Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

11-02-2022 | Año 4 | N°136

Boletín de Seguridad Cibernética

Semana del 4 al 10 de febrero de 2021

La semana en cifras

Hash

126

SHA

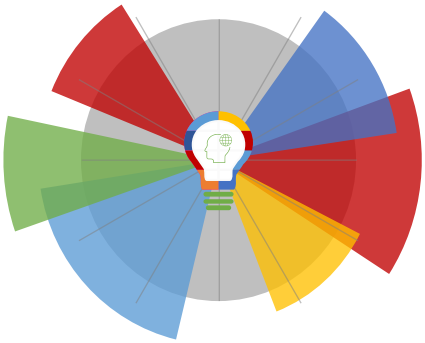
Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron

2

URL

Asociadas a sitios fraudulentos y campañas de phishing y malware.



Parches

63

para vulnerabilidades

Las mitigaciones son útiles en productos de Microsoft y Adobe.

IP

134

Informadas

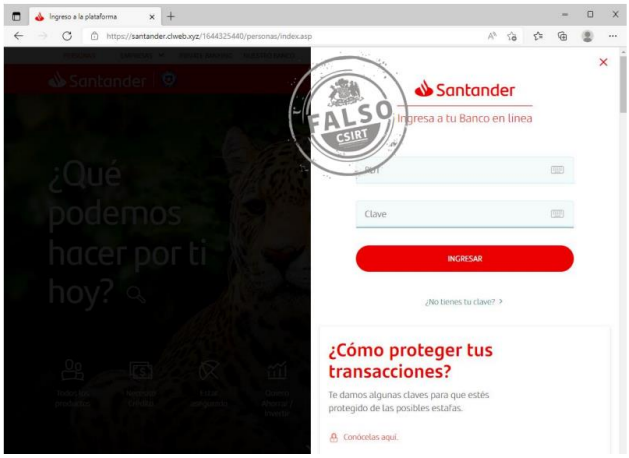
Listado de IP advertidas en múltiples campañas de phishing y de malware.

*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

Sitios fraudulentos



CSIRT alerta sitio web que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR22-01053-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de febrero de 2022
Última revisión	8 de febrero de 2022
Indicadores de compromiso	
URL sitio falso	
https://santander.clweb[.]xyz/1644325440/personas/index.asp	
IP	
[198.187.29.29]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01053-01/	
https://www.csirt.gob.cl/media/2022/02/8FFR22-01053-01.pdf	

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

Phishing

CSIRT advierte phishing con falsos puntos para canjear del Banco Itaú	
Alerta de seguridad cibernética	8FPH22-00470-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de febrero de 2022
Última revisión	8 de febrero de 2022
Indicadores de compromiso	
URL sitio falso	
https://itaupersonayempresacl.itauempresaspuntos[.]info/726a292db52f7f5/html/index.php	
IP	
[3.80.211.121]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00470-01/	
https://www.csirt.gob.cl/media/2022/02/8FPH22-00470-01.pdf	

Vulnerabilidades

CSIRT comparte vulnerabilidades informadas por Microsoft en su Update Tuesday Febrero 2022	
Alerta de seguridad cibernética	9VSA22-00575-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de febrero de 2022
Última revisión	9 de febrero de 2022

CVE

CVE-2022-23254	CVE-2022-22002	CVE-2022-22709
CVE-2022-21986	CVE-2022-22001	CVE-2022-21968
CVE-2022-21965	CVE-2022-22000	CVE-2022-21957
CVE-2022-23276	CVE-2022-21999	CVE-2022-21981
CVE-2022-23280	CVE-2022-21998	CVE-2022-21984
CVE-2022-23274	CVE-2022-21997	CVE-2022-22718
CVE-2022-23273	CVE-2022-21996	CVE-2022-21985
CVE-2022-23272	CVE-2022-21995	CVE-2022-22717
CVE-2022-23271	CVE-2022-21994	CVE-2022-22715
CVE-2022-23269	CVE-2022-21993	CVE-2022-22712
CVE-2022-23256	CVE-2022-21992	CVE-2022-21974
CVE-2022-23255	CVE-2022-21991	CVE-2022-21971
CVE-2022-23252	CVE-2022-21989	CVE-2022-21927
CVE-2022-22003	CVE-2022-21988	CVE-2022-21926
CVE-2022-22005	CVE-2022-21987	CVE-2022-21844
CVE-2022-22004	CVE-2022-22716	CVE-2022-22710

Fabricante

Microsoft

Productos afectados

HEVC Video Extensions
Microsoft Dynamics 365 (on-premises) version 9.0, version 8.2
Microsoft Teams Admin Center
Microsoft Teams for Android, for iOS
Microsoft SharePoint Foundation 2013 Service Pack 1
Microsoft SharePoint Server Subscription Edition
Microsoft SharePoint Server 2019
Microsoft SharePoint Enterprise Server 2016
Windows 10 Version 21H2 for x64-based Systems
Windows 10 Version 21H2 for ARM64-based Systems
Windows 10 Version 21H2 for 32-bit Systems
Windows 11 for ARM64-based Systems
Windows 11 for x64-based Systems
Windows Server, version 20H2 (Server Core Installation)
Windows 10 Version 20H2 for ARM64-based Systems
Windows 10 Version 20H2 for 32-bit Systems

Windows 10 Version 20H2 for x64-based Systems
Windows Server 2022 & 2022 Server Core installation
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 10 Version 1909 for ARM64-based Systems
Windows 10 Version 1909 for x64-based Systems
Windows 10 Version 1909 for 32-bit Systems
Windows Server 2019 & 2019 Server Core installation
Windows 10 Version 1809 for ARM64-based Systems
Windows 10 Version 1809 for x64-based Systems
Windows 10 Version 1809 for 32-bit Systems
Windows Server 2016 & 2016 Server Core installation
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1607 for 32-bit Systems
Windows Server 2012 R2 (Server Core installation)
Windows Server 2012 R2
Windows Server 2012 (Server Core installation)
Windows Server 2012
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows RT 8.1
Windows 8.1 for x64-based systems
Windows 8.1 for 32-bit systems
Windows 7 for x64-based Systems Service Pack 1
Windows 7 for 32-bit Systems Service Pack 1
Windows 10 for x64-based Systems
Windows 10 for 32-bit Systems
Windows Server 2022 Azure Edition Core Hotpatch
.NET 6.0
.NET 5.0
Visual Studio 2019 for Mac version 8.10
Microsoft Visual Studio 2022 version 17.0
Microsoft Visual Studio 2019 version 16.11 (includes 16.0 – 16.10)
Microsoft Visual Studio 2019 version 16.9 (includes 16.0 – 16.8)
Microsoft SharePoint Enterprise Server 2013 Service Pack 1
Microsoft Office LTSC 2021 for 32-bit editions
Microsoft Office LTSC 2021 for 64-bit editions
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft 365 Apps for Enterprise for 32-bit Systems

Microsoft Office 2019 for 64-bit editions
Microsoft Office 2019 for 32-bit editions
Visual Studio Code
Microsoft Office 2013 Service Pack 1 (64-bit editions)
Microsoft Office 2013 Service Pack 1 (32-bit editions)
Microsoft Office 2013 RT Service Pack 1
Microsoft Office 2016 (64-bit edition)
Microsoft Office 2016 (32-bit edition)
Microsoft Office LTSC for Mac 2021
Microsoft Office 2019 for Mac
Microsoft Office 2013 Click-to-Run (C2R) for 64-bit editions
Microsoft Office 2013 Click-to-Run (C2R) for 32-bit editions
VP9 Video Extensions
Microsoft Office Web Apps Server 2013 Service Pack 1
Microsoft Excel 2013 Service Pack 1 (64-bit editions)
Microsoft Excel 2013 Service Pack 1 (32-bit editions)
Microsoft Excel 2013 RT Service Pack 1
Microsoft Excel 2016 (64-bit edition)
Microsoft Excel 2016 (32-bit edition)
Microsoft Office Online Server
PowerBI-client JS SDK
OneDrive for Android
Azure Data Explorer
Microsoft Dynamics GP
SQL Server 2019 for Linux Containers
Microsoft Outlook 2016 for Mac
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00575-01/
https://www.csirt.gob.cl/media/2022/02/9VSA22-00575-01.pdf

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

CSIRT alerta de nuevas vulnerabilidades en productos de Adobe		
Alerta de seguridad cibernética	9VSA21-00576-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	10 de febrero de 2022	
Última revisión	10 de febrero de 2022	
CVE		
CVE-2022-23203	CVE-2022-23192	CVE-2022-23197
CVE-2022-23186	CVE-2022-23193	CVE-2022-23198
CVE-2022-23189	CVE-2022-23194	CVE-2022-23199
CVE-2022-23190	CVE-2022-23195	CVE-2022-23188
CVE-2022-23191	CVE-2022-23196	CVE-2022-23200
Fabricante		
Adobe		
Productos afectados		
Photoshop 2021 22.5.4 y anteriores. Para Windows y macOS. Photoshop 2022 23.1 y anteriores. Para Windows y macOS. Illustrator 2022 26.0.2 y anteriores. Para Windows y macOS. Illustrator 2021 25.4.3 y anteriores. Para Windows y macOS. Adobe After Effects: 18.0 a 22.1.1		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00576-01/		
https://www.csirt.gob.cl/media/2022/02/9VSA22-00576-01.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
0a4ad68bbf810d760ba140ecc845b008492cb65cc37be91c139edd344451647e	RTF/Abnormal	2CMV22-00271-01
a63dba13a566923ccc781e6aef5cabedd64c7707a5907889a36f095ee3279df3	FSA/RISK_HIGH	2CMV22-00271-01
9d5330a6dec7db52785a19c5c0e2120bb8cb8fd91304b86157907005df8b4def	FSA/RISK_HIGH	2CMV22-00271-01
36137293cb5983e04e490d81e83f7a44acd2d26ac200f2131a5e9bf48c121954	MSIL/AgentTesla	2CMV22-00271-01
67d0a8c8afbf98ee137a930d55c747ba04d7a6b65faf3d2cd852a1d04ab44739	W32/Injector	2CMV22-00271-01
bdd6cd92ccb63c3f153416135dde40feb589c5f6194e21dabd091e90770f996c	MSIL/Kryptik	2CMV22-00271-01
391720ecf31772662bea40f54d2d6b5d0c2f2aff2717ebb6cca1d2961b4065f8	PossibleThreat	2CMV22-00271-01
748691b8c66818cf40ca7fba10c7a4c9d0fb0f71e6b61c231e267daa6a252d56	MSIL/Kryptik	2CMV22-00271-01
f6f0c0f4b3c1264305cf52532620c590384da93abc82ef005bb8a45c41b6711a	MSIL/Kryptik	2CMV22-00271-01
a98d9f66b3340e4a6d1c08ffee85a6e44ae666c5c1665fb0334b1026d0ec1200	PossibleThreat	2CMV22-00271-01
6d9435008371e7ad62d708c26f6f23b04167ffc3835ddfd5a610943a0f875fe5	W32/Injector	2CMV22-00271-01
1759f22d27c17ab6cfe1b56da876dcc135f0819e7333f39f0c1962399c91602a	HTML/Phishing	2CMV22-00271-01
5cf33071ac6ed04fb750080f28e65d3416f39216c0f68758585d679b0d0b51bc	MSIL/Kryptik	2CMV22-00271-01
b84c0e38f1a3beba4c500955dc98faf0b8484e879ddd6930b95f82da250cf78f	VBA/Dloader	2CMV22-00271-01
53d8cbc8cbd0c1a591d2ee257b47dd0811ead2447ded9b983cc5895f2b4c198f	MSIL/Kryptik	2CMV22-00271-01
f91e8419595b8bbdb66a9887e6b42ce72c69f2e7189f9d7015f3931dbea368c1	RTF/Abnormal	2CMV22-00271-01

24dbb253ec491a1aa8a809bce303afb4a31090d687331677787846fb2c4c137c	Malware_Generic	2CMV22-00271-01
6d3162f26448bf2e2e642c54aac2e4a6705bb3fe58c6c809ea742fe0cc99ddd6	RTF/Abnormal	2CMV22-00271-01
8ad48dacb70de86bca0165c8c71b2352558fe2fc12e443e07c7491cad7c41ebb	MSIL/Kryptik	2CMV22-00271-01
4c5c6b851042b92111344e43f879e83dd0208a21ea5a10b3dad4ff438a297091	MSIL/Kryptik	2CMV22-00271-01
f3eda43df12c8676f3982dd9605fdb60f47fa79d35ef80ed81fc85cd75b7d994	MSIL/Kryptik	2CMV22-00271-01
4323a9daff5c3ee3953b2476942eccff3760d3c8baa4ba44f0e43be0783e4232	MSIL/Kryptik	2CMV22-00271-01
8747ba44fa2edeea9224a567812ddee34c2479c43564b5f1e96fdffd01bfe9ce	MSIL/Kryptik	2CMV22-00271-01
54ae84338a651c275d0d7b96792eec4e742c71fbeee5ae23dee06030ed0665b9	MSIL/Kryptik	2CMV22-00271-01
0ce8385ffe600a91fa0f6152ea403f699662f338276e06266632a10e1df1b4f0	MSIL/Kryptik	2CMV22-00271-01
4cf4f66d06a13bc533d617a63b4adabeae353289c08bb9f9e8a43b2f2eceabea	HTML/Phishing	2CMV22-00271-01
bd93529d6d6a1222d28a5fd4d179dfa24bdf66e5d04e0ea5e9f670e4149e7e6e	MSExcel/CVE_2017_11882	2CMV22-00271-01
675da2c4e21e1573ff242ff6e01e3ff4ac2a6e71388a5308d9fb24252786cba4	FSA/RISK_HIGH	2CMV22-00271-01
c2c6425e03a35aa313972c8d9a9c96bb7d823e2f8cd4eb6def68090571b6d9bd	MSIL/Kryptik	2CMV22-00271-01
0c0bff4acceaf8498633616e84b6af21dadbc81e95ddea70decfeab123bd99d4	MSIL/Kryptik	2CMV22-00271-01
2f80c6cab5bf6ad5ca48de8117b348d2803e637f4641b31d784702ad721ca3d7	HTML/Phishing	2CMV22-00271-01
a1abe95e521e6d449ac5c109c927bd22034ce874ea5e6247f1dd4afdb80a351a	MSExcel/CVE_2017_11882	2CMV22-00271-01
e2fc1583476b718d57b1cbad65c6e210beb4a9397a2cc50ddd96d9ced77aa482	HTML/PhishingAgent	2CMV22-00271-01
3f4de7f20adea312c6144440a18a8d4e0e180b29fae203383138483b02f2dffa	MSIL/Kryptik	2CMV22-00271-01
2cde32d868432213e7e5d3d97dec597850761694a1f97a25ee305fe7151e3299	MSIL/Kryptik	2CMV22-00271-01
8268e28ddef3e7b332266c8d8a787ec3dcc7065b27978d826c2df82c7bf9f7a6	Riskware/POC	2CMV22-00271-01
4a90f3650442cd5b2241bb4733c8550dc0beb2166ef35b5ae	MSIL/Kryptik	2CMV22-00271-01

c71c437b6db8a20		
48812117e231d3a3b536b8f5c21a83882ab00cb95038cd973b44e42a349cffc9	MSIL/Kryptik	2CMV22-00271-01
0b0174fd4e35d8aecfb199f7789f91264521fc6dfefc8de365667dfeccc5c311	MSIL/Kryptik	2CMV22-00271-01
ab445e04707a8c688e62fb06a5ffcffe421335892609b2678edaa2e55f300d32	MSIL/Kryptik	2CMV22-00271-01
4d8e3b71ce2411fb1bfe0525c83984467a0daa69f1fa6545980c623f1ac5ba59	HTML/PhishingAgent	2CMV22-00271-01
03e0f4c14b272a66106972f19d4654382372899c3082fa5d7c3ce919ae80a3f7	MSIL/Kryptik	2CMV22-00271-01
8d148f3d372f59e0d5f597ec952b1f0bead06faa543db902c5fc86924dedbdaa	MSIL/Kryptik	2CMV22-00271-01
2f3b1af496bb6d0acd3539202877161f5cb94997b1db7a24d804c1cab4465a24	MSIL/Kryptik	2CMV22-00271-01
13ea9c9335082ac58e9bacb7d96b66dc4c2eaecd4c5d533432170f591109501c	MSIL/Kryptik	2CMV22-00271-01
eb9fd135850ac65897c264abfe01dbddb43662b6ebcc5c792cdfd0cfee9d373e	MSIL/Kryptik	2CMV22-00271-01
9aba85bea4835cd9e4fc350119e8477f9a4e555c7e298bfb9cce7bcc2618ace3	Malicious_Behavior	2CMV22-00271-01
83d516cb902497732edf822f972467d58b58cef9958b5b96e92b326a37cf984c	HTML/Phishing	2CMV22-00271-01
80201005b89d1caa5378e965348310ccd6d9ac92dad994d30fcbffa18ad13762	FSA/RISK_HIGH	2CMV22-00271-01
614e9bd49c8e4fb32c65acc5f4099a099cf90e4cbe4c073d84063e392f5b4367	HTML/PhishingAgent	2CMV22-00271-01
ebe6031b6ed934118df5e0e90e9129f3bf5ab2d3dc42afba5f400685d40dd8b1	MSIL/CoinMiner	2CMV22-00271-01
023d98c23927c2004923ce5b70285fa60d76fa2693673ea71e9ca3bde50a42fa	FSA/RISK_HIGH	2CMV22-00271-01
e5bdf5fd4ed0db5dc440144ebbaea7e79d4fdc65678a68a36416e8ab88d76aee	FSA/RISK_HIGH	2CMV22-00271-01
83ffe578d39bc85893606143565e56ebf26729c124d56d7fbb69c66cb597c2ec	MSIL/CoinMiner	2CMV22-00271-01
41134d8905d47f84971085a6093a85bf6563b93865519d4c5660950941861665	PossibleThreat	2CMV22-00271-01
d505037a15e00b8173156842186f791dbc39ca2ad775448a65a300ed65407ddc	FSA/RISK_HIGH	2CMV22-00271-01
77d225ede649e70b6456974ee1b17bcf462ba7f756e188fc934dd80312c78492	FSA/RISK_HIGH	2CMV22-00271-01
ada818cf9ea2a109125a562d17278476a1e1c890a31cbf1a4	MSIL/CoinMiner	2CMV22-00271-01

180462a91fbf378		
cf94f3e3892883755cf365af88614406befb21b14353bac5172ef9a7e174d853	FSA/RISK_HIGH	2CMV22-00271-01
a89c44ffdb1abe3d533edd368d87786e6309ebf56154d33336c94790610cc058	FSA/RISK_HIGH	2CMV22-00271-01
03a01120ce941951e563115c7e66d73b045248dffa66b7ff70aa00a0780b9872	HTML/Phishing	2CMV22-00271-01
acd6eb3ec81eb9b1fc30e58453696761faab712d8467ec004672b4088c4c507d	FSA/RISK_HIGH	2CMV22-00271-01
8cb512b687278ba571f4bb80f84949ac7d957de043fc2029c569127ea6825b30	MSOffice/Scam	2CMV22-00272-01
b64988fe8d0aa76483014e3af670e7b5f0529341a339948967d8a5ba0a44fec3	MSExcel/Phishing	2CMV22-00272-01
6b3e0716dbf2dfb8673b91813c2636588e27359313f1719adafb3e638d636a83	FSA/RISK_HIGH	2CMV22-00272-01
8bf1a6585351707c17fd18446c873d1f9238e15827ab8c237dd4206520f070a0	RTF/Abnormal	2CMV22-00272-01
f241927d24963ce87262abf70c073ac9f804cc2107bd632d39728d931a0a1688	Malicious_Behavior	2CMV22-00272-01
d8ca20b521c655d63e9d5dc692922adc4e8e097f08c7eb6b2b65f8947aa2306e	Malicious_Behavior	2CMV22-00272-01
ace4e240f1ca6a6864a2f3266c482f73df2832d05414664eed4afaf788167af6	VBA/Logan	2CMV22-00272-01
c428fe9738c914d47ff89c0b641d9a40d5ff096316fa8f7636c6d8456da57c70	Malware_Generic	2CMV22-00272-01
82eb15705eb4787fdf0cfd3b4fd90098904ee61ac11fe6e722b93f44c26d1563	W32/Malicious_Behavior	2CMV22-00272-01
4ad7cdcff5d21c09bc0ac8f4a9015966b97fac39c2fb40e756f052cf4c1360b9	MSIL/Kryptik	2CMV22-00272-01
1f741efaaae54d6e30a488150b53ddde2343a3581bbcda0672c367b16facc15f	FSA/RISK_HIGH	2CMV22-00272-01
8136b47cb2f2e1fecbe556e7631548969c3dbd659a08918fc83079c9c8829a0a	Malicious_Behavior	2CMV22-00272-01
44ddcb794dd0b7c2cc6d07fe397e6c2afa4c63d72d772364d6bbb14db7ec1578	W32/Malicious_Behavior	2CMV22-00272-01
2d006d53fa034eb4fc84314bcfaac158060c99a6b8254231bc4d6595be8239b1	Malicious_Behavior	2CMV22-00272-01
73e13cce94f79361f590bc566a28b0434685b05419685da43e0163a05132a5d3	RTF/Abnormal	2CMV22-00272-01
85eca9e674589c7aca68319bdf525c7fd861be4885d4681e2985c768d9ce1c72	FSA/RISK_HIGH	2CMV22-00272-01
c0261b4f10d5fa5998f9837a0aeaf9018b27e083be0d3b56e	W32/Malicious_Beha	2CMV22-00272-01

a601ac551dc1a6b	vior	
59b2b057daaffad480af92e5656e3ce7c3f8db5e572b525bca87e02f7d31c53f	HTML/Phishing	2CMV22-00272-01
fe9a6d533996cd764247e0c2b28f63349ce93d526a630b8f998be6867f005886	W32/Agent	2CMV22-00272-01
389d2fabd37ed450263502fc8caaa1b64fc001cab76f505c3217de687944f760	MSIL/Kryptik	2CMV22-00272-01
bf6d3af1779c30c61dc8522a814b655a613d34256a6506f8e22a5c3d80d38538	Malicious_Behavior	2CMV22-00272-01
5575946e2e5cfa95bc31c0cfad4235e997230534135733b339fadb1c7dbeae85	FSA/RISK_HIGH	2CMV22-00272-01
f3896ceed60e07e3d048afa5ebebab6798098bebabcc49c55253c2e9a54a7bb8	HTML/Phish	2CMV22-00272-01
725615e061efdfcebbd4c21b927cc3561698d87743286ef84d9e90bcaf551028	PossibleThreat	2CMV22-00272-01
1299c1168e4958567314cc8109e37b20c5511002770554988a6fa25cb8e5aa4f	FSA/RISK_HIGH	2CMV22-00272-01
2e49fbb3cc2392ae127f91587a2a08de041092f2e718a2b47ba3737ed8086b3d	RTF/Abnormal	2CMV22-00272-01
1c354ebaa77f412ba48823e050a4ab10680f5b50386ec61022f9b10f6c47bec6	MSIL/Kryptik	2CMV22-00272-01
921756beccce3e982552419c17d3d8420bf35ac9bb2e10be578e26973d2704ff	MSIL/Kryptik	2CMV22-00272-01
c47ae5b202cdbc7ff50409ff1a09e7e5123f587ae18a1cdd4509b26aed621f4d	HTML/PhishingAgent	2CMV22-00272-01
071f6d7243eebcd858b1e4a3698c94c093f3344893469bf7690810377ca0877a	HTML/Phishing	2CMV22-00272-01
cc4429d5fce4efc3163fa0670555e27b38c33153bae6c51613f91daa15e2febc	MSExcel/CVE_2017_11882	2CMV22-00272-01
2e80e34afab07f4266287c972d7d2d80e702d7fbf82db4eed34f9012d480bad7	HTML/Agent	2CMV22-00272-01
7e89c45be86a80a5d51ffe87e69896ee6058773c15d040b200bb8989a7489eb2	VBA/Logan	2CMV22-00272-01
59fae225be2e4027df7d2e2ee257e01fc412ca94ff04dfe2375bab8dabc2c342	VBA/Logan	2CMV22-00272-01

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
185.222.58.40	RootLayer Web Services Ltd.	2CMV22-00271-01
185.222.57.71	RootLayer Web Services Ltd.	2CMV22-00271-01
45.10.152.173	DediPath	2CMV22-00271-01
23.237.68.50	Cogent Communications	2CMV22-00271-01
159.203.118.205	DigitalOcean	2CMV22-00271-01
185.222.58.57	RootLayer Web Services Ltd.	2CMV22-00271-01
45.137.22.115	RootLayer Web Services Ltd.	2CMV22-00271-01
195.33.210.155	Tellcom Iletisim Hizmetleri A.s.	2CMV22-00271-01
142.93.36.51	DigitalOcean	2CMV22-00271-01
2.56.57.212	Serverion LLC	2CMV22-00271-01
103.133.109.178	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP	2CMV22-00271-01
66.226.72.146	Codero-DFW	2CMV22-00271-01
138.68.26.118	DigitalOcean	2CMV22-00271-01
37.0.8.214	Delis LLC	2CMV22-00271-01
62.197.136.254	Des Capital B.V.	2CMV22-00271-01
185.222.58.55	RootLayer Web Services Ltd.	2CMV22-00271-01
209.85.166.193	Google LLC	2CMV22-00271-01
172.107.237.60	Psychz Networks	2CMV22-00271-01
85.202.169.54	Des Capital B.V.	2CMV22-00271-01
185.222.57.153	RootLayer Web Services Ltd.	2CMV22-00271-01
165.227.6.48	DigitalOcean	2CMV22-00271-01
103.133.107.188	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP	2CMV22-00271-01
185.222.57.188	RootLayer Web Services Ltd.	2CMV22-00271-01
84.246.209.97	Axarnet Comunicaciones, S.l.	2CMV22-00271-01
212.192.241.97	Delis LLC	2CMV22-00271-01
172.245.25.189	ColoCrossing	2CMV22-00271-01

185.222.57.183	RootLayer Web Services Ltd.	2CMV22-00271-01
185.222.57.190	RootLayer Web Services Ltd.	2CMV22-00271-01
183.181.88.14	Xserver Inc.	2CMV22-00271-01
2.56.59.36	Serverion LLC	2CMV22-00271-01
185.222.58.47	RootLayer Web Services Ltd.	2CMV22-00271-01
92.204.71.143	Host Europe GmbH	2CMV22-00272-01
138.36.19.12	Internap Holding LLC	2CMV22-00272-01
103.153.204.47	NPO Yutopianet	2CMV22-00272-01
183.181.88.14	Xserver Inc.	2CMV22-00272-01
180.214.236.86	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP	2CMV22-00272-01
103.133.109.178	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP	2CMV22-00272-01
103.133.107.188	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP	2CMV22-00272-01
167.99.111.204	DigitalOcean, LLC	2CMV22-00272-01
165.227.6.48	DigitalOcean, LLC	2CMV22-00272-01
159.203.118.205	DigitalOcean, LLC	2CMV22-00272-01
142.93.36.51	DigitalOcean, LLC	2CMV22-00272-01
138.68.40.100	DigitalOcean, LLC	2CMV22-00272-01
138.68.26.118	DigitalOcean, LLC	2CMV22-00272-01
194.233.89.206	Contabo Asia Private Limited	2CMV22-00272-01
200.35.157.95	Gtd Internet S.A.	2CMV22-00272-01
200.14.114.11	Gtd Internet S.A.	2CMV22-00272-01
15.235.35.39	OVH SAS	2CMV22-00272-01
52.49.14.50	Amazon.com, Inc.	2CMV22-00272-01
23.237.68.50	Cogent Communications	2CMV22-00272-01
180.179.213.26	Netmagic Datacenter Mumbai	2CMV22-00272-01
66.226.72.146	Codero	2CMV22-00272-01
66.23.225.60	Interserver, Inc	2CMV22-00272-01
185.50.45.69	Grupo Loading Systems, S.L.	2CMV22-00272-01
212.111.96.64	Internet Xpress	2CMV22-00272-01
185.17.151.222	IOMART CLOUD SERVICES LIMITED	2CMV22-00272-01
2.57.238.26	SD4 SAS	2CMV22-00272-01
185.104.188.31	Jose Poyato Prieto	2CMV22-00272-01

37.0.8.214	Delis LLC	2CMV22-00272-01
37.0.11.89	Delis LLC	2CMV22-00272-01
212.193.30.52	Delis LLC	2CMV22-00272-01
212.192.241.97	Delis LLC	2CMV22-00272-01
194.99.46.235	Delis LLC	2CMV22-00272-01
189.193.226.2	Mega Cable, S.A. de C.V.	2CMV22-00272-01
45.227.162.89	Allytech S.A.	2CMV22-00272-01
153.128.188.40	NTT Communications Corporation	2CMV22-00272-01
153.128.188.38	NTT Communications Corporation	2CMV22-00272-01
143.90.14.65	SoftBank Corp.	2CMV22-00272-01
143.90.14.6	SoftBank Corp.	2CMV22-00272-01
143.90.14.5	SoftBank Corp.	2CMV22-00272-01
143.90.14.4	SoftBank Corp.	2CMV22-00272-01
58.137.249.55	CS LOXINFO PUBLIC COMPANY LIMITED	2CMV22-00272-01
203.146.58.25	CS LOXINFO PUBLIC COMPANY LIMITED	2CMV22-00272-01
203.146.237.187	CS LOXINFO PUBLIC COMPANY LIMITED	2CMV22-00272-01
221.163.187.53	Korea Telecom	2CMV22-00272-01
84.246.209.97	AXARNET COMUNICACIONES, S.L.	2CMV22-00272-01
207.180.206.103	Contabo GmbH	2CMV22-00272-01
45.137.22.115	RootLayer Web Services Ltd.	2CMV22-00272-01
185.222.58.57	RootLayer Web Services Ltd.	2CMV22-00272-01
185.222.58.55	RootLayer Web Services Ltd.	2CMV22-00272-01
185.222.58.47	RootLayer Web Services Ltd.	2CMV22-00272-01
185.222.58.40	RootLayer Web Services Ltd.	2CMV22-00272-01
185.222.57.71	RootLayer Web Services Ltd.	2CMV22-00272-01
185.222.57.190	RootLayer Web Services Ltd.	2CMV22-00272-01
185.222.57.188	RootLayer Web Services Ltd.	2CMV22-00272-01
185.222.57.183	RootLayer Web Services Ltd.	2CMV22-00272-01
185.222.57.153	RootLayer Web Services Ltd.	2CMV22-00272-01
103.28.13.251	PT Qwords Company International	2CMV22-00272-01
45.79.51.124	Linode, LLC	2CMV22-00272-01
103.3.61.8	Linode, LLC	2CMV22-00272-01

200.49.140.84	Telecom Argentina S.A.	2CMV22-00272-01
157.7.231.33	GMO Internet,Inc	2CMV22-00272-01
109.111.252.23	Drustvo za telekomunikacije	2CMV22-00272-01
112.199.97.221	Eastern Telecoms Phils., Inc.	2CMV22-00272-01
85.202.169.54	Des Capital B.V.	2CMV22-00272-01
85.202.169.22	Des Capital B.V.	2CMV22-00272-01
85.202.169.138	Des Capital B.V.	2CMV22-00272-01
62.197.136.4	Des Capital B.V.	2CMV22-00272-01
62.197.136.254	Des Capital B.V.	2CMV22-00272-01

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
AWB-SHIPMENT#5829571263.HTML	2CMV22-00271-01
BANK SLIP.zip	2CMV22-00271-01
BL COPY, COMMERCIAL INVOICE, PACKING LIST.r00	2CMV22-00271-01
BL NO 1KT331459.rar	2CMV22-00271-01
Confirmation of Order_PO EM41170402.img.rar	2CMV22-00271-01
credito.exe	2CMV22-00271-01
Data Sheet and Drawings.zip	2CMV22-00271-01
DECOR RFQ936796654.doc	2CMV22-00271-01
DEPARTAMENTO INTERNACIONAL DE MOLOTERIA..docx	2CMV22-00271-01
DHL PARCEL NODL7593462.xlsx	2CMV22-00271-01
DOC.r15	2CMV22-00271-01
documents.xlsx	2CMV22-00271-01
ETD - Dhl shipping invoice Bill of lading.htm	2CMV22-00271-01
ETD - Shipping bill of lading.htm	2CMV22-00271-01
FedEx Express AWB_Invoice#5674.cab	2CMV22-00271-01
informe_410784.xls	2CMV22-00271-01
INV28159. doc.iso	2CMV22-00271-01
Invoice 16-36-55.zip	2CMV22-00271-01

Invoice request.zip	2CMV22-00271-01
msg14987.pif	2CMV22-00271-01
NEW REQUIREMENTS 2022937373.rar	2CMV22-00271-01
Orden de compra..zip	2CMV22-00271-01
orden de compra.zip	2CMV22-00271-01
ORDER 07022022.zip	2CMV22-00271-01
Order Datasheet & Specifications.xlsx	2CMV22-00271-01
order request 2.7.22.gz	2CMV22-00271-01
Packing list.zip	2CMV22-00271-01
paymemt.ace	2CMV22-00271-01
payment details.zip	2CMV22-00271-01
pedido.zip	2CMV22-00271-01
PO - 138 - New Order MIB 9 MIB.zip	2CMV22-00271-01
PO#4500550329.zip	2CMV22-00271-01
PO(47581).r00	2CMV22-00271-01
Proposal_xls.htm	2CMV22-00271-01
informe-315.xls	2CMV22-00272-01
cotizacin.zip	2CMV22-00272-01
Lista_81280523220.xls	2CMV22-00272-01
CHINESE REOPENS FOR BUSINESS MEMO.doc	2CMV22-00272-01
purchase order..rar	2CMV22-00272-01
documento_08022022.xlsm	2CMV22-00272-01
NEW ORDER (Order#-01172320202.zip	2CMV22-00272-01
pedido de imÃ¡genes del producto.exe.xz	2CMV22-00272-01
IHARA RFQ_20983764_pdf.arj	2CMV22-00272-01
PR001N220151963.7z	2CMV22-00272-01
Revised PI.r15	2CMV22-00272-01
SOA_Balance_Paymen.doc	2CMV22-00272-01
INVOICE #7833.r17	2CMV22-00272-01
Invoice.doc	2CMV22-00272-01
DHL AWB130501923096PDF.LZH	2CMV22-00272-01
FedEx Express Commercial Invoice_Packing\x09List.cab	2CMV22-00272-01
PAYMENT.HTML	2CMV22-00272-01
creditos.exe	2CMV22-00272-01

nueva cotizaciÃ³n y confirmaciÃ³n de los productos adjuntos.pdf.uu	2CMV22-00272-01
ETD - shipping invoice documents.rar	2CMV22-00272-01
remittance advice.r17	2CMV22-00272-01
AWB _8120260724.html	2CMV22-00272-01
SHIPPING BILL.zip	2CMV22-00272-01
scan 2022-36S.doc	2CMV22-00272-01
Pago-0173411_____.gz	2CMV22-00272-01
Payment.pdf._____.gz	2CMV22-00272-01
0100006319_202103.htm	2CMV22-00272-01
wire transfer slip.xlsx	2CMV22-00272-01
27099788_20220118152009.docx	2CMV22-00272-01
RIE 61353.xls	2CMV22-00272-01
938_69.xls	2CMV22-00272-01
detalles_4302619279.xls	2CMV22-00272-01
adjunto_086.xlsm	2CMV22-00272-01
099891916017243849175.xls	2CMV22-00272-01
Info 08022022.xls	2CMV22-00272-01
sin ttulo-07022022.xlsm	2CMV22-00272-01
paquete_87602.xlsm	2CMV22-00272-01
x-95940.xls	2CMV22-00272-01
Lista-08022022.xls	2CMV22-00272-01
??-efischerg VoiceMailT-new.html	2CMV22-00272-01
Mensaje-87.xls	2CMV22-00272-01
detalles_5199492.xls	2CMV22-00272-01
Documentos 10566353.xls	2CMV22-00272-01
Doc-09.xlsm	2CMV22-00272-01
97HZA_789183.xlsm	2CMV22-00272-01
x-4206.xlsm	2CMV22-00272-01
documento 7278904912.xlsm	2CMV22-00272-01
paquete 19296432.xlsm	2CMV22-00272-01
Info_527662803483.xlsm	2CMV22-00272-01
DOC-27951531638.xlsm	2CMV22-00272-01
adjunto_547417461.xlsm	2CMV22-00272-01
Aviso 13021577.xlsm	2CMV22-00272-01

ESCANEAR-0802.xlsm	2CMV22-00272-01
Archivo-08022022.xlsm	2CMV22-00272-01
838-04807553.xls	2CMV22-00272-01
documentacin_580102.xls	2CMV22-00272-01
DETALLES_0802.xls	2CMV22-00272-01
detalles_08022022.xls	2CMV22-00272-01
Info_0802.xlsm	2CMV22-00272-01
Aviso-0802.xls	2CMV22-00272-01
49 33466658.xls	2CMV22-00272-01
Datos-015979.xls	2CMV22-00272-01
Doc 08022022.xls	2CMV22-00272-01
documentacin_5121963.xlsm	2CMV22-00272-01
0444-6432.xls	2CMV22-00272-01
bObk_79.xls	2CMV22-00272-01
lista_774395.xls	2CMV22-00272-01
DETALLES 2667308.xlsm	2CMV22-00272-01
informe 324.xlsm	2CMV22-00272-01
informe 383936932.xlsm	2CMV22-00272-01
documento_10880.xlsm	2CMV22-00272-01
Aviso_6345252.xlsm	2CMV22-00272-01
O-0702.xlsm	2CMV22-00272-01
DOC_61.xlsm	2CMV22-00272-01
paquete_08022022.xls	2CMV22-00272-01
factura bancaria_7654.BZ2	2CMV22-00272-01
informe 0702.xlsm	2CMV22-00272-01
TNT Shipping Documents PDF.zip	2CMV22-00272-01

Actualidad

Día Internacional de la Internet Segura: Ciberconsejos de navegación

Cada 8 de febrero se celebra el Día Internacional de Internet Segura, una iniciativa que busca promover el uso seguro, respetuoso y responsable de las tecnologías digitales. El CSIRT de Gobierno junto a Entel decidieron entregar una serie de recomendaciones para, precisamente, navegar en internet de forma más segura. Encuentra la información completa aquí: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-una-navegacion-segura/.

Ciberconsejos para un teletrabajo más seguro

Esta semana en Ciberconsejos te entregamos recomendaciones para un teletrabajo más seguro. Así, en las imágenes encontrarán consejos útiles tanto para trabajadores como para sus organizaciones. El enlace para compartir: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-un-teletrabajo-mas-seguro/.

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

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.

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.02.11 17:05:44 -03'00'

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