Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

01-07-2022 | Año 4 | N°156

Boletín de Seguridad Cibernética

Semana del 24 al 30 de junio de 2022

Boletín de Seguridad Cibernética N°156

Semana del 24 al 30 de junio de 2022

13BCS22-00165-01

TLP: BLANCO (la información puede ser distribuida sin restricciones, sujeta a controles de copyright)

La semana en cifras

Parches

57

para vulnerabilidades

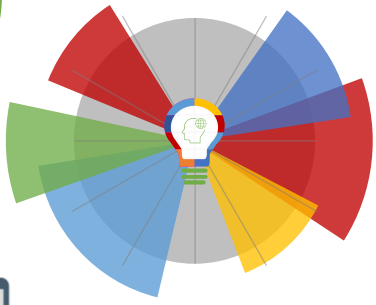
Mitigaciones son útiles en productos Drupal, Microsoft, Adobe, Cisco, Emerson, Honeywell, Bently Nevada, Siemens, Motorola, Omron, Phoenix Contact, Yokogawa, JTEKT y Google.

Hash

24

SHA

Asociadas a múltiples campañas de phishing con archivos que contienen malware



Se advirtieron

8

URL

Asociadas a sitios fraudulentos y campañas de phishing y malware.

IP

70

Informadas

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

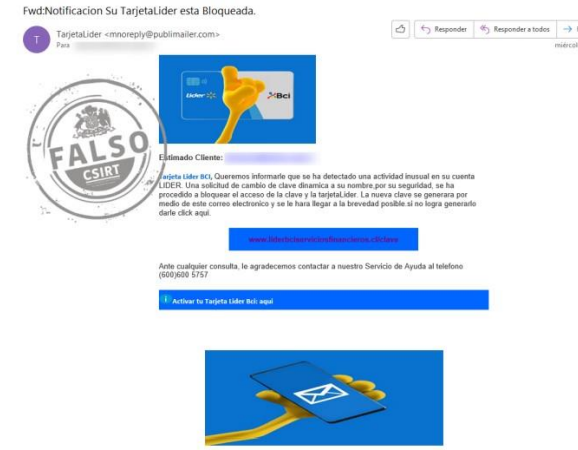
*Los datos recopilados corresponden a información publicada en diferentes secciones del sitio web https://www.csirt.gob.cl.

Contenido

Phishing 2
Malware 3
Vulnerabilidades 4
IoC Malware 8
IoC Ataques de Fuerza Bruta 13
Actualidad 14
Muro de la Fama 17

Phishing

Imagen del mensaje

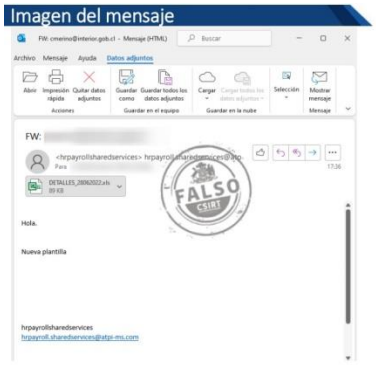


CSIRT informa phishing que suplanta a Lider BCI	
Alerta de seguridad cibernética	8FPH22-00548-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de junio de 2022
Última revisión	29 de junio de 2022
Indicadores de compromiso	
URL Redirección	
http://bit[.]ly/3OxexAr	
http://brombalplatform[.]com/disegnatori/bootstrap/enviar02.php	
https://bit[.]ly/3Nv8Mlx	
https://tfpconstruction[.]com/activacion/cuenta-ptrp/	
URL sitio falso	
https://liderbciserviciosfinancieros.cl.wavlinkwifisetup[.]com/1656508442/login	
IP	
[103.84.193.3]	
[89.25.241.179]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00548-01/	
https://www.csirt.gob.cl/media/2022/06/8FPH22-00548-01.pdf	

Imagen del mensaje

CSIRT informa phishing que suplanta al Banco de Chile	
Alerta de seguridad cibernética	8FPH22-00549-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de junio de 2022
Última revisión	29 de junio de 2022
Indicadores de compromiso	
URL Redirección	
https://bit[.]ly/3NbCsUs	
https://gocloudasiaacademe[.]com/?id=231	
https://login.portal.bancochlle.cl.iranorganic[.]org/	
IP	
[98.142.111.77]	
[168.195.204.51]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00549-01/	
https://www.csirt.gob.cl/media/2022/06/8FPH22-00549-01.pdf	

Malware



CSIRT advierte campaña de phishing con malware	
Alerta de seguridad cibernética	2CMV21-00304-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Enero de 2021
Última revisión	04 de Enero de 2021
Indicadores de compromiso	
Hash	
d69450df6cd1f5533347c2578c54c49d858c38348ac107c561c5c09f3d07b400	
c62d72b1a9be3b574d734d3d88bf85d1654b1475e808c8a7f9a2aa0892a65e18	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00304-01/	
https://www.csirt.gob.cl/media/2022/06/2CMV22-00304-01.pdf	

Vulnerabilidades

CSIRT alerta de vulnerabilidades en dispositivos industriales de varios proveedores	
Alerta de seguridad cibernética	9VSA22-00666-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de junio de 2022
Última revisión	24 de junio de 2022
CVE	
Emerson	
CVE-2022-29957	
CVE-2022-29962	
CVE-2022-29963	
CVE-2022-29964	
CVE-2022-29969	
CVE-2022-29960	
CVE-2022-29961	
CVE-2022-29954	
CVE-2022-29955	
CVE-2022-29956	
CVE-2022-30260	
CVE-2022-30267	
CVE-2022-30262	
CVE-2022-30261	
CVE-2022-30264	
CVE-2022-30266	
CVE-2022-30263	
CVE-2022-30265	
CVE-2022-30268	
Honeywell	
CVE-2022-30312	
CVE-2022-30313	
CVE-2022-30314	
CVE-2022-30315	
CVE-2022-30316	
CVE-2022-30317	
CVE-2022-30318	
CVE-2022-30319	
CVE-2022-30320	
JTEKT	
CVE-2022-29951	
CVE-2022-29958	
Bently Nevada	
CVE-2022-29952	
CVE-2022-29953	

Siemens CVE-2022-33139 **Motorola** CVE-2022-30276 CVE-2022-30273 CVE-2022-30270 CVE-2022-30271 CVE-2022-30274 CVE-2022-30275 CVE-2022-30269 CVE-2022-30275 **Omron** CVE-2022-31204 CVE-2022-31205 CVE-2022-31207 CVE-2022-31206 **Phoenix Contact** CVE-2022-31800 CVE-2022-31801 **Yokogawa** CVE-2022-29519 CVE-2022-30997 FSCT-2022-0039
Fabricantes
Emerson, Honeywell, JTEKT, Bently Nevada, Siemens, Motorola, Omron, Phoenix Contact y Yokogawa
Productos afectados
Emerson CVE-2022-29957: DeltaV. CVE-2022-29962, CVE-2022-29963, CVE-2022-29964 y CVE-2022-29965: Controladores DeltaV. CVE-2022-29966: Ovation. CVE-2022-29959 y CVE-2022-29960: OpenBSI. CVE-2022-29961, CVE-2022-29954, CVE-2022-29955 y CVE-2022-29956: ControlWave, Bristol Babcock 33xx. CVE-2022-30260: Controladores DeltaV M-series/S-series/P[1]series, IO cards (CIOC/EIOC/WIOC) y nodos DeltaV/Ovation SIS (SLS1508/CSLS/LSNB/LSNG). CVE-2022-30267: Controladores Ovation OCR400, OCR1100 módulos IO relacionados. CVE-2022-30262: ControlWave. CVE-2022-30261, CVE-2022-30264: ROC, FloBoss CVE-2022-30266: PLC PACsystems (excepto modelos que soportan HTTPS como IC695, CPE330, CPE400). CVE-2022-30263 y CVE-2022-30265: PLC Fanuc/PAC Systems. CVE-2022-30268: PLC Fanuc/PAC Systems excepto ciertos modelos RX3i (CPx330, CPx400, CPx410) y RSTi-EP (CPE100, CPE115).

Honeywell
CVE-2022-30312: Controles TREND que usen el protocolo IC.
CVE-2022-30313, CVE-2022-30314, CVE-2022-30316: Experion PKS Safety Manager.
CVE-2022-30315: Experion PKS Safety Manager (SM y FSC).
CVE-2022-30317: Experion LX.
CVE-2022-30318: ControlEdge.
CVE-2022-30319 y CVE-2022-30320: Controladores PCD – Sala Burgess Controls (SBC).

JTEKT
CVE-2022-29951 y CVE-2022-29958: TOYOPUC.

Bently Nevada
CVE-2022-29952: Bently Nevada 3701.
CVE-2022-29953: Productos que usen el protocolo TDI.

Siemens
CVE-2022-33139: WinCC OA.

Motorola
CVE-2022-30273: MDLC
CVE-2022-30275: MOSCAD/STS Toolbox, StarControls staRTU.
CVE-2022-30276, CVE-2022-30269, CVE-2022-30270, CVE-2022-30271, CVE-2022-30274 y CVE-2022-30272: ACE1000

Omron
CVE-2022-31204: SYSMAC CS1/CJ1/CP1/CP2 series.
CVE-2022-31205: SYSMAC CP series.
CVE-2022-31207: SYSMAC CS/CJ/CP series
CVE-2022-31206: SYSMAC NJ/NX.

Phoenix Contact
CVE-2022-31800, CVE-2022-31801: ProConOS/eCLR Runtime.

Yokogawa
CVE-2022-29519, CVE-2022-30997, FSCT-2022-0039: STARDOM.

Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00666-01/
https://www.csirt.gob.cl/media/2022/06/9VSA22-00666-01-1.pdf

CSIRT alerta por vulnerabilidad crítica en OpenSSL	
Alerta de seguridad cibernética	9VSA22-00667-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de junio de 2022
Última revisión	28 de junio de 2022
CVE	
Vulnerabilidad que no cuenta con CVE	
Fabricante	
OpenSSL	
Productos afectados	
OpenSSIL 3.0.4 x64 con el AVX-512 instruction set.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00667-01/	
https://www.csirt.gob.cl/media/2022/06/9VSA22-00667-01.pdf	

CSIRT alerta de vulnerabilidades ChromeOS	
Alerta de seguridad cibernética	9VSA22-00656-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de junio de 2022
Última revisión	28 de junio de 2022
CVE	
CVE-2022-1853 CVE-2022-1855 CVE-2022-1861 CVE-2022-1862 CVE-2022-1866 CVE-2022-1863 CVE-2022-1865	
Fabricante	
Chrome	
Productos afectados	
Chrome OS anteriores a 96.0.4664.214.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00668-01/	
https://www.csirt.gob.cl/media/2022/06/9VSA22-00668-01.pdf	

IoC Malware

A continuación, se comparten los Indicadores de Compromisos que fueron detectados durante la semana pasada por el Equipo del CSIRT de Gobierno.
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	Documento web
d69450df6cd1f5533347c2578c54c49d858c38348ac107c561c5c09f3d07b400	XF/CoinMiner	2CMV22-00303-01
248afc87ac9723820d97227bcf7bf8d621805a7b6fb7044324b90e3d8be0655c	RTF/CVE_2017_11882	2CMV22-00303-01
dc51417399862b1fef10dc05222266931c00bc44c65c8510a9561de0cfa1b300	MSExcel/CVE_2017_11882!exploit	2CMV22-00303-01
5660ee546c3a75b373af637a20ba9daa2ed6f52201b4aaa8c42596004235e835	MSExcel/CVE_2017_11882!exploit	2CMV22-00303-01
97b2a411f2ea38e77a03f9bb502a7a2c123edbfa20adc56b4dfc672c24add829	PossibleThreat	2CMV22-00303-01
3ca51efbc492b4b519050419b8b68b62f74b07ae8d1066aef540c10d5791058d	Malicious_Behavior	2CMV22-00303-01
26b14b79c80d395141bceb2294b3ce8badd977b789158a5890743f2f359c3bd2	Malware_Generic	2CMV22-00303-01
61548e27d883de30704f2569a58b1a2b1be69f8360234f99be013a3a3516b7ec	MSIL/Agent.MJJ!tr	2CMV22-00303-01
22ffaee9a79a9b1537a7195f2460a6156634b6396c757a73b72c76af6d7c3fe5	MSIL/GenKryptik	2CMV22-00303-01
618bbbba4ca1ee491b9a5ed62847124ba166215905a302312e2177cdd700b76b	MSIL/GenKryptik	2CMV22-00303-01
84caa576cdfea20e6e44c709699714026b87dc02c01ec75935a537462be66a57	PossibleThreat	2CMV22-00303-01
af64d169c79c34397382c4a2ec4d8a7db3caa07b2ab3ba40c1c9b1bfb438b46a	XF/CoinMiner	2CMV22-00303-01
d958fe80b1ba071fe95b6c549639070c7a871e743a8a82859734a300dca74915	MSIL/GenKryptik	2CMV22-00303-01
e6bcf73dfd9fb1622830ed694be2c0aea6bac3e1443bb7ce01718cf33cffeff0	HTML/Phishing	2CMV22-00303-01
a8f295b6346e094a388df74c39eec95d5de375729e7d17553b2a0e58dff08182	HTML/Phishing	2CMV22-00303-01
e480a896b459dd9476175411d6bf759cf7e7a962880405deb5f90b0fc6390a99	HTML/Phishing	2CMV22-00303-01
43a817ce7cb5019d22ad0ea7ff45bf56d822d5eb68664a563fcce564f85c1a1b	MSIL/Kryptik	2CMV22-00303-01
588d2be55b6cbc691b19ab1a51b33fe5ad1618c3f5dcc038dd2171a6599cf295	VBA/Agent	2CMV22-00303-01
a96b8cb2c893b776384cae4be4afbf545f3410223724c5a507fe470387035d8a	HTML/Phish	2CMV22-00303-01
d5417dce5fa94a66256cd146db74e502569ab35f3cb7eaf8dd1876958454cc4d	MSIL/GenKryptik	2CMV22-00303-01
c8a2d7fe935322abe5bb782f87bebde4c41c4dfbf655958ee1bedad09bc05474	MSIL/GenKryptik	2CMV22-00303-01
efd7419b4d206b430ac72ba668439db4fa4e593441c0f493bc0945d1b737910e	MSIL/GenKryptik	2CMV22-00303-01

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	ASN	Documento web
98.142.233.71	TERRA-NETWORKS-MIAMI	AS 40260	2CMV22-00303-01
94.46.23.48	Almouroltec Servicos De Informatica E Internet Lda	AS 24768	2CMV22-00303-01
92.223.159.2	Fastweb	AS 12874	2CMV22-00303-01
89.252.151.33	Kapteyan Bilisim Teknolojileri San. ve Tic. A.S.	AS 207429	2CMV22-00303-01
86.35.15.78	Orange Romania Communication S.A	AS 9050	2CMV22-00303-01
69.174.99.150	ASN-QUADRANET-GLOBAL	AS 8100	2CMV22-00303-01
45.83.122.239	IT WEB LTD	AS 200313	2CMV22-00303-01
45.61.171.224	Hyonix LLC	AS 213122	2CMV22-00303-01
216.59.16.169	IMMEDION	AS 15085	2CMV22-00303-01
212.36.80.195	OGIC Informatica S.L.	AS 15699	2CMV22-00303-01
207.180.218.28	Contabo GmbH	AS 51167	2CMV22-00303-01
202.55.133.137	VIETSERVER SERVICES TECHNOLOGY COMPANY LIMITED	AS 63737	2CMV22-00303-01
201.76.49.98	Locaweb Servicos de Internet SA	AS 27715	2CMV22-00303-01
201.76.49.49	Locaweb Servicos de Internet SA	AS 27715	2CMV22-00303-01
201.76.49.48	Locaweb Servicos de Internet SA	AS 27715	2CMV22-00303-01
201.76.49.242	Locaweb Servicos de Internet SA	AS 27715	2CMV22-00303-01
201.76.49.224	Locaweb Servicos de Internet SA	AS 27715	2CMV22-00303-01
201.76.49.199	Locaweb Servicos de Internet SA	AS 27715	2CMV22-00303-01
201.76.49.198	Locaweb Servicos de Internet SA	AS 27715	2CMV22-00303-01
201.76.49.177	Locaweb Servicos de Internet SA	AS 27715	2CMV22-00303-01
201.76.49.176	Locaweb Servicos de Internet SA	AS 27715	2CMV22-00303-01
201.76.49.159	Locaweb Servicos de Internet SA	AS 27715	2CMV22-00303-01
201.76.49.149	Locaweb Servicos de Internet SA	AS 27715	2CMV22-00303-01
201.76.49.142	Locaweb Servicos de Internet SA	AS 27715	2CMV22-00303-01
201.76.49.131	Locaweb Servicos de Internet SA	AS 27715	2CMV22-00303-01
201.76.49.123	Locaweb Servicos de Internet SA	AS 27715	2CMV22-00303-01
201.76.49.116	Locaweb Servicos de Internet SA	AS 27715	2CMV22-00303-01
201.76.49.115	Locaweb Servicos de Internet SA	AS 27715	2CMV22-00303-01
200.80.10.72	Locaweb Servicos de Internet SA	AS 27715	2CMV22-00303-01
200.14.80.165	Locaweb Servicos de Internet SA	AS 27715	2CMV22-00303-01

200.1.126.24	Locaweb Servicos de Internet SA	AS 27715	2CMV22-00303-01
194.87.84.98	Delis LLC	AS 211252	2CMV22-00303-01
189.126.112.58	Locaweb Servicos de Internet SA	AS 27715	2CMV22-00303-01
189.126.112.56	Locaweb Servicos de Internet SA	AS 27715	2CMV22-00303-01
189.126.112.51	Locaweb Servicos de Internet SA	AS 27715	2CMV22-00303-01
189.126.112.33	Locaweb Servicos de Internet SA	AS 27715	2CMV22-00303-01
189.126.112.31	Locaweb Servicos de Internet SA	AS 27715	2CMV22-00303-01
187.95.145.190	Horizons Telecomunicacoes e Tecnologia S.A.	AS 262318	2CMV22-00303-01
185.32.188.2	Sampling Line-servicos E Internet, Lda	AS 62416	2CMV22-00303-01
177.36.34.54	BRASIL TECNOLOGIA E PARTICIPACOES SA	AS 262907	2CMV22-00303-01
164.163.56.10	PALA PABLO FEDERICO	AS 265781	2CMV22-00303-01
154.0.169.134	Afrihost	AS 37611	2CMV22-00303-01
152.89.247.36	combahton GmbH	AS 30823	2CMV22-00303-01
146.190.56.140	DIGITALOCEAN-ASN	AS 14061	2CMV22-00303-01
143.90.14.67	SoftBank Corp.	AS 4725	2CMV22-00303-01
142.44.204.137	OVH SAS	AS 16276	2CMV22-00303-01
120.50.33.23	M1 NET LTD	AS 17547	2CMV22-00303-01
103.167.84.102	VIETSERVER SERVICES TECHNOLOGY COMPANY LIMITED	AS 63737	2CMV22-00303-01
103.118.24.195	NSS INTL CO., LTD.	AS 131626	2CMV22-00303-01
200.201.195.236	DC MATRIX INTERNET SA	AS 10733	2CMV22-00303-01
200.195.200.141	Horizons Telecomunicacoes e Tecnologia S.A.	AS 262318	2CMV22-00303-01
195.248.231.195	Data Rush IT Services, S.L.	AS 199581	2CMV22-00303-01
189.126.112.208	Locaweb Servicos de Internet SA	AS 27715	2CMV22-00303-01
189.126.112.164	Locaweb Servicos de Internet SA	AS 27715	2CMV22-00303-01
189.126.112.116	Locaweb Servicos de Internet SA	AS 27715	2CMV22-00303-01
185.102.170.127	Des Capital B.V.	AS 213035	2CMV22-00303-01

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
mensaje 2135453.xls	2CMV22-00303-01
Escanear_28062022.xls	2CMV22-00303-01
detalles_3142030441.xls	2CMV22-00303-01
R 2806.xls	2CMV22-00303-01
informe_047.xls	2CMV22-00303-01
LYN 2043354.xls	2CMV22-00303-01
archivo 646113.xls	2CMV22-00303-01
paquete_2806.xls	2CMV22-00303-01
PO NO865.doc	2CMV22-00303-01
Mensaje 90365798.xls	2CMV22-00303-01
documento_2806.xls	2CMV22-00303-01
LATCO_773464.xlsx	2CMV22-00303-01
DATOS 2806.xls	2CMV22-00303-01
ESCANEAR 400.xls	2CMV22-00303-01
archivo 0.xls	2CMV22-00303-01
informe_2806.xls	2CMV22-00303-01
ESCANEAR-28062022.xls	2CMV22-00303-01
Info-64808469685.xls	2CMV22-00303-01
Correo_2806.xls	2CMV22-00303-01
DETALLES_2806.xls	2CMV22-00303-01
Info_0657125509.xls	2CMV22-00303-01
102Q_34544.xls	2CMV22-00303-01
detalles_85798133049.xls	2CMV22-00303-01
detalles 2806.xls	2CMV22-00303-01
adjuntos-863134497.xls	2CMV22-00303-01
AWB # Ref 0926317468.pdf.iso	2CMV22-00303-01
lista-2806.xls	2CMV22-00303-01
83 335644216.xls	2CMV22-00303-01
PO_87910219.zip	2CMV22-00303-01
25644022.xls	2CMV22-00303-01

sin ttulo_2806.xls	2CMV22-00303-01
Purchase Order 28th June.img	2CMV22-00303-01
detalles_28062022.xls	2CMV22-00303-01
adjunto-892.xls	2CMV22-00303-01
RZZJY-299.xls	2CMV22-00303-01
nrle-28062022.xls	2CMV22-00303-01
comentarios 021533.xls	2CMV22-00303-01
DOCUMENTO 28062022.xls	2CMV22-00303-01
ARCHIVO-3.xls	2CMV22-00303-01
DHL0038747896.7z	2CMV22-00303-01
04427208.xls	2CMV22-00303-01
cotizaciÃ³n y nuevo pedido.pdf.001	2CMV22-00303-01
Quotation Request28June2022Phnom Penh, Port to EU NGC92728.gz	2CMV22-00303-01
Escanear_38263.xls	2CMV22-00303-01
PO 28.06.2022.xlsx	2CMV22-00303-01
DocuSign_INV089881.htm	2CMV22-00303-01
New Order.rar	2CMV22-00303-01
shipping document.xlsx	2CMV22-00303-01
mp3wav010_Prochilenl_soundmp3_.html	2CMV22-00303-01
vsl particulars & packing list.zip	2CMV22-00303-01
NEW_ORDER_LIST.IMG	2CMV22-00303-01

IoC Ataques de Fuerza Bruta

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) ha identificado una serie de intentos de acceso a servidores de correos del sector público y privado. Estos ataques de fuerza bruta intentan vulnerar la autenticación del protocolo para transferencia simple de correos (SMTP), con el fin de suplantar un remitente original y así depositar correos con contenido o enlaces maliciosos en las bandejas de entrada de sus potenciales víctimas.

IP	Etiqueta de sistema autónomo	Nombre sistema autónomo	Documento web
5.34.207.209	AS 15828	Blue Diamond Network Co., Ltd.	4IIA22-00052-01
5.34.207.213	AS 15828	Blue Diamond Network Co., Ltd.	4IIA22-00052-01
103.153.79.225	AS 135905	Vietnam Posts And Telecommunications Group	4IIA22-00052-01
2.56.58.92	AS 399471	AS-SERVERION	4IIA22-00052-01
103.147.185.238	AS 135905	Vietnam Posts And Telecommunications Group	4IIA22-00052-01
45.133.1.52	AS 211252	Delis LLC	4IIA22-00052-01

Actualidad

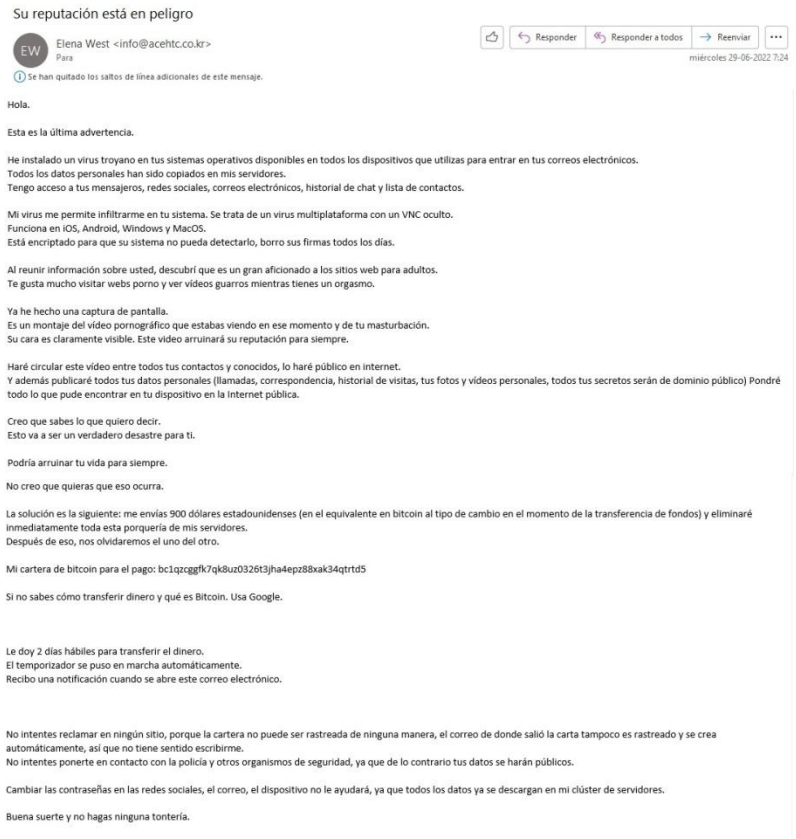
Alerta de Seguridad Cibernética | Campaña de phishing con sextorsión

El CSIRT de Gobierno informa sobre la detección y notificación de correos electrónicos maliciosos que buscan extorsionar a las personas, amenazándolos con arruinar su reputación si no realizan una transferencia en bitcoin.

Es importante recalcar que el mensaje que se envía es falso, el remitente no posee dichas imágenes comprometedoras y el correo es enviado indiscriminadamente a miles de personas.

La sextorsión es una estafa que busca, por lo general, obtener desde la víctima altas sumas de dinero o generar un daño moral o emocional. Es una de las principales amenazas cibernéticas y consiste en un chantaje, amenazando con la difusión de imágenes, videos o mensajes de contenido sexual.

También disponible aquí: https://www.csirt.gob.cl/noticias/phishing-sextorsion/



Su reputación está en peligro

EW Elena West <info@acehtc.co.kr>
Para

Responder | Responder a todos | Reenviar

miércoles 29-06-2022 7:24

Se han quitado los saltos de línea adicionales de este mensaje.

Hola.

Esta es la última advertencia.

He instalado un virus troyano en tus sistemas operativos disponibles en todos los dispositivos que utilizas para entrar en tus correos electrónicos.
Todos los datos personales han sido copiados en mis servidores.
Tengo acceso a tus mensajeros, redes sociales, correos electrónicos, historial de chat y lista de contactos.

Mi virus me permite infiltrarme en tu sistema. Se trata de un virus multiplataforma con un VNC oculto.
Funciona en iOS, Android, Windows y MacOS.
Está encriptado para que su sistema no pueda detectarlo, borro sus firmas todos los días.

Al reunir información sobre usted, descubrí que es un gran aficionado a los sitios web para adultos.
Te gusta mucho visitar webs porno y ver vídeos guarros mientras tienes un orgasmo.

Ya he hecho una captura de pantalla.
Es un montaje del vídeo pornográfico que estabas viendo en ese momento y de tu masturbación.
Su cara es claramente visible. Este video arruinará su reputación para siempre.

Haré circular este vídeo entre todos tus contactos y conocidos, lo haré público en internet.
Y además publicaré todos tus datos personales (llamadas, correspondencia, historial de visitas, tus fotos y vídeos personales, todos tus secretos serán de dominio público) Pondré todo lo que pude encontrar en tu dispositivo en la Internet pública.

Creo que sabes lo que quiero decir.
Esto va a ser un verdadero desastre para ti.

Podría arruinar tu vida para siempre.

No creo que quieras que eso ocurra.

La solución es la siguiente: me envías 900 dólares estadounidenses (en el equivalente en bitcoin al tipo de cambio en el momento de la transferencia de fondos) y eliminaré inmediatamente toda esta porquería de mis servidores.
Después de eso, nos olvidaremos el uno del otro.

Mi cartera de bitcoin para el pago: bc1qzcggfk7qk8uz0326t3jha4epz88xak34qtrtd5

Si no sabes cómo transferir dinero y qué es Bitcoin. Usa Google.

Le doy 2 días hábiles para transferir el dinero.
El temporizador se puso en marcha automáticamente.
Recibo una notificación cuando se abre este correo electrónico.

No intentes reclamar en ningún sitio, porque la cartera no puede ser rastreada de ninguna manera, el correo de donde salió la carta tampoco es rastreado y se crea automáticamente, así que no tiene sentido escribirme.
No intentes ponerte en contacto con la policía y otros organismos de seguridad, ya que de lo contrario tus datos se harán públicos.

Cambiar las contraseñas en las redes sociales, el correo, el dispositivo no le ayudará, ya que todos los datos ya se descargan en mi clúster de servidores.

Buena suerte y no hagas ninguna tontería.

Ciberconsejos | 5 formas de protección para una pyme cibersegura

Desde las grandes a las medianas y pequeñas empresas, la ciberseguridad debe ser una prioridad, ya que algunos de los riesgos a los que expuestos son pérdida temporal de acceso a archivos, interrupción de sitios web, corrupción de programas o sistemas y pérdida permanente de archivos y del acceso a servicios.

Por lo anterior, el CSIRT de Gobierno entregó recomendaciones clave para proteger a las pymes de los ciberdelincuentes en: https://www.csirt.gob.cl/recomendaciones/pyme-cibersegura/

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.

- Raúl Beyzaga
- Humberto Morales
- Sandra Cortés
- Carolina Díaz
- Valeria Cañas
- Jair Palma
- Cristián Acuña
- Jean Catalán
- Mauricio Alarcón