01/	
https://www.csirt.gob.cl/media/2020/10/8FFR20-00789-01.pdf	

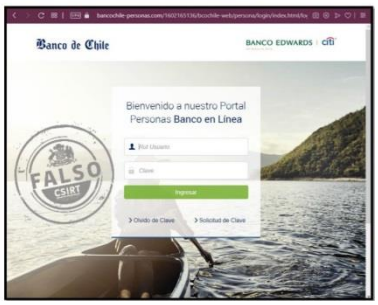
Imagen del sitio

CSIRT informa suplantación sitio bancario	
Alerta de seguridad cibernética	8FFR20-00790-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Octubre de 2020
Última revisión	08 de Octubre de 2020
Indicadores de compromiso	
URL	
santanndermovil[.]link/1602101007/personas/index[.]asp	
IP	
162[.]0[.]232[.]252	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00790-01/	
https://www.csirt.gob.cl/media/2020/10/8FFR20-00790-01.pdf	

Imagen del sitio

CSIRT advierte página de banco falsa	
Alerta de seguridad cibernética	8FFR20-00791-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Octubre de 2020
Última revisión	08 de Octubre de 2020
Indicadores de compromiso	
URL	
www[.]phone-experts[.]at/_personas/www[.]bancoestado[.]cl/pagina/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
77[.]244[.]243[.]53	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00791-01/	
https://www.csirt.gob.cl/media/2020/10/8FFR20-00791-01.pdf	

Imagen del sitio



CSIRT advierte de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00792-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Octubre de 2020
Última revisión	08 de Octubre de 2020
Indicadores de compromiso	
URL	
bancochile-personas[.]com	
IP	
162[.]214[.]160[.]59	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00792-01/	
https://www.csirt.gob.cl/media/2020/10/8FFR20-00792-01.pdf	

Imagen del sitio

CSIRT advierte de sitio bancario falso	
Alerta de seguridad cibernética	8FFR20-00793-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Octubre de 2020
Última revisión	09 de Octubre de 2020
Indicadores de compromiso	
URL	
santanndermovil[.]biz	
IP	
162[.]0[.]235[.]11	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00793-01/	
https://www.csirt.gob.cl/media/2020/10/8FFR20-00793-01.pdf	

Imagen del sitio

CSIRT advierte suplantación de página de streaming	
Alerta de seguridad cibernética	8FFR20-00794-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Octubre de 2020
Última revisión	09 de Octubre de 2020
Indicadores de compromiso	
URL	
www[.]netflix22[.]com	
IP	
209[.]85[.]234[.]121	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00794-01/	
https://www.csirt.gob.cl/media/2020/10/8FFR20-00794-01.pdf	

Imagen del sitio

CSIRT informa de sitio falso de plataforma de almacenamiento	
Alerta de seguridad cibernética	8FFR20-00795-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Octubre de 2020
Última revisión	09 de Octubre de 2020
Indicadores de compromiso	
URL	
appleverificationalert[.]com	
IP	
35[.]164[.]12[.]178	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00795-01/	
https://www.csirt.gob.cl/media/2020/10/8FFR20-00795-01.pdf	

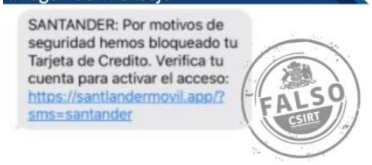
Imagen del sitio

CSIRT advierte de sobre sitio de suplantación bancario	
Alerta de seguridad cibernética	8FFR20-00796-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de Octubre de 2020
Última revisión	12 de Octubre de 2020
Indicadores de compromiso	
URL	
https[:]//santaandermovil[.]xyz/1602345690/personas/index[.]asp	
IP	
199.188.201.85	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00796-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00772-01.pdf	

CSIRT advierte de sitio de pagos online fraudulento	
Alerta de seguridad cibernética	8FFR20-00797-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Octubre de 2020
Última revisión	13 de Octubre de 2020
Indicadores de compromiso	
URL	
Urls sitio falso http[:]//da822325-313f-4f85-b334-d9b00a2d64da[.]htmlcomponentservice[.]com/get_draft?id=da8223_943e1deadfc8b224198f3740580b37aa[.]html	
IP	
64[.]233[.]191[.]121	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00797-01/	
https://www.csirt.gob.cl/media/2020/10/8FFR20-00797-01.pdf	

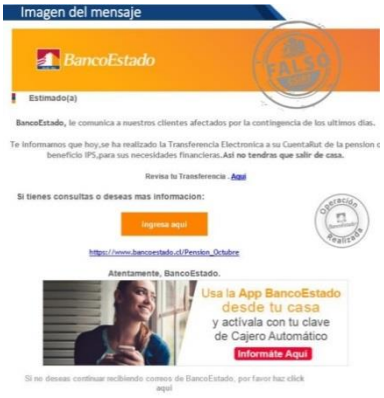
Phishing

Imagen del mensaje



CSIRT advierte de smishing bancario por bloqueo de tarjeta	
Alerta de seguridad cibernética	8FPH20-00313-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Octubre de 2020
Última revisión	07 de Octubre de 2020
Indicadores de compromiso	
URL	
Hxxps[:]//santlandermovil[.]app/?sms=Santander	
Hxxps[:]//bancosaander-movil[.]link/1602628985/personas/index[.]asp	
IP	
162[.]0[.]235[.]9	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00313-01/	
https://www.csirt.gob.cl/media/2020/10/8FPH20-00313-01.pdf	

Imagen del mensaje



CSIRT advierte phishing bancario por transferencia de beneficios social	
Alerta de seguridad cibernética	8FPH20-00314-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Octubre de 2020
Última revisión	14 de Octubre de 2020
Indicadores de compromiso	
URL	
https://bit[.]ly/3lBAUFQ?l=www.bancoestado.cl	
https[:]//www.phone-experts[.]at/dir/www.bancoestado.cl/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
77.244.243.53	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00314-01/	
https://www.csirt.gob.cl/media/2020/10/8FPH20-00314-01.pdf	

Vulnerabilidades

CSIRT comparte actualizaciones liberadas por Microsoft	
Alerta de seguridad cibernética	9VSA20-00302-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Octubre de 2020
Última revisión	14 de Octubre de 2020

CVE

ADV200012	CVE-2020-16928	CVE-2020-16942
CVE-2020-16889	CVE-2020-16929	CVE-2020-16947
CVE-2020-16896	CVE-2020-16930	CVE-2020-16949
CVE-2020-16897	CVE-2020-16931	CVE-2020-16954
CVE-2020-16901	CVE-2020-16932	CVE-2020-16955
CVE-2020-16904	CVE-2020-16933	CVE-2020-16957
CVE-2020-16914	CVE-2020-16934	CVE-2020-16969
CVE-2020-16918	CVE-2020-16937	CVE-2020-16995
CVE-2020-16919	CVE-2020-16938	
CVE-2020-16921	CVE-2020-16941	

Vulnerabilidades adicionales informadas

CVE-2020-0764	CVE-2020-16905	CVE-2020-16944
CVE-2020-1047	CVE-2020-16907	CVE-2020-16945
CVE-2020-1080	CVE-2020-16908	CVE-2020-16946
CVE-2020-1167	CVE-2020-16909	CVE-2020-16948
CVE-2020-1243	CVE-2020-16910	CVE-2020-16950
CVE-2020-16863	CVE-2020-16911	CVE-2020-16951
CVE-2020-16876	CVE-2020-16912	CVE-2020-16952
CVE-2020-16877	CVE-2020-16913	CVE-2020-16953
CVE-2020-16885	CVE-2020-16915	CVE-2020-16956
CVE-2020-16886	CVE-2020-16916	CVE-2020-16967
CVE-2020-16887	CVE-2020-16920	CVE-2020-16968
CVE-2020-16890	CVE-2020-16922	CVE-2020-16972
CVE-2020-16891	CVE-2020-16923	CVE-2020-16973
CVE-2020-16892	CVE-2020-16924	CVE-2020-16974
CVE-2020-16894	CVE-2020-16927	CVE-2020-16975
CVE-2020-16895	CVE-2020-16935	CVE-2020-16976
CVE-2020-16898	CVE-2020-16936	CVE-2020-16977
CVE-2020-16899	CVE-2020-16939	CVE-2020-16978
CVE-2020-16900	CVE-2020-16940	CVE-2020-16980
CVE-2020-16902	CVE-2020-16943	CVE-2020-17003

Fabricante

Microsoft

Productos afectados

3D Viewer
Adobe Flash Player
Azure Functions
Dynamics 365 Commerce
Microsoft .NET Framework
0 Service Pack 2

5
5 y 4.6.2/4.7/4.7.1/4.7.2
5 y 4.6/4.6.1/4.6.2
5 y 4.7.1/4.7.2
5 y 4.7.2
5 y 4.8
5.1
5.2
6
6/4.6.1/4.6.2/4.7/4.7.1/4.7.2
8
Microsoft 365 Apps for Enterprise (32-bit y 64-bit)
Microsoft Dynamics 365 (on-premises) version 8.2 y 9.0
Microsoft Excel
2010 Service Pack 2 (32-bit y 64-bit)
2013 RT Service Pack 1
2013 Service Pack 2 (32-bit y 64-bit)
2016 (32-bit y 64-bit)
Microsoft Excel Web App 2010 Service Pack 2
Microsoft Exchange Server
2013 Cumulative Update 23
2016 Cumulative Update 17
2016 Cumulative Update 18
2019 Cumulative Update 6
2019 Cumulative Update 7
Microsoft Office
2010 Service Pack 2 (32-bit y 64-bit editions)
2013 Click-to-Run (C2R) (32-bit y 64-bit editions)
2013 RT Service Pack 1
2013 Service Pack 1 (32-bit y 64-bit editions)
2016 (32-bit y 64-bit editions)
2016 for Mac
2019 (32-bit y 64-bit editions)
2019 for Mac
Online Server
Web Apps 2013 Service Pack 1
Web Apps 2010 Service Pack 2
Microsoft Outlook
2010 Service Pack 2 (32-bit y 64-bit editions)
2013 RT Service Pack 1
2013 Service Pack 1 (32-bit y 64-bit editions)
2016 (32-bit y 64-bit editions)
Microsoft SharePoint
Enterprise Server 2013 Service Pack 1
Enterprise Server 2016
Foundation 2010 Service Pack 2
Foundation 2013 Service Pack 1
Server 2010 Service Pack 2
Server 2019
Microsoft Word
2010 Service Pack 2 (32-bit y 64-bit editions)

2013 RT Service Pack 1 2013 Service Pack 1 (32-bit y 64-bit editions) 2016 (32-bit y 64-bit editions) Network Watcher Agent virtual machine extension for Linux PowerShellGet 2.2.5 Visual Studio Code Windows 10 (32-bit y 64-bit) Version 1607, 1709, 1803, 1809, 1903, 1909, 2004, para 32 bit, 64 bit y ARM64-based Windows 7 32-bit Systems Service Pack 1 x64-based Systems Service Pack 1 Windows 8.1 32-bit systems x64-based systems Windows RT 8.1 Windows Server 2008 32-bit Systems Service Pack 2 32-bit Systems Service Pack 2 (Server Core installation) x64-based Systems Service Pack 2 x64-based Systems Service Pack 2 (Server Core installation) R2 for x64-based Systems Service Pack 1 R2 for x64-based Systems Service Pack 1 (Server Core installation) Windows Server 2012 2012 Server Core installation R2 y R2 (Server Core installation) Windows Server 2016 2016 Server Core installation Windows Server 2019 2019 Server Core installation Windows Server version 1903 (Server Core installation) version 1909 (Server Core installation) version 2004 (Server Core installation)
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00302-01/
https://www.csirt.gob.cl/media/2020/10/9VSA20-00302-01.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.
CSIRT recomienda a los administradores y usuarios bloquear los hash publicados en este informe, y mantener un permanente monitoreo sobre el resto de los Indicadores de Compromiso.

Hash reportados (se recomienda bloquear)

25b871c94fcc1825b19de313875a06512f650480b6623ec678dee76732c52e0b	e6656ed1edab164c4265d570612ec29b3b6cf3ba3dece150fd79b6c72eae5915
9448ce645e7ef7b92ff30c17421ed56b4f3bbe4fce2b4628a48b3cfa8ed02ac7	2c625a1699cdcee6b7e861b1efac690e1b8ee1b2e3c48531c114f51c26cff0d2
d5a68a111c359a22965206e7ac7d602d92789dd1aa3f0e0c8d89412fc84e24a5	b39fcf25539085d53a8b25521c1575252fc848d771f07c6a47b301ddd0de8eb0
c76a517fd1250e77c7bd26fe7223022d0e71bb2e75e3ca5c482face6185f1dc4	946bf30ffb29a1059ae80c7e097b0de738bebd31f464fb6b49e90e1ccc896ddb
951056d1e8f319981af056a90c40242d9395e15514b1b1fd21b9195ecca86cf7	6aa6dd4f298a8a76d5fab78b73d4f6cad58a2433dfea5cc8c73e6843beb55fb2
b8bd6daac2cd0522341b9ff441e1e2de2743cf81a5be741b85ada3ed846a44ab	f312e194afb25bbe4a19df14123d1943d11f6157322f6cfc6a8652debe57cb01
986d13ef556fa85418e10e1d257128863978b00fdd6f472d7ea562fdb934fde5	2cf0dd02b4ac5b4a4eb95e478c1e145f0434764848f7d553620a139e5592e768
2e2fdc459173a51caa1daf9e0ebb7fbfde276af0c0475e0976fc765f0c41a496	4305a26fa817354b7d255344e4f38a4ffa90dd777e2b2d36fbd1474a5948f082
98b8260952aab2ef1951e2d44220099cbb7d9f41e6ae02d24263b37eb4f1940e	b880aa0040b5f386b895c23af6b05c18473eb9db95ec3942e713fc454c6f4cef
e12c89c9008e11dc9aa6a149891d1fb3fbd3ee36b3f8bac80678501ef84b55ea	baa4377dd7c181c1972988831c2937f2b580c824001330acf0ca30a2fbf6c629
a64a09207ffc6026ce5328160b8f03896fcf99591d9412882073b871e074e422	2cc4dd8780ab90a62026b5a0a1f381f8f85ea4c95b7d9ded566c11def61abadc
754043513b719af4582157adb569baa9b9576db59c2044360c1cfd64c55be667	02125959734adf9a58e54d61f5f552653d516427221e9cacd06fe64764afbfd6
707801ccfb066a8838ababb07c44745055f848a670c4bf5daa2cfbb5b26f0a76	587b89a514b829530288000449bcbcc41ab09583a07d1a88bc7f4b039d6318a4
fa6e36ba51f502c55fe5f336911f3b6ceb01c71b8dff340add249982a20d74ec	1ff7fe031157a4aa850e07c245724cb4b195b180027a60e672dd38964972255a
064adbd5640ef3fda23824886ee23921c5a3e50d8e7a2906bdd636e1c982aa9a	c47b8924773dd748e6368815239ac9ddba31aaf0d4ce309edf74427137ef61d5
bf8ee01a9c299fdfaa7fa6f61e9e04bb31b5f56300c4570228e524796c8a45ab	40a0260a9aa72cb24c10efec5a8715c35a647b5b580a64a6672acdf3ecd44280
4e2c7d269a6ac0822ab6f3045c0352299c4cc28a7cb08bcb3d1fd3bcfed4d7aa	7397def823ca9bcfdb5fd0de99d9a21b4d8673041883877e52753ba3186d1538
9cdefce35cdb78bfad530dc47d20a2497159cfaff4df8e163843ece18a16396c	3afb8b0d508b9c991684aca6b9a84832947be2e6e4cf5bf4ab56ad279a729c4c
a1c53669a74c641f7a0eed1bbec5529242618aa390c71a3072d430a21d3fee06	dade6e39f4c9cdabbb12d2b5216fa5a1a84a2d375074484d57a728997cc372d4
b8f2d69f5d20a8093f4818f97e7132a4f3f2c13efe56bde8c964e774476a81ba	

Archivos reportados (se recomienda mantener en monitoreo)

64.188.9.85	66.146.0.201	210.56.11.43
108.179.219.57	41.221.32.207	47.88.189.81
156.96.156.196	51.75.202.197	212.39.90.97
5.206.224.7	65.254.254.80	185.222.57.174
45.153.242.51	199.168.188.91	94.46.167.170
37.187.67.12	109.205.64.52	193.23.127.34
103.114.106.7	64.69.218.92	185.19.185.40
83.167.244.173	184.106.54.106	185.222.57.174
156.96.44.206	109.205.64.59	185.222.57.81
23.251.226.1	89.40.4.85	159.89.173.209
37.49.225.235	202.66.174.108	196.46.192.26
23.251.226.2	66.84.15.151	210.134.165.80
23.251.226.4	202.66.173.167	185.222.57.73
23.251.226.6	185.222.57.234	

URL

hxxp://savetheboom[.]com/admin_access/xht/
hxxps://dakwahwisata[.]net/wp-admin/c/
hxxps://popcornv[.]com/wp-includes/KHKX/
hxxps://dusitserve[.]com/gethits/o3A/
hxxps://asc-kl[.]com/v2/Ztf/
hxxp://gaashaan[.]com/cgi-bin/O/
hxxp://inmaainv[.]com/site/cLDOJFI/
hxxp://wynn838[.]com/wp-content/ZhG/
hxxp://ladsbarbearia[.]com/wp-content/PI/
hxxp://syracusecoffee[.]com/customer/jf/
hxxps://mrveggy[.]com/erros/PO/
hxxp://givingthanksdaily[.]com/5Q/
hxxp://buesink[.]com/Pics-shower/ScE/
hxxp://hottco[.]com/stats/lX/

Actualidad

Ciberconsejos para guiar a la 3era edad en la era digital

Las tecnologías de la información nos permiten seguir conectados para seguir adelante con nuestras vidas, pero de forma virtual. Sin embargo, para nuestros adultos mayores, acostumbrados a sistemas análogos, el salto digital ha sido un poco más complicado y muchos de ellos necesitan de consejos y asistencia para superar las barreras del uso de las tecnologías. Tenemos que ser solidarios con ellos. ¿Cómo acompañar y guiar a la tercera edad en este proceso de cambio?

Ver más: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-guiar-a-la-3era-edad-en-la-era-digital/

Ciberconsejos de seguridad para Pymes

Las amenazas cibernéticas pueden afectar tanto a grandes como a pequeñas y medianas empresas. El problema, es que en ocasiones, la ciberseguridad no es considerada como un pilar fundamental en algunas organizaciones. Sin embargo, el no contar con mínimas medidas de seguridad puede traer como consecuencia el robo o pérdida de información de los clientes e incluso la infección de los equipos con algún malware.

Para contribuir en la prevención, en este Mes de la Ciberseguridad, CSIRT desarrolló la campaña Pymes Seguras con recomendaciones para proteger los datos de los ciberdelincuentes.

Ver más: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-de-seguridad-para-pymes/

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.

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.

- Nicolle Bravo
- Cristóbal Kurte
- Rafael Santibáñez
- Cristóbal Herrera
- Gonzalo Ramírez

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.10.16 12:13:32 -03'00'