Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

11-03-2022 | Año 4 | N°140

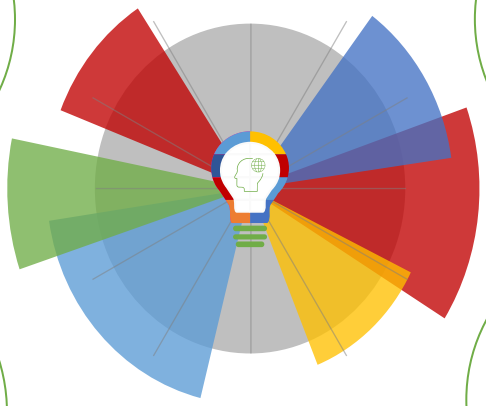
Boletín de Seguridad Cibernética

Semana del 4 al 10 de marzo de 2022

La semana en cifras

Hash
70
SHA
Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron
39
URL
Asociadas a sitios fraudulentos y campañas de phishing y malware.



Parches
113
para vulnerabilidades
Las mitigaciones son útiles en productos Citrix, Cisco, Adobe, Intel, SAP, Microsoft y Mozilla.

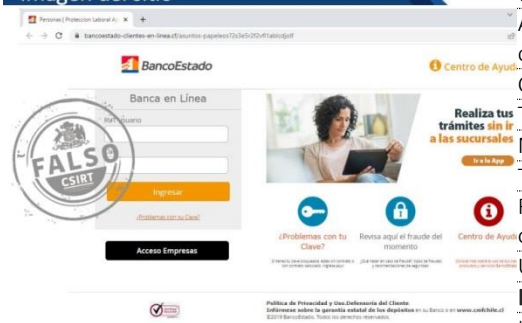
IP
83
Informadas
Listado de IP advertidas en múltiples campañas de phishing y de malware.

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

Contenido

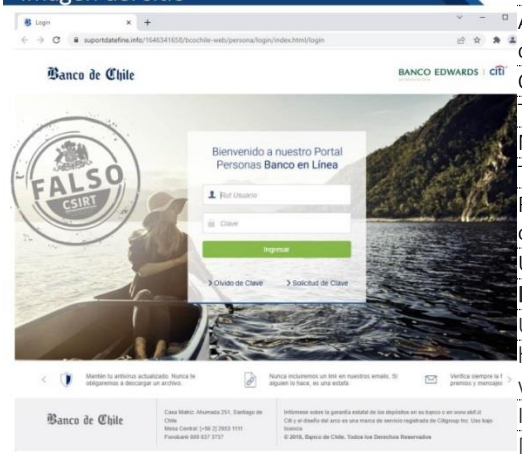
Sitios fraudulentos

Imagen del sitio



CSIRT advierte suplantación de sitio web del Banco Estado	
Alerta de seguridad cibernética	8FFR22-01059-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de marzo de 2022
Última revisión	4 de marzo de 2022
Indicadores de compromiso	
URL sitio falso	
https://bancoestado-clientes-en-linea[.]cf/afiliaciones?5c2er3t5y7laql1mhp7m5	
IP	
[103.155.93.74]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01059-01/	
https://www.csirt.gob.cl/media/2022/03/8FFR22-01059-01.pdf	

Imagen del sitio

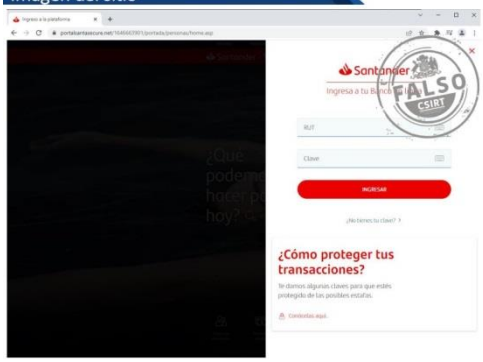


CSIRT informa sitio falso del Banco de Chile	
Alerta de seguridad cibernética	8FFR22-01060-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de marzo de 2022
Última revisión	4 de marzo de 2022
Indicadores de compromiso	
URL sitio falso	
https://suportdatefine[.]info/1646333031/bcochile-web/persona/login/index.html/login	
IP	
[173.236.29.82]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01060-01/	
https://www.csirt.gob.cl/media/2022/03/8FFR22-01060-01.pdf	

Imagen del sitio

CSIRT informa sitio fraudulento del Banco Estado	
Alerta de seguridad cibernética	8FFR22-01061-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de marzo de 2022
Última revisión	4 de marzo de 2022
Indicadores de compromiso	
URL sitio falso	
http://www.katka-masopustova[.]cz/p0rt4bl3/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[46.101.52.30]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01061-01/	
https://www.csirt.gob.cl/media/2022/03/8FFR22-01061-01.pdf	

Imagen del sitio



CSIRT advierte página web falsa del Banco Santander	
Alerta de seguridad cibernética	8FFR22-01062-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de marzo de 2022
Última revisión	7 de marzo de 2022
Indicadores de compromiso	
URL sitio falso	
https://portalsantasecure[.]net/16466632 53/portada/personas/home.asp	
IP	
[184.154.47.82]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01062-01/	
https://www.csirt.gob.cl/media/2022/03/8FFR22-01062-01.pdf	

Phishing

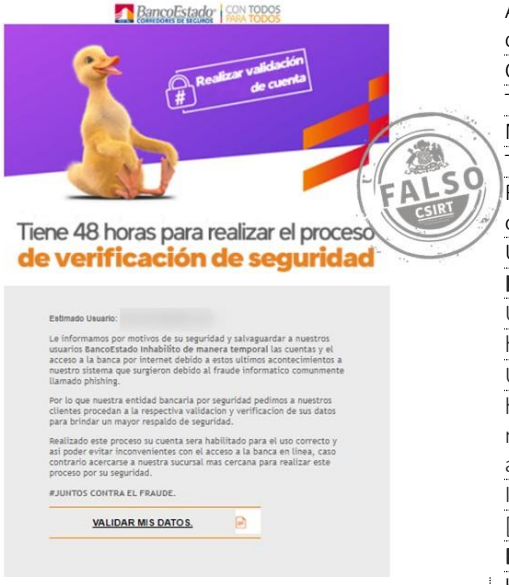
Imagen del mensaje

CSIRT advierte phishing que suplanta al Banco Estado	
Alerta de seguridad cibernética	8FPH22-00478-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de marzo de 2022
Última revisión	4 de marzo de 2022
Indicadores de compromiso	
URL redirección	
http://ns1.inmystream[.]net/activacion/cuenta-fdun/	
URL sitio falso	
https://chinabank.joinon[.]cn/schile/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[121.199.12.163]	
[45.7.230.246]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00478-01/	
https://www.csirt.gob.cl/media/2022/03/8FPH22-00478-01-1.pdf	

Imagen del sitio

CSIRT informa phishing con falso sorteo con motivo del Día de la Mujer	
Alerta de seguridad cibernética	8FPH22-00479-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de marzo de 2022
Última revisión	4 de marzo de 2022
Indicadores de compromiso	
URL sitio falso	
https://tinyurl2[.]ru/p853844860/#1646339639854	
IP	
[172.67.186.238]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00479-01/	
https://www.csirt.gob.cl/media/2022/03/8FPH22-00479-01.pdf	

Imagen del mensaje



CSIRT advierte phishing que suplanta al Banco Estado	
Alerta de seguridad cibernética	8FPH22-00480-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de marzo de 2022
Última revisión	4 de marzo de 2022
Indicadores de compromiso	
URL redirección	
https://red2play.net/activacion/cuenta-dfop/	
URL sitio falso	
http://www.katka-masopustova[.]cz/c4teg0r14/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[46.101.52.30]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00480-01/	
https://www.csirt.gob.cl/media/2022/03/8FPH22-00480-01.pdf	

Malware

Imagen del mensaje

CSIRT advierte campaña de malware Emotet	
Alerta de seguridad cibernética	2CMV21-00277-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de marzo de 2022
Última revisión	4 de marzo de 2022

Indicadores de compromiso

IP

[189.126.112.5]

SHA256

67C2C56708BDF1F4E4309389EC43252A1AF1E903C91266208C011734F4B456AB
8E622B97F789CF5A1EEE79006E4784EEC229F0D89EF09E2579787313AB961301
11E7227AFB354863F537601E49853BA245F7B31278A7B05A9F23AFD0E996DAD9

IoC URL

http://touqarrayan[.]com/wp-content/RoiB
http://nayzaqaljanoob-iq[.]com/sapbush/tylhe1
http://cabinet-bribech[.]com/wp/DyMNglRY5B4abPy1hH
http://retailhpsinterview[.]com/cgi-bin/dJp9RYh
https://lisalmcgee[.]com/images/xpl7i1ETzHPwaFd89HS
https://collision-staging[.]com/wp-content/94PQ1

Enlaces para revisar el informe:

https://www.csirt.gob.cl/alertas/2cmv22-0277-01/
https://www.csirt.gob.cl/media/2022/03/2CMV22-00277-01.pdf

Imagen del mensaje

CSIRT informa campaña de malware Emotet	
Alerta de seguridad cibernética	2CMV21-00278-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de marzo de 2022
Última revisión	4 de marzo de 2022

Indicadores de compromiso

IP

[186.202.7.186]

SHA256

0B6EB2EF79A8C88BC41F5B5609C6F3FED66E126151AFE11F79697BC68CCDECF7
6F565E1DE6A1FB4F760096303575EDE6173906FCDFA4764990EF44137A2E430E

IoC URL

http://suleyera[.]com/components/CNGhltc5v2K6
http://sociallysavvyseo[.]com/PinnacleDynamicServices/pRlYMzvfuu5B/
http://moveit.savvyint[.]com/config/DsfssbO7BYG/
https://schwizer.net/styled/D0MG/
http://shabeerpv.atwebpages[.]com/css/ww6if1YAsMpjpuGz
http://shimal.atwebpages[.]com/wp-content/xkaRkHr/

Enlaces para revisar el informe:

https://www.csirt.gob.cl/alertas/2cmv22-0278-01/
https://www.csirt.gob.cl/media/2022/03/2CMV22-00278-01.pdf

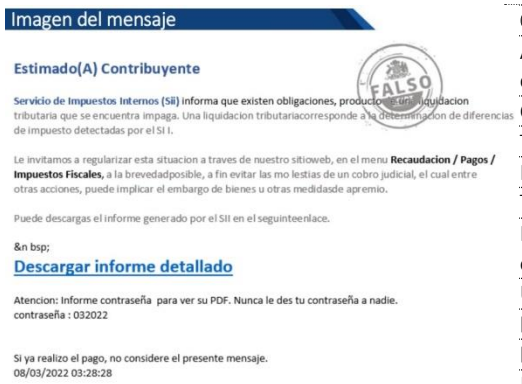


Imagen del mensaje

Estimado(A) Contribuyente

FALSO

Servicio de Impuestos Internos (SII) informa que existen obligaciones, producto de una liquidacion tributaria que se encuentra impaga. Una liquidacion tributariacorresponde a la determinacion de diferencias de impuesto detectadas por el SI I.

Le invitamos a regularizar esta situacion a traves de nuestro sitioweb, en el menu **Recaudacion / Pagos / Impuestos Fiscales**, a la brevedadposible, a fin evitar las mo lestias de un cobro judicial, el cual entre otras acciones, puede implicar el embargo de bienes u otras medidasde apremio.

Puede descargas el informe generado por el SII en el seguinteenlace.

&n bsp;

Descargar informe detallado

Atencion: Informe contraseña para ver su PDF. Nunca le des tu contraseña a nadie.
contraseña : 032022

Si ya realizo el pago, no considere el presente mensaje.
08/03/2022 03:28:28

CSIRT advierte campaña de malware suplantando al SII	
Alerta de seguridad cibernética	2CMV21-00280-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de marzo de 2022
Última revisión	9 de marzo de 2022
Indicadores de compromiso	
IP	
[102.130.118.158]	
SHA256	
5C4E6F90364DFEB19C1E7EA55B516F8BA211B2DCE1FF4F93B7C8DD32A61F2CC6 85EB1D4FD5DC78552361BB1DA4422C0865BBAE3784470C2FAA551E461FB35D52	
IoC URL	
https://5aa20a4eab0b.ngrok[.]io/PDF-0027430505S3B101lF3.zip https://makeupkala[.]com/well-known/acme-challenge/l/z/c218B3505l1016S502i3.zip https://zakatalquds[.]org/profiles/contts/hd218b0s5S20d1l322cj.php	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-0280-01/	
https://www.csirt.gob.cl/media/2022/03/2CMV22-00280-01.pdf	

Vulnerabilidades

CSIRT alerta de vulnerabilidades críticas en Firefox	
Alerta de seguridad cibernética	9VSA22-00584-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de marzo de 2022
Última revisión	7 de marzo de 2022
CVE	
CVE-2022-26485 CVE-2022-26486	
Fabricante	
Firefox	
Productos afectados	
Versiones anteriores a Firefox 97.0.2, Firefox ESR 91.6.1, Firefox for Android 97.3, Focus 97.3 y Thunderbird 91.6.2	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00584-01/	
https://www.csirt.gob.cl/media/2022/03/9VSA22-00584-01-1.pdf	

CSIRT alerta de vulnerabilidades comunicadas por Microsoft en su Update Tuesday de marzo 2022	
Alerta de seguridad cibernética	9VSA22-00585-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Bajo
TLP	Blanco
Fecha de lanzamiento original	9 de marzo de 2022
Última revisión	9 de marzo de 2022
CVE	
CVE-2020-8927 - CVE-2022-0789 - CVE-2022-0790 CVE-2022-0791 - CVE-2022-0792 - CVE-2022-0793 CVE-2022-0794 - CVE-2022-0795 - CVE-2022-0796 CVE-2022-0797 - CVE-2022-0798 - CVE-2022-0799 CVE-2022-0800 - CVE-2022-0801 - CVE-2022-0802 CVE-2022-0803 - CVE-2022-0804 - CVE-2022-0805 CVE-2022-0806 - CVE-2022-0807 - CVE-2022-0808 CVE-2022-0809 - CVE-2022-21967 - CVE-2022-21975 CVE-2022-21977 - CVE-2022-21990 - CVE-2022-22006 CVE-2022-22007 - CVE-2022-22010 - CVE-2022-23265 CVE-2022-23266 - CVE-2022-23277 - CVE-2022-23278 CVE-2022-23281 - CVE-2022-23282 - CVE-2022-23283 CVE-2022-23285 - CVE-2022-23286 - CVE-2022-23287 CVE-2022-23288 - CVE-2022-23294 - CVE-2022-23295	

CVE-2022-23297	CVE-2022-23298	CVE-2022-23299
CVE-2022-23300	CVE-2022-23301	CVE-2022-24451
CVE-2022-24452	CVE-2022-24453	CVE-2022-24456
CVE-2022-24457	CVE-2022-24460	CVE-2022-24461
CVE-2022-24462	CVE-2022-24463	CVE-2022-24465
CVE-2022-24467	CVE-2022-24468	CVE-2022-24469
CVE-2022-24470	CVE-2022-24471	CVE-2022-24501
CVE-2022-24502	CVE-2022-24503	CVE-2022-24505
CVE-2022-24506	CVE-2022-24508	CVE-2022-24509
CVE-2022-24510	CVE-2022-24511	CVE-2022-24512
CVE-2022-24515	CVE-2022-24517	CVE-2022-24518
CVE-2022-24519	CVE-2022-24520	CVE-2022-24522
CVE-2022-24525	CVE-2022-24526	

Fabricante
Microsoft

Productos afectados
.NET 5.0
.NET 6.0
.NET Core 3.1
Azure Site Recovery VMWare to Azure
HEIF Image Extension
HEVC Video Extension
HEVC Video Extensions
Intune Company Portal for iOS
Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Defender for Endpoint for Android
Microsoft Defender for Endpoint for Linux
Microsoft Defender for Endpoint for Mac
Microsoft Defender for Endpoint for Windows
Microsoft Defender for IoT
Microsoft Exchange Server 2013 Cumulative Update 23
Microsoft Exchange Server 2016 Cumulative Update 21
Microsoft Exchange Server 2016 Cumulative Update 22
Microsoft Exchange Server 2019 Cumulative Update 10
Microsoft Exchange Server 2019 Cumulative Update 11
Microsoft Office 2019 for 32-bit editions
Microsoft Office 2019 for 64-bit editions
Microsoft Office 2019 for Mac
Microsoft Office LTSC 2021 for 32-bit editions
Microsoft Office LTSC 2021 for 64-bit editions
Microsoft Office LTSC for Mac 2021
Microsoft Visual Studio 2019 version 16.11 (includes 16.0 – 16.10)
Microsoft Visual Studio 2019 version 16.7 (includes 16.0 – 16.6)
Microsoft Visual Studio 2019 version 16.9 (includes 16.0 – 16.8)
Microsoft Visual Studio 2022 version 17.0
Microsoft Word 2013 RT Service Pack 1
Microsoft Word 2013 Service Pack 1 (32-bit editions)
Microsoft Word 2013 Service Pack 1 (64-bit editions)

Microsoft Word 2016 (32-bit edition)
Microsoft Word 2016 (64-bit edition)
Paint 3D
Raw Image Extension
Remote Desktop client for Windows Desktop
Skype Extension for Chrome
Visual Studio Code
VP9 Video Extensions
Windows 10 for 32-bit Systems
Windows 10 for x64-based Systems
Windows 10 Version 1607 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows 10 Version 1809 for x64-based Systems
Windows 10 Version 1909 for 32-bit Systems
Windows 10 Version 1909 for ARM64-based Systems
Windows 10 Version 1909 for x64-based Systems
Windows 10 Version 20H2 for 32-bit Systems
Windows 10 Version 20H2 for ARM64-based Systems
Windows 10 Version 20H2 for x64-based Systems
Windows 10 Version 21H1 for 32-bit Systems
Windows 10 Version 21H1 for ARM64-based Systems
Windows 10 Version 21H1 for x64-based Systems
Windows 10 Version 21H2 for 32-bit Systems
Windows 10 Version 21H2 for ARM64-based Systems
Windows 10 Version 21H2 for x64-based Systems
Windows 11 for ARM64-based Systems
Windows 11 for x64-based Systems
Windows 7 for 32-bit Systems Service Pack 1
Windows 7 for x64-based Systems Service Pack 1
Windows 8.1 for 32-bit systems
Windows 8.1 for x64-based systems
Windows RT 8.1
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Server 2012
Windows Server 2012 (Server Core installation)
Windows Server 2012 R2
Windows Server 2012 R2 (Server Core installation)
Windows Server 2016
Windows Server 2016 (Server Core installation)

Windows Server 2019 Windows Server 2019 (Server Core installation) Windows Server 2022 Windows Server 2022 (Server Core installation) Windows Server 2022 Azure Edition Core Hotpatch Windows Server, version 20H2 (Server Core Installation)
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00585-01/
https://www.csirt.gob.cl/media/2022/03/9VSA22-00585-01-1.pdf

CSIRT alerta vulnerabilidades en productos de SAP	
Alerta de seguridad cibernética	9VSA22-00586-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de marzo de 2022
Última revisión	9 de marzo de 2022
CVE	
CVE-2022-22536 - CVE-2021-24396 - CVE-2022-26101 CVE-2022-22542 - CVE-2022-24395 - CVE-2022-23497 CVE-2022-26104 - CVE-2022-24395 - CVE-2022-24397 CVE-2022-26104 - CVE-2022-26102 - CVE-2021-24399 CVE-2022-22547 - CVE-2022-24398 - CVE-2022-26100 CVE-2022-26103	
Fabricante	
SAP	
Productos afectados	
SAP Web Dispatcher, Versions -7.49, 7.53, 7.77, 7.81, 7.85, 7.22EXT, 7.86, 7.87. SAP Content Server, Version -7.53. SAP NetWeaver and ABAP Platform, Versions -KERNEL 7.22, 8.04, 7.49, 7.53, 7.77, 7.81, 7.85, 7.86, 7.87, KRNL64UC 8.04, 7.22, 7.22EXT, 7.49, 7.53, KRNL64NUC 7.22, 7.22EXT, 7.49. Simple Diagnostics Agent 1.0. Fiori Launchpad, Versions 754, 755, 756. SAP-JEE, Version 6.40 SAP-JEECOR, Versions 6.40, 7.00, 7.01. SERVERCORE, Versions 7.10, 7.11, 7.20, 7.30, 7.31. SAPS/4HANA (Supplier Factsheet and Enterprise Search for Business Partner, Supplier and Customer), Versions -104 a 106. SAP NetWeaver Enterprise Portal, Versions 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50 SAP Financial Consolidation, Version10.1. SAP NetWeaver Application Server for ABAP, Versions700, 701, 702, 731. SAP Focused Run, Versions 200, 300. Simple Diagnostics Agent, Versions=>1.0, < 1.58.	

SAP Business Objects Business Intelligence Platform, Version420, 430. SAPCAR, Version7.22. SAP NetWeaver AS JAVA (Portal Basis), Version 7.50.
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00586-01/
https://www.csirt.gob.cl/media/2022/03/9VSA22-00586-01.pdf

CSIRT alerta de nuevas vulnerabilidades en productos de Adobe	
Alerta de seguridad cibernética	9VSA22-00587-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de marzo de 2022
Última revisión	10 de marzo de 2022
CVE	
CVE-2022-23187 CVE-2022-24094 CVE-2022-24095 CVE-2022-24096 CVE-2022-24097 CVE-2022-24090	
Fabricante	
Adobe	
Productos afectados	
Adobe Illustrator 26.0.3 y anteriores. Adobe Photoshop 2021 22.5.5 y anteriores. Adobe Photoshop 2022 23.1.1 y anteriores. Adobe After Effects 22.2 y anteriores. Adobe After Effects 18.4.4 y anteriores.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00587-01/	
https://www.csirt.gob.cl/media/2022/03/9VSA22-00587-01.pdf	

CSIRT alerta de nuevas vulnerabilidades en productos de Citrix	
Alerta de seguridad cibernética	9VSA22-00588-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de marzo de 2022
Última revisión	10 de marzo de 2022
CVE	
CVE-2022-23034 CVE-2022-23035 CVE-2022-26355 CVE-2021-26401	
Fabricante	
Citrix	
Productos afectados	
Citrix Hypervisor Citrix XenServer Citrix Federated Authentication Service 7.17 – 10.6	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00588-01/	
https://www.csirt.gob.cl/media/2022/03/9VSA22-00588-01.pdf	

CSIRT alerta ante vulnerabilidades en productos de Intel	
Alerta de seguridad cibernética	9VSA22-00589-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de marzo de 2022
Última revisión	10 de marzo de 2022
CVE	
CVE-2021-33150 CVE-2022-0001 CVE-2022-0002	
Fabricante	
Intel	
Productos afectados	
6th Gen Intel® Core™ Processors 7th Gen Intel® Core Processors 8th Gen Intel® Core™ Processors 10th Gen Intel® Core™ Processors Intel Atom® processor A series Intel Atom® processor C3000 Automated Driving series Intel Atom® processor C3000 series Intel Atom® processor X E3900 series Intel® 100 series chipset	

Intel® 200 series chipset
Intel® 300 series chipset
Intel® C230 series chipset
Intel® C240 series chipset
Intel® C420 chipset
Intel® C620 series chipset
Intel® Celeron® Processor 3000 Series (38XX and 39XX)
Intel® Celeron® Processor 4000 Series (42XX and 43XX)
Intel® Celeron® processor J3000/N3000 series
Intel® Celeron® processor J4000/N4000 series
Intel® Pentium® Gold Processor Series (44XX and 65XX)
Intel® Pentium® Gold Processor Series (54XX)
Intel® Pentium® Processor 4000 Series (44XX)
Intel® Pentium® processor J4000/N4000 series
Intel® Pentium® processor J5000/N5000 series
Intel® X299 chipset
Intel® Xeon® D processor 2000 series
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00589-01/
https://www.csirt.gob.cl/media/2022/03/9VSA22-00589-01.pdf

CSIRT alerta de vulnerabilidades de alto riesgo en productos Cisco	
Alerta de seguridad cibernética	9VSA22-00590-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de marzo de 2022
Última revisión	10 de marzo de 2022
CVE	
CVE-2021-1577	
CVE-2021-1579	
CVE-2021-1580	
CVE-2021-1581	
Fabricante	
Cisco	
Productos afectados	
Cisco APIC y Cisco Cloud APIC.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00590-01/	
https://www.csirt.gob.cl/media/2022/03/9VSA22-00590-01.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	Tipo Malware	N° Documento
00694960f423969978e9e59173747489b9f4b01213dc5cb773376a9512270a57	PossibleThreat	2CMV22-00276-01
8ba1cd4d03d8c50eaa726c4f7d23c33403f689330b09f2cf6fa5d1b1d2d3aebc	Riskware/POC_Iframe_CID	2CMV22-00276-01
b105cec0b378c6165161d0894716b19b8aa378e4993068f65cf0547a7915570b	MSExcel/Sneaky	2CMV22-00276-01
adb0ed7840b087c4def89aa8011bc775ccdea36259163e11c7e63a1ca0a371b8	MSIL/Kryptik	2CMV22-00276-01
6e9c7910a419ff375b1572f62c1029bb857dd66e67caadc341de867f2aeedf69	MSExcel/Agent	2CMV22-00276-01
75864d6fcd2e7da03df0471a95ad5df89c8df53d356fc4851bb279ab12921b50	Malicious_Behavior	2CMV22-00276-01
bf91586eb1dd0325caa1e1c88f20763b7695298158e514d25dbe1383201ebe27	FSA/RISK_HIGH	2CMV22-00276-01
9603bfe9526bc0ecca7bb316076182426692d394038bd53058f4fbf12b99ec4b	MSExcel/Sneaky	2CMV22-00276-01
11c4609a467b9b533fee7e8c05d16550113600b8cd0d03412166b48886e0744c	W32.Injector	2CMV22-00276-01
375511fcaec20c4d0a78413c0e3a27f5e36e88ef910d7f1ac6956b4ac940bc73	MSIL/Kryptik	2CMV22-00276-01
78ec26b74ebb7fe88854265f8dfe40a025e5711426422670e42613dae0c6b40d	W32/Injector	2CMV22-00276-01
ea68b93e8d4d8867a0f900258b9976b5e5a9ea32ecdf9daec4f27e1438e55fe7	MSExcel/CVE_2017_11882	2CMV22-00276-01
6b9a39bea713ed377c8383e4510ccdfe1e16e725a7f92a75f99923b8c0cae73d	MSIL/Kryptik	2CMV22-00276-01
ec4d5729e0c5cf1bac80aa8a3c8debde962dd6236f2f2a3cdd2ddd76549fcfb8	MSExcel/CVE_2017_11882	2CMV22-00276-01
8aa9783829ad9ab0cffedc904b169cf6a9baddf86d60ab2d97afdae61ef00931	MSExcel/CVE_2017_11882	2CMV22-00276-01
811975898be7b81982bf43bbd843fe2519e935b181a1d71fc7afa2f3236406fd	MSExcel/Sneaky	2CMV22-00276-01
c6ce7ea76a677e095190fde32326a791c46f901f3f7a25b7dc2e3682c4e2a6b2	MSIL/Kryptik	2CMV22-00276-01
e87487d2b9498c50b0b043f0ef92cd84a07da73aacb4c6f7632cf8785f42bb99	MSExcel/CVE_2017_11882	2CMV22-00276-01
a3b219e4785fa8136735bf13b002f8a54b6aaba957ccd940e8ddcb0e0faaa29e	FSA/RISK_HIGH	2CMV22-00276-01
54ce709147ee22fbf06505e6cc8d8289280a4c9230a18eb25da02cfb0ffd27a7	PossibleThreat	2CMV22-00276-01
70f829b2922ca1e061b1abdf377cb612cad53791b19d271ce512365a7fd645f9	MSIL/Kryptik	2CMV22-00276-01
354af94565f8125a8817cc581bf07e0c73124810446ffd727634bb9ee7019837	PossibleThreat	2CMV22-00276-01
0d81b36c19aa158b7fa01b9bc5db12ac61413b0213fa205e654d348a0f91fea7	MSExcel/CVE_2017_11882	2CMV22-00276-01
6a3db937a1aaa1e6619e3525963e74eafff6ac89a8e560f9bd02be5bdfbaef53	PossibleThreat	2CMV22-00276-01
8b7abf93c2d1a95a821a76046f28cb13d0243bb6cec50898424973498afc1bec	Malicious_Behavio	2CMV22-00276-01
83cfa992d45b7a4616b6c28c39b4f5b81a1690457b17efdec663d8eed298f88c	Malware_Generic	2CMV22-00279-01
fb7d841b757d358d483bc9f10dac3eb083fb0dfbfcb3a09d2b2da0f0d5a09da0	MSIL/GenKryptik	2CMV22-00279-01
5b15b1dcfd70e561edc74cf47f03237289287ff9d730ad448ace7d00981931db	MSIL/GenKryptik	2CMV22-00279-01
10a0ecc8af1839ef0f6663466486c51402b9a0c092eed0757c3078684cd34d9d	MSIL/GenKryptik	2CMV22-00279-01
1f22331fb0b0dc20a2b688e8055d77f0c48358b20a0bfff91bc22ca36dee44bf	MSIL/GenKryptik	2CMV22-00279-01
fcebacfc06e3cde9fc0a5360292ab11e74b09254b76a37f12809e196bb41e0b5	HTML/Phishing	2CMV22-00279-01
1c1975697dc5223f7b49f929f2cd7b7ea56f1e82fb7a0851a35feec1e05ff565	MSIL/Kryptik	2CMV22-00279-01
f9ca79ca37bed24745837dedbe6ca6fb25cbfe1d77b75d745fb575d481ee2e79	MSIL/Kryptik	2CMV22-00279-01
9b7e50a009ea82edcd7de887a6179a4def1b9bba6a05b26c06f70bd33874ca08	Riskware/Application	2CMV22-00279-01
62816a26c1b16eb5e22abad0c841cf2b80a8162e2b94aa0ff753ee31444e7612	MSIL/GenKryptik	2CMV22-00279-01
2446309f61a8f555341050a21d23ae03fffada95dfaa88ccae812ba306e3dfcc	MSIL/GenKryptik	2CMV22-00279-01
87bd2a598147349dacc5bb0028daffcbff25ca9058a27048846856c788cccab7	Malware_Generic	2CMV22-00279-01
9e625dded055750e06e2ada33cb0f6f5aa902d6fbbeaa122731d28d487a57873	MSIL/Agent	2CMV22-00279-01
a5010a9bf89afd01b276dff22cc0cd4dc511e84bd66966a0ba0cd7e42d904cfb	MSIL/Kryptik	2CMV22-00279-01
573acd351ca811a5dc54151dd71b91be95ecb3ee502a4b94912c5a7ee006d6b6	PossibleThreat	2CMV22-00279-01
0f9819f7aa606121d751ef601db450be1d54389a307c92434c213e1c1b35f927	W32/Injector	2CMV22-00279-01

42f94398776f3d359411089057952ac252fc2ba2c80314c7c28ffe0092fe767e	Malware_Generic	2CMV22-00279-01
e8d4e10769505d71c18eab7a9828c4988e1e7526c8a026da951197230014b4f4	PossibleThreat	2CMV22-00279-01
30a6a60bc57b3460afbc3be37d33eb56337ed81c77a0939312dfe8bc74d70c39	PossibleThreat	2CMV22-00279-01
f6ddbd5cf3a27e0b6f6cc5b36cb9f63438132fe3a3a24257f424c2f9f5cb15c1	MSOffice/Scam	2CMV22-00279-01
443b95ceb8fa87ba09937fcf08da5bc2a63d7242bcaf558bd3415fe68dde3191	PossibleThreat	2CMV22-00279-01

Direcciones IP de servidor SMTP donde es enviado el correo malicioso. Recomendamos establecer cuarentena preventiva para estos indicadores de compromiso, previa evaluación del impacto en los servicios productivos. Una vez que sus plataformas de monitoreo no detecten actividad maliciosa, puede evaluar la posibilidad de liberar el bloqueo. Es importante considerar que podrían aparecer direcciones de IP de servicios Cloud reconocidos o amenazas mitigadas.

IP	Etiqueta de sistema autónomo	Documento web
212.192.241.164	Delis LLC	2CMV22-00276-01
147.135.38.57	OVH SAS	2CMV22-00276-01
181.198.19.213	Telconet S.A	2CMV22-00276-01
185.222.57.135	RootLayer Web Services Ltd	2CMV22-00276-01
185.222.57.246	RootLayer Web Services Ltd.	2CMV22-00276-01
185.222.58.61	RootLayer Web Services Ltd.	2CMV22-00276-01
185.222.58.86	RootLayer Web Services Ltd.	2CMV22-00276-01
185.222.58.92	RootLayer Web Services Ltd	2CMV22-00276-01
189.193.232.2	RootLayer Web Services Ltd	2CMV22-00276-01
2.58.149.226	AS-SERVERION	2CMV22-00276-01
2.58.149.236	AS-SERVERION	2CMV22-00276-01
2.58.149.77	AS-SERVERION	2CMV22-00276-01
200.30.145.122	Newcom Limited	2CMV22-00276-01
209.85.160.171	Google LLC	2CMV22-00276-01
209.85.160.194	Google LLC	2CMV22-00276-01
209.85.166.53	Google LLC	2CMV22-00276-01
209.85.166.68	Google LLC	2CMV22-00276-01
45.137.22.148	RootLayer Web Services Ltd.	2CMV22-00276-01
45.137.22.55	RootLayer Web Services Ltd.	2CMV22-00276-01
45.137.22.62	RootLayer Web Services Ltd.	2CMV22-00276-01
45.174.244.14	Jose Gonzalo Olivares Madrigal	2CMV22-00276-01
45.85.190.96	Des Capital B.V.	2CMV22-00276-01
5.249.152.9	Aruba S.p.A.	2CMV22-00276-01
185.222.57.201	RootLayer Web Services Ltd.	2CMV22-00279-01
82.148.101.68	Ooredoo QSC	2CMV22-00279-01
185.222.58.50	RootLayer Web Services Ltd.	2CMV22-00279-01
45.137.22.72	RootLayer Web Services Ltd.	2CMV22-00279-01
45.137.22.190	RootLayer Web Services Ltd.	2CMV22-00279-01
96.125.178.141	DATABANK-DFW	2CMV22-00279-01
185.222.57.94	RootLayer Web Services Ltd.	2CMV22-00279-01

175.177.155.115	Its communications Inc.	2CMV22-00279-01
209.85.160.169	Google LLC	2CMV22-00279-01
209.85.219.54	Google LLC	2CMV22-00279-01
209.85.216.52	Google LLC	2CMV22-00279-01
45.9.168.157	MAXKO j.d.o.o.	2CMV22-00279-01
209.85.166.196	Google LLC	2CMV22-00279-01

Nombres de archivo: Corresponden a aquellos documentos que vienen adjuntos en las campañas de phishing con malware. El CSIRT de Gobierno recomienda que cada institución analice las extensiones de los archivos y evalúe cuáles serán bloqueadas o permitidas. Asimismo se deben ejecutar de forma permanente las actualizaciones de los módulos de antivirus de los antispam y de las estaciones de trabajo.

Nombres de archivos con malware	Documento web
$46,567,19_202019153048.xlsx	2CMV22-00276-01
Aviso 25022022.xlsm	2CMV22-00276-01
conocimiento de embarque y factura comercial_XLSx.img	2CMV22-00276-01
cotizacin_____pdf.rar	2CMV22-00276-01
Info 2302.xls	2CMV22-00276-01
informe 456496.xlsm	2CMV22-00276-01
invoice.r17	2CMV22-00276-01
iQqD-06705669.xlsm	2CMV22-00276-01
message1433.zip	2CMV22-00276-01
new order#098799.r15	2CMV22-00276-01
Order.zip	2CMV22-00276-01
payment advice.7z	2CMV22-00276-01
Payment for Outstanding Invoices (SOA).r00	2CMV22-00276-01
payment swift.zip	2CMV22-00276-01
PO 4100066995.rar	2CMV22-00276-01
PO22-0452.r15	2CMV22-00276-01
proforma invoice.xlsx	2CMV22-00276-01
RÃ¡pido del pago pdf.exe.xz	2CMV22-00276-01
RFQ#103243.xlsx	2CMV22-00276-01
scanned custom declartion.zip	2CMV22-00276-01
SHIPPING INSTRUCTIONS.rar	2CMV22-00276-01
Statement.xlsx	2CMV22-00276-01
URGENT INQUIRY.r00	2CMV22-00276-01
5345678.zip	2CMV22-00279-01
bank details.zip	2CMV22-00279-01
CUSTOM DECLARATION.zip	2CMV22-00279-01
NEW PAYMENT.zip	2CMV22-00279-01
Outstanding_payment202047654Outstanding_payment202047654.rar	2CMV22-00279-01

Pedido.gz	2CMV22-00279-01
Pedido.r00	2CMV22-00279-01
PO 67890231.zip	2CMV22-00279-01
PO#03082022.7z	2CMV22-00279-01
PO#4500550329.xlsx	2CMV22-00279-01
PO.r15	2CMV22-00279-01
Purchase Order 0062101239.r15	2CMV22-00279-01
Quotation Edge cutter Machine.zip	2CMV22-00279-01
SCAN_112877484993940484_jpg.iso	2CMV22-00279-01
SHIPPING ADVICE DOCS#202203.zip	2CMV22-00279-01
TELEX.zip	2CMV22-00279-01

Indicadores de Compromiso de campaña de Emotet

Servidores	IP
server242-1.web-hosting.com	[199.188.200.56]
vnit-services.com	[124.158.12.177]
hm1480-40.locaweb.com.br	[201.76.49.171]
mcegress-30-lw-144.correio.biz	[191.252.30.144]
mcegress-30-lw-131.correio.biz	[191.252.30.131]
cookpower2.dnsnoc123.com	[59.125.33.116]
gmmr3.centrum.cz	[46.255.225.251]
mcrelay.correio.biz	[201.76.49.48]
post3-gw.beenets.com	[119.63.80.29]
host16.dnsforindia.com	[103.235.105.142]
vmi753156.contaboserver.net	[109.205.179.110]
mitsuwa-logi.co.jp	[122.28.35.224]
doxon.jp	[211.129.7.126]
hm1480-16.locaweb.com.br	[201.76.49.113]
mail49228.hm1479.locaweb.com.br	[201.76.49.228]
mail.pppipe.co.th	[203.156.127.25]
mail49233.hm1315.locaweb.com.br	[201.76.49.233]
cs66.hostneverdie.com	[27.254.86.17]
smtp-sp221-75.uni5.net	[191.6.221.75]
vps53977.inmotionhosting.com	[104.247.76.50]
mail4977.hm1479.locaweb.com.br	[201.76.49.77]
hm1480-n-202.locaweb.com.br	[189.126.112.202]
bigpopcorn3.fastcloud.id	[103.28.12.47]

hm1481-22.locaweb.com.br	[201.76.49.144]
hm1831-8.locaweb.com.br	[189.126.112.28]
mail.kapersul.com.br	[200.160.25.22]
smtp-sp217-31.kinghost.net	[191.6.217.31]
mail9070.maychuemail.com	[112.213.90.70]
mail.coway.co.th	[122.155.167.4]
mitsuwa-logi.co.jp	[122.28.35.224]
hm1480-40.locaweb.com.br	[201.76.49.171]
cs66.hostneverdie.com	[27.254.86.17]
mail.ecohost.la	[201.220.156.239]
hm1480-39.locaweb.com.br	[201.76.49.170]
mcegress-30-lw-154.correio.biz	[191.252.30.154]
calig105111.dedicados.cl	[201.148.105.111]

Hash
0FCC8815284E3A8CF16C1EB8BB041DAD7375C88F3D8F01EB16540C6A16137D02
BD03B70BE5358EF31B8E6BCA9B8646DB88C977E4B1E93C4CBABFD06558A8C7CA
5214E05A00490891064917DB3463B844F7932F5777D56CD66BEB509F8E056808
0FCC8815284E3A8CF16C1EB8BB041DAD7375C88F3D8F01EB16540C6A16137D02
F90BBA8F2B1F7E9757CB9961D99562FDBBAA35C906ED22ACB4A8199A962469CC
F90BBA8F2B1F7E9757CB9961D99562FDBBAA35C906ED22ACB4A8199A962469CC
3A1CBECA7CBCC7DF6081818277D2D93AB133EE1CEABF2787368C18B7BCE1DF61
0D90E20D8F3F9FDB60FF8F671FA7A399A06CF90435B459CDF55A6E9D822BF7D1
1753CFCA314EE99336CDBA3AFF129A90381A38DE778F6D77410E9C46C2BB3B35
0D90E20D8F3F9FDB60FF8F671FA7A399A06CF90435B459CDF55A6E9D822BF7D1
62D9DDEA21249160090AE3E61611F513717D9813E2A8F62E6BCD2ECB39272022
1753CFCA314EE99336CDBA3AFF129A90381A38DE778F6D77410E9C46C2BB3B35
DB9192EFFE5D186572A91514169AE20AEA737D93196C283A4AE8CA2FF406932
1E4BBC492019F0A71D57D5C0F77843E71C1170EEDAE91D1C4310DE188AF7F42F
4C0928D3F7DED6095DD67C634270AF7FA1E0E74F262756636E525D7B04AAE8C3
F1DF8D1AFC0D97FCEA291E6BF4E5F0A77C0BEEA592A674E7D93E1A5B53C1D6FB
1E4BBC492019F0A71D57D5C0F77843E71C1170EEDAE91D1C4310DE188AF7F42F

IoC URLS
http://edicatiefarahotare[.]royalwebhosting.net/8Q33O8v63Ei2h2g/
http://estetaaaaa.125mb[.]com/admin/IE5zu5A9ly/
http://fasovitrine[.]com/wp-admin/5EhPJ14tOSzT/
http://gaddco[.]com/cgi-bin/sARa39due/
https://www.hih7[.]com/wp-admin/EQZYT/
https://www.yesdeko[.]com/be/6yhOfqLH2NMVtUQuPYD/
https://jonaloredo[.]com/inc/G6mr1U5rfD7XeX/
http://matskigroup[.]com/wp-admin/nqGatgYyNskXXqEnJw/
http://safecampus[.]net/wp-includes/YUeG3uumtePP/
http://akbakan[.]com/aQonQ0Rc/
http://hippocrates-poetry[.]org/10th-annual-hippocrates/uS0IeOAAuoQ7NP9cm/
http://cabinetcecaf[.]com/wp-admin/DhqUy/
http://digidist[.]com/y3/PfakjJB/
https://cloud-ci[.]online/backup/dBsIP/

Actualidad

Día Internacional de la Mujer: Ciberconsejos para estar más protegidas en el mundo virtual

Con la conmemoración de un nuevo Día Internacional de la Mujer, aprovechamos de recordar algunos de los principales riesgos al desenvolverse en la red, que impactan seriamente a las mujeres, y algunas conductas seguras que es recomendable adoptar para reducirlos. La campaña se puede visitar aquí: https://www.csirt.gob.cl/recomendaciones/dia-internacional-de-la-mujer-ciberconsejos-para-estar-mas-protegidas-en-el-mundo-virtual/.

Recomendaciones y buenas prácticas

- 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 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 (https://www.csirt.gob.cl o al teléfono + (562) 2486 3850) siempre que hayan aportado información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- Patricio Moraga
- Sebastián Guevara
- Moisés Moya
- Bárbara Palacios
- Felipe Chamorro
- Fernando González