CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

10-12-2020 | Año 2 | N°75

Boletín de Seguridad Cibernética

Semana del 03 al 09 de Diciembrede 2020

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

262

Sha 256

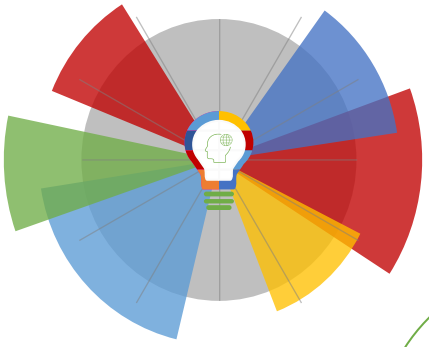
Asociadas a múltiples campañas de phishing son archivos que contienen malware

Se advirtieron

5

URLs

Asociadas a sitios fraudulentos y campañas de phishing



Parches

69

para vulnerabilidades

Las mitigaciones son útiles para productos Thunderbird, VMware, Google Chrome, Drupal y Microsoft.

IPs

89

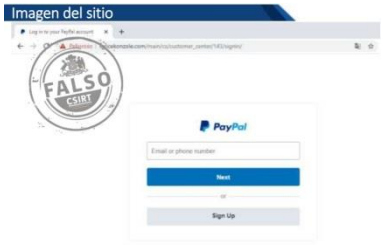
Informadas

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



CSIRT informa de sitio de pago en línea fraudulento	
Alerta de seguridad cibernética	8FFR20-00843-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Diciembre de 2020
Última revisión	09 de Diciembre de 2020
Indicadores de compromiso	
URL	
http://www.igricekonzole[.]com/main/cs/customer_center/143/signin/	
IP	
[192.185.119.38]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00843-01/	
https://www.csirt.gob.cl/media/2020/12/8FFR20-00843-01.pdf	

Phishing

Imagen del mensaje

CSIRT informa phishing de supuesta operación irregular	
Alerta de seguridad cibernética	8FPH20-00330-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Diciembre de 2020
Última revisión	07 de Diciembre de 2020
Indicadores de compromiso	
URL	
https[:]//santander.logincl[.]online/	
IP	
[34.94.19.208]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00333-01/	
https://www.csirt.gob.cl/media/2020/12/8FPH20-00333-01.pdf	

Imagen del mensaje

CSIRT advierte phishing por cierre de cuenta	
Alerta de seguridad cibernética	8FPH20-00334-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Diciembre de 2020
Última revisión	07 de Diciembre de 2020
Indicadores de compromiso	
URL	
https://bit[.]ly/2JWg06Y?l=www.bancoestado.cl	
http://mobilewifi.rs/wn/www.bancoestado.cl/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[213.190.161.151]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00334-01/	
https://www.csirt.gob.cl/media/2020/12/8FPH20-00334-01-2.pdf	

CSIRT advierte phishing con falso programa de gobierno	
Alerta de seguridad cibernética	8FPH20-00335-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Diciembre de 2020
Última revisión	09 de Diciembre de 2020
Indicadores de compromiso	
URL	
https://programatarjetafamilia.org/	
IP	
[216.246.112.173]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00335-01/	
https://www.csirt.gob.cl/media/2020/12/8FPH20-00335-01.pdf	

Vulnerabilidades

CSIRT comparte mitigación para vulnerabilidad de Thunderbird	
Alerta de seguridad cibernética	9VSA20-00329-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Diciembre de 2020
Última revisión	03 de Diciembre de 2020
CVE	
CVE-2020-26970	
Fabricante	
Thunderbird	
Productos afectados	
La vulnerabilidad afecta al cliente de correo Thunderbird desde la versión 78.5.0 hacia atrás.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00329-01/	
https://www.csirt.gob.cl/media/2020/12/9VSA20-00329-01.pdf	

CSIRT comparte vulnerabilidad obtenida de VMware	
Alerta de seguridad cibernética	9VSA20-00330-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Diciembre de 2020
Última revisión	03 de Diciembre de 2020
CVE	
CVE-2020-4006	
Fabricante	
VMware	
Productos afectados	
Workspace One Access 20.10 y 20.01 para Linux. Identity Manager 3.3.3, 3.3.2 y 3.3.1 para Linux. Identity Manager Connector 3.3.2 y 3.3.1 para Linux. Identity Manager Connector 3.3.3, 3.3.2 y 3.3.1 para Windows.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00330-01/	
https://www.csirt.gob.cl/media/2020/12/9VSA20-00330-01.pdf	

CSIRT comparte mitigación para vulnerabilidad de Drupal	
Alerta de seguridad cibernética	9VSA20-00331-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Diciembre de 2020
Última revisión	03 de Diciembre de 2020
CVE	
CVE-2020-28948 - CVE-2020-28949	
Fabricante	
Drupal	
Productos afectados	
Drupal desde la versión 9.0.9 hasta la 9.0, desde la 8.9.9 hasta la 8.9, desde la 8.8.11 hasta la 8.8 y anteriores, y desde la 7.74 hasta la 7 y anteriores.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00330-01/	
https://www.csirt.gob.cl/media/2020/12/9VSA20-00331-01.pdf	

CSIRT comparte mitigaciones para vulnerabilidad de Google Chrome	
Alerta de seguridad cibernética	9VSA20-00332-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Diciembre de 2020
Última revisión	03 de Diciembre de 2020
CVE	
CVE-2020-16037 - CVE-2020-16038 - CVE-2020-16039 CVE-2020-16040 - CVE-2020-16041 - CVE-2020-16042	
Fabricante	
Google	
Productos afectados	
Google Chrome versiones anteriores a la 87.0.4280.88 en Windows, Linux y Mac.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00332-01/	
https://www.csirt.gob.cl/media/2020/12/9VSA20-00332-01.pdf	

CSIRT comparte actualizaciones de vulnerabilidades de Microsoft	
Alerta de seguridad cibernética	9VSA20-00333-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Diciembre de 2020
Última revisión	03 de Diciembre de 2020

CVE

CVE-2020-16996 - CVE-2020-17124 - CVE-2020-17142
CVE-2020-17094 - CVE-2020-17125 - CVE-2020-17143
CVE-2020-17095 - CVE-2020-17126 - CVE-2020-17144
CVE-2020-17096 - CVE-2020-17127 - CVE-2020-17147
CVE-2020-17098 - CVE-2020-17128 - CVE-2020-17148
CVE-2020-17099 - CVE-2020-17129 - CVE-2020-17152
CVE-2020-17115 - CVE-2020-17130 - CVE-2020-17153
CVE-2020-17119 - CVE-2020-17132 - CVE-2020-17156
CVE-2020-17120 - CVE-2020-17133 - CVE-2020-17158
CVE-2020-17121 - CVE-2020-17138 - CVE-2020-17160
CVE-2020-17122 - CVE-2020-17140 - CVE-2020-17123
CVE-2020-17141

Vulnerabilidades adicionales informadas:

ADV200013 - CVE-2020-17002 - CVE-2020-17135
CVE-2020-16958 - CVE-2020-17089 - CVE-2020-17136
CVE-2020-16959 - CVE-2020-17092 - CVE-2020-17137
CVE-2020-16960 - CVE-2020-17097 - CVE-2020-17139
CVE-2020-16961 - CVE-2020-17103 - CVE-2020-17145
CVE-2020-16962 - CVE-2020-17117 - CVE-2020-17150
CVE-2020-16963 - CVE-2020-17118 - CVE-2020-17159
CVE-2020-16964 - CVE-2020-17131 - CVE-2020-16971
CVE-2020-17134

Fabricante

Microsoft

Productos afectados

Azure DevOps Server
2019 Update 1.1
0.1
2020
Azure SDK for Java
Azure Sphere
C SDK for Azure IoT
ChakraCore
Dynamics 365 for Finance and Operations
Microsoft 365 Apps for Enterprise (para sistemas 32-bit y 64-bit)
Microsoft Dynamics 365 (on-premises) versiones 8.2 y 9.0
Microsoft Dynamics NAV 2015
Microsoft Edge (EdgeHTML-based)
Microsoft Edge for Android
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 Exchange Server
2010 Service Pack 3 Update Rollup 31
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)
2016 (32-bit y 64-bit editions)
2019 (32-bit y 64-bit editions)
2019 for Mac
Online Server
Web Apps 2010 Service Pack 2
Web Apps 2013 Service Pack 1
Microsoft Outlook
2010 Service Pack 2 (32-bit y 64-bit)
2013 RT Service Pack 1
2013 Service Pack 1 (32-bit y 64-bit)
2016 (32-bit y 64-bit)
Microsoft PowerPoint
2010 Service Pack 2 (32-bit y 64-bit)
2013 RT Service Pack 1
2013 Service Pack 1 (32-bit y 64-bit)
2016 (32-bit y 64-bit)
Microsoft SharePoint
Enterprise Server 2016
Foundation 2010 Service Pack 2
Foundation 2013 Service Pack 1
Server 2010 Service Pack 2
Server 2019
Microsoft Visual Studio
2017 version 15.9 (includes 15.0 – 15.8)
2019 version 16.0
2019 version 16.4 (includes 16.0 – 16.3)
2019 version 16.7 (includes 16.0 – 16.6)
2019 version 16.8
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)
Office Online Server
Team Foundation Server
2015 Update 4.2
2017 Update 3.1
2018 Update 1.2
2018 Update 3.2

Visual Studio Code Language Support for Java Extension Remote – SSH Extension TS-Lint Extension Windows 10 (32-bit y 64-bit) Version 1607, 1709, 1803, 1809, 1903, 1909, 2004, 20H2, 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) version 20H2 (Server Core installation)
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00333-01/
https://www.csirt.gob.cl/media/2020/12/9VSA20-00333-01.pdf

IoC - Malware

A continuación, se comparten los Indicadores de Compromisos que fueron detectados durante la semana pasada por el Equipo del CSIRT.
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 de archivos maliciosos

20e49601d3c3f811584cd3f9a4adc6f72b8f007cd81ab6ac9f2d13e4fc1409ee	7f64b55a15ab71a87d0a0b4ecf6501a481bf38993086dc147b762a35998bb335
356eb3c03cb41d52634744186249d60dc809d1fb16d03b99e5a3b5a8eb056f0a	c4067ab8587a745baded7185f8251d2903000eb0b5086d59e20abdbdbf5c3cdf
25be9bae7867c044eacdbc37da12a4e695f753dc5ba80a20f002f46658167ff3	bc9c106b7c6f368b67928c5c2816950a87c4740888084ff979d18ad827f035dc
3107b12be468882524367760b47673a5f8239f1b833d02379486583ae010b2da	68dfa8b97cf4c154144c8b22699299baa9268a4e99d244e390ec0e631e90c118
832c0dd17cdf0e06d2084cdb17df2281718e49f043972edfb2186678741fab8d	3273929750b6275aaab083c9d1447b02ca2daec64103ad625c245ca3d0df72a3
3b8599823538e250751d035244c594d277b73e461f0b56dec5da071d994a757a	87cec7157fbc1ae1a93084c75617e9d7f7f7f38bb3933d9c80ee40cf9bcb3ea9
4a5b45c05af823c7a950a5043164c64fb7a07a3f2d4dcc19ae131e0b90eaee1d	8a94ad4994026dcc0b21689ae9d7117d3a669ca4f72587790bca1d57828ae5f6
86aa4147a3b2051ed62ce861aded30843e89ef24e9666b76150d09fa699d4ce0	b99b976c72d127f4e9ad07b28370bfd82f7b83b8ac2ff2e90bdc33078df7994e
07371b9cba8eb2248cc9cb5c0a6818236c544149fdb70ef3ffc9965eb596b034	8ac3d76ca3ec0ed1159e6cb730640ca011a8b34d9c8f6e23b8c4144b6001664c
a536c4c6c0f003f1303076a10b1a83dab5e59ad2332cd42fb841ff0ff3024d6c	268b776e09ac5b5046d52d378535a09e0ae697206f7a876dc7b968652031d915
c66e04998c8482195f75fa15a53a1e849c04f98bba2a6a668157410463818cd3	f1a8f60b5c0d0f27a96ae964ae128a2b0dac1b41565fcbff1dc0e1c1388e81b6
80028712c0edab8e54e6d2d4a3c7d62fc4bde0d286c2289e7d47e17cf781ca65	083d123a88baae5297d7bd9502996c1e9d3099fd5bc0c49e9ab15e63af95e2cf
55e57003e341d3c9062f52cf1d556dab89c37eaed6198650a452fcd2b8a6cf57	fc8603ed398ca67e284552d9583873838e9e1ed9630274b5185acf65d0b92f3c
7cae5178159e99dd4124e8b8322345e7138f44dbca732298ca824acffa92891e	5f7a6d3e56100370191ca035130b2a92f4cd0b29a1b0e8d522d96f3509d6ff9a
2ebe22d3f2fddd0ab6c2d7c22c62c3ed52824586501d5b6f3daabdd627d9a3dc	fd6f2e561d29ab419cb23058b6eb83b1e52920223f9b9ec329743d4d835d7cc0
0ceccbcd2c5c50b6964326739dd31b81f6c20803bffdbaee08be69328b421309	f5dec96dd046d6652f635ef153a02adbd0eec3d4162f0d17a1ad198220272120
a76a78a5de712d9307d534e4d2fb4030a099d0d5d9a4d19979e4d7261b6e00f4	708a35ded9723a51b5592a0f01e8fba604a2932412621f8a2119ab5997bd6488
df22bef91bd6e5d09d148ac4a6970542528472dfd5bf9b8e50a12e30fa5ed0fc	a6b3a4cd2ca7a12cb0d9d0ad6295069e2a5e6abcb5db2738b1892cf93f702944
3100c6e502c67b3dfe1f2d4285873e38dd56af5b1b7b183fda7921b72c201065	6d784a18fc1c88be72f1eeb3680d6e538ad183ec575db6755bbd7d6fd9d8cef6
a125f2b7c899bf6ac8fbc97d03048bd0ea20f1a4d8548b35067754f04b0da896	16122ec37d00d139c9a265e07dc2d25f7b3395155e2b59e5411afe3305609211
7b70cb1c42403754d724d3f7d3890c3318894d9b543ebba69cd17e08395be076	093651079b677053b6f7cdd03ce237826d7622dba03fb835a6884241677d16ae
cd4fceff454842324aac2bd956a98a3a0a896a73c792c57f0c5d9e0440c94851	facb7ebe32b4b4e7599013a3bc9e97841317d88d3c7f4020e9deac0b78d84fb4
652705d8f04fa2f2fb97433644bb5397cdef2c9417b3079dd1e41cc7c8f07619	f219222e6f7b05998545007eda7cabf603096c01ba806e70637f6bb67d90c128
4afed815e6df3bacc14f9dcb38986545410526e048b9f54e87ba75aea9e72925	71c38c59c5c34dd9d83233926f3ed26382adc33212ee879d1897b60e4b3f94a8
246571f3e1bd35fe88b902b0bb39313765f7986c27bfc40df4fb21bb5b5c61ee	c8dd925839946efee38a49361b534797cd9852a9af09f15649a416fd19481492
ff6d26a9e1ac8211679d41ef66321ee52b2bc859ac8d6f5c4c5a2d2c63c0f959	df245e812c7c1eef8f74fb5ea8a8229956ee713dea65119930d457491e9a598a
6e15c2d53500ec9e301cdde1086665ad0a81741df49e266fb6a6f2ac4d1b7c98	cde30d29561964f33cc20b1fdca53601226597d933ae67e0e23d7534a7c66e10
72806788cd2d99e46df58805baa0eacd165801f17adb6a1ad6c270778ef07411	6ae002072ff8d8224c7a4c9cdb78d59e3420ee825b45ad5496919b349679efed
6db56233f20a843cc990a7c8899bb7befc6185e4a257a90665399568e4770979	076303408e66936f28b185c55619713bca90eb7f7384283dfc19da7df160badd
914b2613b63f7c8c491c754333dfd6cf12206e43337aa8c44b7b05ef3c3e9e93	6c018708ac2dd05c4162da8957dc713ffdca62b0a589c3b9f23e482c28221008
c03bb8cfa927896e934681bec434f7003ddd411783ba29113708ba1000067f97	e951ea771c36d4eb5074742a2854717ca55a2173500fbc482f44c77557aab4f6
83b64d3526a7247913c079fae316e57e79c1b6a2c7e508effb47c2094c20af06	314aef2e6f2ce6fe6a949400e9105e20858029ae5647166a618d73f863c430d0
6478055748ac89bf856d49e276a3395502004e9c9286429a73b8834bdfd509b0	a0e67e607c494288aa0a60be1f50cd9d22fe478e6507be372d15fbcadb13ce46
92a38e6894e87a65200720942bea58dcaf8d2676436373bbc730dbe350955dec	69aabb7b7dcc041e7f18e6245b55c7fd08c8251b6cd7422552fe5c31b2059d94
10cfc3771ec97ba627cae9f4f8bfea3b00c05010dec08b32e9fe1b8aaf02368b	84de1b4af1f994fdb247051d6391e3fa0426ef826302d2534e4751427662ae3f
499c9e0deb2c7d27b243afee6b0b872d9d66074eb66a0ceafaf2cb7fcc42cfe5	6f285aa796635e35235dbfb8dc812a7dffeaee3f4aecff36d810d883e9b2bbfe
0dbef86453f0f353e6c51b52076e0aaaadf8ddc06798a0fcdfb8ccadfbbb8d1e	b880933ddc28a5cab114d4f2d4590c774ba1c6a326e7660e8d02da39816f38b6

4376dd490accb479b6d98f1c60f63d7b645b8762f81e25b321e7bde66dc3efbf	4933996b18b79868a198ed6f8c3674da0958ef2476d5872b2bc5e7b08d6c93aa
526f4050777b1702ebbe18e28d90a61388d482952097919ea6720e38f7089b32	b9e9144a22315da62d27177065db5671abefac2d151f7754595e65683a4da8b4
63db0b3ac2eeeca6568ea73e1d8a5acd7662c8db360b65a8cd0888fbfba7181c	d2258ca49d6814cfdac39dee7df860e2c9d8d21cb6edf44770784ad0983ccc08
9eb3d442a99cadb948f9c0de983d4d0bbc29f4e861f7ccb10028ce4888d174dd	99b6ebbc1f4335a6a8771afbbeb78e8cafb7285565fb98eb9d232f2e53bbfc97
02d332fd2dcf9e84e88289ee5cbb1bb7031f6cfce0fe9f825156ccdf4c84d37c	ef8de17509942828ff51f6e878dc0d4d80c9498ed2540e68d5a0e3eeb68aabfb
37457c6e0eb8a8875692495386 49c065f9570d3241bb952d1809c58b3a5605d2	d1e2b6c748d9056cb37cb389752d8a1d40aaeeaba54d99665728f93d1ab3f804
15c19cf0415abe0c957dabc7a11885236280293637 4207c9ba7ccc38bf0d61eb	373f0c565b3ead1177a018368db6acf6a699a8c7643afa106a4f79fdb5742ecc
cffd778ff7121a473d77b79a9c8e384ad1a4dad2e4facd0fff9bb8bd656bc6ea	dde3196479b2359316e407728ca144f1fccf9d8951bdf3c2c7e31da80c8ee85e
529ae91045a2aafa09e16b4358307b3cfd3cc1c7d304e145b88a3cf6e86fdda6	cc953fe0297a6052651a8c0f35f7a10632e36d44486875068bfd25f605ef5cca
5d32dccc1a571e18d24d9577ab698f5acefbef6f1ed75606e23cac635abbd2f0	6bb1a92d5d5e3d5468aee07412e0920022482d3452a3143c9e94caa527b798d0
0e1e989e4cb87dfe31912df4a49fda438e69a48a2af58cb867c99d78cf83da66	8f91f709f471d2c29568d5575f1a8a09ba69c17f54244d6582d8833c76dd407f
7d406ddbdc9ccf5076c7c688c2a1165ff84d20d7e77fe9cbcd9948228af391cf	d19e2c8b0e0b362a01637639b823d2bd6805d59d537f9ec7426d6ddb6a595c05
cc81731e0a3c8ef6da1f4ca801c11c331f55632ec95c331e0c88bd376daeddf6	b161e8d87ac54274063c7499d500c0e0a2b74cd6821bc6de66e44afdec7d2453
aac26333f0874bf65e91be81a9f124491914e42aca8306762e9e013544740651	a26248d33bcb16c51305782f4653f32c830f2f7c2c834fc4f1f83ef95cc96ace
f5fa37fded8b2176e046fec16a28fb8fa4f0fc0129547944374d6810faa00791	902ffe57a43576737cbdae0d0646a18c109c89521b9041004c23d32fdd330804
63945c9fbeb75c40412a521f686db792686e125757892e0af8c4d5e57bd5fe2f	2f993d351794e2fe050f9e09bc93a75af40bdedf8088a6580586ff31a1ddbb59
a7159570ec3544431e8942d3567633cc9aaae323afa5f1bc87aa81770f7623fc	bfaf23d54a6ceeb83f098fd066f9e0fee8665a0c6dead7aeb7a2c1b944572562
1e0d97f22df7df6e48d8002f1e1e25a14c939516508a6930169e406a22c7fce6	fa6c0ffc3d67100e0b9323687481b54133c3296b478e252ca73309f1e8680278
d21f035d94c119b51069abf96bf7e6172509a25ba6c163e2bb759bf6f95dba30	e6f0bb3844831bf7766adcae75946c4c1529d618c61b870551935ff0516dcb2c
fba367fb13c4ed43243ae58ac1c56011f32dc7ac8ce17acf4c91a3bd63b5e415	59c85a6810802f702b9831c26b00d42d02237225a424edbc097f427b6d0d035c
7d54f26a3deca5a6e63c2b3e4b4de6fae30e6a8091a42ca790842931559b5626	8d060492686b3b0839b775f93fe428c43a93e4273271102ebc2ba6286bdcabd6
4a03f202852020e631038c35b177acdc6146da88e0ef7dec850002d4d97bdc42	1b4c3513ec0377df3c246a2d66c90a764c6eaea93483ec768ffb1c8c0a5296d0
e8864ea5bdaa7b8e4dd81e0aae5f6016a8961ac243b68ff674cb48e54f88ab71	5a42c85c4f5b755f69c28709cf12c76fe759df0249662823980e815b43741057
0553d6e858a477b3674f075e2e670fad3c645dc61e804192e74331b99b4f47df	480f7bb46a7c921074aaa57baf59f28d79acb1b07deb17af9139b41e755f4432
dbf2653afdc143f7410b7f7348c9e12085e28e112f019343a91455e0b7b4e64c	01f1c2d801b69e811dbb1f8871aa974216b2d0f8adc3581a222e72b2cef1ce30
372b5e4fd8ed3e048bf267073c00cc72cd9f8e580dcca57387d83944cd0171fd	93c87d9f39467b3655a6320fa42c5e15568de422ecd6432b57a47e5c8c6f9173
588c060957e39ca924acebf835bc7c1e901a3c7c82452a139602e0fc2ae3d0c8	5e8edfffc3a41574fe6984f0846182a78293d42e78997fb7708f33314b57e976
7f2139bf7d7be00a060a7164773ac8596d9f65eb7da524ae72f5b435c1cbd858	e298fb131a75911eb773c8715eb6e92a9bef80e8199437bb0c14cffee29a7a7c
7fd30edb5eb626b08d2ffd03da8f065ad7fa196635c3841eafdea577195a8af0	2c9477f57313e342b03c60d777c1b9267a125cb81d439ed469f14ce4056163d7
e060b6a6d6195120cd31c7bcc5100fceb4216a3daff6134d734aec3059d48aeb	9263c66063a288b1316a4d4278b1fc0c29ff9dcdff31d03c93b0eddb8ecabd77
81bfacf756480710af634eefbddbac0254663ad6d955e9f0a3df8d4c8d27bd56	12b0adf7c10a67d360762bcea893807421a2ec0a5db867d181958e5c9876d71e
d8976a52eda1b7c0925e80dea399b6691c646030d7c00c87763f7ce509d9cbaf	5e7463993db29b4e4a2ae7a8de3549efd0e0c3ab62741142d640cfdd49deeb17
ed374d6e0847e13804357419d1f3f7a30e5a8346cb74029eeb3c715e15d4a423	ab07e25ae9bca8a4cc537917a11eea1ab8fc072e42dc93b7fb9332c11b9ca9f4
e6ef22f5b7ab77d365dd4b60c578715c06578ab5dea406e59a66478908b435d4	3c232a747185cbc67960d4ee61eefc42829731f932ecaf2df433024f1bdc48f5
b2c26965a57e71a1c2acb14e129840f7ecdf89c1a83740c9a04aba600e9dc02d	6fa44d9fd0ab01c3fcd3b13e5308ea4095fb5f929989adfbbb6e3bc58e9e207c
23c16f27cfdfc15d0e69792e45ac0aeae9aab196d94528d1dd82b91c3d615820	016b0a86cc1ca211525ab5f91c46928feb0eaf4dcbeb3cba78f41ca331262c10
42431bdd431f17d50cdeeeacea1c91a7a868d570d39b328f9bddebf6f4250f24	648e99cc251c7a37dbd5d0aaa03ae8c766e876f080eda792ae1405e8ff010113
80b55f96d2421b97ec780796acff0ed733229896ddebd14e021f9923b4aa75a4	16da512ac0f51cddefed20ba52d1554d927b54adb51dd71ad22a51fc97fddab4
c2bd8f9917ff4956ef0f3f0c616cc49e45eac0271b2a57c63081f540c0edd0e7	7226ffbb3c0693dcb38ff8f1002f05b93fcbbc0ae8ddfdabf4b95bb2456843e0
757c2bb6f932ead8840a7247ea9aba9b3b6a55ce99a387f721e280f51aa2c8aa	9ae1df4d19aa63e39e68e6b2c07048b57a2ca3a14bd39df8da45cb63b2230057
fe26aafbb4012b307de4f55b2efd20f705cabbfcd5115dfc1fbdc2c62c6380d6	cdd42323a4d9d96e4c38f0b2081dccb8ee31fabe54a0058f7950bcb1fb097b21
7bd48a169803019c087b690a7d4a3d6d019c0f1dd3f85444452b7cc7145914c8	500b679288aef73c10d18e1bcdb66e2643913519ae20bc876b412003c916a572
682ac972e6527d3541cf0187dcbb5c8b9e3665d3e3962f083eb87afea3c41c44	1c6fa053006657befa1e675b31d1b437e44d38b87d0e577f8f37804fb4d05217
33912557061a7770ea55e9368367af6f4aeb34c155d6e3775a15c7a4bba452e3	7a26cbe187ab1cb9800dd110db09fa55eeada7186e7ab08d84832a13dcef43b7
394461a2d2daa07601109b7a5c69bc93d2ab1c25d4e2406955a8ca31f46bc853	af84016db20d85ce3c7ac04951322c75f19c7b05562c44ff41c9190d449ae001
620f44a6c18b5ec86c797877d4ecbd857d7ffad1e3519042a44935831249bcf9	b84455b7b203c2820ad2880af740af662904efedf450c21ec48bd5601d78feeb

d7a2bec527f01d593c3cae068b7e69f0e279be57062fdc3f4f62d987f338dd95	1f7bb993f32effd03ec46d94afff9d0dba59b89d891cfc8e3505ea7ede6d74fe
ba89a28ff31ce143ca2baf664ae7a15d675933520e3107c4355233315fb4c87d	422cc0ef7b40e52cff95f611e2421b7beee1f3e935cf2a6cba269cadaee88cdf
b73ebd0e5295e8e3762e9cb34ecd03b70ce661e1c687c0d08edc9e5c36354508	d537151dafb8d055c843ad26ac0bf70c9c70efe04c1e77cd4b47006fcf069486
0a4c78db13a0e32a0b6bae6c8692d729d5418d46c2f66a9fb03ae0a5e40155e5	b2a10c95f2fb347ea5a8cc3c7872e18b66e2305ee9c2a2707c96316d29898859
ea3deaefc1fdce63917184c158a3cdd0402244d4a96a74532b1dcabd26dcb01a	db0b2075872a34ed8ca37e3f8b96a4994ed033085cfcf94695b8a5fe15ec0cb0
53e1c4a8b538725cbe339dd101efee9a2a8133600ada9d8bddff03574849367e	6ed56e89cd1c60c303e83b70efe82c249a07974e11c17afbe7b06a0bc8ca7b91
452c6361e1aa1f7c440a62307b4517c47e32f2dbebcc20d5e70a44c33e8ea434	a0e0cc3a355b8cc120db4f39075f7b22e596c5c83bebfc04b307dfe9bf2aaa26
ea914804ed564cc1bff287a99feb245b3239128d8833407b9ad20fe5a960b126	12ad75f57d22c23a61a5fcb4d31904c4f1e5074ec6c24009ea29cc1c22aa09fa
a6793c3d55e7ecb5ce787c9238145957943a9a0ee94e4e5a743875dc42ff51f1	628824a251667a17a1e574e2de35196695e747a6b467e5acd19162f4d94f8e4a
d089eabc33af4d46eabebfe5e1daa27aaf00ad4316e4f17cb1d185781752e5cd	0a454ea27e9b1a3619a2fa0ab207c2c68fcbdbee947b9875e53dbf5201a86c5d
ae4229465a4affc0ce5db8a04c6057ca134b3715567280ebb52418e02fc74e68	56f2a8ce2375d417640530bd0507e8d9045848262ab5cd15b7d0e757ceb13882
3db1645da329db133422580f08fc00efc17e78b36391f9621768b1839144cb12	87c1cf8e6c73f84bf90a54ce1b8c1256c69d27604dfafd05e903ea61a8df8693
4bce4a37c46c2d4363233c765be3cbb1f09175b50cdf0bc478277fdc339de223	7e2f4e51ed6b64b87970c67759fd9b597fbdf05aee1b1d914698935ae0d7e373
5b6b7091336852b3387dd61a8f5582b8cd37c588a97097b065fd880a87d26fc5	55de847d736a894978b932e82edeb440f2e0cda66fd3ac7c9afc98a7d519a336
6563bd898c439db46cb97c53dd8d9eaed24c1f8eb7078ba6a3c94d102580ac58	ce473cafff5825ba7456a44bd909c6fefe5c7699d9d3f7c3859b2c06578efe27
7536f9bad9507f873f8ee30ee5183bbe9b8ab4f264f47c8f64a9a6e46900ef1c	98931c4be0e11f73ae12ec03a854721813ac9542e2e97866304e83a165275d44
775ec2cefa2f4a37b05c04f1fe940795a0e2a3bdb3378e9165a9583ff6077eca	463e43ef25d470d6216048100a46222b97fb60f2595752cf473e782f0fd2e107
85838d336fd5ee8fd104a18889abd32421058048f2e20214e6e59129c3911d8e	ea913f0e0f155150b9e03e3f37fcb2da2c41b27ac92caa0f88b72bf0c0193f7a
990b8fa9568fb787fc4fdada1881b706484fd4944b77f1704913927c9f7590a4	79c70ad06a35af3ea1373ae00dfb396e01f9a648bc9ba7494b36318c96b9302f
ca4ca641512bf28bf726e62e22e166ec57f923c6fb20ea38d9bc06f5355608d5	9d615e6868a8642729093d03a6fe5ab22e79e2ee1a6395899b17afcd28050d34
d310f011b50e507121cb5949d18dbb864759ff9d0eac0b28f60db8f33f37f2b0	51e19536560b14709c4d3fa54ec82d86d3c139d406f878e434a25318e5f3eb1a
eb0be54dca8a4bb378534e01eaf53e4634b52009e519f6fb4f285a81bcc86a65	47e95ca99985fbaaa75e87da84e99aaba8f93980b9bfa8a57f3e0b596d7f8f9b
f0466c8703e9dc96c1fcc6c22166d582f9a193dd191770c461099e0998a97f8e	df8cea6e081e23dd3b018834e6f105d130137d7085bd19831f1c921945a73a76
40163293e560074504l81e4d20306bbc36ec41509b7304d13c443674f6d518a68	9e41a8dc6d2a8440a923680385cbdc08bb9646857ce3932fee7f0f32c745d962
f26c76eb48a4ae8478360253e00ca44cf6c5045ac3e3f3d0148d5b38a5c26321	82cdd2c8b28c06a0e2f1a16d65c48906fa6a915d643bd3e2e406fbba6c060308
85e9be4fe718ad146a49146e588b8099f40b7a2dd6b26860eb6b05c9b31b3a1c	7b4aa598ea2dc76d7049e9cac7aefe65b56c4715d264ec036541e02fcd599912
a748bdd411b3592a56a7993b5785cebb7bb13eb552383fca6245c3103276b833	63054565fa6c11269110108c08c663c9bf8a8acee62e8ae97ea8eae26b72fdab
b00b6f3ce3756c72f0808117a4ef7753208f6f413a047d936128625930348 7ad	7024e75171ec251c544c1b606fe729a7afdaf76d801a33a9876e25832a29e15b
e2c660cdb5229ba6377e338b8eb6ac02f4106fbff269027054c55d2af0728b79	b1817451cd2d46e505f7ca0a9ea39c51db15f8af0f2caf22cb2406a9993f6ead
11715829aedf7b06d8b6716fda75ec9f25d779e0fe227ceb51aeb0d82d784eef	59f1e5b98227a042fce4846f0cedc9b7bd98793e76c491fb573ccafee1d0dcbf
35d1b3637470071518196798 9b910bfb47bf0cd682f5c8811885413334ed4dac	86f11cf1ba511f63d2e50cf27151a79c26902c03b44f1579959f3c5e2a1142c3
91c714124fa647bc291e83e46e4882a73e7bf31034cd72d413abde1e1267b796	21c591652b258851d6b168fd4fdf1a0bb1cbb05854b912482c5e72cf55767d8d
57799329c68da2990157058ef59cfc15da9a3875da175f248525705528510c2a	9103fadc07e6a5672e10d0eb8dbd3b7bb921b7793dca8e58a3b9878a203682e4
ca353515dfc1f64e9883d1e92ff9f45a424496db4a812da30f97f591f916bbaa	4eff8cd24770ebf30e55ca49d285bef1e18fc5fbb31039be7187760eaef7f093
2de5e427def2caaa7f267a5970e65701e8944121d4858f4132184040e5fbf31e	814d9a2a6ccec46b658b3de5d2562938c02820939b021b4cf8e739f01319d360
fff5304eda64cef33eab40b0d6ebe741135e2788745ad64a9f854996fc51813b	7ec3ef1ee0f1c6201135169bc1e0551f8d10681ce26ad2d3cd1b1813732488f5
534b8b02f2361e0ae0ca2c2e83bfd835fedfc7ca0ae13431290d2fb0809c149c	fb6b3ca2054e2020b1533d04d1f6203d874bcaece3ac5cbd5faf5f5be9f0b5a9
8412ee8a0e6396fc3c8026848de3636a7139fce697d069f6ab9dd068443692e0	2e8f5a6079fdc94cec2c20f34c071412e92137171e57993ac97c9594a3ec1874
cd973d40d820077b4e35b06997a17badde2fa165845b59a2f12fa1e15fe8dd13	3c76987afd8fac28bae611d1ccf3d01ee28344ea99401e08cb76c1692745cb05
ff47c7feb4f969b908b3619d3192fd2a7ec3b380348e6924f9571555dc5ffb78	c45824e7dc1ce2814585092b54620b078830e6bfc3ad59831b3c7642c1ea8a26
67224e4c3e8fab45349075b6b4acfa1214f0156acf548ea73efb07c89a79af53	d0f88c88b00f2e3ede60713b5d058f152eaa329798eff2c99df8b63067b98ca9
8d15ec4bef58c6c98ec2e3f0764349ea17b75a4e22a2cef04ea3a09dd9c804c1	4384b5d01fb648f1819df40aee3101259d2c09205b6a9174dd38e49d044b5dcb
b19c7b8f030ac7fc4c98345b5ebd3436c737f0b88ece8f5a1785a54a650d4f31	94a4512503ef843ee4dde69c7aba8be818bf2d87f4e57158d9733da7a77cf220
627c977d85cebb499a0ff2676b06115366c826dbe8c5d061886c9d7376a59cf8	82848f816df06491dd41b521fd8166128494b6d577c39c563c45d0cf3984ef6a
49ec0a1fd224ab90ff5925a682f46873c8773b6f821aa0bae68749b4de972a88	b40e36c6be49ad8967fb81bbed7d6a4d1f36e8f2df4ed0117170b7ee5a858cd9
30ace8ae3dfb87e545d4e2192484e4f86a10658742d401f5b9bd61e1e4e88a29	075179eafe77f1a7251383aefa3dfa89217179e8bc56d6f8a2d4f2e45e1b4250

085c0b5c2715700d222449e8a4997f6d9a71d760e199a130c76bb7a50d818279	12b50f4a699ee6d98081af2c80aa96bb2d34cef4d5edf40bfe99c41740df0fa2
e8910db8687ca30ff84a544c98c44f74c18562ce2993349b5af3f5540cfd9bc0	

Correos electrónicos de donde son enviados los archivos adjunto con malware

Aktar@sprintservis.com
doc@jabsinternational.com
export02@easytourchina.com
fmarroni@havermexicana.com.mx
Mike.Yang@viajesprimavera.com
nfo@shortconnection.com
pharma12@cyber.net.pk
procure.a29@partner.samsung.com
quinantoto.olivia@jgc.com
ramazan@cabatravel.com
sarahbrautigam0@gmail.com
shipment@mail.tnt.com
supritareddy@vijayadiagnostic.in
vijaynasre@confidencegroup.co
dmconstrucciones@adinet.com.uy
administrator@postmaster.net
spunkycats23@yahoo.com
ostrum@surry.net
hhafeez@takweenai.com
Hanan@dhl.com
Alex@lhdottie.com
mayzin.kywe@hoysan.com
info@ouchem.cn
shipping@dhl.com
boskotech2@gmail.com
chanauspicious@gmail.com

Direcciones IP de servidor SMTP donde es enviado el correo malicioso

45.137.22.150	197.156.74.216
151.253.82.37	62.149.156.61
217.145.240.67	213.149.114.180
156.96.113.102	40.74.76.112
194.126.4.82	84.199.100.34
212.70.50.150	153.101.215.167
41.226.21.40	62.149.157.103
62.149.156.45	106.75.78.159
62.149.157.75	144.208.127.40
185.136.167.200	85.17.131.131
62.149.156.180	185.222.57.177
80.125.180.12	62.149.156.91
205.211.224.118	203.123.46.242
195.101.66.53	92.196.158.220
62.149.158.150	66.6.200.103
190.224.160.69	62.149.156.76
212.62.57.187	212.114.52.95
62.149.157.71	45.153.203.51
84.206.43.8	185.156.172.18
210.87.250.171	173.0.137.124
168.95.6.56	106.75.103.187
88.119.209.196	173.215.166.166
213.149.114.173	200.115.177.8
213.149.114.173	82.137.200.129
213.149.114.183	93.87.24.140
213.149.114.183	190.34.219.186
81.192.56.15	190.128.171.214
81.192.56.14	62.149.156.60
62.149.157.238	190.228.29.30
62.149.158.120	211.150.64.100
212.51.163.145	24.232.0.140
62.149.156.46	200.76.152.220
62.149.156.106	45.137.22.59
196.29.169.55	103.133.107.14
62.149.158.105	86.96.198.177
185.222.58.118	133.183.100.20
131.161.42.68	74.208.175.156

193.33.165.251	37.49.225.143
203.101.175.37	190.210.15.194
62.149.158.135	179.41.18.118
41.79.4.10	103.99.1.174
210.245.31.30	68.183.86.92
45.35.196.138	

Actualidad

Ciberconsejos para una Navidad Segura

Con la llegada de diciembre, muchas personas ya comienzan a planificar sus compras navideñas. Si este año preferirás los canales digitales, el CSIRT junto con la PDI prepararon los siguientes consejos para comprar de forma segura y así evitar ser víctima de alguna estafa o fraude cibernético.

Ver más: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-una-navidad-segura/

Cibersucesos n°4

CSIRT comparte la 5ta edición de Cibersucesos. Como pieza central en esta publicación recordamos los pasos clave para unas fiestas de fin de año sin exponernos de más a fraudes y ataques cibernéticos. En la misma línea y por ser los regalos más populares para Navidad, repasamos los principales conceptos para entender el mundo de los videojuegos en línea, junto con los riesgos que corren los niños que los usan y cómo prevenirlos, por ejemplo, a través de herramientas de control parental.

Más allá de las fiestas, en la sección Tendencias de este mes se explica el denominado descubrimiento pasivo, una técnica con la que agentes maliciosos hacen más efectivos sus ataques gracias a la revisión de las redes sociales de sus víctimas y otra información disponible en internet.

Comunidad Hacker trae el testimonio de Jessica Matus, creadora de Datos Protegidos, fundación dedicada a la defensa de la privacidad de la información personal en Chile. Matus nos cuenta sobre sus más recientes proyectos, como la investigación de la moderación de contenidos en internet en Chile, y la campaña “No doy mi RUT”.

Sigue en igual tono el apartado Legal, que describe los denominados derechos ARCO, de acceso, rectificación, cancelación y oposición, consignados en el artículo 19° de nuestra Constitución. También se explican dos nuevos derechos nacidos en Europa, denominados derecho al olvido y de portabilidad.

Ver más: https://www.csirt.gob.cl/recomendaciones/cibersucesos-n5/

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.

- Juan Pablo Berríos
- Alejandra Lutz
- Constanza Botello