Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

12-02-2021 | Año 3 | N°84

Boletín de Seguridad Cibernética

Semana del 4 al 11 de Febrero de 2021

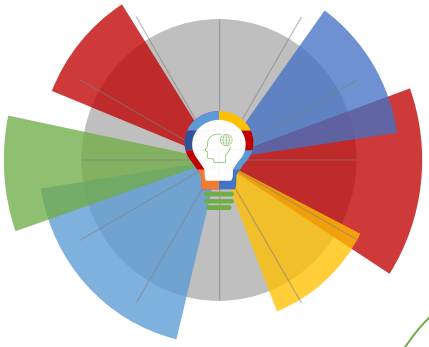
Resumen de la semana en cifras

Hash

22

Sha

Asociadas a múltiples campañas de phishing con archivos que contienen malware



Se advirtieron

19

URLs

Asociadas a sitios fraudulentos y campañas de phishing

Parches

100

para vulnerabilidades

Las mitigaciones son útiles para productos Mozilla, Apache, Apple y Google.

IPs

36

Informadas

Listado de IPs 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

Sitios fraudulentos

Imagen del sitio

CSIRT advierte página bancaria fraudulenta	
Alerta de seguridad cibernética	8FFR21-00887-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Febrero de 2021
Última revisión	04 de Febrero de 2021
Indicadores de compromiso	
URL sitio falso	
https://banco-santander.cl-xh[.]buzz/1612441092/index.asp	
IP	
[172.67.204.155]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00887-01/	
https://www.csirt.gob.cl/media/2021/02/8FFR21-00887-01.pdf	

Imagen del sitio

CSIRT informa suplantación de página de sitio bancario	
Alerta de seguridad cibernética	8FFR21-00888-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Febrero de 2021
Última revisión	04 de Febrero de 2021
Indicadores de compromiso	
URL sitio falso	
https://www.sss.kibrisecurity[.]com/33bf210f051b497d6923a04e33b4677c/index.asp	
IP	
[198.46.134.245]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00888-01/	
https://www.csirt.gob.cl/media/2021/02/8FFR21-00888-01.pdf	

CSIRT informa portal bancario falso	
Alerta de seguridad cibernética	8FFR21-00889-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Febrero de 2021
Última revisión	04 de Febrero de 2021
Indicadores de compromiso	
URL sitio falso	
https://santanderchile.rcrasociados[.]cl/1612446640/index.asp	
IP	
[186.64.116.45]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00889-01/	
https://www.csirt.gob.cl/media/2021/02/8FFR21-00889-01.pdf	

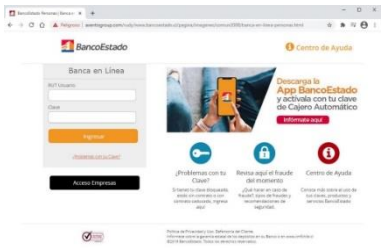
CSIRT advierte página de banco fraudulenta	
Alerta de seguridad cibernética	8FFR21-00890-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Febrero de 2021
Última revisión	04 de Febrero de 2021
Indicadores de compromiso	
URL sitio falso	
https://santand-er-personas[.]ltd/1612446150/personas/index.asp	
IP	
[198.54.115.239]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00890-01/	
https://www.csirt.gob.cl/media/2021/02/8FFR21-00890-01.pdf	

Imagen del sitio

CSIRT advierte suplantación de sitio bancario	
Alerta de seguridad cibernética	8FFR21-00891-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Febrero de 2021
Última revisión	11 de Febrero de 2021
Indicadores de compromiso	
URL sitio falso	
https://santand-er-personas[.]live/1613073431/personas/index.asp	
IP	
[198.54.121.237]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00891-01/	
https://www.csirt.gob.cl/media/2021/02/8FFR21-00891-01.pdf	

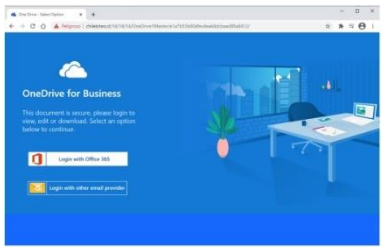
Imagen del sitio

CSIRT informa página bancaria fraudulenta	
Alerta de seguridad cibernética	8FFR21-00892-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Febrero de 2021
Última revisión	11 de Febrero de 2021
Indicadores de compromiso	
URL sitio falso	
https://sant-ander-actualizacion-de-datos[.]app/1613073959/personas/index.asp	
IP	
[198.54.121.237]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00892-01/	
https://www.csirt.gob.cl/media/2021/02/8FFR21-00892-01.pdf	



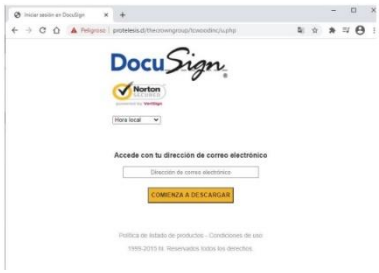
CSIRT informa portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR21-00893-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Febrero de 2021
Última revisión	11 de Febrero de 2021
Indicadores de compromiso	
URL sitio falso	
http://axentisgroup[.]com/rudy/www.bancoestado.cl/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[185.98.131.140]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00893-01/	
https://www.csirt.gob.cl/media/2021/02/8FFR21-00893-01.pdf	

Imagen del sitio



CSIRT advierte página falsa de servicio de alojamiento de archivos	
Alerta de seguridad cibernética	8FFR21-00894-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Febrero de 2021
Última revisión	11 de Febrero de 2021
Indicadores de compromiso	
URL sitio falso	
https://chileloteo[.]cl/14/14/14/OneDrive1Master/e1a7b55b00dfec4ea64dcbaad88a8412/	
IP	
[66.232.107.218]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00894-01/	
https://www.csirt.gob.cl/media/2021/02/8FFR21-00894-01.pdf	

Imagen del sitio



CSIRT advierte suplantación de página de firma electrónica	
Alerta de seguridad cibernética	8FFR21-00895-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Febrero de 2021
Última revisión	11 de Febrero de 2021
Indicadores de compromiso	
URL sitio falso	
http://protelesis[.]cl/thecrowngroup/tcwoodinc/u.php	
IP	
[186.64.116.220]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00895-01/	
https://www.csirt.gob.cl/media/2021/02/8FFR21-00895-01.pdf	

Phishing

Imagen del mensaje

CSIRT advierte phishing de cuenta de streaming suspendida	
Alerta de seguridad cibernética	8FPH21-00366-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Febrero de 2021
Última revisión	04 de Febrero de 2021
Indicadores de compromiso	
URL redirección	
hxxps://datingoneviral[.]com/.well-known/FAMOUSHOUSE/	
URL sitio falso	
hxxps://datingoneviral[.]com/.well-known/FAMOUSHOUSE/d23a5a94aa2bfc2592bbf5cf896ff54c/	
IP	
[69.12.92.254]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00366-01/	
https://www.csirt.gob.cl/media/2021/02/8FPH21-00366-01.pdf	

Imagen del mensaje

CSIRT informa phishing de cuenta bancaria bloqueada	
Alerta de seguridad cibernética	8FPH21-00367-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Febrero de 2021
Última revisión	04 de Febrero de 2021
Indicadores de compromiso	
URL redirección	
hxxps://bit[.]ly/2LM7GrO?l=www.santander.cl	
URL sitio falso	
hxxp://gaborestarsa2005[.]hu/wp-includes/www.santander.cl/pagina/login.asp	
IP	
[185.6.139.216]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00367-01/	
https://www.csirt.gob.cl/media/2021/02/8FPH21-00367-01.pdf	

CSIRT advierte phishing de retiro de bono del 10%	
Alerta de seguridad cibernética	8FPH21-00368-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Febrero de 2021
Última revisión	04 de Febrero de 2021
Indicadores de compromiso	
URL sitio falso	
http://valpanet[.]com/L3N0V0S1GNUM/imagenes/comun2008/banca-en-linea-personas.html	
IP	
186.64.117.245	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00368-01/	
https://www.csirt.gob.cl/media/2021/02/8FPH21-00368-01.pdf	

CSIRT informa phishing con falsa transferencia electrónica	
Alerta de seguridad cibernética	8FPH21-00369-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Febrero de 2021
Última revisión	04 de Febrero de 2021
Indicadores de compromiso	
Urls Redirección	
http://www.jazzbox-radio[.]fr/wp-content/themes/cli/enviar02.php?l=1058512047	
URL sitio falso	
http://paracels[.]one/wp-content/www.bancoestado.cl/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
181.176.35.17	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00369-01/	
https://www.csirt.gob.cl/media/2021/02/8FPH21-00369-01.pdf	

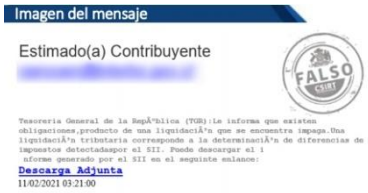
Imagen del mensaje

CSIRT advierte phishing de cuenta suspendida	
Alerta de seguridad cibernética	8FPH21-00370-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Febrero de 2021
Última revisión	10 de Febrero de 2021
Indicadores de compromiso	
URL sitio falso	
https://webpersonasclripley[.]com/login	
IP	
70.37.106.220	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00370-01/	
https://www.csirt.gob.cl/media/2021/02/8FPH21-00370-01.pdf	

Imagen del mensaje

CSIRT informa phishing de tarjeta de crédito bloqueada	
Alerta de seguridad cibernética	8FPH21-00371-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Febrero de 2021
Última revisión	10 de Febrero de 2021
Indicadores de compromiso	
Urls Redirección	
https://sant-ander-app[.]app/?sms=santander	
URL sitio falso	
https://sant-ander-app[.]live/16129711129/personas/index.asp	
IP	
198.54.125.16	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00371-01/	
https://www.csirt.gob.cl/media/2021/02/8FPH21-00371-01.pdf	

Malware



CSIRT advierte malware con supuestas obligaciones impagas	
Alerta de seguridad cibernética	2CMV21-00144-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Febrero de 2021
Última revisión	11 de Febrero de 2021
Indicadores de compromiso	
SHA256	
F3F9F269C75D5F7085A3D401C83600EE14E1D6920F60336D864BF38C211438E8	
AA295649CBF6159FE91D2CEBC2E641988D827EF37B7C7BF0D1273C5A2C9737A4	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv21-00144-01/	
https://www.csirt.gob.cl/media/2021/01/2CMV21-00144-01.pdf	

CSIRT informa malware con una supuesta prueba de pago	
Alerta de seguridad cibernética	2CMV21-00145-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Febrero de 2021
Última revisión	11 de Febrero de 2021
Indicadores de compromiso	
SHA256	
399A9435EE5CC7337D31AF4AE62F8571BBA3C29EE5B2DB75259EF941E0D68DE1	
4658D8F42B5D604A4ECEBAA26C21268CA5C88CCE743D37ABEB67CC6D18F7B4FE	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv21-00145-01/	
https://www.csirt.gob.cl/media/2021/01/2CMV21-00145-01-1.pdf	

Vulnerabilidades

CSIRT advierte vulnerabilidades de dos productos de SolarWinds	
Alerta de seguridad cibernética	9VSA21-00383-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Febrero de 2021
Última revisión	04 de Febrero de 2021
CVE	
CVE-2021-25274 CVE-2021-25275 CVE-2021-25276	
Fabricante	
SolarWinds	
Productos afectados	
SolarWinds plataforma Orion SolarWinds Serv-U FTP para Windows	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00383-01/	
https://www.csirt.gob.cl/media/2021/01/9VSA21-00383-01.pdf	

CSIRT comparte mitigaciones obtenidas por Red Hat	
Alerta de seguridad cibernética	9VSA21-00384-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Febrero de 2021
Última revisión	04 de Febrero de 2021
CVE	
CVE-2020-15685 CVE-2020-26976 CVE-2021-23953 CVE-2021-23954 CVE-2021-23960 CVE-2021-23964	
Fabricante	
Red Hat	
Productos afectados	
Mozilla Thunderbird (Red Hat package) 78.3.1-1.el8_1 a la 78.6.1-1.el8_1 Red Hat Enterprise Linux for Power, little endian Ext. Update Support 8.1 Red Hat Enterprise Linux for x86_64 – Extended Update Support 8.1 Red Hat Enterprise Linux Server – Update Services para SAP 8.1 Red Hat Enterprise Linux Server (IBM Power LE) Update Services p. SAP 8.1.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00384-01/	
https://www.csirt.gob.cl/media/2021/02/9VSA21-00384-01-1.pdf	

CSIRT advierte vulnerabilidad crítica de Google Chrome	
Alerta de seguridad cibernética	9VSA21-00385-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	05 de Febrero de 2021
Última revisión	05 de Febrero de 2021
CVE	
CVE-2021-21148	
Fabricante	
Apple	
Productos afectados	
Google Chrome, versiones de la 88.0.4324.0 a la 88.0.4324.149	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00385-01/	
https://www.csirt.gob.cl/media/2021/02/9VSA21-00385-01.pdf	

CSIRT comparte mitigaciones obtenidas de Fortinet	
Alerta de seguridad cibernética	9VSA21-00386-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	08 de Febrero de 2021
Última revisión	08 de Febrero de 2021
CVE	
CVE-2021-21465 CVE-2020-29016 CVE-2020-29017 CVE-2020-29018	
Fabricante	
Fortinet	
Productos afectados	
Fortinet FortiWeb versiones 6.3.7 y anteriores. Fortinet FortiDeceptor versiones 3.1.0 y anteriores.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00386-01/	
https://www.csirt.gob.cl/media/2021/02/9VSA21-00386-01.pdf	

CSIRT advierte vulnerabilidades de NextGen Gallery de WordPress	
Alerta de seguridad cibernética	9VSA21-00387-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Febrero de 2021
Última revisión	09 de Febrero de 2021
CVE	
CVE-2020-35942 CVE-2020-35943	
Fabricante	
Imagely	
Productos afectados	
Plugin NextGen Gallery para WordPress.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00387-01/	
https://www.csirt.gob.cl/media/2021/02/9VSA21-00387-01.pdf	

CSIRT comparte vulnerabilidades que afectan a Microsoft	
Alerta de seguridad cibernética	9VSA21-00388-01
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 2021
Última revisión	10 de Febrero de 2021
CVE	
CVE-2021-1639 CVE-2021-1698 CVE-2021-1721 CVE-2021-1722 CVE-2021-1724 CVE-2021-1726 CVE-2021-1727 CVE-2021-1728 CVE-2021-1730 CVE-2021-1731 CVE-2021-1732 CVE-2021-1733 CVE-2021-1734 CVE-2021-24066 CVE-2021-24067 CVE-2021-24068 CVE-2021-24069 CVE-2021-24070 CVE-2021-24071	

CVE-2021-24072
CVE-2021-24073
CVE-2021-24074
CVE-2021-24075
CVE-2021-24076
CVE-2021-24077
CVE-2021-24078
CVE-2021-24079
CVE-2021-24080
CVE-2021-24081
CVE-2021-24082
CVE-2021-24083
CVE-2021-24084
CVE-2021-24085
CVE-2021-24086
CVE-2021-24087
CVE-2021-24088
CVE-2021-24091
CVE-2021-24092
CVE-2021-24093
CVE-2021-24094
CVE-2021-24096
CVE-2021-24098
CVE-2021-24099
CVE-2021-24100
CVE-2021-24101
CVE-2021-24102
CVE-2021-24103
CVE-2021-24105
CVE-2021-24106
CVE-2021-24109
CVE-2021-24111
CVE-2021-24112
CVE-2021-24112
CVE-2021-24112
CVE-2021-24114
CVE-2021-25195
CVE-2021-25195
CVE-2021-26700
Fabricante
Microsoft
Productos afectados
Microsoft .NET 5.0, Core 2.1 y Core 3.1.
Microsoft .NET Framework 4.6.2 al 4.8.
Microsoft 365 Apps for Enterprise para sistemas 32 bit y 64 bit.
Microsoft Azure Kubernetes Service.
Microsoft Defender.
Microsoft Dynamics 365 on-premises versiones 8.2 y 9.0.
Microsoft Dynamics 365 Business Central 2020 Release Wave 1 y 2.
Microsoft Dynamics NAV 2015, 2016, 2017 y 2018.
Microsoft Edge for Android.

Microsoft Endpoint Protection. Microsoft Excel 2010 Service Pack 2 32-bit y 64-bit. Microsoft Exchange Server 2016 Cumulative Update 18 y 19, 2019 Cumulative Update 7 y 8. Microsoft Lync Server 2013. Microsoft Teams for iOS. Microsoft Office 2019 32-bit y 64-bit. Microsoft Office 2019 para Mac. Microsoft Office Online Server. Microsoft Office Web Apps Server 2013 Service Pack 1. Microsoft Office Online Server. Microsoft Security Essentials. Microsoft SharePoint Enterprise Server 2016. Microsoft SharePoint Foundation 2010 Service Pack 2. Microsoft SharePoint Foundation 2013 Service Pack 1. Microsoft SharePoint Server 2019. Microsoft System Center 2012 Endpoint Protection, 2012 R2 Endpoint Protection. Microsoft System Center Endpoint Protection. Microsoft Visual Studio 2017 versión 15.9 y 2019 versiones 16.4, 16.7 y 16.8. Microsoft Visual Studio Code y npm-script Extension. Skype for Business Server 2015 CU 8, y 2019 CU2. System Center 2019 Operations Manager. Windows 7 Service Pack 1. Windows 8.1. Windows RT 8.1 Windows 10, versiones 20H2, 1607, 1803, 1809, 1909 y 2004. Windows Server versiones 2004, 2016, 2019, 2019 20H2, 2019 1909 y 2019 2004. Windows Server 2012, Windows Server 2012 R2, Windows Server 2012 R2 (Server Core installation), Windows Server 2012 (Server Core installation). Windows Server 2008 R2, Windows Server 2008 R2 (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). WindowsServer versiones 1909 (Server Core installation), 2004 (Server Core installation) y 20H2 (Server Core Installation).
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00388-01/
https://www.csirt.gob.cl/media/2021/02/9VSA21-00388-01-1.pdf

CSIRT comparte mitigaciones obtenidas de Adobe	
Alerta de seguridad cibernética	9VSA21-00389-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Febrero de 2021
Última revisión	11 de Febrero de 2021
CVE	
CVE-2021-21046 CVE-2021-21017 CVE-2021-21037 CVE-2021-21036 CVE-2021-21045 CVE-2021-21042 CVE-2021-21034 CVE-2021-21061 CVE-2021-21044 CVE-2021-21038 CVE-2021-21058 CVE-2021-21059 CVE-2021-21062 CVE-2021-21063 CVE-2021-21057 CVE-2021-21060 CVE-2021-21041 CVE-2021-21040 CVE-2021-21039 CVE-2021-21035 CVE-2021-21033 CVE-2021-21028 CVE-2021-21021	
Fabricante	
Adobe	
Productos afectados	
Acrobat Reader DC versiones 2020.013.20074 y anteriores para Windows y macOS. Acrobat Reader 2017 versiones 2017.011.30188 y anteriores para Windows y macOS. Acrobat Reader 2020 versiones 2020.001.30018 y anteriores para Windows y macOS.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00389-01/	
https://www.csirt.gob.cl/media/2021/02/9VSA21-00389-01.pdf	

CSIRT comparte vulnerabilidad que afecta a SAP Commerce	
Alerta de seguridad cibernética	9VSA21-00390-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Febrero de 2021
Última revisión	11 de Febrero de 2021
CVE	
CVE-2021-21477	
Fabricante	
SAP	
Productos afectados	
SAP Commerce versiones 1808, 1811, 1905, 2005 y 2011.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00390-01/	
https://www.csirt.gob.cl/media/2021/02/9VSA21-00390-01.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	Tipo de Malware	Documento web
ab7c46fafb73625c9bc58a6b15a7ad52cedbdd5886b85d717b778c9a40193dc9	MSIL/Kryptik - Ransomware	2CMV21-00146-01
507fb91596e6dd95613d904b1f6dc86fd72c4d6deaee18839f8f3726ce5be670	MSIL/Kryptik - Ransomware	2CMV21-00146-01
b6c5511697a047d1d608f32dd0d9f6f235a91543896ec052c24b23c0a4478d59	MSIL/Kryptik - Ransomware	2CMV21-00146-01
9299a3dd0540b4f75af5d12c704c8c3ecd47b25c51c306924b437c2eb775becc	MSIL/Kryptik - Ransomware	2CMV21-00146-01
399a9435ee5cc7337d31af4ae62f8571bba3c29ee5b2db75259ef941e0d68de1	MSIL/Kryptik - Ransomware	2CMV21-00146-01
706510df18e068c711cfb975f00d1aeb1046787906d3cda0a3fc1f65b3be2282	MSIL/Kryptik - Ransomware	2CMV21-00146-01
e1f8e1e3b6cfee7a4e599abbd8324bb5108833119ba962984b86636c68ab05a1	MSIL/Kryptik - Ransomware	2CMV21-00146-01
1f6e98fa8b73a3e5304424d15a2d87d95ceb7e1b201732bd5cf7d2beb51d9c01	MSIL/Kryptik - Ransomware	2CMV21-00146-01
504c437eb6137e7bfaaf311d8b0bf3209ee5737a4cc0d787eb39bd8f61de0a80	MSIL/Kryptik - Ransomware	2CMV21-00146-01
ee7607a15c6026a59f52a0ed0ca8817835a713c12fd14b3f3348e5bdf8692700	MSIL/Kryptik - Ransomware	2CMV21-00146-01
7c4543586d38c0599ce0c712d2689cfec66bc862a1796f48784be6250ca5d97a	MSIL/Kryptik - Ransomware	2CMV21-00146-01
a052adecf1d257ebb7e99ace172086279e8232a69eff5f1e67eeb7d7cbc253f6	MSIL/Kryptik - Ransomware	2CMV21-00146-01
77ee808fba1f3c3ff78f2bcfe345876b68194831c91ae3186dca552b2e0bda01	MSIL/Kryptik - Ransomware	2CMV21-00146-01
ca947a5c7c0303ff1a61935527a1d6d35f0379a9728d18a364259db7729cefde	MSIL/Kryptik - Ransomware	2CMV21-00146-01
5564713f24f79a2fa73d6ff90de5ca49d139f88588ac9c9635df5e54ea468ff1	MSIL/Kryptik - Ransomware	2CMV21-00146-01
d7d76fb7adc91c1f533131372caf8b532cdf322e461230b44c43bb5993f8e4b0	MSIL/Kryptik - Ransomware	2CMV21-00146-01
a0c15fcd0d4a98382f73154b9003ef407962c5d986e577c0e2e2411c58c3bb42	MSIL/Kryptik - Ransomware	2CMV21-00146-01
b98df3a3770bdb3853e8a455a26b80783de34f60879dd282fc2d2e953832b9ee	MSIL/Kryptik - Ransomware	2CMV21-00146-01

Correo electrónico desde donde son enviados los archivos	Tipo de Malware	Documento web
account@trenchless.in	MSIL/Kryptik - Ransomware	2CMV21-00146-01
support@chinesestandard.net	MSIL/Kryptik - Ransomware	2CMV21-00146-01
gerencia@inemflex.com.co	MSIL/Kryptik - Ransomware	2CMV21-00146-01
sventa02@lustingsons.cl	MSIL/Kryptik - Ransomware	2CMV21-00146-01
claudete.lima@excelbr.com.br	MSIL/Kryptik - Ransomware	2CMV21-00146-01
phil@cyber.net.pk	MSIL/Kryptik - Ransomware	2CMV21-00146-01
customercare@oswalcastings.co.in	MSIL/Kryptik - Ransomware	2CMV21-00146-01
power@poweronline.com.mx	MSIL/Kryptik - Ransomware	2CMV21-00146-01
imports@tutanota.com.de	MSIL/Kryptik - Ransomware	2CMV21-00146-01
nour.fawaz@intertech-group.com	MSIL/Kryptik - Ransomware	2CMV21-00146-01
bizinfo@sg.marshallcavendish.com	MSIL/Kryptik - Ransomware	2CMV21-00146-01
account@staroverseas.co.th	MSIL/Kryptik - Ransomware	2CMV21-00146-01
purchase@arabico.ae	MSIL/Kryptik - Ransomware	2CMV21-00146-01
account@trenchless.in	MSIL/Kryptik - Ransomware	2CMV21-00146-01
Catharina.dew@accellgroup.com	MSIL/Kryptik - Ransomware	2CMV21-00146-01

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	Tipo Malware	Documento web
180.214.239.43	Vietnam Posts And Telecommunications Group	MSIL/Kryptik - Ransomware	2CMV21-00146-01
173.0.142.242	APYLI-AS	MSIL/Kryptik - Ransomware	2CMV21-00146-01
46.16.59.84	10dencehispahard, S.L.	MSIL/Kryptik - Ransomware	2CMV21-00146-01
66.96.184.10	BIZLAND-SD	MSIL/Kryptik - Ransomware	2CMV21-00146-01
185.4.132.177	Enartia S.A.	MSIL/Kryptik - Ransomware	2CMV21-00146-01
103.99.1.147	Vietnam Posts And Telecommunications Group	MSIL/Kryptik - Ransomware	2CMV21-00146-01
45.11.19.224	combahton GmbH	MSIL/Kryptik - Ransomware	2CMV21-00146-01
45.137.22.121	RootLayer Web Services Ltd.	MSIL/Kryptik - Ransomware	2CMV21-00146-01
185.235.165.234	VDI-NETWORK	MSIL/Kryptik - Ransomware	2CMV21-00146-01
103.145.255.216	Vietnam Posts And	MSIL/Kryptik - Ransomware	2CMV21-00146-01

	Telecommunications Group		
77.247.110.116	ABC Consultancy	MSIL/Kryptik - Ransomware	2CMV21-00146-01
84.38.133.27	DataClub S.A.	MSIL/Kryptik - Ransomware	2CMV21-00146-01
103.141.138.131	Vietnam Posts And Telecommunications Group	MSIL/Kryptik - Ransomware	2CMV21-00146-01
193.142.58.49	M247 Ltd	MSIL/Kryptik - Ransomware	2CMV21-00146-01

IoC Ataques de Fuerza Bruta

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

IP	Etiqueta de sistema autónomo	Documento web
141.98.80.130	NForce Entertainment B.V	4IIA21-00029-01
5.188.206.205	Krez 999 Eood	4IIA21-00029-01
103.156.93.150	Vietnam Posts And Telecommunications Group	4IIA21-00029-01
87.246.7.242	Internet Hosting LTD	4IIA21-00029-01
46.252.101.236	Broadmax Iletisim Ltd	4IIA21-00029-01
177.10.240.110	Midasnet Telecomunicacoes Ltda	4IIA21-00029-01
45.181.31.215	Nataly Oliveira Block Provedor de Internet	4IIA21-00029-01

Actualidad

Día Internacional de Internet Segura: Ciberconsejos para navegar por internet

Con el objetivo de promover el uso seguro, respetuoso y responsable de las tecnologías digitales, el 9 de febrero se celebra el Día Internacional de Internet Segura, una iniciativa promovida por Insafe/Inhope con el apoyo de la Comisión Europea. Tanto los adultos, jóvenes y niños están expuestos a distintas amenazas, ¿cómo cuidarse?

Ver más: https://www.csirt.gob.cl/recomendaciones/dia-internacional-de-internet-segura-ciberconsejos-para-navegar-por-internet/

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.

- Cristóbal Herrera
- Diego Echeverría
- Jorge

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.02.12 17:03:09 -03'00'