Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

15-10-2021 | Año 3 | N°119

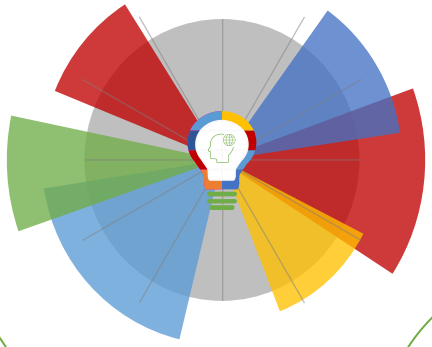
Boletín de Seguridad Cibernética

Semana del 08 al 14 de octubre de 2021

La semana en cifras

Hash
72
SHA
Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron
1
URL
Asociadas a sitios fraudulentos y campañas de phishing



Parches
114
para vulnerabilidades
Las mitigaciones son útiles en productos de Dell, Apple y Microsoft.

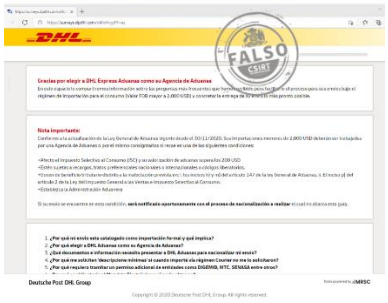
IP
19
Informadas
Listado de IP advertidas en múltiples campañas de phishing y de malware.

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

Contenido

Malware

Imagen del Mensaje



CSIRT alerta de campaña de phishing con malware que suplanta a DHL	
Alerta de seguridad cibernética	2CMV21-00230-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de octubre de 2021
Última revisión	12 de octubre de 2021
Indicadores de compromiso	
SHA256	
2C61B110A73C1500A26B65B187BC3DFAD7367921213B95AAFC19887D132EF2D4 DB125EA0B4C9F1EA9A2634240EA3A4CDF3A317FA545BC98E83367802CFB1B3D8	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00230-01/	
https://csirt.gob.cl/media/2021/10/2CMV21-00230-01.pdf	

Imagen del Mensaje

CSIRT alerta de campaña de phishing que difunde malware a través de falsa factura	
Alerta de seguridad cibernética	2CMV21-00231-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de octubre de 2021
Última revisión	12 de octubre de 2021
Indicadores de compromiso	
SHA256	
BAF44BB98D0A2D4B651A8A1785AE58DAC47692B296F4807614B9894434CBB09F F67B83F5CFB5D9EEE0B50739AEEE606E79B627AF3409A9730BC7B02CBC45F9B0	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00231-01/	
https://csirt.gob.cl/media/2021/10/2CMV21-00231-01.pdf	

CSIRT alerta de campaña de phishing que difunde malware a través de falsa factura	
Alerta de seguridad cibernética	2CMV21-00233-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de octubre de 2021
Última revisión	14 de octubre de 2021
Indicadores de compromiso	
SHA256	
3ABBD1C38BEB68EB619BDEF475357BFD21541C7CA1EAFBB4460274B88665A670 8D7FCAD51BB22CF1C005080D3444B9D7568A9BF878ACBD6913933A0413F309D4	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00233-01/	
https://csirt.gob.cl/media/2021/10/2CMV21-00233-01.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.

No.	Hash de archivos maliciosos	Tipo de malware	Documento web
1	3a770b73665621c5ca5c3fcc5478d39ea130cc31eeeaff926d9b3ec39c7048d4	MSIL/GenKryptik.FLYH!tr	2CMV21-00232-01
2	ec1ebb7d6744634e8f82e87c03e821a90e84ea038760dbec89e2c75ede498547	MSIL/GenKryptik.FLYH!tr	2CMV21-00232-01
3	e13afdd0fd1fb07099a8caa32bdba8c0d15ab2b5ad40f9bee89d88556e60bf34	MSIL/GenKryptik.FLYH!tr	2CMV21-00232-01
4	e6322af0f75dcb3b545798985a6d2e70f57cdf2abc91048aecdb8ac464fe6db4	MSIL/GenKryptik.FLYH!tr	2CMV21-00232-01
5	1290ef7be0befbdc31eb2dc29ba4ae7526e74d3a1c085f51762b03475a9ef4d5	MSIL/GenKryptik.FLYH!tr	2CMV21-00232-01
6	44a4ae7b430c4159409101b325d8122dbadfbd4e9d6b9275aaba7589a831ceca	MSIL/GenKryptik.FLYH!tr	2CMV21-00232-01
7	551c222081882fcb8968d315fd1c74b57572404d9f1a0d15767c4a2ed9ca348e	MSIL/GenKryptik.FLYH!tr	2CMV21-00232-01
8	c13a3022f2212e4e16fb2147f6fd0c09ed4439a49b4313603a5e48b7b3174167	MSOffice/Agent.GV!tr	2CMV21-00232-01
9	bcb06cd6c24b4d5d8cfef85a519fe11ea51f70ce7c27eab722647c14fd566bda	HTML/Phish.081B!tr	2CMV21-00232-01
10	b204a44b893af9affc8791266472d7d588d726eae2ea80be76f5d8dec872b497	MSIL/GenKryptik.FLYH!tr	2CMV21-00232-01
11	dcef89febad36a6f8d08588731f337077c1291d750e4ea1774b731520f5791cf	MSIL/GenKryptik.DYQU!tr	2CMV21-00232-01
12	24d19268e9534a4aebc6b70334b552779b06759612002545a901771ce5a42126	MSIL/GenKryptik.FLYH!tr	2CMV21-00232-01
13	af8d202e018654f3726733634610ade28f16d01db80490d18e3b678460e1751e	HTML/Phishing.BEK!tr	2CMV21-00232-01
14	3cf850b14aa5ccb72108e860c789ee89b413f2c1656965e788f8b9be6439b775	HTML/Phishing.BEK!tr	2CMV21-00232-01
15	8a70bba72136c9b91823ef1d98addd5531cf1f9068d34eb9ba8fccb2fe5bb79b	HTML/Phishing.BEK!tr	2CMV21-00232-01
16	8327b44284237279b83ce93229f789149a36176dd4ccb9e762f75c25f875bea7	HTML/Phishing.BEK!tr	2CMV21-00232-01
17	b83387eb700c463dfa62960861a237e70859704f9941f7323c3a6c88e686444d	HTML/Phishing.BEK!tr	2CMV21-00232-01
18	d979bed683723bfed4bd772156f2b3886982dbafab1088e3161968eed062b2b4	HTML/Phishing.BEK!tr	2CMV21-00232-01
19	394d5fb455fe2342e6f9c4cc0110cb3676913a33a32fa12bb39eb81c186a8917	HTML/Phishing.BEK!tr	2CMV21-00232-01

20	0ae635296c372922f9c3ce3d99448c4f304f8e b5b3590015141d1f7cb4a0253c	HTML/Phishing.BEK!tr	2CMV21-00232-01
21	f4718c0c07b79e8815f966701ee6c433e83c08 a5c80afa5081747548ef02adc8	HTML/Phishing.BEK!tr	2CMV21-00232-01
22	1cad9a70978d0a20f1971405b8fca0cbaea59f 9873e5475acbc07c3c6382c751	HTML/Phishing.BEK!tr	2CMV21-00232-01
23	4ca3a94aa79b0176a132e3fbc0f6e0879ab738 da90f2d052dcfb42c305a0aa8d	HTML/Phishing.BEK!tr	2CMV21-00232-01
24	0463dd0a9db07cd789455c6b1e4a35e75361 e261b4e9e9cbef29e43312179467	HTML/Phishing.BEK!tr	2CMV21-00232-01
25	28a875e447fb2c017ba2aee1dee6d6f2c0b4a d9a87139f3563eb57f107e42ab3	HTML/Phishing.BEK!tr	2CMV21-00232-01
26	1b799d74d26a4db5e9d88c4ba9577acf6d0b0 afc0131bb28f182a586872c9d2e	HTML/Phishing.BEK!tr	2CMV21-00232-01
27	ad4f6b93a3bb80e3bfe1b9942439447e94999 39d6bb55da1e7c7c6622cceb112	HTML/Phishing.BEK!tr	2CMV21-00232-01
28	a8fdb0ef76dfdf5d2b3cf46444c67f190ebe54a 1c4fe11f4a319f35366c9f23f	HTML/Phishing.BEK!tr	2CMV21-00232-01
29	991ab954b535a7ea751b884014e54d6c85a4 730b0a08125c5e0b6f567d787657	HTML/Phishing.BEK!tr	2CMV21-00232-01
30	031206e4c2e7efef7cf1468a330eeae338a03b 7fb8540207d347c3ca367f92ba	HTML/Phishing.BEK!tr	2CMV21-00232-01
31	2b98b9c4f0e1ab05b493d404480e580a5aa0b 8cdd8da9ac7b3e5c095a14ff995	HTML/Phishing.BEK!tr	2CMV21-00232-01
32	bd320d6b811d03cc6c6dbd17f39b2eabf4080 99d8a75ee9a37480845103e12f1	HTML/Phishing.BEK!tr	2CMV21-00232-01
33	509f6e362059becf86d2dca7fda7bcb24ab374 fc16f5ae25e2ada184ef770771	HTML/Phishing.BEK!tr	2CMV21-00232-01
34	1cf47a430e3e32a6b980d9bf09db6077d22af 86e10425247fe92e378186525d6	HTML/Phishing.BEK!tr	2CMV21-00232-01
35	2e44f5358b35f29f2c327bf1aa34ca289556f1b d2877fc2006fef071d753ced9	HTML/Phishing.BEK!tr	2CMV21-00232-01
36	c3262d1804750736f48f347f4bf07ec9796996 61b191cedc8ff16cc41a9a426f	HTML/Phishing.BEK!tr	2CMV21-00232-01
37	8ec7234527d959f65f769855ba9b505bbe769 c15ca0b5a477d23028ad99d3e99	HTML/Phishing.BEK!tr	2CMV21-00232-01
38	d3dab5f7d68f7c0b84ea53de750204f675ec07 9abf61d5ca64cc2f4df9a3d2d2	HTML/Phishing.BEK!tr	2CMV21-00232-01
39	d72bebc5929f441370e2333a7647abfa3b6d8 8c1547e63f179fcfcc2ea49641c	HTML/Phishing.BEK!tr	2CMV21-00232-01
40	5cc807ba226cb53589e8a470b1394a51c81c5 bb22c97a496c3115131b80d72b1	HTML/Phishing.BEK!tr	2CMV21-00232-01
41	c112d7a36323b5776d3bcdde85d861382c50 e51b3f79231c50c96f8772622510	HTML/Phishing.BEK!tr	2CMV21-00232-01
42	b9d5fd8fb71343e0a954e98e53ea8a0b3804ff ec8ff0519c2c657d4f09147c27	HTML/Phishing.BEK!tr	2CMV21-00232-01
43	be43e27a16f5fbf6890def5a7c2cba9e7d9ae9 ce52db6c739ea672f97aac1c03	HTML/Phishing.BEK!tr	2CMV21-00232-01
44	a5d0f8abafed61c9230536234517cdf5e50680 78df417637f0c38d19658587f5	HTML/Phishing.BEK!tr	2CMV21-00232-01

45	cb1493c7e850d97fd843c1a00f11a481baf5fbd3892d22ae83efaecd532776d8	HTML/Phishing.BEK!tr	2CMV21-00232-01
46	884832a7270da0513e77c376564423f0e10236818c121f1630ebd4cb9304828a	HTML/Phishing.BEK!tr	2CMV21-00232-01
47	1915c34909dac35ee5fa31fe8ffbbc762b01a906b4ac21964c24dcd2560f1348	HTML/Phishing.BEK!tr	2CMV21-00232-01
48	eb75baa713c06b6a6fb1557d91a9ac1ec2b1bc9bcda4ad1253d09fbdf6c487fc	HTML/Phishing.BEK!tr	2CMV21-00232-01
49	f14dad1ab1bf4da70481bdcbcdf31fa0642a2f85c5176c405ba9f783f6002763	HTML/Phishing.BEK!tr	2CMV21-00232-01
50	16fcc6562a9b381d646605065e2c0d07d4313703752ad75aafd2cb98b721e4f9	HTML/Phishing.BEK!tr	2CMV21-00232-01
51	23ea4752dc2df4d8087579e950e670753347e6fda7b82d3a2a044013e9c77c0d	HTML/Phishing.BEK!tr	2CMV21-00232-01
52	5f725d2e82b54b288198dbf25495ac5b017f6fbe1ba927ade0352ec20ea76122	HTML/Phishing.BEK!tr	2CMV21-00232-01
53	7b2f0e5b8c504207bd11299908c0c8e254a4583923dbad4428928dad8f5b140a	RTF/CVE_2017_11882.C!exploit	2CMV21-00232-01
54	f8e5931926034fb027649ebd98867c41315b44bd05c7bb56f5f506a170162010	MSOffice/Agent.GV!tr	2CMV21-00232-01
55	4b2be6731f01d01fca26a96260020ee62a266f018d081d170c30043c0191fe76	W32/Injector.EQGK!tr	2CMV21-00232-01
56	87ef5fdc453362f2a6472c66db59645a6efae8b1f67ba95cfb2b5c9184c0eee5	PossibleThreat.PALLASNET.H	2CMV21-00232-01
57	401ca80a6909af5525501f14a2deedc569ab3ba4e276c77ca1b6fc2e820a5c53	W32/Injector_AGen.AG!tr	2CMV21-00232-01
58	b277c57c94e4063b679e9d6e181a58aa82697773f98e40a5f68fa4db785e1986	Malware_Generic.P0	2CMV21-00232-01
59	fe50b5d75c26eb3d727b32a031f726df6f6447a97340cba0ac89ace8e812ab23	Malware_Generic.P0	2CMV21-00232-01
60	3b895f545a3e92575e0b7971e061c929ad1f3913c1d3db3acc8a58e3e25a45be	W32/Injector.EQAC!tr	2CMV21-00232-01
61	d610a9f285980c3838bbc11fbef2c5b999b20f81149328a809d41e6bf97b54cb	W32/Injector.EQGK!tr	2CMV21-00232-01
62	033372113246279f04ccac1fab6748a2bfd2ed9b9c5cb980534f444dac558af8	MSOffice/Agent.GV!tr	2CMV21-00232-01
63	80658759ad67edd23bc4cbfaba5e2add421ff794772ddffe24174b6f25904087	Java/GenericGB.29230!tr	2CMV21-00232-01
64	d09bc5f5e58e844d5739c655830b27c55e2b784d4b65d3f676df60383a8eae27	MSIL/Kryptik.ACTW!tr	2CMV21-00232-01
65	40bf30e02d39fb1cca08b9cc64005f86c33b181628fcf6c50b3f21d00eef37da	Malicious_Behavior.SB	2CMV21-00232-01

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.

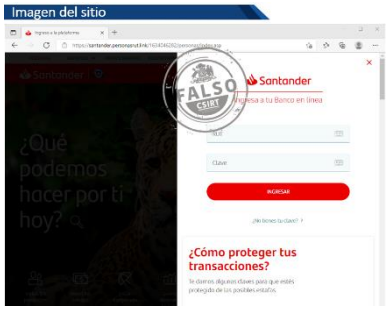
No.	IP	Etiqueta de sistema autónomo	Documento web
1	62.113.202.103	23M GmbH	2CMV21-00232-01
2	77.247.110.172	ABC Consultancy	2CMV21-00232-01
3	103.232.55.238	VIETSERVER SERVICES TECHNOLOGY COMPANY LIMITED	2CMV21-00232-01
4	134.209.231.21	DIGITALOCEAN-ASN	2CMV21-00232-01
5	138.197.163.80	DIGITALOCEAN-ASN	2CMV21-00232-01
6	143.198.71.50	DIGITALOCEAN-ASN	2CMV21-00232-01
7	162.144.153.50	UNIFIEDLAYER-AS-1	2CMV21-00232-01
8	176.61.147.211	Domios S.A	2CMV21-00232-01
9	185.222.57.88	RootLayer Web Services Ltd	2CMV21-00232-01
10	185.222.58.136	RootLayer Web Services Ltd	2CMV21-00232-01
11	185.222.58.154	RootLayer Web Services Ltd	2CMV21-00232-01
12	188.126.94.39	GleSYS AB	2CMV21-00232-01
13	212.193.30.112	Des Capital B.V.	2CMV21-00232-01
14	45.137.22.137	RootLayer Web Services Ltd	2CMV21-00232-01
15	45.137.22.38	RootLayer Web Services Ltd	2CMV21-00232-01
16	45.137.22.60	RootLayer Web Services Ltd	2CMV21-00232-01
17	45.137.22.70	RootLayer Web Services Ltd	2CMV21-00232-01
18	45.137.22.90	RootLayer Web Services Ltd	2CMV21-00232-01
19	64.44.168.170	NEXON	2CMV21-00232-01

Nombres de archivos con malware:

N°	Archivo Malware	
1	Price Inq 01.xls.zip	2CMV21-00232-01
2	SOA.UUE	2CMV21-00232-01
3	Swift copy.r15	2CMV21-00232-01
4	Invoice0012.iso	2CMV21-00232-01
5	Remitance Aowl internationa co.limited SWIFT-$ 111,480.GZ	2CMV21-00232-01
6	REMITTANCE-54324.rar	2CMV21-00232-01
7	Purchase order.r15	2CMV21-00232-01
8	Shipping documents.xlsx	2CMV21-00232-01
9	DHL PARCEL.HTML	2CMV21-00232-01
10	SOA.lzh	2CMV21-00232-01
11	Payment_MT103.r09	2CMV21-00232-01
12	New Purchase Order.img	2CMV21-00232-01
13	AWB 101221_pdf.rar	2CMV21-00232-01
14	Documents.html	2CMV21-00232-01
15	PI- 202110088.doc	2CMV21-00232-01
16	TransportLabel_1189160070.xlsx	2CMV21-00232-01
17	signed copy.rar	2CMV21-00232-01
18	First enquiry.zip	2CMV21-00232-01
19	Nueva lista de pedidos.zip	2CMV21-00232-01
20	file31.cab	2CMV21-00232-01
21	SOA.xlsx	2CMV21-00232-01
22	BANK INFORMATION.r15	2CMV21-00232-01

Phishing

Imagen del sitio



CSIRT alerta de una página fraudulenta que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR21-01013-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de octubre de 2021
Última revisión	12 de octubre de 2021
Indicadores de compromiso	
URL sitio falso	
https://santander.personasrut[.]link/1634046282/personas/index.asp	
IP	
[198.54.115.18]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01013-01/	
https://www.csirt.gob.cl/media/2021/08/8FFR21-01013-01.pdf	

Vulnerabilidades

CSIRT advierte de vulnerabilidades en Dell EMC Enterprise Hybrid Cloud update for VMware	
Alerta de seguridad cibernética	9VSA21-00504-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de octubre de 2021
Última revisión	13 de octubre de 2021
CVE	
CVE-2021-21975	CVE-2021-21983
CVE-2021-22012	CVE-2021-22002
CVE-2021-22006	CVE-2021-21984
CVE-2021-22007	CVE-2021-21985
CVE-2021-22008	CVE-2021-21986
CVE-2021-22009	CVE-2021-21997
CVE-2021-22010	CVE-2021-21999
CVE-2021-22011	CVE-2021-21994
CVE-2021-22013	CVE-2021-21995
CVE-2021-21993	CVE-2021-22003
CVE-2021-22014	CVE-2021-21991
CVE-2021-22015	CVE-2021-22022
CVE-2021-22016	CVE-2021-22023
CVE-2021-22017	CVE-2021-22024
CVE-2021-22018	CVE-2021-22025
CVE-2021-22019	CVE-2021-22026
CVE-2021-22020	CVE-2021-22027
CVE-2021-22005	CVE-2021-22021
CVE-2021-21992	
Fabricante	
Dell	
Productos afectados	
Dell Enterprise Hybrid Cloud: 4.1.0, 4.1.1.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00504-01	
https://www.csirt.gob.cl/media/2021/10/9VSA21-00504-01.pdf	

CSIRT comparte vulnerabilidades informadas por Microsoft en su Update Tuesday de octubre	
Alerta de seguridad cibernética	9VSA21-00505-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de octubre de 2021
Última revisión	14 de octubre de 2021

CVE

CVE-2021-41346	CVE-2021-26427	CVE-2021-41335	CVE-2021-40470
CVE-2021-40474	CVE-2021-40457	CVE-2021-41334	CVE-2021-40467
CVE-2021-41345	CVE-2021-40481	CVE-2021-41332	CVE-2021-40466
CVE-2020-1971	CVE-2021-40480	CVE-2021-41331	CVE-2021-40465
CVE-2021-3449	CVE-2021-41344	CVE-2021-41330	CVE-2021-40468
CVE-2021-3450	CVE-2021-40484	CVE-2021-26442	CVE-2021-40463
CVE-2021-41361	CVE-2021-41343	CVE-2021-26441	CVE-2021-40464
CVE-2021-40479	CVE-2021-41342	CVE-2021-40489	CVE-2021-40462
CVE-2021-36953	CVE-2021-41357	CVE-2021-40488	CVE-2021-40460
CVE-2021-40455	CVE-2021-41353	CVE-2021-40487	CVE-2021-40461
CVE-2021-41347	CVE-2021-40471	CVE-2021-40486	CVE-2021-40456
CVE-2021-41354	CVE-2021-40472	CVE-2021-40483	CVE-2021-40473
CVE-2021-41352	CVE-2021-40454	CVE-2021-40482	CVE-2021-40449
CVE-2021-36970	CVE-2021-40485	CVE-2021-40478	CVE-2021-40450
CVE-2021-41363	CVE-2021-41340	CVE-2021-40477	CVE-2021-40443
CVE-2021-41350	CVE-2021-41339	CVE-2021-40476	CVE-2021-38672
CVE-2021-41348	CVE-2021-41338	CVE-2021-40475	CVE-2021-38663
CVE-2021-34453	CVE-2021-41337	CVE-2021-40469	CVE-2021-38662
CVE-2021-41355	CVE-2021-41336		

Fabricante

Microsoft

Productos afectados

.NET 5.0
Intune management extension
Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Dynamics 365 (on-premises) version 9.0 y 9.1
Microsoft Dynamics 365 Customer Engagement V9.0
Microsoft Dynamics 365 Customer Engagement V9.1
Microsoft Excel 2013 RT Service Pack 1
Microsoft Excel 2013 Service Pack 1 32-bit editions y 64-bit editions
Microsoft Excel 2016 32-bit edition) y 64-bit edition
Microsoft Exchange Server 2013 Cumulative Update 10, 11, 21 y 22
Microsoft Office 2013 RT Service Pack 1
Microsoft Office 2013 Service Pack 1 32-bit editions y 64-bit editions
Microsoft Office 201632-bit editions y 64-bit editions
Microsoft Office 2019 32-bit editions y 64-bit editions
Microsoft Office 2019 for Mac
Microsoft Office LTSC 2021 32-bit editions y 64-bit editions
Microsoft Office LTSC for Mac 2021
Microsoft Office Online Server

Microsoft Office Web Apps Server 2013 Service Pack 1
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 Visual Studio 2017 version 15.9 (includes 15.0 – 15.8)
Microsoft Visual Studio 2019 version 16.11 (includes 16.0 – 16.10)
Microsoft Visual Studio 2019 version 16.4 (includes 16.0 – 16.3)
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 Word 2013 RT Service Pack 1
Microsoft Word 2013 Service Pack 1 32-bit editions y 64-bit editions
Microsoft Word 2016 32-bit editions y 64-bit editions
System Center 2012 R2 Operations Manager
System Center 2016 Operations Manager
System Center 2019 Operations Manager
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 2004 for 32-bit Systems
Windows 10 Version 2004 for ARM64-based Systems
Windows 10 Version 2004 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 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 2004 (Server Core installation)
Windows Server, version 20H2 (Server Core Installation)
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00505-01
https://www.csirt.gob.cl/media/2021/10/9VSA21-00505-01.pdf

CSIRT alerta de vulnerabilidades en productos Apple	
Alerta de seguridad cibernética	9VSA21-00506-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de octubre de 2021
Última revisión	14 de octubre de 2021
CVE	
CVE-2021-30883 CVE-2021-30858 CVE-2021-30860	
Fabricante	
Apple	
Productos afectados	
Apple iOS 14.0 a 15.0.2 iPadOS 14.0 a 15.0.2 macOS Big Sur Safari	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00506-01	
https://www.csirt.gob.cl/media/2021/09/9VSA21-00506-01.pdf	

Actualidad

«Siete Grandes Ciberriesgos para Niños, Niñas y Adolescentes», una nueva ciberguía para este Mes de la Ciberseguridad

Cada octubre conmemoramos en Chile y el Mundo un nuevo Mes de la Ciberseguridad. Y en esta ocasión decidimos hacerlo con guías que apuntan a algunos de los grupos que son más vulnerables a los ataques cibernéticos: niños, niñas y adolescentes, pymes y adultos mayores.

Así es que, como primera guía este Mes de Ciberseguridad, presentamos la que decidimos llamar «Siete Grandes Ciberriesgos para Niños, Niñas y Adolescentes», que describe estos peligros y da consejos para que padres y apoderados asistan y enseñen a los menores para que puedan evitarlos. Pueden descargarla aquí, ¡no olviden también compartirla con amigos y familiares!:
https://www.csirt.gob.cl/recomendaciones/siete-grandes-ciberriesgos-nna/.

Continúa la campaña del CSIRT de Gobierno y CSIRTAmericas por el Mes de la Ciberseguridad: Esta semana el foco fueron los niños, niñas y adolescentes

Este Mes de la Ciberseguridad, 12 CSIRT del continente — reunidos en CSIRTAmericas— y el Programa de Ciberseguridad de la Organización de los Estados Americanos (OEA) decidieron compartir una serie de ciberconsejos de concientización alineados según cuatro temas, uno cada semana.

La presente segunda semana fue el turno de niños, niños y adolescentes, con publicaciones realizadas por los CSIRT de Paraguay, Uruguay y Buenos Aires, las que fueron replicados por los demás participantes. Todas fueron diseñadas por el CSIRT del Gobierno de Chile. Las siguientes temáticas serán pymes y adultos mayores.

La idea, presentada por el CSIRT del Gobierno de Chile a CSIRTAmericas y adoptada rápidamente, ha sido plasmada en imágenes en nuestro país recopilando consejos enviados por cada uno de los CSIRT partícipes: Buenos Aires y Neuquén en Argentina, Chile, Colombia, Costa Rica, Ecuador, Estados Unidos, Jamaica, Panamá, Paraguay, República Dominicana y Uruguay. Las publicaciones son hechas en inglés y castellano y podrán verlas aparecer durante todo el mes en https://twitter.com/CSIRTGOB.


Ciberconsejos para el
MES DE LA CIBERSEGURIDAD
NIÑOS, NIÑAS Y ADOLESCENTES
HABLA con tus hijos sobre el uso de Internet y redes sociales.
ACUERDA en familia pautas para el uso de la tecnología en casa.
CUIDA la huella digital de tus hijos y lo que publicas sobre ellos en redes sociales.
CSIRTAmericas Network
Ciberconsejos para el
MES DE LA CIBERSEGURIDAD
NIÑOS, NIÑAS Y ADOLESCENTES
Si eres responsable de niños, niñas o adolescentes...
RECUERDA depende de ti que puedan hacer pleno ejercicio de sus derechos digitales.
TEN PRESENTE que los entornos digitales tienen igual potencial de dañar que las acciones realizadas en el mundo material.
SE CONSCIENTE de que la dimensión digital de la identidad es hoy muy importante para todos. Piensa bien antes de publicar sobre los más pequeños.
CSIRTAmericas Network

El Comando de la Semana | No. 21 HostHunter

El Comando de la Semana esta vez se trató de HostHunter, una herramienta para descubrir y extraer eficientemente los nombres de host que proporcionan un gran conjunto de direcciones IP de destino. HostHunter utiliza técnicas sencillas de OSINT para mapear direcciones IP con nombres de host virtuales y genera un archivo CSV o TXT con los resultados del reconocimiento. Esta herramienta llega con la actualización de Kali Linux 2021.3.

Con los comandos que compartimos semanalmente no pretendemos reemplazar una auditoria de código o evaluación de vulnerabilidades, sino que establecer capacidades básicas de chequeo y obtención de información de manera rápida para temas específicos, como por ejemplo la verificación de la subsanación de alertas o vulnerabilidades reportadas por el CSIRT de Gobierno.

Encuentra el comando de la semana que termina, aquí: https://www.csirt.gob.cl/estadisticas/el-comando-de-la-semana-no-21/.

El Control de la Semana | No. 15 Instalación de Software en Sistemas Operacionales

La Ficha de Control Normativo de la segunda semana de octubre trata sobre los procedimientos para la Instalación de Software en Sistemas Operacionales, siendo estos últimos todos aquellos programas destinados a prestar servicio en una institución, como por ejemplo sistemas operativos, firmware, aplicativos operacionales y sistemas para la prestación de servicios, entre muchos otros.

En el documento descargable a continuación encontrarán todos los detalles del control la semana que termina: https://www.csirt.gob.cl/estadisticas/el-control-de-la-semana-no-15/.

Recomendaciones y buenas prácticas

Recomendaciones generales de seguridad

- 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.

- Gonzalo Andrés Ramírez Cabrera
- Ricardo Konopnicki Wenzel
- Diego Alberto Sandoval Burgos

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.10.15 12:01:35 -03'00'