CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 4 | N.º 189

SEMANA DEL 10 AL 16 de FEBRERO 2023

LA SEMANA EN CIFRAS

PARCHES COMPARTIDOS

114

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

IP INFORMADAS

18

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

URL ADVERTIDAS

24

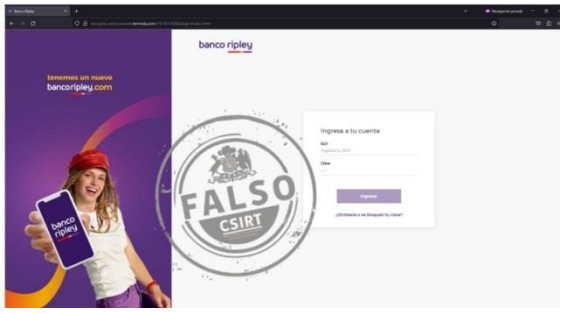
Asociadas a sitios fraudulentos y campañas de phishing y malware

CONTENIDO

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

1. Sitios fraudulentos

Imagen del sitio

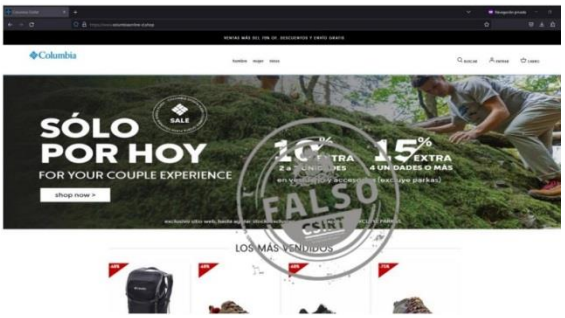


CSIRT alerta de página fraudulenta que suplanta a Banco Ripley	
Alerta de seguridad cibernética	8FFR23-01207-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de febrero de 2023
Última revisión	13 de febrero de 2023
Indicadores de compromiso	
URL sitio falso	
http://bcoripley-personasweb.lemmda[.]com/1676319384/login/index.html	
Dirección IP	
[66.29.132.80]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01207-01/	
https://www.csirt.gob.cl/media/2023/02/8FFR23-01207-01.pdf	

Imagen del sitio

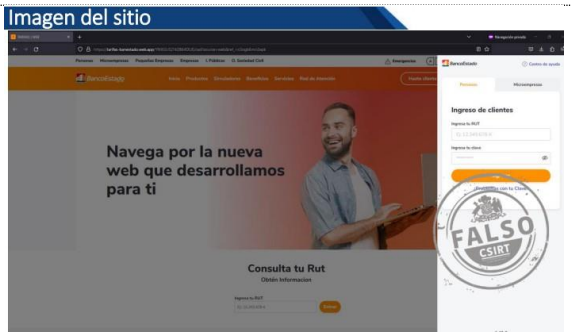
CSIRT alerta de una página fraudulenta que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR23-01208-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de febrero de 2023
Última revisión	14 de febrero de 2023
Indicadores de compromiso	
URL sitio falso	
https://cc85642.tw1[.]ru/correoscl/correos-jdida/pack/	
Dirección IP	
[92.53.118.39]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01208-01/	
https://www.csirt.gob.cl/media/2023/02/8FFR23-01208-01.pdf	

Imagen del sitio



CSIRT alerta de página fraudulenta que suplanta a Columbia	
Alerta de seguridad cibernética	8FFR23-01209-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de febrero de 2023
Última revisión	14 de febrero de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.columbiaonline-cl[.]shop/	
Dirección IP	
[172.67.199.42]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01209-01/	
https://www.csirt.gob.cl/media/2023/02/8FFR23-01209-01.pdf	

Imagen del sitio



CSIRT advierte sitio fraudulento del Banco Estado	
Alerta de seguridad cibernética	8FFR23-01210-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de febrero de 2023
Última revisión	15 de febrero de 2023
Indicadores de compromiso	
URL sitio falso	
https://bit[.]ly/3BohsH2	
http://157.245.104[.]204/565TRDTDIFIYTDTYJIU/N6744SXGXHGJHFJHCGFXGF-AAA/YYJVHHGCGRXFDZDA789GCJFHDZGSDZHXCVNBHMGCGF/eded35JLHJFDGRERWEQSDFGVGFXHFDSFESRX/	
https://tarifas-banestado.web[.]app/EMPEJNJN/2K7369H72LA3	
https://tarifas-banestado.web[.]app/YNXGUQ742B64DUE/cad?source=web&ref_=c3ogb6mn2epk	
Dirección IP	
[199.36.158.100]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01210-01/	
https://www.csirt.gob.cl/media/2023/02/8FFR23-01210-01.pdf	

Imagen del sitio

CSIRT advierte sitio que suplanta al Banco Falabella	
Alerta de seguridad cibernética	8FFR23-01211-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de febrero de 2023
Última revisión	15 de febrero de 2023
Indicadores de compromiso	
URL sitio falso	
https://falabellaprochilesecure.dembele000.repl[.]co/	
Dirección IP	
[34.149.204.188]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01211-01/	
https://www.csirt.gob.cl/media/2023/02/8FFR23-01211-01.pdf	

Imagen del sitio

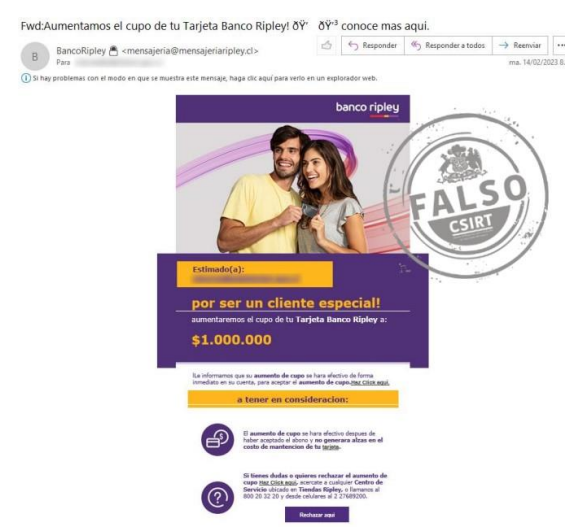
CSIRT avierte sitio falso que suplanta a Skechers	
Alerta de seguridad cibernética	8FFR23-01212-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de febrero de 2023
Última revisión	16 de febrero de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.runshoecls[.]shop/	
Dirección IP	
[107.150.173.212]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01212-01/	
https://www.csirt.gob.cl/media/2023/02/8FFR23-01212-01.pdf	

2. Phishing

Imagen del mensaje	CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado con falso pago FOGAPE	
	Alerta de seguridad cibernética	8FPH23-00745-01
	Clase de alerta	Fraude
	Tipo de incidente	Phishing
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	13 de febrero de 2023
	Última revisión	13 de febrero de 2023
	Indicadores de compromiso	
	URL redirección	
	https://ucmstudio[.]info/activacion/cuenta-innr/	
	URL sitio falso	
	https://smestadofogape[.]online/1676290544/imagenes/_personas/home/default.asp	
	Dirección IP	
	[202.89.39.2]	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8fph23-00745-01/	
	https://www.csirt.gob.cl/media/2023/02/8FPH23-00745-01.pdf	

Imagen del mensaje	CSIRT alerta de nueva campaña de phishing que suplanta al Servicio de Impuestos Internos (SII)	
	Alerta de seguridad cibernética	8FPH23-00746-01
	Clase de alerta	Fraude
	Tipo de incidente	Phishing
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	13 de febrero de 2023
	Última revisión	13 de febrero de 2023
	Indicadores de compromiso	
	URL redirección	
	https://luzca[.]com/img2/?98SUDF80SYGF8DSGHISDVHDU	
	URL sitio falso	
	https://facturas4[.]click/?pAleZ85aIcHAwGMSJETsLhkLdKHRUsrFuhnzP8cwpAleZ85aIcHAwGMSJETsLhkLdKHRUsrFuhnzP8cw	
	Dirección IP	
	[66.29.132.88]	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8fph23-00746-01/	
	https://www.csirt.gob.cl/media/2023/02/8FPH23-00746-01.pdf	

Imagen del mensaje



CSIRT alerta de nueva campaña de phishing que suplanta a Banco Ripley	
Alerta de seguridad cibernética	8FPH23-00747-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de febrero de 2023
Última revisión	14 de febrero de 2023
Indicadores de compromiso	
URL redirección	
https://bit[.]ly/3lpPk13?l=www.bancoripley.cl	
https://sam-tech[.]jp/bancoripley/cuenta-tugk/	
URL sitio falso	
https://www-banco.ripley-cl.gkmayprop[.]com/1676379786/login	
Dirección IP	
[130.51.180.17]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00747-01/	
https://www.csirt.gob.cl/media/2023/02/8FPH23-00747-01.pdf	

Imagen del mensaje

CSIRT alerta campaña de phishing que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FPH23-00748-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de febrero de 2023
Última revisión	15 de febrero de 2023
Indicadores de compromiso	
URL redirección	
https://cartoonpuzzl3s[.]com/activacion/cuenta-buqj/	
URL sitio falso	
https://nwmpatitocliente[.]lol/1676474686/imagenes/_personas/home/default.asp	
Dirección IP	
[104.21.94.102]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00748-01/	
https://www.csirt.gob.cl/media/2023/02/8FPH23-00748-01.pdf	

Imagen del mensaje

CSIRT alerta campaña de phishing que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH23-00749-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de febrero de 2023
Última revisión	16 de febrero de 2023
Indicadores de compromiso	
URL redirección	
https://t[.]co/0EUMFOBG06	
https://appscl[.]website/	
https://forum.boombang[.]tv/profile/bancoripley.cl	
URL sitio falso	
http://bancoripleymovil.cl.hotelalpinodearmenia[.]com/1676486521/login/index.html	
Dirección IP	
[198.54.126.39]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00749-01/	
https://www.csirt.gob.cl/media/2023/02/8FPH23-00749-01.pdf	

Imagen del mensaje

CSIRT alerta nueva campaña de phishing que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH23-00750-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de febrero de 2023
Última revisión	16 de febrero de 2023
Indicadores de compromiso	
URL redirección	
https://bit[.]ly/3xvQB9q?l=www.bancoripley.cl	
URL sitio falso	
https://web.bancoripley.cl.imexcomed.com[.]bo/1676558297/login	
Dirección IP	
[69.73.184.9]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00750-01/	
https://www.csirt.gob.cl/media/2023/02/8FPH23-00750-01.pdf	

3. Fuerza Bruta

CSIRT alerta de ataques de fuerza bruta contra SMTP	
Alerta de seguridad cibernética	4IIA23-00062-01
Clase de alerta	Intentos de Intrusión
Tipo de incidente	Intentos de acceso – Fuerza bruta
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de febrero de 2023
Última revisión	15 de febrero de 2023
Indicadores de compromiso	
Direcciones IP	
46.148.40.177 46.148.40.91 80.94.95.204 185.36.81.70 103.74.107.101 103.74.104.32	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/4iia23-00062-01/	
https://www.csirt.gob.cl/media/2023/02/4IIV22-00062-01.pdf	

4. Vulnerabilidades

CSIRT comparte vulnerabilidades parchadas en Google Chrome 110		
Alerta de seguridad cibernética	9VSA23-00786-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Crítico	
TLP	Blanco	
Fecha de lanzamiento original	13 de febrero de 2023	
Última revisión	13 de febrero de 2023	
CVE		
CVE-2023-0696	CVE-2023-0700	CVE-2023-0703
CVE-2023-0697	CVE-2023-0701	CVE-2023-0704
CVE-2023-0698	CVE-2023-0702	CVE-2023-0705
CVE-2023-0699		
Fabricante		
Google		
Productos afectados		
Google Chrome anteriores a la versión 110.		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00786-01/		
https://www.csirt.gob.cl/media/2023/02/9VSA23-00786-01.pdf		

CSIRT comparte vulnerabilidades parchadas por Microsoft en su Update Tuesday de febrero 2023		
Alerta de seguridad cibernética	9VSA23-00787-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Crítico	
TLP	Blanco	
Fecha de lanzamiento original	14 de febrero de 2023	
Última revisión	14 de febrero de 2023	
CVE		
CVE-2023-21524	CVE-2023-21766	CVE-2023-21681
CVE-2023-21538	CVE-2023-21765	CVE-2023-21680
CVE-2023-21549	CVE-2023-21771	CVE-2023-21679
CVE-2023-21773	CVE-2023-21741	CVE-2023-21678
CVE-2023-21768	CVE-2023-21755	CVE-2023-21677
CVE-2023-21767	CVE-2023-21779	CVE-2023-21676
CVE-2023-21764	CVE-2023-21745	CVE-2023-21675
CVE-2023-21763	CVE-2023-21762	CVE-2023-21674
CVE-2023-21760	CVE-2023-21761	CVE-2023-21563
CVE-2023-21758	CVE-2023-21752	CVE-2023-21561
CVE-2023-21757	CVE-2023-21527	CVE-2023-21560
CVE-2023-21754	CVE-2023-21743	CVE-2023-21559
CVE-2023-21749	CVE-2023-21759	CVE-2023-21558
CVE-2023-21748	CVE-2023-21753	CVE-2023-21557
CVE-2023-21787	CVE-2023-21746	CVE-2023-21556
CVE-2023-21785	CVE-2023-21739	CVE-2023-21555
CVE-2023-21783	CVE-2023-21733	CVE-2023-21552

CVE-2023-21793	CVE-2023-21744	CVE-2023-21551
CVE-2023-21791	CVE-2023-21742	CVE-2023-21550
CVE-2023-21786	CVE-2023-21738	CVE-2023-21548
CVE-2023-21784	CVE-2023-21737	CVE-2023-21543
CVE-2023-21782	CVE-2023-21736	CVE-2023-21542
CVE-2023-21781	CVE-2023-21735	CVE-2023-21541
CVE-2023-21776	CVE-2023-21734	CVE-2023-21540
CVE-2023-21774	CVE-2023-21732	CVE-2023-21539
CVE-2023-21747	CVE-2023-21730	CVE-2023-21547
CVE-2023-21525	CVE-2023-21728	CVE-2023-21546
CVE-2023-21792	CVE-2023-21726	CVE-2023-21537
CVE-2023-21790	CVE-2023-21725	CVE-2023-21536
CVE-2023-21789	CVE-2023-21724	CVE-2023-21531
CVE-2023-21788	CVE-2023-21683	CVE-2023-21535
CVE-2023-21750	CVE-2023-21682	CVE-2023-21532
CVE-2023-21772		

Fabricante

Microsoft

Productos afectados

.NET 6.0
3D Builder
Azure Service Fabric 8.2
Azure Service Fabric 9.0
Azure Service Fabric 9.1
Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Exchange Server 2013 Cumulative Update 23
Microsoft Exchange Server 2016 Cumulative Update 23
Microsoft Exchange Server 2019 Cumulative Update 11
Microsoft Exchange Server 2019 Cumulative Update 12
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 SharePoint Enterprise Server 2013 Service Pack 1
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Foundation 2013 Service Pack 1
Microsoft SharePoint Server 2019
Microsoft SharePoint Server Subscription Edition
Microsoft Visio 2013 Service Pack 1 (32-bit editions)
Microsoft Visio 2013 Service Pack 1 (64-bit editions)
Microsoft Visio 2016 (32-bit edition)
Microsoft Visio 2016 (64-bit edition)
PowerShell 7.2
Visual Studio Code
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 21H2 for 32-bit Systems Windows 10 Version 21H2 for ARM64-based Systems Windows 10 Version 21H2 for x64-based Systems Windows 10 Version 22H2 for 32-bit Systems Windows 10 Version 22H2 for ARM64-based Systems Windows 10 Version 22H2 for x64-based Systems Windows 11 version 21H2 for ARM64-based Systems Windows 11 version 21H2 for x64-based Systems Windows 11 Version 22H2 for ARM64-based Systems Windows 11 Version 22H2 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 Malicious Software Removal Tool 32-bit Windows Malicious Software Removal Tool 64-bit 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)
	Enlaces para revisar el informe:
	https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00787-01/
	https://www.csirt.gob.cl/media/2023/02/9VSA23-00787-01.pdf

CSIRT comparte vulnerabilidades y mitigaciones para Adobe Photoshop	
Alerta de seguridad cibernética	9VSA23-00788-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	15 de febrero de 2023
Última revisión	15 de febrero de 2023
CVE	
CVE-2023-21574 CVE-2023-21575 CVE-2023-21576 CVE-2023-21577 CVE-2023-21578	
Fabricantes	
Adobe	
Productos afectados	
Photoshop 2022: 23.5.3 y versiones anteriores para Windows y macOS Photoshop 2023: 24.1 y versiones anteriores para Windows y macOS	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00778-01-2/	
https://www.csirt.gob.cl/media/2023/02/9VSA23-00788-01.pdf	

CSIRT comparte vulnerabilidades en la biblioteca de escaneo de terceros ClamAV de Cisco	
Alerta de seguridad cibernética	9VSA23-00789-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	16 de febrero de 2023
Última revisión	16 de febrero de 2023
CVE	
CVE-2023-20032 CVE-2023-20052	
Fabricante	
Cisco	
Productos afectados	
ClamAV versiones 1.0.0 y anteriores; 0.105.1 y anteriores; y 0.103.7 y anteriores	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00789-01/	
https://www.csirt.gob.cl/media/2023/02/9VSA23-00789-01.pdf	

5. Concientización

Ciberconsejos para evitar el catfishing

El catfishing es una técnica que se utiliza para engañar en redes sociales, app de citas o internet, a personas que buscan encontrar pareja, configurando un perfil falso e incluso creando una personalidad y carácter. Caer en este tipo de estafa puede traer consigo distintos riesgos, entre ellos, acoso, fraudes económicos, grooming, daño emocional, venganzas amorosas, entre otros.

Ciberdiccionario Volumen 30

Esta semana en el ciberdiccionario del CSIRT de Gobierno explicamos los conceptos: ciberguerra, cyberflashing, certificado SSL y algoritmo.

6. 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 que los sitios web a los que se ingrese sean los oficiales.

7. 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.

- Javier Godoy
- Felipe Cortés
- Andrés Rojas
- Juan Alfredo Blanco
- Hernán Vega

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.02.17 17:27:48 -03'00'