Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

15-07-2022 | Año 4 | N°158

Boletín de Seguridad Cibernética

Semana del 8 al 14 de julio de 2022

La semana en cifras

Parches

164

para vulnerabilidades

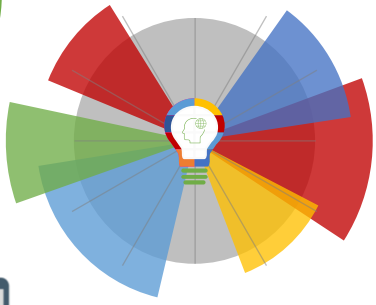
Las mitigaciones son útiles en productos de Google Cisco, Fortinet, Microsoft, OpenSSL y SAP.

Hash

5

SHA

Asociadas a múltiples campañas de phishing con archivos que contienen malware



Se advirtieron

19

URL

Asociadas a sitios fraudulentos y campañas de phishing y malware.

IP

6

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

Malware

CSIRT alerta por phishing con malware que se difunde alegando falsa multa	
Alerta de seguridad cibernética	2CMV21-00306-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Julio de 2021
Última revisión	11 de Julio de 2021
Indicadores de compromiso	
SHA256	
Nombre: Lod78y12jdhjas.zip SHA256: 9ce103595678802f7572ac4af61777531468d2c9e222a593662e8dc9f990b044 Nombre: d78y12jdhjas.msi SHA256: 3da7ee4007a3b168ae07c66934e8e62468d83293be7bb18a960de1d38cf01177 Nombre: cavalo5.exe SHA256: 3242e0a736ef8ac90430a9f272ff30a81e2afc146fcb84a25c6e56e8192791e4 Nombre: JSON.ahk SHA256: bb85e4530ccd6355b3ef3506548b4f513bea844d1af37a69624c9c455521c70f Nombre: cavalo5.ahk SHA256: 209d428be623f793c46726a87149730ccd0b11ebbf159df10765b4fb77199c6e	
IoC URL	
sameh-advisor[.]com hXXp://18.234.175.226/clientes/?hash=ZWdhbGF6Y0BpbnRlcmlvci5nb2IuY2w= hXXp://18.234.175.226/clientes/te.html hXXps://www.sameh-advisor[.]com/css/style/cpanel/brume.php	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00305-01/	
https://www.csirt.gob.cl/media/2022/07/2CMV22-00306-PH-01.pdf	

Phishing

Imagen del mensaje

CSIRT advierte phishing que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH22-00554-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de julio de 2022
Última revisión	8 de julio de 2022
Indicadores de compromiso	
URL Redirección	
https://bit[.]ly/3yPCjlC?l=www.bancoripley.cl https://seaturtlerentals[.]com/wp-content/languages/plugins/enviar02.php?l=606052081 https://bit[.]ly/3OOZUIK?l=www.bancoripley.cl https://kinkhair.co[.]uk/activacion/cuenta-ebuu/	
URL sitio falso	
http://bancoripley.cl.i-fitt[.]com/1657304337/login	
IP	
[103.27.34.1]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00554-01/	
https://www.csirt.gob.cl/media/2022/07/8FPH22-00554-01.pdf	

Imagen del mensaje

CSIRT alerta de campaña de phishing que suplanta a Microsoft	
Alerta de seguridad cibernética	8FPH22-00555-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de julio de 2022
Última revisión	8 de julio de 2022
Indicadores de compromiso	
URL sitio falso	
https://cranstonfamilyclinic[.]com/webup/Cgw/Lern/Del/Will/	
IP	
[45.60.96.242]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00555-01/	
https://www.csirt.gob.cl/media/2022/07/8FPH22-00555-01.pdf	

CSIRT alerta de campaña de phishing que suplanta a Cencosud	
Alerta de seguridad cibernética	8FPH22-00556-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de julio de 2022
Última revisión	12 de julio de 2022
Indicadores de compromiso	
URL Redirección	
https://bit[.]ly/3uCHOSf	
URL sitio falso	
https://www3mirtajelacencsud.codnechile[.]com/1657653938/TarjetaMasWEB/login	
IP	
[172.67.205.199]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00556-01/	
https://www.csirt.gob.cl/media/2022/07/8FPH22-00556-01.pdf	

CSIRT advierte de campaña de phishing que suplanta al Banco de Chile	
Alerta de seguridad cibernética	8FPH22-00557-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de julio de 2022
Última revisión	12 de julio de 2022
Indicadores de compromiso	
URL Redirección	
https://bit[.]ly/3RrcMXa	
URL sitio falso	
https://login.portal-bancochlle.cl.realshoes[.]it/1657655443/bcochile-web/persona/login/index.html/login	
IP	
[89.40.173.174]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00557-01/	
https://www.csirt.gob.cl/media/2022/07/8FPH22-00557-01.pdf	

Imagen del mensaje

CSIRT alerta de phishing por email que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FPH22-00558-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de julio de 2022
Última revisión	14 de julio de 2022
Indicadores de compromiso	
URL Redirección	
https://bit[.]ly/3Pn3mu2?l=www.santander.cl http://brombalplatform[.]com/disegnatori/bootstrap/enviar02.php?l=1038686473 https://bit[.]ly/3PoGyKn?l=www.santander.cl https://gurujam[.]com/activacion/cuenta-viwq/	
URL sitio falso	
http://banco.santander[.]cl.afsarsports.com/1657817237/portada/personas/home.asp	
IP	
[162.222.227.230]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00558-01/	
https://www.csirt.gob.cl/media/2022/07/8FPH22-00558-01.pdf	

Imagen del mensaje

CSIRT alerta ante phishing que suplanta al BancoEstado con falsa compra en Israel	
Alerta de seguridad cibernética	8FPH22-00559-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de julio de 2022
Última revisión	14 de julio de 2022
Indicadores de compromiso	
URL Redirección	
https://contribvalpa[.]com/promocion/cuenta-wwju/	
URL sitio falso	
https://sistema.proexito.com[.]mx/wavdfr/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[166.62.116.177]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00559-01/	
https://www.csirt.gob.cl/media/2022/07/8FPH22-00559-01.pdf	

Vulnerabilidades

CSIRT comparte vulnerabilidades críticas de Cisco	
Alerta de seguridad cibernética	9VSA22-00671-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de julio de 2022
Última revisión	8 de julio de 2022

CVE

CVE-2022-20812	CVE-2022-20800	CVE-2022-20671
CVE-2022-20813	CVE-2022-20791	CVE-2022-20672
CVE-2022-20808	CVE-2022-20651	CVE-2022-20673
CVE-2022-20752	CVE-2022-20666	CVE-2022-20674
CVE-2022-20862	CVE-2022-20667	CVE-2022-20828
CVE-2022-20859	CVE-2022-20668	CVE-2022-20829
CVE-2022-20768	CVE-2022-20669	CVE-2022-20802
CVE-2022-20815	CVE-2022-20670	

Fabricantes

Cisco

Productos afectados

Cisco Expressway Series y Cisco TelePresence Video Communication Server (VCS) (CVE-2022-20812 y CVE-2022-20813).
Cisco Smart Software Manager On-Prem: CVE-2022-20808.
Cisco Unified Communications Products; CVE-2022-20752, CVE-2022-20859, CVE-2022-20815, CVE-2022-20800, CVE-2022-20791.
Cisco Unified Communications Manager: CVE-2022-20862.
Cisco TelePresence Collaboration Endpoint (CE) y RoomOS: CVE-2022-20768.
Cisco Adaptive Security Device Manager: CVE-2022-20651.
Cisco Common Services Platform Collector (CSPC): CVE-2022-20666, CVE-2022-20667, CVE-2022-20668, CVE-2022-20669, CVE-2022-20670, CVE-2022-20671, CVE-2022-20672, CVE-2022-20673, CVE-2022-20674.
Cisco FirePOWER Software for Adaptive Security Appliance (ASA): CVE-2022-20828.
Cisco Adaptive Security Device Manager y Adaptive Security Appliance Software: CVE-2022-20829.
Cisco Enterprise Chat and Email: CVE-2022-20802.

Enlaces para revisar el informe:

https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00671-01/
https://www.csirt.gob.cl/media/2022/07/9VSA22-00671-01.pdf

CSIRT alerta de vulnerabilidades de alto riesgo en productos Fortinet	
Alerta de seguridad cibernética	9VSA22-00672-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de julio de 2022
Última revisión	8 de julio de 2022
CVE	
CVE-2021-43072 CVE-2021-41031 CVE-2022-30302 CVE-2022-26117	
Fabricante	
Fortinet	
Productos afectados	
CVE-2021-43072: FortiAnalyzer, FortiManager, FortiOS y FortiProxy. CVE-2021-41031: FortiClient. CVE-2022-30302: FortiDeceptor versiones 1.0.0 a 4.0.1. CVE-2022-26117: FortiNAC versiones 8.3.7 a 9.2.3.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00672-01/	
https://www.csirt.gob.cl/media/2022/07/9VSA22-00672-01.pdf	

CSIRT alerta de vulnerabilidad de alto riesgo en OpenSSL	
Alerta de seguridad cibernética	9VSA22-00673-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de julio de 2022
Última revisión	11 de julio de 2022
CVE	
CVE-2022-2274	
Fabricante	
OpenSSL	
Productos afectados	
OpenSSL 3.0.4	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00673-01/	
https://www.csirt.gob.cl/media/2022/07/9VSA22-00673-01.pdf	

CSIRT comparte vulnerabilidades del Update Tuesday julio 2022 de Microsoft	
Alerta de seguridad cibernética	9VSA22-00674-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de julio de 2022
Última revisión	12 de julio de 2022

CVE

CVE-2022-22048	CVE-2022-33632	CVE-2022-22026
CVE-2022-22047	CVE-2022-22050	CVE-2022-22025
CVE-2022-23825	CVE-2022-22049	CVE-2022-22024
CVE-2022-33672	CVE-2022-30187	CVE-2022-22023
CVE-2022-33671	CVE-2022-33678	CVE-2022-22022
CVE-2022-33669	CVE-2022-33677	CVE-2022-30226
CVE-2022-33668	CVE-2022-33676	CVE-2022-30225
CVE-2022-33667	CVE-2022-33675	CVE-2022-30224
CVE-2022-33666	CVE-2022-33674	CVE-2022-30223
CVE-2022-33665	CVE-2022-33673	CVE-2022-30222
CVE-2022-33664	CVE-2022-33641	CVE-2022-30220
CVE-2022-33663	CVE-2022-33637	CVE-2022-30216
CVE-2022-33662	CVE-2022-27776	CVE-2022-30215
CVE-2022-33661	CVE-2022-33633	CVE-2022-30214
CVE-2022-33660	CVE-2022-22045	CVE-2022-30213
CVE-2022-33659	CVE-2022-22043	CVE-2022-30212
CVE-2022-33658	CVE-2022-22042	CVE-2022-30211
CVE-2022-33657	CVE-2022-22041	CVE-2022-30209
CVE-2022-33656	CVE-2022-22040	CVE-2022-30208
CVE-2022-33655	CVE-2022-22039	CVE-2022-30206
CVE-2022-33654	CVE-2022-22038	CVE-2022-30205
CVE-2022-33653	CVE-2022-22037	CVE-2022-30203
CVE-2022-33652	CVE-2022-22036	CVE-2022-30202
CVE-2022-33651	CVE-2022-22034	CVE-2022-30181
CVE-2022-23816	CVE-2022-22031	CVE-2022-22711
CVE-2022-33650	CVE-2022-22029	CVE-2022-33644
CVE-2022-33643	CVE-2022-22028	CVE-2022-30221
CVE-2022-33642	CVE-2022-22027	CVE-2022-21845

Fabricante

Microsoft

Productos afectados

Azure Site Recovery VMWare to Azure
Azure Storage Blobs client library for .NET
Azure Storage Blobs client library for Java
Azure Storage Blobs client library for Python
Azure Storage Queues client library for .NET
Azure Storage Queues client library for Python
Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems

Microsoft Defender for Endpoint for Linux
Microsoft Lync Server 2013 CU10
Microsoft Office 2013 RT Service Pack 1
Microsoft Office 2013 Service Pack 1 (32-bit editions)
Microsoft Office 2013 Service Pack 1 (64-bit editions)
Microsoft Office 2016 (32-bit edition)
Microsoft Office 2016 (64-bit edition)
Microsoft Office 2019 for 32-bit editions
Microsoft Office 2019 for 64-bit editions
Microsoft Office LTSC 2021 for 32-bit editions
Microsoft Office LTSC 2021 for 64-bit editions
Remote Desktop client for Windows Desktop
Skype for Business Server 2015 CU12
Skype for Business Server 2019 CU6
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 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, version 20H2 (Server Core Installation)
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00674-01/
https://www.csirt.gob.cl/media/2022/07/9VSA22-00674-01.pdf

CSIRT comparte vulnerabilidades publicadas por Android	
Alerta de seguridad cibernética	9VSA22-00675-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de julio de 2022
Última revisión	13 de julio de 2022

CVE		
CVE-2022-20219	CVE-2022-20230	CVE-2022-20216
CVE-2022-20228	CVE-2022-20228	CVE-2022-20217
CVE-2022-20229	CVE-2022-20220	CVE-2022-20236
CVE-2022-20222	CVE-2022-20227	CVE-2022-20238
CVE-2021-0981	CVE-2022-20083	CVE-2022-22096
CVE-2022-20223	CVE-2022-21744	CVE-2022-22058
CVE-2022-20226	CVE-2022-21767	CVE-2022-25667
CVE-2022-20224	CVE-2022-21768	CVE-2022-25658
CVE-2022-20225	CVE-2022-21763	CVE-2022-25659
CVE-2022-20221	CVE-2022-21764	

Fabricante
Google
Productos afectados
Android OS con parches anteriores al 5 de julio de 2022.
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00675-01/
https://www.csirt.gob.cl/media/2022/07/9VSA22-00675-01.pdf

CSIRT comparte vulnerabilidades que afectan a productos SAP	
Alerta de seguridad cibernética	9VSA22-00676-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de julio de 2022
Última revisión	13 de julio de 2022

CVE

CVE-2022-35228	CVE-2022-35170	CVE-2022-31598
CVE-2022-32249	CVE-2022-35225	CVE-2022-31597
CVE-2022-28771	CVE-2022-32247	CVE-2022-35168
CVE-2022-31593	CVE-2022-35224	CVE-2022-32248
CVE-2022-29619	CVE-2022-35227	CVE-2022-31592
CVE-2022-22542	CVE-2022-35169	CVE-2022-35171
CVE-2022-29611	CVE-2022-31591	CVE-2022-31594
CVE-2022-35172	CVE-2022-32246	

Fabricante

SAP

Productos afectados

SAP BusinessObjects Business Intelligence Platform (Central management console), versiones 420 a 430.
SAP Business One, Version -10.0.
SAP Business One License serviceAPI, Version -10.0.
SAP Business One, Version -10.0.
SAP BusinessObjects Business Intelligence Platform 4.x, versiones 420 a 430.
SAPS/4HANA (Supplier Factsheet and Enterprise Search for Business Partner, Supplier and Customer), versiones 104 a 106.
SAP NetWeaver Application Server for ABAP and ABAP Platform, versiones 700 a 788.
SAP NetWeaver Enterprise Portal, Versions -7.10 a 7.50.
SAP BusinessObjects Business Intelligence Platform (LCM), versiones -420 a 430.
SAP BusinessObjects BW Publisher Service, versiones -420, 430.
SAP BusinessObjects Business Intelligence Platform (Visual Difference Application), versiones 420 a 430.
SAP Business Objects,Version -420
SAPS/4HANA, Versions -S4CORE 101 a 127
SAP Business one, Version -10.0
SAP Enterprise Extension Defense Forces & Public Security (EA-DFPS),Versions -605, 606, 616,617,618, 802, 803, 804, 805, 806
SAP3D Visual Enterprise Viewer, Version -9.0
SAP Adaptive Server Enterprise (ASE),Versions -KERNEL 7.22, 7.49, 7.53, KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC 7.22, 7.22EXT, 7.49, 7.53

Enlaces para revisar el informe:

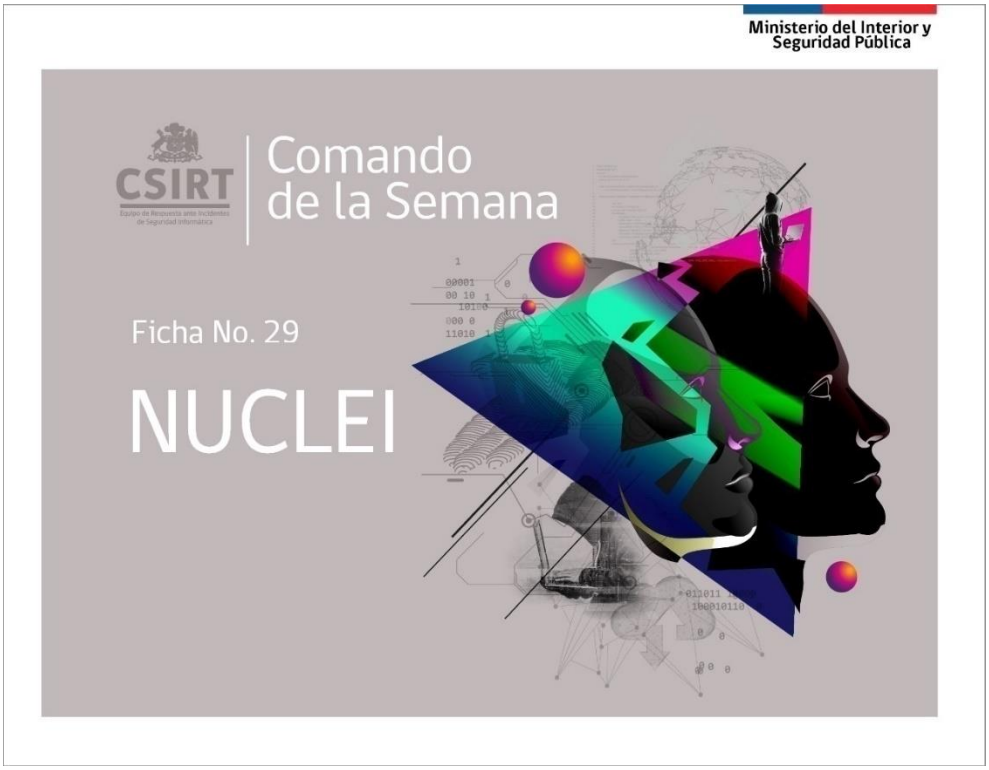
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00676-01/
https://www.csirt.gob.cl/media/2022/07/9VSA22-00676-01.pdf

Actualidad

El Comando de la Semana | No. 29 Nuclei

En esta ocasión, el Comando de la Semana nos presentó a Nuclei, una herramienta que permite ejecutar pruebas de pentesting sobre aplicaciones web y otros servicios, reduciendo al máximo los falsos positivos.

Descarga el Comando de la Semana aquí: https://www.csirt.gob.cl/estadisticas/el-comando-de-la-semana-no-29/.



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 campañas de phishing, malware y/o sitios fraudulentos.**

El CSIRT de Gobierno destaca en este segmento a quienes reportaron incidentes utilizando canales formales (https://www.csirt.gob.cl o al teléfono **1510** siempre que hayan aportado información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- Rodrigo Andrés Cortés Cortés
- Ámbar Campos
- Óscar Alejandro Baier Aguayo
- Felipe Pizarro Astudillo
- Claudio González Pauzoca
- Christian Abarca
- Jean Pablo Catalán Marín
- Sergio
- Andrés Aldana F.
- Jair Palma
- Gonzalo Venegas Aguirre
- Javier Karmy Selman
- Gonzalo Araya Navarrete
- Camilo Ignacio Ortúzar Aránguiz
- Fernando Marcelo Cruces González