Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

18-02-2022 | Año 4 | N°137

Boletín de Seguridad Cibernética

Semana del 11 al 17 de febrero de 2021

La semana en cifras

Hash

42

SHA

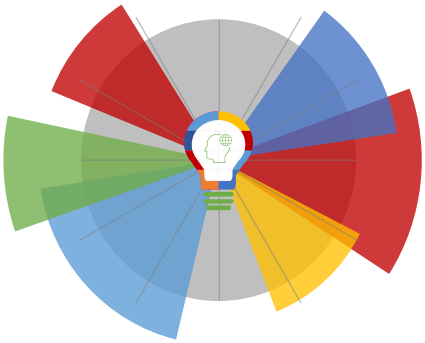
Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron

10

URL

Asociadas a sitios fraudulentos y campañas de phishing y malware.



Parches

6

para vulnerabilidades

Las mitigaciones son útiles en productos de Adobe, VMware y Apache.

IP

17

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

https://www.csirt.gob.cl
+ (562) 2486 3850
@csirtgob
@CSIRTConciencia
https://www.linkedin.com/company/csirt-gob

Malware

CSIRT alerta ante campaña de malware con falsa cotización	
Alerta de seguridad cibernética	2CMV21-00274-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de febrero de 2022
Última revisión	11 de febrero de 2022

Indicadores de compromiso

SHA256

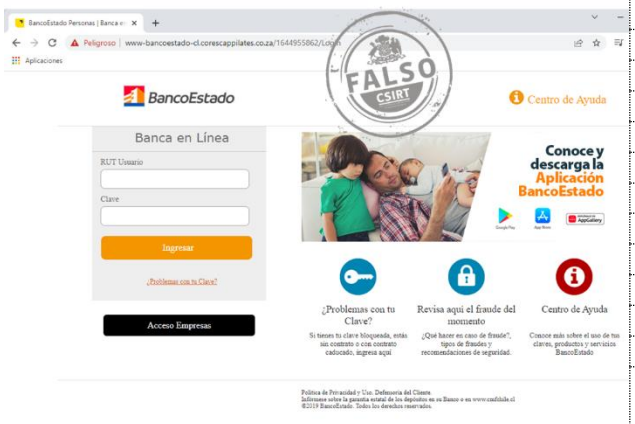
8E3DF87566EE830AAD2E0DD252D5003F689B3B03B5729B9212CA74E53A08FC61
B2DA3C044CC32224951309BD2CFEE81DF26FD54C08712FE4CB3277870 37C3F65

Enlaces para revisar el informe:

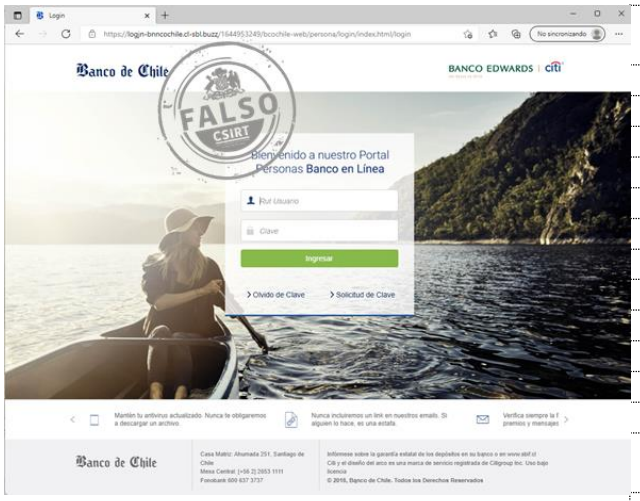
https://www.csirt.gob.cl/alertas/2cmv21-00274-01/
https://www.csirt.gob.cl/media/2022/02/2CMV22-00274-01-1.pdf

https://www.csirt.gob.cl + (562) 2486 3850 @csirtgob @CSIRTConciencia https://www.linkedin.com/company/csirt-gob

Phishing



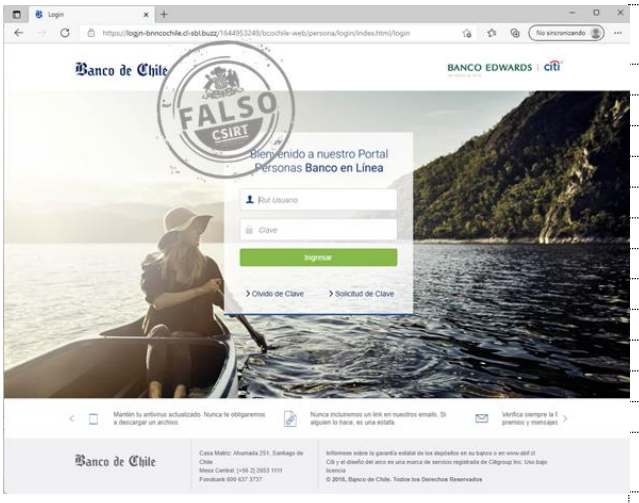
CSIRT alerta por campaña de phishing que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FPH22-00472-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de febrero de 2022
Última revisión	11 de febrero de 2022
Indicadores de compromiso	
URL sitio redirección	
http://toybeachclub[.]com/activacion/cuenta-tfqr/	
URL sitio falso	
https://itaupersonayempresacl.itauempresaspuntos[.]info/726a292db52f7f5/html/index.php	
IP	
[1.33.169.198]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00472-01/	
https://www.csirt.gob.cl/media/2022/02/8FPH22-00472-01.pdf	



CSIRT alerta de una nueva campaña de phishing que suplanta al Banco de Chile	
Alerta de seguridad cibernética	8FPH22-00473-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de febrero de 2022
Última revisión	15 de febrero de 2022
Indicadores de compromiso	
URL redirección	
https://bit[.]ly/portal-banchile	
https://diarioedomex[.]com/banchile.php	
URL sitio falso	
https://itaupersonayempresacl.itauempresaspuntos[.]info/726a292db52f7f5/html/index.php	
IP	
[104.21.86.153]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00473-01/	
https://www.csirt.gob.cl/media/2022/02/8FPH22-00473-01.pdf	

https://www.csirt.gob.cl + (562) 2486 3850 @csirtgob @CSIRTConciencia https://www.linkedin.com/company/csirt-gob

CSIRT advierte nueva campaña de phishing que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FPH22-00474-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de febrero de 2022
Última revisión	16 de febrero de 2022
Indicadores de compromiso	
URL redirección	
https://bit[.]ly/36dBrLR?l=www.bancoestado.cl	
http://www.meiyiyan[.]net/wp-content/languages/plugins/enviar02.php?l=884710907	
https://bit[.]ly/3GUv4JY?l=www.bancoestado.cl	
https://easycoquine[.]com/activacion/cuenta-htug/	
URL sitio falso	
https://www-bancoestado-cl.corescappilates[.]co.za/	
IP	
[5.77.50.29]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00474-01/	
https://www.csirt.gob.cl/media/2022/02/8FPH22-00474-01.pdf	



CSIRT alerta sobre una nueva campaña de phishing contra clientes del BancoEstado	
Alerta de seguridad cibernética	8FPH22-00475-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de febrero de 2022
Última revisión	15 de febrero de 2022
Indicadores de compromiso	
URL redirección	
https://bit[.]ly/portal-banchile	
https://diarioedomex[.]com/banchile.php	
URL sitio falso	
https://itaupersonayempresacl.itauempresaspuntos[.]info/726a292db52f7f5/html/index.php	
IP	
[104.21.86.153]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00475-01/	
https://www.csirt.gob.cl/media/2022/02/8FPH22-00475-01.pdf	

Vulnerabilidades

CSIRT alerta de vulnerabilidades en Adobe Commerce y Magento	
Alerta de seguridad cibernética	9VSA22-00577-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de febrero de 2022
Última revisión	15 de febrero de 2022
CVE	
CVE-2022-24086	
Fabricante	
Adobe	
Productos afectados	
Adobe Commerce 2.4.3-p1 y versiones anteriores, 2.3.7-p2 y versiones anteriores. Magento Open Source 2.4.3-p1 y versiones anteriores, 2.3.7-p2 y versiones anteriores.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00577-01/	
https://www.csirt.gob.cl/media/2022/02/9VSA22-00577-01.pdf	

CSIRT alerta de vulnerabilidades graves en productos WMware		
Alerta de seguridad cibernética	9VSA21-00578-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	16 de febrero de 2022	
Última revisión	16 de febrero de 2022	
CVE		
CVE-2021-22040 CVE-2021-22041	CVE-2021-22042 CVE-2021-22043	CVE-2021-22050 CVE-2022-22945
Fabricante		
VMware		
Productos afectados		
ESXi, Workstation, Fusion, Cloud Foundation y NSX Data Center para vSphere.		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00578-01/		
https://www.csirt.gob.cl/media/2022/02/9VSA22-00578-01.pdf		

https://www.csirt.gob.cl + (562) 2486 3850 @csirtgob @CSIRTConciencia https://www.linkedin.com/company/csirt-gob

CSIRT alerta de vulnerabilidad grave en Apache Cassandra	
Alerta de seguridad cibernética	9VSA21-00579-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de febrero de 2022
Última revisión	17 de febrero de 2022
CVE	
CVE-2021-44521	
Fabricante	
Apache	
Productos afectados	
Apache Cassandra open-source NoSQL.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00579-01/	
https://www.csirt.gob.cl/media/2022/02/9VSA22-00579-01.pdf	

IoC Malware

A continuación, se comparten los Indicadores de Compromisos que fueron detectados durante la semana pasada por el CSIRT de Gobierno. Recomendamos 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	Documento web
1e10035051f5a988c16c6c8d705e7222001036d49739f91d8467ded9401c506b	FSA/RISK_HIGH	2CMV22-00275-01
3edf50ef922360c2848d8da74ac8204b3c3fbc39065bba34c9be3d5a8df81192	VBA/Agent	2CMV22-00275-01
e24aca8faabd0f1544519b6060b9cadaed01401895d72bb5157c2d28f86c1b89	MSIL/Kryptik	2CMV22-00275-01
cbd56858c70e150a5f631ab39a0bb3e7e085da1b7f6b7d80543668cbbbb5e09f	HTML/GenericKDZ	2CMV22-00275-01
b5b9fa7a242d729528b9317f1d31158230a18abc3b5de7d3cecf122b8fea7db0	W32/Agent	2CMV22-00275-01
4eb4ce61aeb329fbbb7457727bb39ad97164a76129166e7ad97639db74dcffec	MSIL/Kryptik	2CMV22-00275-01
a93ec52f7ba4265acfe5f94eb0d8dbb6af8e39f5c27eed51db7219d27a678afb	MSIL/Kryptik	2CMV22-00275-01
bc9f97d8273b5c2da60474613a131b9f107bb6715865fc3a654ad6f71eb42754	MSIL/Razy	2CMV22-00275-01
8e3df87566ee830aad2e0dd252d5003f689b3b03b5729b9212ca74e53a08fc61	MSIL/Kryptik	2CMV22-00275-01
8fe2177eef34c533216e3abf1afbdb20f07d659a0a9e71cef7b7d8bac54fb626	W32/GenKryptik	2CMV22-00275-01
c3fd5b99f313ae21b04baccd25cb0b0dbc5db509bd1912b5234f4a372f92b962	MSIL/CoinMiner	2CMV22-00275-01
3bbb076be6f5fe876634fc3424a41080e295829dd70d26c8f38d3d6704958285	FSA/RISK_HIGH	2CMV22-00275-01
47af29e1c88a20d331b7b3016600d5cd5544ab2dbe2e582d16d0d3d99c6c1d36	MSIL/Kryptik	2CMV22-00275-01
1d2ea705b33041009cd57d7c3274b2378f6d2d249320d62aeaeff012348f1835	MSIL/Razy	2CMV22-00275-01
2333696e93b3d3c45ba9e6de7ca44cbb87d3a7b1d623c6866341026cc802db36	HTML/Agent	2CMV22-00275-01
c4508064ead99ddadffc037bf177c04094f2b2e561ba45bc157f29fef1967a2d	Riskware/POC_Iframe_CID	2CMV22-00275-01
37c6d438bc28ad226d5c1557d2154dcfd2ad7cac6936e8d5bf72f8b612c3f0f9	MSExcel/CVE_2017_11882	2CMV22-00275-01

f6454a224e138cfd3de67d047a667641c8ce26b5188f0a2eb642fc77d12a4251	PossibleThreat	2CMV22-00275-01
ae1c162420b99c55f92ac1de3787d8bf45a203f8f6ced6b84203f3b5df592e2b	W32/Kryptik	2CMV22-00275-01
ada149a359790167c1368f862aa6d53132f3b6d7bdba2fc9dfab805332391426	MSIL/Agent	2CMV22-00275-01
3571cbbb01a0d3f39231ad8e32869b4d739fad87b2b9679f8e734011f979a70a	MalwThreat!57f9IV	2CMV22-00275-01
8f88422708a15f55dced75e62d85bc4c4ae595630f534893d072cff57b6e0539	Malware_Generic	2CMV22-00275-01
8b4bb61801f2118c1d460752659ba6caedcef3b132f0adf1ec5cdd222e9bcaed	Malware_Generic	2CMV22-00275-01
4ff4c218f8f952bdeb22dbbaa0a459c7450234456f474ebe660cbe79c6377ee9	PossibleThreat	2CMV22-00275-01
64b13fb51affdd02f7313c8125ecffbe689991494702e66c4054efd76d01f35e	Malware_Generic	2CMV22-00275-01
82f76e45d3e353bb1fe4aae0935139df903ac023d459ba85b8fb864a3d6d4035	PossibleThreat	2CMV22-00275-01
c07e38348293f1d9f3960272b93567a678005b6ad8036886d439b31f351095e1	MSIL/Kryptik	2CMV22-00275-01
aa97877609e2a461e914804cdd278293881cef70879939b3ef3ae414b058d9bb	PossibleThreat	2CMV22-00275-01
195c64e1ebaabf8d0bf624658861d0c14bd72b5280e42bb3e505211ad8f92e0d	RTF/Abnormal	2CMV22-00275-01

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
68.183.120.227	DIGITALOCEAN-ASN	2CMV22-00275-01
212.192.246.113	AS-SERVERION	2CMV22-00275-01
103.139.45.124	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP	2CMV22-00275-01
111.90.149.200	Shinjiru Technology Sdn Bhd	2CMV22-00275-01
137.184.93.247	DIGITALOCEAN-ASN	2CMV22-00275-01
15.235.36.253	OVH SAS	2CMV22-00275-01
169.45.173.211	SOFTLAYER	2CMV22-00275-01

185.222.58.48	RootLayer Web Services Ltd.	2CMV22-00275-01
185.222.58.61	RootLayer Web Services Ltd.	2CMV22-00275-01
185.55.229.83	Delta HighTech Ltd.	2CMV22-00275-01
192.3.3.134	AS-COLOCROSSING	2CMV22-00275-01
2.56.56.152	AS-SERVERION	2CMV22-00275-01
45.137.22.171	RootLayer Web Services Ltd.	2CMV22-00275-01

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.

Nombre del archivo malicioso	Documento web
Walmart Purchase Order.uue	2CMV22-00275-01
Vessel's particulars.doc	2CMV22-00275-01
UPDATED PRICE LIST INQ.___Pdf.iso	2CMV22-00275-01
Solicitud de cotizacion.zip	2CMV22-00275-01
shipping docs PL, BL.zip	2CMV22-00275-01
RFQ-FIRE0022.gz	2CMV22-00275-01
RFQ - refMGI(NHE)00-0041(U).uue	2CMV22-00275-01
RF48950CHILE.exe	2CMV22-00275-01
Revised invoice.r00	2CMV22-00275-01
QUOTATION FROM ESV-20220210.PDF.Z	2CMV22-00275-01
products.doc	2CMV22-00275-01
PI.html	2CMV22-00275-01
Pago de facturas PDF.ppam	2CMV22-00275-01
P INVOICE.uue	2CMV22-00275-01
OP.zip	2CMV22-00275-01
Nueva lista de pedidos.zip	2CMV22-00275-01
mail18427.pif	2CMV22-00275-01
Lista de orden.zip	2CMV22-00275-01
Invoice.lzh	2CMV22-00275-01
Invoice.cab	2CMV22-00275-01

FT. PRO INVOICE N. 6 DATE 28.01.2022.img.rar	2CMV22-00275-01
fedex logistic shipping files.htm	2CMV22-00275-01
Euro_swiftcopy.rar	2CMV22-00275-01
Estimado cliente_XLSx.lzh	2CMV22-00275-01
DRAFT QUOTATION 20220130.rar	2CMV22-00275-01
DHL CUSTOM INVOICE SHIPMENT WAYBILL DOC.rar	2CMV22-00275-01
Complete Docs & ISO-Certificate this certificate.r15	2CMV22-00275-01
CI PL.xlsx	2CMV22-00275-01
BL COPY-PACKING LIST & CMR DOC.rar	2CMV22-00275-01
BID TENDER DOCUMENTS.zip	2CMV22-00275-01
BE415054 NEW ORDER .doc	2CMV22-00275-01

Actualidad

Día Internacional de la Internet Segura: Ciberconsejos de navegación

El regreso a clases trae consigo los desafíos de mantener una buena convivencia entre los distintos miembros de la comunidad educativa, lo que requiere estar al tanto no solo de su interacción física, sino también de distintas amenazas digitales como el cyberbullying y el grooming. Encuentra la infografía completa en PDF aquí: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-una-navegacion-segura/.

https://www.csirt.gob.cl
+ (562) 2486 3850
@csirtgob
@CSIRTConciencia
https://www.linkedin.com/company/csirt-gob

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.

https://www.csirt.gob.cl
+ (562) 2486 3850
@csirtgob
@CSIRTConciencia
https://www.linkedin.com/company/csirt-gob

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 (csirt.gob.cl o al 1510) siempre que hayan aportado información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- Cristián Acuña
- Alberto Campusano
- Maldito Informático
- Bárbara Palacios Cabezas
- Felipe Andrés Pizarro Astudillo
- Marcelo Donaire
- José