Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

16-04-2021 | Año 3 | N°93

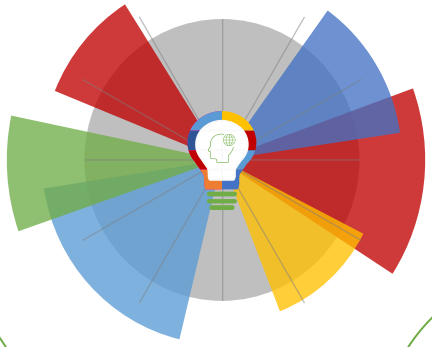
Boletín de Seguridad Cibernética

Semana del 09 al 15 de abril de 2021

La semana en cifras

Hash
68
SHA
Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron
15
URL
Asociadas a sitios fraudulentos y campañas de phishing



Parches
210
para vulnerabilidades
Las mitigaciones son útiles para productos de VMware, Google, Cisco, WhatsApp, SAP, Microsoft y Siemens

IP
67
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 sitio web

CSIRT alerta de campaña de malware que suplanta al SII	
Alerta de seguridad cibernética	2CMV21-00166-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de abril de 2021
Última revisión	12 de abril de 2021
Indicadores de compromiso	
SHA256	
6ACEC7C336E7E994151E44EB97E245122C6D151FB407313C41A0630E1AC6B8CD 68B1DE0F0C8637AFC19DE4BD5883D04189F58367FD4317DAA1B4691CFA942408 898329D8A1ACE6AA806566A83E8404252B2E4B65056D3D990018EFB856B223CF 237D1BCA6E056DF5BB16A1216A434634109478F882D3B1D58344C801D184F95D 5876B84E7335B307CC94078BAB1A7BBFFEFB3A4A23160E9130751E3BFD58220F	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv21-00166-01/	

Imagen del mensaje

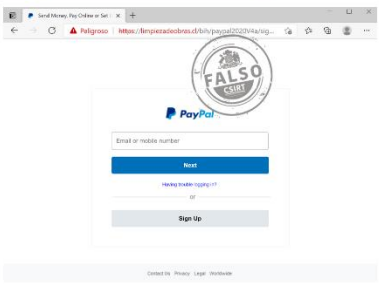
CSIRT alerta por campaña de phishing con falsa factura de Conalum	
Alerta de seguridad cibernética	2CMV21-00168-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de abril de 2021
Última revisión	14 de abril de 2021
Indicadores de compromiso	
SHA256	
C0C93676026C1EF4C660DC3D4F544CAC990B9AF3C556D7648A7E08FDFE38B209 5281533C78892F2B571668EF9C770CE9C04EE249397040DB9B5975ED47601474	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv21-00168-01/	

Imagen del mensaje

CSIRT alerta por campaña de phishing con falsa factura de Masterduct	
Alerta de seguridad cibernética	2CMV21-00169-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de abril de 2021
Última revisión	14 de abril de 2021
Indicadores de compromiso	
SHA256	
c0174ee8d8258280068d157fda171d1d4b67515183a041244127d9dd476b81b3 7ec93defc73ebbf09f244d2b393d475aa34a989d2bf58e9503b43326ad0c9345	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv21-00169-01/	

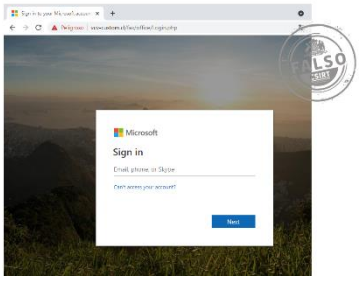
Sitios fraudulentos

Imagen del sitio



CSIRT alerta por web fraudulenta que suplanta a Paypal	
Alerta de seguridad cibernética	8FFR21-00926-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de abril de 2021
Última revisión	9 de abril de 2021
Indicadores de compromiso	
URL sitio falso	
https://limpiezadeobras[.]cl/bih/paypal2020V4a/signin.php	
IP	
[131.72.236.184]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00926-01/	
https://www.csirt.gob.cl/media/2021/04/8FFR21-00926-01.pdf	

Imagen del sitio



CSIRT alerta por web fraudulenta que suplanta a Microsoft	
Alerta de seguridad cibernética	8FFR21-00927-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de abril de 2021
Última revisión	9 de abril de 2021
Indicadores de compromiso	
URL sitio falso	
http://vcv-custom[.]cl/fax/office	
IP	
[192.141.168.137]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00927-01/	
https://www.csirt.gob.cl/media/2021/04/8FFR21-00927-01.pdf	

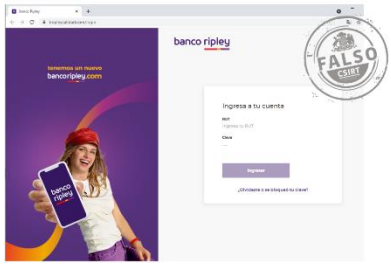
CSIRT alerta ante suplantación de GoDaddy	
Alerta de seguridad cibernética	8FFR21-00928-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de abril de 2021
Última revisión	12 de abril de 2021
Indicadores de compromiso	
URL sitio falso	
https://sso.godaddy.contapro[.]cl/www/secureserver/godaddy.php	
IP	
[138.117.149.176]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00928-01/	
https://www.csirt.gob.cl/media/2021/04/8FFR21-00928-01.pdf	

CSIRT alerta de página fraudulenta que suplanta a la Comisaría Virtual	
Alerta de seguridad cibernética	8FFR21-00929-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de abril de 2021
Última revisión	12 de abril de 2021
Indicadores de compromiso	
URL sitio falso	
http://comisariavirtual[.]website/	
IP	
[31.170.160.142]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00929-01/	
https://www.csirt.gob.cl/media/2021/04/8FFR21-00929-01.pdf	

CSIRT alerta por sitio fraudulento que suplanta a la radio Bio Bio	
Alerta de seguridad cibernética	8FFR21-00930-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de abril de 2021
Última revisión	12 de abril de 2021
Indicadores de compromiso	
URL sitio falso	
https://www.wealthmaster[.]us/cl-biobio-farkas	
IP	
[159.65.217.87]	

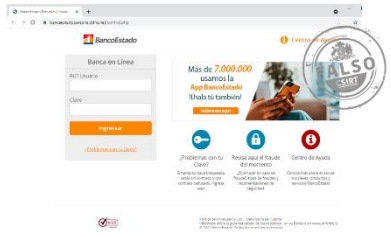
Enlaces para revisar el informe:
https://www.csirt.gob.cl/alertas/8ffr21-00930-01/
https://www.csirt.gob.cl/media/2021/04/8FFR21-00930-01.pdf

Imagen del sitio



CSIRT alerta ante sitio fraudulento que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FFR21-00931-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de abril de 2021
Última revisión	12 de abril de 2021
Indicadores de compromiso	
URL sitio falso	
http://bripleycalidad[.]com/login	
IP	
[186.64.118.235]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00931-01/	
https://www.csirt.gob.cl/media/2021/04/8FFR21-00931-01.pdf	

Imagen del sitio



CSIRT alerta de página fraudulenta que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FFR21-00932-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de abril de 2021
Última revisión	12 de abril de 2021
Indicadores de compromiso	
URL sitio falso	
https://bancaestadopersona.ddns[.]net/control.php	
IP	
[208.123.119.200]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00932-01/	
https://www.csirt.gob.cl/media/2021/04/8FFR21-00932-01.pdf	

Phishing

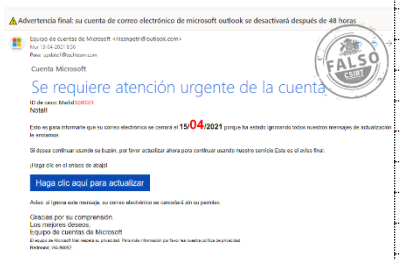
Imagen del mensaje

CSIRT alerta de phishing que suplanta a Apple	
Alerta de seguridad cibernética	8FPH21-00388-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de abril de 2021
Última revisión	12 de abril de 2021
Indicadores de compromiso	
URL sitio falso	
https://inc-segutidad2tatutta.mulrangkalihanja[.]com/account/?view=login&appIdKey=60fa166750dcbb2&country=CL	
IP	
[68.183.14.147]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00388-01/	
https://www.csirt.gob.cl/media/2021/04/8FPH21-00388-01.pdf	

Imagen del mensaje

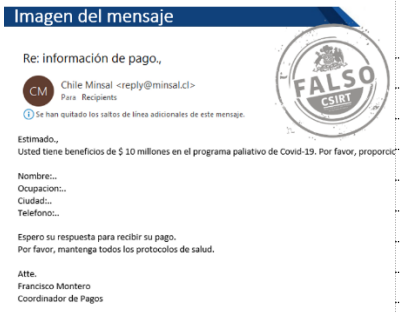
CSIRT alerta de campaña de smishing suplantando al Banco Ripley	
Alerta de seguridad cibernética	8FPH21-00389-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de abril de 2021
Última revisión	14 de abril de 2021
Indicadores de compromiso	
URL sitio falso	
http://www-bancoripleycl.deejayteam.com[.]tr/login	
IP	
[185.52.231.246]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00389-01/	
https://www.csirt.gob.cl/media/2021/04/8FPH21-00389-01.pdf	

Imagen del mensaje



CSIRT alerta por una campaña de phishing que suplanta a Microsoft Outlook	
Alerta de seguridad cibernética	8FPH21-00390-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de abril de 2021
Última revisión	14 de abril de 2021
Indicadores de compromiso	
URL sitio falso	
https://goofy-morse-387b98.netlify[.]app/	
IP	
[138.197.188.142]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00390-01/	
https://www.csirt.gob.cl/media/2021/04/8FPH21-00390-01.pdf	

Imagen del mensaje



CSIRT alerta por phishing que suplanta al Ministerio de Salud con falso pago por covid-19	
Alerta de seguridad cibernética	8FPH21-00391-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de abril de 2021
Última revisión	14 de abril de 2021
Indicadores de compromiso	
URL redirección	
No aplica	
URL sitio falso	
No aplica	
IP	
No aplica	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00391-01/	
https://www.csirt.gob.cl/media/2021/04/8FPH21-00391-01.pdf	

Imagen del mensaje

CSIRT alerta de campaña de phishing que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH21-00392-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de abril de 2021
Última revisión	14 de abril de 2021
Indicadores de compromiso	
URL redirección	
https://bit[.]ly/3tfMIlh?l=www.bancoripley.cl http://terrasplaceaz[.]com/wp-content/mu-plugins/enviar.php?l=1019652525 https://bit[.]ly/3a96wzv?l=www.bancoripley.cl https://ironguard[.]ro/activacion/cuenta-wkzr/	
URL sitio falso	
http://www-bancoripley.cl.mr-green[.]hr/login	
IP	
[195.29.178.17]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00392-01/	
https://www.csirt.gob.cl/media/2021/04/8FPH21-00392-01.pdf	

Vulnerabilidades

CSIRT alerta de vulnerabilidad crítica en VMware Carbon Black	
Alerta de seguridad cibernética	9VSA21-00417-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	9 de abril de 2021
Última revisión	9 de abril de 2021
CVE	
CVE-2021-21982	
Fabricante	
VMware	
Productos afectados	
VMware Carbon Black Workload, versión 1.0.1 y anteriores.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00417-01	
https://www.csirt.gob.cl/media/2021/04/9VSA21-00417-01.pdf	

CSIRT alerta de vulnerabilidades en Google Android	
Alerta de seguridad cibernética	9VSA21-00418-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de abril de 2021
Última revisión	9 de abril de 2021
CVE	
CVE-2020-11237	CVE-2021-0442
CVE-2020-25705	CVE-2021-0439
CVE-2020-11234	CVE-2021-0432
CVE-2020-11210	CVE-2021-0427
CVE-2020-11191	CVE-2021-0426
CVE-2020-11236	CVE-2021-0400
CVE-2020-11242	CVE-2021-0468
CVE-2020-11243	CVE-2021-0428
CVE-2020-11245	CVE-2021-0445
CVE-2020-11246	CVE-2021-0435
CVE-2020-11247	CVE-2021-0446
CVE-2020-11251	CVE-2021-0431
CVE-2020-11252	CVE-2021-0433
CVE-2020-11255	CVE-2021-0429
CVE-2020-15436	CVE-2021-0430
CVE-2021-0444	CVE-2021-0471
CVE-2021-0443	CVE-2021-0436
CVE-2021-0438	CVE-2021-0437
Fabricante	
Google Android	

Productos afectados
Google Android versiones anteriores a la 11.0 2021-04-05.
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00418-01
https://www.csirt.gob.cl/media/2021/04/9VSA21-00418-01.pdf

CSIRT alerta de distintas vulnerabilidades en productos de Cisco	
Alerta de seguridad cibernética	9VSA21-00419-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de abril de 2021
Última revisión	11 de abril de 2021
CVE	
CVE-2021-3449	CVE-2021-1467
CVE-2021-3450	CVE-2021-1420
CVE-2021-1137	CVE-2021-1474
CVE-2021-1479	CVE-2021-1475
CVE-2021-1480	CVE-2021-1413
CVE-2021-1459	CVE-2021-1414
CVE-2021-1472	CVE-2021-1415
CVE-2021-1473	CVE-2021-1463
CVE-2021-1251	CVE-2021-1380
CVE-2021-1308	CVE-2021-1407
CVE-2021-1309	CVE-2021-1408
CVE-2021-1362	CVE-2021-1399
CVE-2021-1386	CVE-2021-1406
CVE-2021-1485	
Fabricante	
Cisco	
Productos afectados	
Cisco SD-WAN vManage Software. Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers Management Interface. Cisco Small Business RV Series. Cisco Unified Communications Products. Cisco Unified Communications Manager Session Management Edition. Cisco Unified Communications Manager IM & Presence Service. Cisco Unity Connection. Cisco Prime License Manager. Cisco IOS XR Software Command. Cisco Webex Meetings para Android. Cisco Webex Meetings. Cisco Umbrella. Cisco RV340, RV340W, RV345, y RV345P Dual WAN Gigabit VPN. Cisco Unified Intelligence Center.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00419-01	
https://www.csirt.gob.cl/media/2021/04/9VSA21-00419-01.pdf	

CSIRT alerta de vulnerabilidad en WhatsApp para Android	
Alerta de seguridad cibernética	9VSA21-00420-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de abril de 2021
Última revisión	12 de abril de 2021
CVE	
CVE-2021-24026	
Fabricante	
WhatsApp (Facebook)	
Productos afectados	
WhatsApp Messenger para Android, versiones hasta la 2.21.2.11.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00420-01	
https://www.csirt.gob.cl/media/2021/04/9VSA21-00420-01.pdf	

CSIRT alerta de vulnerabilidad en diversos productos de Microsoft		
Alerta de seguridad cibernética	9VSA21-00421-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	13 de abril de 2021	
Última revisión	13 de abril de 2021	
CVE		
CVE-2021-28452	CVE-2021-28338	CVE-2021-28460
CVE-2021-28447	CVE-2021-28317	CVE-2021-28459
CVE-2021-28440	CVE-2021-28325	CVE-2021-28448
CVE-2021-28437	CVE-2021-28323	CVE-2021-28457
CVE-2021-28345	CVE-2021-26415	CVE-2021-28456
CVE-2021-28344	CVE-2021-26413	CVE-2021-28454
CVE-2021-28342	CVE-2021-27095	CVE-2021-28444
CVE-2021-28341	CVE-2021-28451	CVE-2021-28436
CVE-2021-28334	CVE-2021-28449	CVE-2021-28357
CVE-2021-28330	CVE-2021-28322	CVE-2021-28348
CVE-2021-28446	CVE-2021-28321	CVE-2021-28340
CVE-2021-28445	CVE-2021-28439	CVE-2021-28336
CVE-2021-28443	CVE-2021-28356	CVE-2021-28331
CVE-2021-28442	CVE-2021-28350	CVE-2021-28324
CVE-2021-28441	CVE-2021-28343	CVE-2021-28316
CVE-2021-28329	CVE-2021-28337	CVE-2021-28314
CVE-2021-28328	CVE-2021-28335	CVE-2021-28435
CVE-2021-28327	CVE-2021-28483	CVE-2021-28326
CVE-2021-28355	CVE-2021-28482	CVE-2021-28315
CVE-2021-28354	CVE-2021-28481	CVE-2021-26417
CVE-2021-28319	CVE-2021-28480	CVE-2021-26416
CVE-2021-28318	CVE-2021-28477	CVE-2021-27096
CVE-2021-28313	CVE-2021-28438	CVE-2021-28450

CVE-2021-28312	CVE-2021-28349	CVE-2021-28310
CVE-2021-28453	CVE-2021-28332	CVE-2021-27094
CVE-2021-28434	CVE-2021-28320	CVE-2021-27093
CVE-2021-28358	CVE-2021-28475	CVE-2021-27092
CVE-2021-28353	CVE-2021-28470	CVE-2021-27091
CVE-2021-28347	CVE-2021-28473	CVE-2021-27090
CVE-2021-28339	CVE-2021-28472	CVE-2021-27089
CVE-2021-28333	CVE-2021-28471	CVE-2021-27088
CVE-2021-28311	CVE-2021-28469	CVE-2021-27086
CVE-2021-28309	CVE-2021-28464	CVE-2021-27079
CVE-2021-28352	CVE-2021-28468	CVE-2021-27064
CVE-2021-28351	CVE-2021-28466	CVE-2021-27072
CVE-2021-28346	CVE-2021-28458	CVE-2021-27067

Fabricante

Microsoft

Productos afectados

Windows 10 Version 2004 for ARM64-based Systems
Windows 10 Version 2004 for 32-bit Systems
Windows Server, version 1909 (Server Core installation)
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 (Server Core installation)
Windows Server 2019
Windows 10 Version 1809 for ARM64-based Systems
Windows 10 Version 1809 for x64-based Systems
Windows Server, version 20H2 (Server Core Installation)
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1803 for x64-based Systems
Windows 10 Version 1803 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 7 for x64-based Systems Service Pack 1
Windows 10 Version 20H2 for ARM64-based Systems
Windows 10 Version 20H2 for 32-bit Systems
Windows 10 Version 20H2 for x64-based Systems
Microsoft Outlook 2013 Service Pack 1 (32-bit editions)
Microsoft Outlook 2016 (64-bit edition)
Microsoft SharePoint Enterprise Server 2016
Microsoft Outlook 2013 RT Service Pack 1

Microsoft Outlook 2010 Service Pack 2 (64-bit editions)
Microsoft Outlook 2010 Service Pack 2 (32-bit editions)
Microsoft Outlook 2013 Service Pack 1 (64-bit editions)
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 Visual Studio 2015 Update 3
Microsoft Visual Studio 2019 version 16.7 (includes 16.0 – 16.6)
Microsoft Visual Studio 2019 version 16.4 (includes 16.0 – 16.3)
Microsoft Visual Studio 2017 version 15.9 (includes 15.0 – 15.8)
Microsoft Visual Studio 2019 version 16.9 (includes 16.0 – 16.8)
Microsoft Exchange Server 2019 Cumulative Update 8
Microsoft Exchange Server 2016 Cumulative Update 19
Microsoft Exchange Server 2013 Cumulative Update 23
Microsoft Exchange Server 2016 Cumulative Update 20
Microsoft Exchange Server 2019 Cumulative Update 9
Visual Studio Code
Visual Studio Code – GitHub Pull Requests and Issues Extension
Visual Studio Code – Maven for Java Extension
VP9 Video Extensions
Raw Image Extension
Azure Sphere
Azure DevOps Server 2020.0.1
Visual Studio Code – Kubernetes Tools
Microsoft Office 2010 Service Pack 2 (32-bit editions)
Microsoft Excel 2010 Service Pack 2 (64-bit editions)
Microsoft Excel 2010 Service Pack 2 (32-bit editions)
Microsoft Office 2016 (64-bit edition)
Microsoft Office 2016 (32-bit edition)
Microsoft Excel 2016 (64-bit edition)
Microsoft Excel 2016 (32-bit edition)
Microsoft Office Online Server
Microsoft Word 2013 Service Pack 1 (64-bit editions)
Microsoft Word 2013 Service Pack 1 (32-bit editions)
Microsoft Word 2013 RT Service Pack 1
Microsoft Word 2010 Service Pack 2 (64-bit editions)
Microsoft Word 2010 Service Pack 2 (32-bit editions)
Microsoft SharePoint Server 2010 Service Pack 2
Microsoft Office Web Apps 2010 Service Pack 2
Microsoft Office 2010 Service Pack 2 (64-bit editions)
Microsoft Word 2016 (64-bit edition)
Microsoft Word 2016 (32-bit edition)
Microsoft Office 2019 for Mac
Microsoft SharePoint Server 2019
Microsoft SharePoint Enterprise Server 2013 Service Pack 1
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 SharePoint Foundation 2010 Service Pack 2
Azure DevOps Server 2020

Azure DevOps Server 2019 Update 1.1 Azure DevOps Server 2019 Update 1 Team Foundation Server 2015 Update 4.2 Team Foundation Server 2018 Update 3.2 Team Foundation Server 2018 Update 1.2 Team Foundation Server 2017 Update 3.1 Azure DevOps Server 2019.0.1.
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00421-01
https://www.csirt.gob.cl/media/2021/04/9VSA21-00421-01.pdf

CSIRT alerta de vulnerabilidad en diversos productos de SAP	
Alerta de seguridad cibernética	9VSA21-00422-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de abril de 2021
Última revisión	13 de abril de 2021
CVE	
CVE-2021-27602 CVE-2021-21482 CVE-2021-21483 CVE-2021-27608 CVE-2021-21485 CVE-2021-27598 CVE-2021-27603 CVE-2021-27599 CVE-2021-27604	CVE-2021-27600 CVE-2021-27601 CVE-2021-27609 CVE-2021-21492 CVE-2021-27605 Actualización de CVE-2021-21481 Actualización de CVE-2020-26832 Actualización de CVE-2021-21491
Fabricante	
SAP	
Productos afectados	
Google Chromium con SAP Business Client 6.5. SAP Commerce, versiones de la 1808 a la 2011. SAP NetWeaver Master Data Management, versions 710 y 710.750. SAP Solution Manager 7.20. SAP NetWeaver AS para Java. SAP NetWeaver AS para ABAP, versions 731, 740 y 750. SAP NetWeaver AS ABAP y SAP S4 HANA. SAP Setup 9.0. SAP Process Integration (Integration Builder Framework), versiones 7.10 a la 7.50. SAP Manufacturing Execution (System Rules) versions 15.1 a 15.4. SAP Focused RUN versions 200, 300. SAP Fiori Apps 2.0 for Travel Management en SAP ERP, version 608.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00422-01	
https://www.csirt.gob.cl/media/2021/04/9VSA21-00422-01.pdf	

CSIRT alerta de vulnerabilidad en Mendix de Siemens	
Alerta de seguridad cibernética	9VSA21-00423-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	15 de abril de 2021
Última revisión	15 de abril de 2021
CVE	
CVE-2021-27394	
Fabricante	
Siemens	
Productos afectados	
Mendix Applications con Mendix 7 hasta versión anterior a la V7.23.19. Mendix Applications con Mendix 8 hasta versión anterior a la V8.17.0. Mendix Applications con Mendix 8 (V8.12) hasta versión anterior a V8.12.5. Mendix Applications con Mendix 8 (V8.6) hasta versión anterior a la V8.6.9. Mendix Applications con Mendix 9 hasta la versión anterior a la V9.0.5.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00423-01	
https://www.csirt.gob.cl/media/2021/04/9VSA21-00423-01.pdf	

CSIRT alerta de vulnerabilidad en Google Chrome	
Alerta de seguridad cibernética	9VSA21-00424-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de abril de 2021
Última revisión	15 de abril de 2021
CVE	
CVE-2021-21201	CVE-2021-21202
CVE-2021-21212	CVE-2021-21210
CVE-2021-21219	CVE-2021-21209
CVE-2021-21218	CVE-2021-21208
CVE-2021-21217	CVE-2021-21207
CVE-2021-21216	CVE-2021-21221
CVE-2021-21215	CVE-2021-21205
CVE-2021-21214	CVE-2021-21204
CVE-2021-21213	CVE-2021-21203
CVE-2021-21211	
Fabricante	
Google	
Productos afectados	
Google Chrome, versiones 87.0.4280.66 a 89.0.4389.128	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00424-01	
https://www.csirt.gob.cl/media/2021/04/9VSA21-00424-01.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 de archivos maliciosos	Documento web
067891a085c756cb42a25b5f44f4c70aada0387d45dd770f3fbd04eeb452e1c3	2CMV21-00167-01
0b74cd4f19b653ad69092aca426c9a0b4c3c1c8955190e31b35adda745328f40	2CMV21-00167-01
1ffe786b417bd3c497a54d155250f3b98169c8cb04b7c6f9baf2986b7a4e9932	2CMV21-00167-01
3aefe663c05a360af6ffe3fd24e45ccbc54fef89eec7f86339be393777257903	2CMV21-00167-01
62fa63a5bf893f47c3c36c648b166320bd825b3426bb201c3902b44f969ef9d1	2CMV21-00167-01
832c205b709352275a289829f1288730513d33aa9c4fcc616eb1d7f89e9c13e1	2CMV21-00167-01
9046a3aedd8c56480f28639fecc3c5a3e0946e8abd82307629b431f730f4845c	2CMV21-00167-01
92fce158932d1475979ba37f95d56d67f420a33f920d979c1721cb6dc7c1cf16	2CMV21-00167-01
9b748165c79e8dfec8456c9d7ec72f157c4b970c49e9dcf335b2386a23c71feb	2CMV21-00167-01
af9480578fc1e827dbeb7c7058e1d5a8dd7f952ac6b778f27609daea4d426dcc	2CMV21-00167-01
ba95b71048599f50d62ef3de3591c33743d15429578edafd63fc6f15f8b57f33	2CMV21-00167-01
c079d7f1e900307b7c737719d5fecb17c9add2fefefbed9adcf382d9a6a469d4	2CMV21-00167-01
c1d1ae27fe10af0148e098128cb2f507a62991273b1696db271bb47d68fb836b	2CMV21-00167-01
d2da50fc1ec949499663cf5f7f9c3803362abdc0c3aba27870997d0cb20e9c54	2CMV21-00167-01
d4fb2d8e452906ba9a906087d7e608fb00525084946657ee8ff116a8b5de901f	2CMV21-00167-01
deb636a9d2e6c066135fdc2d6db90334663a4875cb661ebd3571eca286c02a1a	2CMV21-00167-01
e843baf121ef14b2caf149761c0352b6924504cb4ce2861a461bc7ba6a0226fa	2CMV21-00167-01
e98b38362bade8bdd0d0d6aa7460aa7c6731e514c0c658faf04f074a66c5c94c	2CMV21-00167-01
f8e06434c2744d6511998689ea9598d6b3dedf65f73cccba91b721160058ecf6	2CMV21-00167-01
0358e02c5b696cf867e13e9fc31215096c89c5c7c54c6dc20bfad2460bb2071d	2CMV21-00170-01
07748256a49b688f94b55b6e74605e51a65eed567c6b918c9ab327767da3fadc	2CMV21-00170-01
09f429899bed3319187f6cdb997a22363afe93c0499b52a6875fc2c546ea18c4	2CMV21-00170-01
0a1af6c76063a6376d9e429d509db694755fd18afa66dae26bff031c39df5daa	2CMV21-00170-01
0c3b6a854c644957375ae60a9e2360a1946ca256778c271df732e1a5c9c05a80	2CMV21-00170-01
1d6610614c1222783842a9ed5eb17b6a979d5f2f3c0aeb5e6385e3f328b1b28c	2CMV21-00170-01
27224d98fd286dbb4d0af2402451100d1ade77c0511c61d34ad52e4c7bd60bd4	2CMV21-00170-01
2742dd7711fd160ef35d0fd84d0b3692d300c56c77c1dddc0518f4e6b3371063	2CMV21-00170-01
2e5eabee7001e4a5adec24a18e680548ce354128edfdb10946fe4ee8a15b92cf	2CMV21-00170-01

325cc69b292b049784e205302186b2bb80d8ed53897fef477ce7f8b40ba50c6b	2CMV21-00170-01
3c8ff249cffc95b8e488e89fd5321f5d46f7d46c69e8492edb3c27be0ff36eb1	2CMV21-00170-01
3d9de99af7ffc3838175094ab6907b9f2e0874ce9bc0940ae6eeb5ff6f3642d6	2CMV21-00170-01
4984833558c538d2b83301198bcee5d3c7d88b75e42de4c841a6574d660cd58c	2CMV21-00170-01
5ad75cd42177471314c568c0c6cb2f5cc1199bddf69a764bac42d746cad66231	2CMV21-00170-01
5fd672cb50cbbb9f78bfde3d7e4c1a03402254ba6607a4d3e2e3f80a35cadb7e	2CMV21-00170-01
618e79e4384366fd6dc1f620349875b42c0c4442f88b2b5f081622c44883bdaf	2CMV21-00170-01
64f05cf1b07cf3f8a09fa166d53c6246e4d41e68020d8a90c18fd4dbd02a48ae	2CMV21-00170-01
65d5b3854d9f411a21a4431ac74d6af08f7e379c46cec462a831db5fea8fbb7e	2CMV21-00170-01
6820993a825541a851d2c1c21d5c2a09ab7a44f19158f6343532f1bde43ed01a	2CMV21-00170-01
70b3a2be72a209a45291c06b46d534cc75b5b8d98987eb95a29602b5ad82f2d6	2CMV21-00170-01
720e1f850bf693b9e873dbeb0ae0608b25849c8d82f51978fa87ff86be7a523f	2CMV21-00170-01
0acc507306ecd1611dd25529edfc2700e540691a6134fbc4ed7f60a4f39c55c7	2CMV21-00171-01
15766952153a9e11676b5e11bfdd1c456a8b3e4cbd198ed7103f41d974147c33	2CMV21-00171-01
1f5eab05d75803151d380e314f83814132be888c7a985f403ef7430b2c2e5b2a	2CMV21-00171-01
21dd819d9eb7c012ab9cf32789bcabcc23cefb43a985b752e1df1b4d4bfc77d3	2CMV21-00171-01
36f496f8ef4c2987ce15ce583eca5c02c87e15bc58372b5d12e3679ea639915c	2CMV21-00171-01
5d5010a70fffdbc9a2e229f3cdb33d49d8a37a07f56835a9d4e16b2af8b604e9	2CMV21-00171-01
69194d64960f6ddbdcc748818b968edeedfc68540ad179a3cb4f3f13f2368f06	2CMV21-00171-01
7bff738ef69a4dd506b2756139505771dfb37290f256a9f77ce9a5403ce90e2b	2CMV21-00171-01
9c345ffc9965f975a5c357720e6ee0b95bc07dfc37e61d9ad987476b5c25efd8	2CMV21-00171-01
ba7935cac92628b2817a4f5722e6b3e639d532e282d9ec3877a3170fb77e41d3	2CMV21-00171-01
d277995849e24f93dd53f665c59f06d16539d56a11a2e6bebb2397b61c35cdf0	2CMV21-00171-01
d6d47c457f5d2c398322b919b3af8f635b5f261c255088e2d474922a94302728	2CMV21-00171-01
db23e995afa20a9f2d33773e61a9983abbc990ff4ab81ae07e9410eb3f9fa4ad	2CMV21-00171-01
db793419bfd833fe3372878bb5d037daefb29de2b6686b978c84c3c1de6820f2	2CMV21-00171-01
de1e9817130936360966c279d3455f06d6f2e8168a392530a97a618306d89c0f	2CMV21-00171-01
f2b3eaa3cb510f72e8ba0b9634dac29624ccfe7a467c78531f77c65a7de5b64b	2CMV21-00171-01
f53dce28d8632d54070cd42aa0ad8cc7af986aa25588a9f5ab2b90a0400a7f59	2CMV21-00171-01
f7b378f89cddd83d1629f8eea60468d1d9855221c1e652bacebba1f429a90140	2CMV21-00171-01

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
89.45.201.102	Fx software srl	2CMV21-00167-01
219.117.204.232	Ntt pc communications, inc.	2CMV21-00167-01
178.212.120.3	Akasha.net sp. Z o.o	2CMV21-00167-01
51.81.12.236	Ovh sas	2CMV21-00167-01
165.227.228.231	Digitalocean-asn	2CMV21-00167-01
23.83.209.30	Gossamerthreads	2CMV21-00167-01
66.154.98.28	Performive	2CMV21-00167-01
185.121.120.199	Des capital b.v.	2CMV21-00167-01
51.79.142.218	Ovh sas	2CMV21-00167-01
84.38.134.26	Dataclub s.a.	2CMV21-00167-01
45.137.22.86	Rootlayer web services ltd.	2CMV21-00167-01
187.141.128.42	Uninet s.a. De c.v.	2CMV21-00167-01
181.30.31.40	Telecom argentina s.a.	2CMV21-00167-01
45.137.22.56	Rootlayer web services ltd.	2CMV21-00170-01
182.73.253.3	Bharti airtel ltd	2CMV21-00170-01
118.140.126.254	Hgc global communications limited	2CMV21-00170-01
165.84.218.244	4d data centres limited	2CMV21-00170-01
188.213.48.94	Taz it services sr	2CMV21-00170-01
134.209.153.90	Digitalocean-asn	2CMV21-00170-01
103.99.1.145	Vietnam posts and telecommunications group	2CMV21-00170-01
79.155.25.116	Telefonica de espana	2CMV21-00170-01
185.251.118.50	As40676	2CMV21-00170-01
46.101.61.67	Digitalocean-asn	2CMV21-00170-01
170.245.204.28	Vsp informatica ltda	2CMV21-00170-01
149.62.173.210	Infortelecom hosting s.l.	2CMV21-00170-01
107.173.23.198	As-colocrossing	2CMV21-00170-01
207.224.19.109	Centurylink-us-legacy-qwest	2CMV21-00170-01
91.216.192.44	Marta poltorak	2CMV21-00170-01
198.36.50.38	Riopl-coge	2CMV21-00170-01
46.199.78.195	Cyprus telecommunications authority	2CMV21-00170-01
104.236.80.225	Digitalocean-asn	2CMV21-00170-01

81.60.176.35	Vodafone ono, s.a.	2CMV21-00170-01
103.150.8.111	Xtom	2CMV21-00170-01
201.149.100.28	Crznet telecom ltda	2CMV21-00170-01
45.137.22.57	Rootlayer web services ltd.	2CMV21-00170-01
162.144.66.130	Unifiedlayer-as-1	2CMV21-00170-01
190.210.186.8	Nss s.a.	2CMV21-00170-01
217.146.81.38	Hyonix llc	2CMV21-00170-01
185.222.57.158	Rootlayer web services ltd.	2CMV21-00170-01
107.148.226.185	Pegtechinc	2CMV21-00170-01
187.217.245.25	Uninet s.a. De c.v.	2CMV21-00170-01
89.163.242.168	Myloc managed it ag	2CMV21-00171-01
84.38.130.192	Dataclub s.a.	2CMV21-00171-01
62.193.52.152	Celeste sas	2CMV21-00171-01
45.144.225.82	Des capital b.v.	2CMV21-00171-01
45.144.225.201	Des capital b.v.	2CMV21-00171-01
45.137.22.118	Rootlayer web services ltd.	2CMV21-00171-01
212.159.66.160	British telecommunications plc	2CMV21-00171-01
206.189.48.231	Digitalocean-asn	2CMV21-00171-01
185.247.34.165	Flex network sarl	2CMV21-00171-01
185.121.120.217	Des capital b.v.	2CMV21-00171-01
168.205.125.1	Brasil digital servicos de informatica e comercio	2CMV21-00171-01
168.167.3.66	Btc-gate1	2CMV21-00171-01
164.163.56.8	Pala pablo federico	2CMV21-00171-01
103.99.1.145	Vietnam posts and telecommunications group	2CMV21-00171-01

Correos electrónicos de donde son enviados los archivos adjunto con malware.

Dirección	Documento web
tan.le@alkuhaimi.com	2CMV21-00167-01
docusign@sairaconstruction.com	2CMV21-00167-01
inbox@pvschemicals.com	2CMV21-00167-01
prudence.hagenes@rempahnusantara.com	2CMV21-00167-01
oversea3@szgw-group.com	2CMV21-00167-01
sale@logsol.hu	2CMV21-00167-01
payment-advice@hsbc.com	2CMV21-00167-01
Shenzhen@alkuhaimi.com	2CMV21-00167-01
bayer@johnwilliams.gq	2CMV21-00167-01
jia@kuwahara.com.kh	2CMV21-00167-01

sales99@yonanac.com	2CMV21-00167-01
dsebeckis@cobralex.cl	2CMV21-00167-01
info@lpsd.com.ar	2CMV21-00167-01
shihas@charlotte.com.qa	2CMV21-00167-01
Cladys@alkuhaimi.com	2CMV21-00170-01
administrator-emailserver@spuredge.com	2CMV21-00170-01
aunivl@1aaaoftexas.com	2CMV21-00170-01
baris.tansever@abkenerji.com	2CMV21-00170-01
baz@1aaaoftexas.com	2CMV21-00170-01
charlotte@ppw1.co.uk	2CMV21-00170-01
cize@1aaaoftexas.com	2CMV21-00170-01
contato@masterduct.com.br	2CMV21-00170-01
dklee@panocean.com	2CMV21-00170-01
echo.xie@dazhi-hk.com	2CMV21-00170-01
euhaami@1aaaoftexas.com	2CMV21-00170-01
eum@1aaaoftexas.com	2CMV21-00170-01
export@heatbird.com	2CMV21-00170-01
f.narita@gmsline.co.jp	2CMV21-00170-01
fanie-feng@wilhelmsen.com	2CMV21-00170-01
ucanturk@teksuas.com	2CMV21-00170-01
yuoukoh@1aaaoftexas.com	2CMV21-00170-01
zawgeqy@1aaaoftexas.com	2CMV21-00170-01
idvd@1aaaoftexas.com	2CMV21-00170-01
info@meridian-ship.eu	2CMV21-00170-01
info@skymedikal.net	2CMV21-00170-01
info@transagro.com.py	2CMV21-00170-01
jaomaf@1aaaoftexas.com	2CMV21-00170-01
jchloeli@zero2ipo.com.cn	2CMV21-00170-01
jessicawang@jsmana.com	2CMV21-00170-01
liuli.hgxs@sinopec.com	2CMV21-00170-01
m.askari@tiamtejarat.com	2CMV21-00170-01
mm@ff-schlingel.de	2CMV21-00170-01
nakib@kuzeyborugroup.com	2CMV21-00170-01
ops.xiamen@jointwin.net	2CMV21-00170-01
oxu@1aaaoftexas.com	2CMV21-00170-01
purchase@wkw.de	2CMV21-00170-01
regala@circuitdelaribera.com	2CMV21-00170-01
ringocck@donago.com	2CMV21-00170-01

ygarcia@macoma.cr	2CMV21-00171-01
waleed@mageneet.com	2CMV21-00171-01
urdinola@pollofelizsaltillo.com.mx	2CMV21-00171-01
redessociales@acciona.com	2CMV21-00171-01
phlau@art-sea.com	2CMV21-00171-01
iss.cpsp@iss-shipping.com	2CMV21-00171-01
info@ic-eg.com	2CMV21-00171-01
docusign@aw-engineering.com	2CMV21-00171-01
chusui@tzdegree.com	2CMV21-00171-01
castro.malu.7@gmail.com	2CMV21-00171-01
ashkansmk@yahoo.com	2CMV21-00171-01
admins@support.com	2CMV21-00171-01
admin@nskmicro.co.jp	2CMV21-00171-01

Actualidad

CSIRT de Gobierno participa de panel sobre transformación digital bancaria en Latinoamérica

El director nacional del CSIRT de Gobierno, Carlos Landeros, participó en el seminario virtual «Tendencias y desafíos de la Transformación Digital para el sector financiero en la región», organizado por la Internet Society Capítulo Colombia (ISOC) e impulsado por la Corfo, ProChile y el Ministerio de Relaciones Exteriores.

En el webinar, nuestro director compartió la experiencia del sector bancario chileno en relación con la ciberseguridad, los principales ataques sufridos en los últimos años, y la importancia de fomentar la cooperación público privada a todo nivel para responder en conjunto a las amenazas.

Todo esto, como parte de un panel en que participaron Ángela Vaca, directora de Nuevos Negocios de Asobancaria en Colombia y coordinadora del CSIRT financiero de ese país y Fernando Sinagra, director de Servicios de Ingeniería Inteligente para Sudamérica de Accenture. El panel estuvo moderado por Martha Sánchez, miembro del directorio de ISOC.

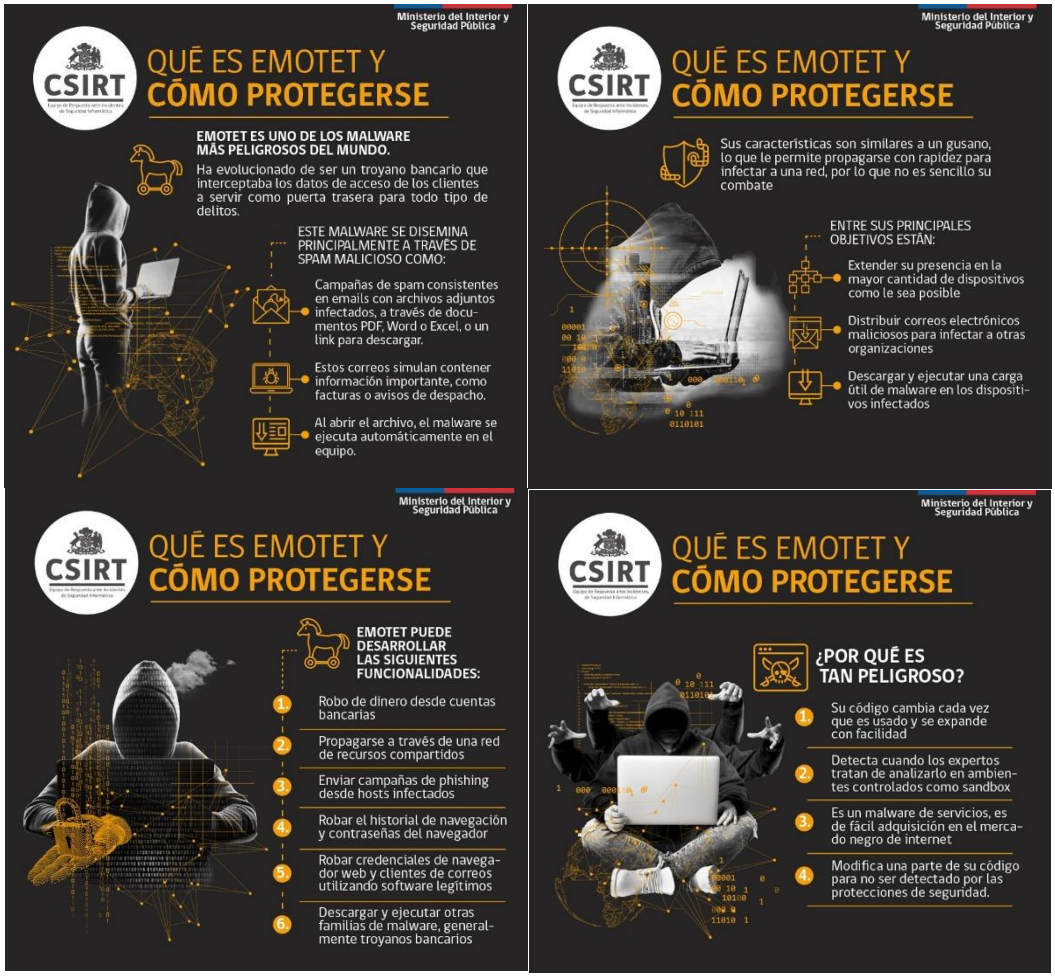
Ricardo Hernández, embajador de Chile en Colombia y Álvaro Undurraga, director regional metropolitano de la CORFO, hicieron la apertura y cierre del seminario, respectivamente.

Los detalles pueden encontrarse aquí: https://www.csirt.gob.cl/noticias/csirt-de-gobierno-participa-de-panel-sobre-transformacion-digital-bancaria-en-latinoamerica/.

Ciberconsejos para protegernos de Emotet

Emotet es uno de los malware más peligrosos del mundo. Ha evolucionado de ser un troyano bancario a servir como puerta trasera para todo tipo de delitos. Cualquier ciberdelincuente puede comprarlo para ingresar a los sistemas de sus víctimas y realizar distintos ataques, como ransomware o robo de datos.

Para más información, visitar aquí: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-emotet/.




Ministerio del Interior y Seguridad Pública
CSIRT
QUÉ ES EMOTET Y CÓMO PROTEGERSE
PRINCIPALES CONSECUENCIAS DE EMOTET:
1 Pérdida temporal o permanente de información confidencial
2 Interrupción de las operaciones regulares
3 Pérdidas financieras para restaurar sistemas y archivos
4 Daño potencial a la reputación de una organización.
Ministerio del Interior y Seguridad Pública
CSIRT
QUÉ ES EMOTET Y CÓMO PROTEGERSE
CÓMO EVITAR LA INFECCIÓN CON EMOTET
No descargar archivos de emails desconocidos o hacer clic en sus enlaces.
Mantener equipos y programas actualizados con los más recientes parches de seguridad.
Si administra un sitio web, revisar periódicamente los equipos, ya que podrían estar infectados con malware.
Realizar campañas de concientización para identificar ataques de phishing.

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 públicos 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 (en el sitio web https://www.csirt.gob.cl y/o al teléfono +(562) 2486 3850) siempre que hayan aportado con información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- Iván Castro
- Manuel Campo Díaz
- Diego Andrés Toledo Flores
- Javiera González

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.04.16 12:31:06 -04'00'