Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

12-11-2021 | Año 3 | N°123

Boletín de Seguridad Cibernética

Semana del 05 al 11 de noviembre de 2021

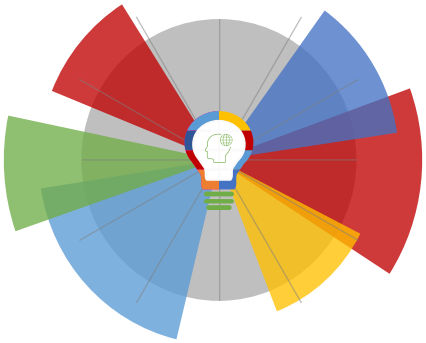
La semana en cifras

Hash

71

SHA

Asociadas a múltiples campañas de phishing con archivos que contienen malware



IP

25

Informadas

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

Parches

73

para vulnerabilidades

Las mitigaciones son útiles en productos de Cisco y Microsoft.

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

Contenido

Vulnerabilidades

CSIRT alerta ante vulnerabilidades en productos Cisco	
Alerta de seguridad cibernética	9VSA21-00518-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Noviembre de 2021
Última revisión	09 de Noviembre de 2021

CVE

CVE-2021-40119
CVE-2021-34795
CVE-2021-40112
CVE-2021-40113
CVE-2021-34739
CVE-2021-34741
CVE-2021-40128
CVE-2021-1500
CVE-2021-40115
CVE-2021-40126
CVE-2021-34773
CVE-2021-40127
CVE-2021-40120
CVE-2021-34784
CVE-2021-34701
CVE-2021-34774
CVE-2021-34731
CVE-2021-40124

Fabricante

Cisco

Productos afectados

Cisco Policy Suite 21.1.0 y anteriores.
Cisco Catalyst PON Switch CGP-ONT-1P
Cisco Catalyst PON Switch CGP-ONT-4P
Cisco Catalyst PON Switch CGP-ONT-4PV
Cisco Catalyst PON Switch CGP-ONT-4PVC
Cisco Catalyst PON Switch CGP-ONT-
Cisco ESA con una versión vulnerable del software Cisco AsyncOS (13.0 y anteriores, 13.5 y 13.7)
Productos Cisco corriendo una versión afectada del firmware:
250 Series Smart Switches
350 Series Managed Switches
350X Series Stackable Managed Switches
550X Series Stackable Managed Switches
Business 250 Series Smart Switches
Business 350 Series Managed Switches
ESW2 Series Advanced Switches
Small Business 200 Series Smart Switches
Small Business 300 Series Managed Switches

Small Business 500 Series Stackable Managed Switches
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00518-01/
https://www.csirt.gob.cl/media/2021/11/9VSA21-00518-01.pdf

CSIRT alerta de vulnerabilidades del Update Tuesday de Microsoft en Noviembre 2021	
Alerta de seguridad cibernética	9VSA21-00519-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Noviembre de 2021
Última revisión	10 de Noviembre de 2021
CVE	
CVE-2021-42298	CVE-2021-42291
CVE-2021-42279	CVE-2021-42287
CVE-2021-42316	CVE-2021-42288
CVE-2021-26443	CVE-2021-42285
CVE-2021-3711	CVE-2021-42284
CVE-2021-38666	CVE-2021-42283
CVE-2021-41351	CVE-2021-42282
CVE-2021-43209	CVE-2021-42278
CVE-2021-43208	CVE-2021-42275
CVE-2021-26444	CVE-2021-42274
CVE-2021-42323	CVE-2021-41373
CVE-2021-42322	CVE-2021-41375
CVE-2021-42321	CVE-2021-41372
CVE-2021-42319	CVE-2021-41368
CVE-2021-41376	CVE-2021-41367
CVE-2021-41374	CVE-2021-40442
CVE-2021-42304	CVE-2021-38631
CVE-2021-42303	CVE-2021-38665
CVE-2021-42302	CVE-2021-42292
CVE-2021-42301	CVE-2021-42286
CVE-2021-42300	CVE-2021-42276
CVE-2021-42305	CVE-2021-41379
CVE-2021-42277	CVE-2021-41377
CVE-2021-42296	CVE-2021-41378
CVE-2021-41366	CVE-2021-41371
CVE-2021-41349	CVE-2021-41370
CVE-2021-41356	CVE-2021-36957
CVE-2021-42280	
Fabricante	
Microsoft	
Productos afectados	
3D Viewer	
Azure RTOS	
Azure Sphere	
FSLogix	

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
Microsoft Dynamics 365 (on-premises) version 9.1
Microsoft Edge (Chromium-based) in IE Mode
Microsoft Excel 2013 RT Service Pack 1
Microsoft Excel 2013 Service Pack 1 (32-bit editions)
Microsoft Excel 2013 Service Pack 1 (64-bit editions)
Microsoft Excel 2016 (32-bit edition)
Microsoft Excel 2016 (64-bit edition)
Microsoft Exchange Server 2013 Cumulative Update 23
Microsoft Exchange Server 2016 Cumulative Update 21
Microsoft Exchange Server 2016 Cumulative Update 22
Microsoft Exchange Server 2019 Cumulative Update 10
Microsoft Exchange Server 2019 Cumulative Update 11
Microsoft Malware Protection Engine
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 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 Office Online Server
Microsoft Office Web Apps Server 2013 Service Pack 1
Microsoft SharePoint Enterprise Server 2013 Service Pack 1
Microsoft Visual Studio 2015 Update 3
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 16.7 (includes 16.0 – 16.6)
Microsoft Visual Studio 2019 version 16.9 (includes 16.0 – 16.8)
Power BI Report Server
Remote Desktop client for Windows Desktop
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 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/9vsa21-00519-01/
https://www.csirt.gob.cl/media/2021/11/9VSA21-00519-01.pdf

IoC Malware

A continuación, se comparten los Indicadores de Compromisos que fueron detectados durante la semana pasada por el Equipo del CSIRT.
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
2c6b26fe3343b2c49bc7c8b06f1c2bf1ae01509ce60de6f9773e5f81816f0296	W32/Injector	2CMV21-00246-01
a0a5b10eae524d3f3a01cc038ba29e5b0b83d39b5938042bfed59b77f28dfffb	W32/Injector	2CMV21-00246-01
7c2043abcbf8b19d2ca6f289d7c55809b95af7f532890ba957d219cfdf3b3788	MSIL/CoinMiner	2CMV21-00246-01
01d22f650ce9d1eda0cb8452f98fd49df6db0450651f63687b72a65e9d5e0296	W32/Injector	2CMV21-00246-01
7766394cc16fdc0698b3c40bea75b6d684b18e10e6bc480bc1048e34e0d05d15	MSIL/CoinMiner	2CMV21-00246-01
0c99cfbc949e95cf393346aeebb948437663dec0a9d0230f9e839daa87135966	MSIL/CoinMiner	2CMV21-00246-01
cb25f18f7a707c922eda0bbd532637eee3d7692e3340a8f8f0f15135bda8bbcc	MSIL/Kryptik	2CMV21-00246-01
51147e1442403de2913d79becd8fdb9baa159b05a239b02f08b84e331e2fa374	W32/Injector	2CMV21-00246-01
d36875fb55641bbc6c3c195cea0ca9b40b2e883be4b4165028cb32881980832d	W32/PossibleThreat	2CMV21-00246-01
cf30963b6ca60dedcb619524ae3f22ed844a3a90387a4860112125269e8f82c0	MSIL/Kryptik	2CMV21-00246-01
17aa677c350f4618dbdd62cec51487113a8b938206d81e169613abc9c859666b	W32/Injector	2CMV21-00246-01
b035d1e81a5ffa7b6f78ba3e130c25e54b994ed3b0ffec9b41d6ac51556b2716	W32/Injector	2CMV21-00246-01
cbdc5fba375e0c9798dba2c7f6fa8b093519cafd763569f34a9c9f88643f2aec	W32/Injector	2CMV21-00246-01
6245debd02d3784f09c2633490c9f46c8ca8da1f737ef23bd6410dfe0413039c	MSIL/Kryptik	2CMV21-00246-01
c93e0de69c4d40ebbd5cf15b3bf2570902d019a8c9d1fe110db0dfb24f90c882	MSIL/CoinMiner	2CMV21-00246-01
6ef22611a11e1c81118df6acb61b1fcd6890229d019c7b662447a85532511a15	PossibleThreat	2CMV21-00246-01
e5107bc5543a73fddd79e375b0aaf8b70b5e539fffe6ded47202bea720353232	PossibleThreat	2CMV21-00246-01
77e5742cd35393d3bde85a0551f2a4c9a416be1170867f0abcb1c9d24ef7637f	MSIL/GenKryptik	2CMV21-00246-01
8fc5e578a00188a3a648450d3965261f61ab3ffef70d86350c3aefb5d8abe121	MSIL/GenKryptik	2CMV21-00246-01
8052651c549ade8346f6982f59f1e961fcfdcb99cec9e4b9e9bd2d4005af7d5c	MSIL/GenKryptik	2CMV21-00246-01
cdc1d762a209a7cd44d6d240582f372d18b62a36eefcdc4b103190cfb4319746	MSIL/GenKryptik	2CMV21-00246-01
3515490d0a5d17802e4b1b76fe205af103d8aae24af542621a75f931814642ca	Malicious_Behavior	2CMV21-00246-01
50d2005b69097eebe97a0aa4a628621d11d1b13953fef319accaaacd21fc7d42	Malicious_Behavior	2CMV21-00246-01
d27259ad893f746615873eacf52f5970866bea3dabdb9605c5a1704dc84adf5d	PossibleThreat	2CMV21-00246-01
12a9903559997d210a4dcb17131238c030a698dae1b76d22a4dd1746cc1e764c	Malicious_Behavior	2CMV21-00246-01
7cc4bb270baee52f24de7f4912a7131a19ab4418ff447ffeef2e2d2f86735f74	W32/Injector	2CMV21-00246-01
16fd16f1795de27c016a22b16c4db01bf7f2197a91dfc98dc8f7ab9c4e85c464	W32/Injector	2CMV21-00246-01
4d37421c4953cd06c480fe440eb1102a3fd258899ad970861f65f06212069853	W32/Injector	2CMV21-00246-01
8102af0dad7506bf788e93788a136a934f7dc3c2b461a352dc7c2419e46d12bb	W32/EQMR	2CMV21-00246-01
71356d02aef498bd0f14a0149fe043c405b55f69855965a25fde522581e97eaf	VBA/Agent	2CMV21-00246-01
bda5add79e9e06801f579e8f7a249a3abf1a7d78ec56275c0ab5ffe8e97176ca	W32/GuLoader	2CMV21-00246-01
f94380f600899a30f325f87a138ed39739a748366afd27cf46f10756ab88c5ed	PossibleThreat	2CMV21-00246-01
fe11cb19519fafea4d0b1f2a0c57cb437363c24756018b7b3aac965c56498676	MSOffice/Agent	2CMV21-00246-01
d5112dbe85aa2bc4f8fcc60da397e1dd436512036ab25bb6327735ab3ff926d3	MSIL/GenKryptik	2CMV21-00247-01
1060cd77d3b53d02466d168aa1eaa8ff9bb27ded165484b56ad61c529d117982	MSIL/GenKryptik	2CMV21-00247-01
5ad0a97284f0fa0c22934b37d45376d2041c90624f73617286164ffa771a3fd1	MSIL/GenKryptik	2CMV21-00247-01
8d9d70bc837d2073fbd7ec216d2cbd36da630544ed7114af717fb1daad420138	MSIL/GenKryptik	2CMV21-00247-01
f217cc024d292764cf387fd52ec78843be77df06bd723219bd15dd655b9399c7	MSIL/GenKryptik	2CMV21-00247-01

3c6ec9674570d6bae26b02e9de162dfaed5d2f62dddcef662944937ca9eff320	MSIL/GenKryptik	2CMV21-00247-01
cebb007462977469cf72f0b159a119708862fca3e0860301ac466f47ed87b839	MSOffice/Agent	2CMV21-00247-01
dc7970b776b58b09ef3b20cd24739e6bb278fd7d51e0523b5bd0c022a67193f3	MSOffice/Agent	2CMV21-00247-01
d4fc82d03b2f147fc6a5cde62812b8c2be27f6eb757052f3b0c0be6da5ef1863	MSIL/GenKryptik	2CMV21-00247-01
44a9fef90c6e055c8f7f322d254b16844d18ce362b97e7949a77f236afba135e	MSIL/GenKryptik	2CMV21-00247-01
e0159c283dc90b92f5da5549b25070a4fd1bb5da20d8d560b412308bd14ed5f4	MSIL/GenKryptik	2CMV21-00247-01
4c12cfee9b47fa96215f17bdcdd51a4af58dcc02f4a1551bcec22232e56d467b	MSIL/GenKryptik	2CMV21-00247-01
832513cdf5d7ffad938a642c017e8c75fff8c3a5625529eb50374f7788f09aa0	MSIL/GenKryptik	2CMV21-00247-01
69822da8ba731e808997989c1792bee4a4402c9f95a604d761215876f4a5f76c	MSIL/GenKryptik	2CMV21-00247-01
451605846ff7dae9159c9ddc64fea1aa02ae5de9f437042bc2a5d57a1afb5d70	MSIL/GenKryptik	2CMV21-00247-01
055a6f97422d7ccae38af943f9e09df59109a6aab611819fac91a51cb07ad876	MSIL/GenKryptik	2CMV21-00247-01
dcd7a0ad48ef82add2cd482a7360566417c9f95afbfb73f24536a1996da1bc12	MSIL/GenKryptik	2CMV21-00247-01
8ab65db8b90e461c915d620d6dd11fb1dd42b6a3e987d17fa8a490c73a29e449	MSIL/GenKryptik	2CMV21-00247-01
e03c20d22ae261c302bb875596acff12e161c0c94c582e1dab7c71c926a69912	MSIL/GenKryptik	2CMV21-00247-01
84b2c2e771da5f3f58cf00f14296ffb67b999781f6c43fdd52c18f876112ed84	MSIL/GenKryptik	2CMV21-00247-01
8856d012bb2216bb3bb44e6cef106e71457bc2ec12024d71b458e8614f1289e9	MSIL/GenKryptik	2CMV21-00247-01
771e4987a7e10c82fd1c92db1c87afbad6297fc046eed080915a13fa1f3425a6	MSIL/GenKryptik	2CMV21-00247-01
20e7e85dc03885c95684a89e78a79383ade8cef7d44529688888498825939096	W32/Injector	2CMV21-00247-01
93f4172e58663ed04f44982fedb3378d71aa15031697015564a9c5eb756c3630	MSOffice/CVE_2017_11882	2CMV21-00247-01
31b52add6c41ed251982b80357ee0f608e5b5a68e2dceeac6ba00d45ef5b0cac	MSIL/GenKryptik	2CMV21-00247-01
680218710b568ed6f5c128f73346d00759912dda019c8056139125da5d3792ea	MSOffice/CVE_2017_11882	2CMV21-00247-01
94bdd033e56083d02932002e85400ac222e7542a217d608812c6f74e8693fad3	MSIL/GenKryptik	2CMV21-00247-01
8d25d496da2b1c32b34930e61849396fbc16a3b10ee2deaa2107c6791a7b346d	MSIL/GenKryptik	2CMV21-00247-01
e518441b1cf382e148be37d636501ad7a9d3645d805de0c218d5c4b8207cf8d0	MSIL/GenKryptik	2CMV21-00247-01
0ef48e5bfad7e6ff5f925073b475fb453a4d991f128dde10afab5bb6bfac5de2	PossibleThreat	2CMV21-00247-01
9144b18f5c53a64c6f6011c86e05f470d59e01e03104e162795548039ffb9608	HTML/Phishing	2CMV21-00247-01
42d964ff532bac8b305a353f8bee9e651b5b466742a66465b552586b1b183225	Malware_Generic	2CMV21-00247-01
c944572b8ac4302c8b4eff402fb4f077c5dee28e77594352478c6cb87b14c4e4	JS/Fphishing	2CMV21-00247-01
f8519c98e952c366af2a078c32062f2f4b023bddf24bbc23bc1fba1136e4fbcf	W32/PossibleThreat	2CMV21-00247-01
f6917cd0e7882b0f63144681515d50ca96ee4d47242ac7f6799f44ce93f68dfe	W32/Injector	2CMV21-00247-01
9d737c9ce96a5d71458dfc9fcc1321ad60ad388b390e8ddd367a1e9fd4ca73b9	Malware_Generic	2CMV21-00247-01
89ebe0bb6837353b522cbc070bf8404a2946e963eaf8e53c7fefe1d2c8fb36eb	W32/Injector	2CMV21-00247-01
415d6bbaafe61f2e1e314a0c8dcd99ff070316081a4671d6e40108773d06a5b3	MSIL/Agent	2CMV21-00247-01

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
45.137.22.45	RootLayer Web Services Ltd.	AS 51447	2CMV21-00246-01
185.222.58.120	RootLayer Web Services Ltd.	AS 51447	2CMV21-00246-01
45.137.22.114	RootLayer Web Services Ltd.	AS 51447	2CMV21-00246-01
195.133.18.211	Delis LLC	AS 211252	2CMV21-00246-01
159.223.65.191	DigitalOcean	AS 14061	2CMV21-00246-01
64.13.224.158	Medoatemple	AS 31815	2CMV21-00246-01
174.142.19.206	IWEB-AS	AS 32613	2CMV21-00246-01
89.252.178.177	Netinternet Bilisim Teknolojileri AS	AS 51559	2CMV21-00246-01
104.168.190.125	Hostwinds	AS 54290	2CMV21-00246-01
45.137.22.69	RootLayer Web Services Ltd.	AS 51447	2CMV21-00246-01
212.192.241.172	Delis LLC	AS 211252	2CMV21-00246-01
134.213.73.207	Rackspace Ltd.	AS 15395	2CMV21-00246-01
37.49.225.119	Peenq NL	AS 212370	2CMV21-00246-01
185.21.206.32	ISIK Bilgisayar Internet ve Yayincilik Hizmetleri	AS 49879	2CMV21-00246-01
103.23.20.233	PT Infinys System Indonesia	AS 58397	2CMV21-00247-01
103.28.70.72	Hyonix LLC	AS 213122	2CMV21-00247-01
143.198.42.128	DIGITALOCEAN-ASN	AS 14061	2CMV21-00247-01
172.245.92.99	AS-COLOCROSSING	AS 36352	2CMV21-00247-01
206.222.8.76	ENET-2	AS 10297	2CMV21-00247-01
37.0.10.139	Delis LLC	AS 211252	2CMV21-00247-01
37.0.11.134	Delis LLC	AS 211252	2CMV21-00247-01
37.0.11.6	Delis LLC	AS 211252	2CMV21-00247-01
45.137.22.135	RootLayer Web Services Ltd.	AS 51447	2CMV21-00247-01
45.137.22.53	RootLayer Web Services Ltd.	AS 51447	2CMV21-00247-01
82.147.40.130	Eidsiva Bredband AS	AS 29492	2CMV21-00247-01

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
20308398738329390280839287 92.arj	2CMV21-00246-01
New order - C.S.I No. 0987.7z	2CMV21-00246-01
#Doc14$.zip	2CMV21-00246-01
Order Confirmation.zip	2CMV21-00246-01
Invoice No ANT19-20646.ARJ	2CMV21-00246-01
PO-BA9000746.7z	2CMV21-00246-01
FUCHS URGENT LIST ORDER11821,pdf.iso	2CMV21-00246-01
Purchase Order - 10,000MT.rar	2CMV21-00246-01
Curriculum Vitae CV Joana Diogo.zip	2CMV21-00246-01
Comprobante-00123232#.pdf.z	2CMV21-00246-01
Doc_#10223023.img	2CMV21-00246-01
tt copy 200393903.arj	2CMV21-00246-01
YWvqk1OliVWNoau.zip	2CMV21-00246-01
PO.No 2100087.gz	2CMV21-00246-01
Unpaid invoice.zip	2CMV21-00246-01
Order Confirmation 6201986.zip	2CMV21-00246-01
STATEMENT OF ACCOUNT.zip	2CMV21-00246-01
COMMERCIAL OFFER.zip	2CMV21-00246-01
New order - C.S.I No. 0987.rar	2CMV21-00246-01
Transfer Request Form.zip	2CMV21-00246-01
Payment invoice.7z	2CMV21-00246-01
QUOTE 002242020.rar	2CMV21-00246-01
PO_IMG-#201820-20193-2021.r00	2CMV21-00246-01
items.doc	2CMV21-00246-01
Proforma Invoice, New order.zip	2CMV21-00246-01
Pharma_Quotation.zip	2CMV21-00246-01
Pago.Confirmacion.xls	2CMV21-00246-01
Purchase Order 30,000MT.rar	2CMV21-00246-01
uCkIzRN4ZzUIzCY.rar	2CMV21-00246-01
Request For Quotation.xlsx	2CMV21-00246-01
DUE INVOICES.xlsx	2CMV21-00246-01
00987654334567.zip	2CMV21-00247-01
PAYMENT DATAILS.zip	2CMV21-00247-01
0JGFOez7vfZ18Tg.rar	2CMV21-00247-01
ls1w#doc.zip	2CMV21-00247-01
UPDATTED S O A.zip	2CMV21-00247-01
R F Q 2000051165.zip	2CMV21-00247-01
PDT_637235373623_153739922773.xlsx	2CMV21-00247-01

PRODUCT LIST.rar	2CMV21-00247-01
PO.rar	2CMV21-00247-01
Invoice.7z	2CMV21-00247-01
SOA.zip	2CMV21-00247-01
file#0017.zip	2CMV21-00247-01
Payment_receipt.r09	2CMV21-00247-01
PO-4999.zip	2CMV21-00247-01
Purchase Order 20000MT.rar	2CMV21-00247-01
zCEr8cPJ5GpDgmz.rar	2CMV21-00247-01
OUSTANDING OVERDUE INVOICES.r09	2CMV21-00247-01
SOA-24th of Oct..xlsx	2CMV21-00247-01
Purchase Order 50,000MT.rar	2CMV21-00247-01
Payment Advice.xlsx	2CMV21-00247-01
PI 1 & PI 2.xlsx	2CMV21-00247-01
Invoice- Shping DOCX.zip	2CMV21-00247-01
MAERSKLINE INV.htm	2CMV21-00247-01
6ZDoc#0021.zip	2CMV21-00247-01
underlivered_mails.html	2CMV21-00247-01
PO-3626357727.PDF.BZ2	2CMV21-00247-01
RFQ-EMP212306308512.7z	2CMV21-00247-01
Transferencia bancaria adjunta pdf.exe.xz	2CMV21-00247-01

Actualidad

Ciberguía y kits de herramientas para mejorar la ciberseguridad de las pymes

La ciberseguridad es relevante de manera transversal, de las empresas pequeñas a los grandes conglomerados y desde altos ejecutivos hasta el ciudadano común en cada hogar. La vida cotidiana de personas y empresas está cruzada por servicios tecnológicos, que con sus vulnerabilidades los exponen a riesgos cibernéticos.

En este contexto, las pymes deben intentar aprovechar las ventajas de los procesos de digitalización y el creciente despliegue de conectividad tanto a nivel nacional como mundial. Pero esta travesía no está exenta de riesgos, los que deben tomarse en cuenta si no se quiere naufragar a mitad de camino.

La tecnología puede ayudar a las pymes en sus procesos de optimización, eficiencia y eficacia, de expansión de sus zonas de alcance, e incluso una potencial internacionalización. ¿Por qué no pensar en dar servicios al mundo desde una pyme en el hogar? Las redes de hoy ya lo permiten y las que están por venir facilitarán aún más estas rutas, con servicios de conectividad avanzados y coordinaciones logísticas que expandirán el alcance geográfico hasta lugares impensados hoy en día.

El CSIRT elaboró una completa guía dirigida a las pymes para apoyarlas en el proceso de digitalización de forma cibersegura, la cual se puede descargar en el siguiente enlace: https://www.csirt.gob.cl/recomendaciones/ciberguia-para-las-pymes/

CiberSucesos Especial Mes de la Ciberseguridad

Octubre es internacionalmente reconocido como Mes de la Ciberseguridad, y por ello se desarrollaron en todo el mundo gran número de actividades para promover prácticas seguras del uso de internet entre la población en general, con foco en los grupos más vulnerables. Con ese objetivo en mente, nuestro CSIRT de Gobierno propuso a sus pares reunidos en CSIRTAmericas —a su vez, inserta en el marco de la Organización de los Estados Americanos (OEA) — llevar nuestros tradicionales ciberconsejos a toda América, iniciativa que fue positivamente recibida.

Así, durante todo octubre, las recomendaciones de 12 CSIRT del continente fueron plasmadas en publicaciones ilustradas, diseñadas por nuestra institución en Chile y difundidas desde Estados Unidos a nuestro Cono Sur, gracias a la participación de los CSIRT y CERT en EE.UU., República Dominicana, Jamaica, Costa Rica, Panamá, Colombia, Ecuador, Paraguay, Uruguay y, en Argentina, los de Neuquén y Buenos Aires.

Con ese mismo espíritu es que decidimos dedicar esta edición especial de nuestra revista CiberSucesos para resumir y poner a disposición de la comunidad las recomendaciones más importantes que es necesario conocer al disfrutar del mundo en línea, y específicamente aquellas dirigidas a los niños, niñas y adolescentes, a las pequeñas y medianas empresas (pymes) y a los adultos mayores.

Los consejos para niños, niñas y adolescentes (NNA) se centran en describir los siete mayores riesgos que apuntan a ellos en internet —como el grooming, el sexting y los retos virales peligrosos—, y las principales formas en que pueden protegerse. Está elaborado de forma de ser leído por padres y tutores solos o en conjunto con los menores.

La guía para adultos mayores se aboca, por su parte, primero a describir y explicar los principales conceptos del mundo digital, y solo tras ello explica varias formas para que los ancianos estén más seguros en línea.

Finalmente entregamos recomendaciones de ciberseguridad para pequeñas y medianas empresas —pymes—, incluyendo herramientas y controles que mejoran la defensa digital de una organización de forma gratuita y accesible, poniendo la ciberseguridad a disposición de firmas que no pueden pagar grandes soluciones en esta materia.

La revista completa aquí:
https://www.csirt.gob.cl/media/2021/11/Master-Rev.-CSIRT-ESPECIAL-Octubre-OK.pdf

Ciberconsejos: Cómo cuidarnos de las fake news en estas elecciones

Cuando se acerca un período de votación también lo hace la desinformación. Por eso, más que nunca debemos ser suspicaces con toda la información que recibimos y nunca compartirla hasta corroborar que sea verdadera, confirmada, por ejemplo, por un medio tradicional.

Por eso, y para ayudarnos a reconocer cuando estamos frente a noticias falsas, reunimos algunos simples consejos que pueden conocer en la siguiente ciberguía. ¡Compártanlo con sus amigos y familiares! Descargando el documento en el siguiente enlace:
https://www.csirt.gob.cl/recomendaciones/ciberconsejos-fake-news-elecciones2021/

Mensaje despedida Director CSIRT

No puedo, no partir agradeciendo al Presidente Sebastián Piñera, al Ministro Andrés Chadwick y al Subsecretario Rodrigo Ubilla, en haber confiado en mi persona para liderar por un lado la creación del programa de ciberseguridad en época de campaña presidencial, como a su vez, liderar este proyecto, cuando ya éramos gobierno. No puedo dejar de agradecer también al Subsecretario Juan Francisco Galli, quien me dio la libertad de poder ejecutar el programa de ciberseguridad alejando los fantasmas de los nombramientos políticos ("zares") a cargo del tema. Finalmente, no puedo, no agradecer a las 75 personas que se atrevieron a venir, que han pasado, que han participado y los que siguen aún por estos casi cuatro años por la División que me ha tocado liderar.

En cuanto a la Red de Conectividad del Estado, uno de los tres departamentos a cargo, hemos modernizado la arquitectura de esta red, por segunda vez en su historia; la primera vez, cuando migramos de una red obsoleta, lenta y sin SLA, a una red de alta velocidad de 10 gb/s, moderna, monitoreada y operada en modo 7x24, y con SLA de cumplimiento y soporte. Hoy, estamos en las etapas finales de procesos licitatorios que permitirán tener adicionalmente y por primera vez una red altamente segura, con equipamiento de ciberseguridad variado y de primer nivel, dando conexión al 70% del Gobierno y con uptime del 100% hace ya más de un año.

En cuanto al Departamento de Informática, propio del Ministerio, totalmente ajeno a la ciberseguridad, pero que nos absorbía de mucho tiempo y recursos diariamente. A ellos, muchas gracias por su sacrificio, esfuerzo y compromiso, en el desarrollo y operación de plataformas de regularización de extranjeros, APEC, COP25, Diario Oficial, Comisaría Virtual, Residencias Sanitarias y tantas otras iniciativas ajenas a su rol propio dentro del Ministerio. Muchas gracias por estar 7x24 junto al CSIRT en la oficina en pleno estallido social, gracias por apoyarnos en plena pandemia en pro del desarrollo y mantención de plataformas vinculadas a la pandemia y beneficiosas para todos los chilenos. No puedo ser hoy más que su escudo protector.

En cuanto a ciberseguridad, uno de los principales logros para proteger la infraestructura crítica del país fue la creación del Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT GOB), que desde agosto de 2019 es el organismo técnico encargado de implementar las medidas que determina el Comité Interministerial de Ciberseguridad (CICS) para la implementación de su agenda. En la misma fecha también fue creada la División de Redes y Seguridad Informática, encargada de materializar la estrategia de ciberseguridad; también se avanzó en:

- Definición de normas urgentes de ciberseguridad para el sector público a través del Instructivo Presidencial N°8(2018).
- Definición de normas de seguridad de la información y ciberseguridad para el sector de Salud Público, Servicios de Salud, Seremis, hospitales públicos y MINSAL nivel central (2021).

- Definición de normativas de ciberseguridad para el sector privado regulado a través de superintendencias:

    - Bancos e instituciones financieras a través de la SBIF/CMF.
    - Empresas de telecomunicaciones a través de SUBTEL.
    - Empresas eléctricas a través del CNE y CEN.
    - Casinos de juegos a través de la Superintendencia de Casinos y Juegos.
    - AFP, a través de la Superintendencia de Pensiones.
    - Mutuales y Cajas de compensación a través de la Superintendencia de Seguridad Social.

- Lanzamiento del primer COSOC de Ciberseguridad para la sociedad civil.
- Obtención de préstamo del BID, para mejorar la ciberseguridad ciudadana del país, por un monto de 26 millones de dólares.
- Reporte a instituciones públicas y privadas de más de diez mil vulnerabilidades y más de treinta y cinco mil incidentes informáticos.
- Revisión y escaneo preventivo de más de dos mil sitios de gobierno a la fecha en búsqueda de brechas de seguridad.
- Monitoreo en formato 7x24 del CSIRT los alrededor de 4000 sitios del Gobierno.
- Revocación y suspensión de más de 45 dominios fraudulentos.
- Se han creado y aplicado a 45 instituciones y empresas críticas, un modelo de encuesta de madurez, la cual es una herramienta que mide el grado de madurez de las instituciones en ciberseguridad.

CSIRT como motor de concientización ciudadana

Considerando que el factor humano es el eslabón más débil ante la protección de un ciberataque, la difusión de campañas de toma de conciencia por parte de la ciudadanía sobre los riesgos de navegar por internet fue uno de los ejes del trabajo realizado por el CSIRT. Con este fin se realizó:

- 1° Campaña nacional de Ciberseguridad (televisiva y radial) “Conciencia digital” para evitar delitos informáticos.
- 2.314 alertas ciudadanas emitidas
- 51 campañas ciudadanas de concientización
- 10 guías ciudadanas de concientización
- 122 boletines de resumen de actividad semanal
- 28 informes de gestión mensual
- 15 revistas mensuales de ciberseguridad

- 24 comandos de la semana
- 17 controles normativos de ciberseguridad

Hemos realizado a nivel de eventos, charlas y capacitación:

- El simposio de ciberseguridad de la OEA con sede en Chile en el año 2019, donde más de 3.000 personas participaron durante una semana.
- Primer y segundo simposio de ciberseguridad para funcionarios públicos en 2020 y 2021.
- Primera versión de Conferencia 8.8 Gobierno.
- Se ha participado en más de 150 charlas como invitados expertos.
- Se ha capacitado a más de 8.000 funcionarios públicos.

En cuanto al desafío global de potenciar el rol de la mujer en el ámbito de la ciberseguridad, se ha buscado disminuir la brecha de género en el sector de seguridad cibernética, fomentando la capacitación y participación femenina en el área a través del desarrollo de 4 versiones de manera consecutiva del Cyberwomen Challenge, ejercicio internacional desarrollado en conjunto con la Organización de Estados Americanos que permitió a más de 300 mujeres con interés y habilidades en la ciberseguridad conocerse, generar contactos y demostrar sus capacidades.

CSIRT como motor de cooperación internacional

En el plano de la cooperación y vinculación con naciones y organismos internacionales especializados en materia de ciberseguridad, se avanzó en fomentar el intercambio de información y las buenas prácticas. En 2018, nos decidimos basar en modelos internacionales exitosos para implementarlos en Chile en forma rápida y eficaz, para ello se suscribieron los siguientes acuerdos con países e instituciones:

- Argentina (abril de 2018);
- Organización de Estados Americanos (OEA) (septiembre de 2018);
- España (octubre de 2018);
- Ecuador (junio de 2019);
- Israel (junio de 2019);
- Colombia (marzo de 2019);
- Reino Unido (septiembre de 2019) y
- Estonia (enero de 2020).

Producto del trabajo realizado desde 2018, Chile se posicionó como un país que ha avanzado notoriamente en ciberseguridad. En el Reporte Regional de Ciberseguridad 2020 (OEA-BID), el país mostró un importante avance en comparación con 2016, dando el paso desde la etapa formativa a la consolidada en varias de las dimensiones evaluadas. Por su parte, en la cuarta versión del Global

Cybersecurity Index de ITU, entregada en 2021, Chile subió nueve lugares a nivel mundial, llegando al puesto 74 y subió dos en términos del continente americano, ubicándose séptimo en la región.

CSIRT como motor de cooperación público-privado

Este plano es esencial en cualquier modelo exitoso de ciberseguridad. Por ello, contamos con importantes alianzas con todos los sectores estratégicos del país, hecho materializado en la suscripción de más de 70 convenios con organizaciones privadas, órganos autónomos, universidades y ONG. Con el fin de convencer al sector privado a atreverse a reportar los incidentes de ciberseguridad, a compartir información a través de la plataforma MISP y generar juntos, planes de concientización como avances en la materia.

CSIRT como motor legislativo

En el año 2018 se ingresó un proyecto de Ley de Delitos Informáticos -en tercer trámite constitucional- que propone derogar la Ley Nº 19.223 y modificar otros cuerpos legales con el objeto de proteger la integridad de los datos y la propiedad sobre sistemas informáticos, en conformidad con el Convenio Internacional de Ciberdelincuencia de Budapest, del cual Chile forma parte desde 2017. Se dejó listo para su pronto despacho al Congreso el proyecto de la Ley Marco de Ciberseguridad e Infraestructura Crítica de la Información que oficializa la Agencia Nacional de Ciberseguridad y busca regular al sector privado y proteger las infraestructuras críticas de la información del país.

Y en estos logros del CSIRT no puedo no agradecer a mis dos jefes de departamentos. Cristián Berrios, quien me ayudó a crearlo, definir sus líneas de operación, su portafolio de producto e incentivar la cultura de “atreverse a reportar” y “transparentar las cifras de ciberataques, vulnerabilidades explotadas y ciberdelitos”. Y a su vez, a Katherina Canales, quien ayudó a potenciar mucho más esta unidad, a desarrollar las iniciativas de concientización, a volver a posicionarnos entre los mejores CSIRT a nivel americano, a mejorar nuestras normativas, decretos y proyectos de ley, y a su vez, por ser el soporte y apoyo necesario cuando la criticada política calculista y partidaria trataba de romper los cimientos que estábamos tratando de construir en ciberseguridad una y otra vez. Muchas gracias a ambos por su compromiso, profesionalismo y amistad; sobre todo a ti Katherina, por tu lealtad incondicional, quien hoy también dejas el cargo de jefa de departamento CSIRT.

El CSIRT ya es una institución consolidada, seria, reconocida, valorada, muy técnica y profesional, haberla creado, haber convencido a las autoridades políticas de la importancia de esta institución, haberla potenciado y dejarla interconectada nacional e internacionalmente ha sido un verdadero honor, muy desafiante y agotador, pero a su vez, es muy satisfactorio ver hoy en qué nos hemos convertido durante estos casi cuatro años. Esperamos que en marzo de 2022, cuando asuma el nuevo(a) Director(a) del CSIRT pueda consolidar aún más a esta institución, desearle el mayor de los éxitos en su gestión y ojalá lo puedan ayudar a realizar cambios y avances que se necesitan,

esperando que sea una administración que avance sobre lo ya construido y que no cometa el error político inicial de partir todo desde cero nuevamente.

Pido mis más sinceras disculpas si en algo nos equivocamos, si nos faltó avanzar mucho más rápido en ciertos tópicos de la ciberseguridad o si algo no cubrimos de la mejor forma.

La gran diferencia que hay entre marzo del 2018 a la fecha es la consolidación de un ecosistema de ciberseguridad nacional con variados actores, como el Gobierno, FF.AA., empresas privadas consumidoras y prestadoras de variados servicios de ciberseguridad, universidades, institutos profesionales, sociedad civil, ONG, investigadores, emprendedores, etc., que han entendido que la mejor forma de avanzar en disminuir los riesgos de la ciberseguridad es cooperar, compartir información, declarar y hacer pública la información de ataques recibidos, interconectarnos y ser comunidad en pro de mantener un ciberespacio nacional libre, abierto, seguro y resiliente. Un honor haber sido parte de este proceso.

Muchas gracias, hasta siempre.

Afectuosamente.

Carlos Landeros
DIRECTOR CSIRT

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 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.

- José Ignacio Parra
- Juan Pablo Escobar
- Francisco Gutiérrez
- Felipe Muñoz
- Giovanni Díaz

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.11.15 11:40:20 -03'00'