10-09-2020 | Año 2 | N°62

Boletín de Seguridad Cibernética

Semana del 03 al 09 de Septiembre de 2020

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

División de Redes y Seguridad Informática.
Gobierno de Chile

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Resumen de la semana en cifras

Body Hash

78

Sha 256

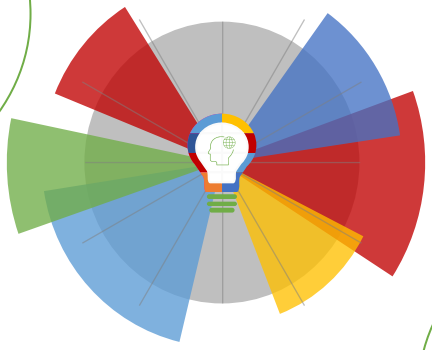
Asociadas a múltiples campañas de phishing son archivos que contienen malware

Se advirtieron

38

URLs

Asociadas a sitios fraudulentos y múltiples campañas de phishing y malware



Parches

154

para vulnerabilidades

Las mitigaciones son útiles para productos Cisco.

IPs

67

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 de sitio de suplantación bancaria	
Alerta de seguridad cibernética	8FFR20-00678-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Septiembre de 2020
Última revisión	03 de Septiembre de 2020
Indicadores de compromiso	
URL	
vito[.]sspu[.]sumy[.]ua/www[.]bancoestado[.]cl/pagina/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
194[.]146[.]181[.]131	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00678-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00678-01.pdf	

Imagen del sitio

CSIRT informa de web que suplanta a sitio bancario	
Alerta de seguridad cibernética	8FFR20-00679-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Septiembre de 2020
Última revisión	03 de Septiembre de 2020
Indicadores de compromiso	
URL	
vito[.]sspu[.]sumy[.]ua/www[.]bancoestado[.]cl/pagina/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
194[.]146[.]181[.]131	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00679-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00679-01.pdf	

Imagen del sitio

CSIRT informa sobre portal de suplantación de sitio de streaming	
Alerta de seguridad cibernética	8FFR20-00680-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Septiembre de 2020
Última revisión	04 de Septiembre de 2020
Indicadores de compromiso	
URL	
net[.]flix-loginhelp[.]com/app/login[.]php	
IP	
45[.]133[.]200[.]3	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00680-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00680-01.pdf	

Imagen del sitio

CSIRT advierte de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00681-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Septiembre de 2020
Última revisión	04 de Septiembre de 2020
Indicadores de compromiso	
URL	
bancosantander-portal-cl[.]cf	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00681-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00681-01.pdf	

Imagen del sitio

CSIRT advierte de web de suplantación de sitio bancario	
Alerta de seguridad cibernética	8FFR20-00682-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Septiembre de 2020
Última revisión	04 de Septiembre de 2020
Indicadores de compromiso	
URL	
bancosantander-portal-cl[.]ml	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00682-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00682-01.pdf	

Imagen del sitio

CSIRT advierte de sitio de streaming fraudulento	
Alerta de seguridad cibernética	8FFR20-00683-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Septiembre de 2020
Última revisión	04 de Septiembre de 2020
Indicadores de compromiso	
URL	
netflix[.]billingprofile[.]com/app/login[.]php	
IP	
45[.]133[.]200[.]3	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00683-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00683-01.pdf	

Imagen del sitio

CSIRT advierte de sitio de suplantación de banco	
Alerta de seguridad cibernética	8FFR20-00684-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Septiembre de 2020
Última revisión	04 de Septiembre de 2020
Indicadores de compromiso	
URL	
santaander-sms[.]xyz/1599241765/index[.]asp	
IP	
162[.]0[.]232[.]163	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00684-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00684-01.pdf	

Imagen del sitio

CSIRT informa de web que suplanta sitio de streaming	
Alerta de seguridad cibernética	8FFR20-00685-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Septiembre de 2020
Última revisión	04 de Septiembre de 2020
Indicadores de compromiso	
URL	
netflix[.]loginbilling[.]com/app/login[.]php	
IP	
45[.]133[.]200[.]3	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00685-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00685-01.pdf	

Imagen del sitio

CSIRT advierte de sitio que suplanta portal de pago online	
Alerta de seguridad cibernética	8FFR20-00686-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Septiembre de 2020
Última revisión	04 de Septiembre de 2020
Indicadores de compromiso	
URL	
www[.]paypal[.]login[.]validate-details-secure[.]com/app/signin[.]php	
IP	
162[.]0[.]232[.]170	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00686-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00686-01.pdf	

Imagen del sitio

CSIRT informa página de streaming fraudulenta	
Alerta de seguridad cibernética	8FFR20-00687-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Septiembre de 2020
Última revisión	08 de Septiembre de 2020
Indicadores de compromiso	
URL	
net[.]flix-help[.]com	
net[.]flix-browse[.]com/app/login[.]php	
IP	
45[.]133[.]200[.]3	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00687-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00687-01.pdf	

CSIRT advierte de página bancaria falsa	
Alerta de seguridad cibernética	8FFR20-00688-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Septiembre de 2020
Última revisión	08 de Septiembre de 2020
Indicadores de compromiso	
URL	
hxxps://santaander-movil[.]link/?sms=1	
IP	
162[.]0[.]232[.]168	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00688-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00688-01.pdf	

CSIRT advierte suplantación de página bancaria	
Alerta de seguridad cibernética	8FFR20-00689-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Septiembre de 2020
Última revisión	08 de Septiembre de 2020
Indicadores de compromiso	
URL	
bancosantander-chile-infos[.]tk	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00689-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00689-01.pdf	

Imagen del sitio

CSIRT informa de sitio de streaming falso	
Alerta de seguridad cibernética	8FFR20-00690-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Septiembre de 2020
Última revisión	08 de Septiembre de 2020
Indicadores de compromiso	
URL	
net[.]flix-signin[.]com/app/login[.]php	
net[.]flix-settings[.]com	
IP	
45[.]133[.]200[.]3	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00690-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00690-01.pdf	

Imagen del sitio

CSIRT advierte de sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00691-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Septiembre de 2020
Última revisión	08 de Septiembre de 2020
Indicadores de compromiso	
URL	
bancosantander-chile-online[.]cf	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00691-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00691-01.pdf	

Imagen del sitio

CSIRT advierte de sitio de suplantación bancaria	
Alerta de seguridad cibernética	8FFR20-00692-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Septiembre de 2020
Última revisión	09 de Septiembre de 2020
Indicadores de compromiso	
URL	
bancosantander-chile-online[.]g	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00692-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00692-01.pdf	

Imagen del sitio

CSIRT advierte de portal que suplanta a sitio web bancario	
Alerta de seguridad cibernética	8FFR20-00693-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Septiembre de 2020
Última revisión	09 de Septiembre de 2020
Indicadores de compromiso	
URL	
www-on-line-banestado[.]tk	
IP	
101[.]99[.]90[.]35	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00693-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00693-01.pdf	

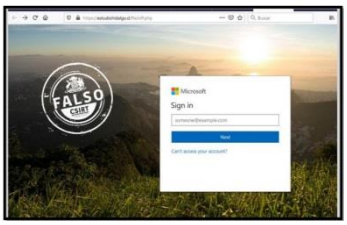
Imagen del sitio

CSIRT informa sobre portal que suplanta a sitio bancario	
Alerta de seguridad cibernética	8FFR20-00694-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Septiembre de 2020
Última revisión	09 de Septiembre de 2020
Indicadores de compromiso	
URL	
bancosantander-chile-online[.]ga	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00694-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00694-01.pdf	

Imagen del sitio

CSIRT advierte de portal que suplanta web de streaming	
Alerta de seguridad cibernética	8FFR20-00695-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Septiembre de 2020
Última revisión	09 de Septiembre de 2020
Indicadores de compromiso	
URL	
account-netflix[.]gq	
IP	
145[.]14[.]144[.]173	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00695-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00695-01.pdf	

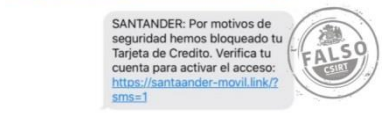
Imagen del sitio



CSIRT informa sobre sitio de suplantación de cuentas de correos	
Alerta de seguridad cibernética	8FFR20-00696-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Septiembre de 2020
Última revisión	09 de Septiembre de 2020
Indicadores de compromiso	
URL	
estudiohidalgo[.]cl/file/Gmaildocs[.]php	
estudiohidalgo[.]cl/file/off[.]php	
IP	
66[.]165[.]231[.]114	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00696-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00696-01.pdf	

Phishing

Imagen del mensaje



CSIRT advierte de phishing bancario por bloqueo de tarjeta	
Alerta de seguridad cibernética	8FPH20-00303-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Septiembre de 2020
Última revisión	08 de Septiembre de 2020
Indicadores de compromiso	
URL	
hxxps://santaander-movil[.]link/?sms=1	
hxxps://santaander-seguridad[.]link/1599572990/index.asp	
IP	
[162.0.232.168]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00303-01/	
https://www.csirt.gob.cl/media/2020/09/8FPH20-00303-01.pdf	

Imagen del mensaje

CSIRT advierte de phishing bancario por promoción de pago de tarjeta	
Alerta de seguridad cibernética	8FPH20-00304-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Septiembre de 2020
Última revisión	08 de Septiembre de 2020
Indicadores de compromiso	
URL	
hxxp://fashioncarry[.]com/sco.php	
hxxps://scotiabankchle[.]gq/1599577707/login/personas/index	
IP	
[103.248.146.11]	
[91.234.99.119]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00304-01/	
https://www.csirt.gob.cl/media/2020/09/8FPH20-00304-01.pdf	

Vulnerabilidades

CSIRT comparte actualizaciones de WhatsApp	
Alerta de seguridad cibernética	9VSA20-00294-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Septiembre de 2020
Última revisión	04 de Septiembre de 2020
CVE	
CVE-2020-1894 - CVE-2020-1891 - CVE-2020-1890 CVE-2020-1889 - CVE-2020-1886 - CVE-2019-11928	
Fabricante	
Whatsapp	
Productos afectados	
WhatsApp para Android versiones anteriores a la 2.20.35. WhatsApp Business para Android versiones anteriores a la 2.20.20. WhatsApp para iPhone versiones anteriores a la 2.20.30. WhatsApp Business para iPhone versiones anteriores a la 2.20.30.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00294-01/	
https://www.csirt.gob.cl/media/2020/09/9VSA20-00294-01.pdf	

CSIRT comparte actualizaciones obtenidas de Joomla!	
Alerta de seguridad cibernética	9VSA20-00295-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Septiembre de 2020
Última revisión	07 de Septiembre de 2020
CVE	
CVE-2020-24599 - CVE-2020-24598 - CVE-2020-24597	
Fabricante	
Joomla!	
Productos afectados	
CMS Joomla! versiones 3.9.0 – 3.9.20.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00295-01/	
https://www.csirt.gob.cl/media/2020/09/9VSA20-00295-01.pdf	

CSIRT comparte actualizaciones obtenidas de Google para Chrome	
Alerta de seguridad cibernética	9VSA20-00296-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Septiembre de 2020
Última revisión	07 de Septiembre de 2020
CVE	
CVE-2020-6563 - CVE-2020-6571 - CVE-2020-6570 CVE-2020-6569 - CVE-2020-6568 - CVE-2020-6567 CVE-2020-6566 - CVE-2020-6565 - CVE-2020-6564 CVE-2020-6562 - CVE-2020-6561 - CVE-2020-6560 CVE-2020-6559 - CVE-2020-6558	
Fabricante	
Google	
Productos afectados	
Google Chrome versiones anteriores a la 85.0.4183.83.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00296-01/	
https://www.csirt.gob.cl/media/2020/09/9VSA20-00296-01.pdf	

CSIRT comparte mitigaciones obtenidas de Microsoft		
Alerta de seguridad cibernética	9VSA20-00297-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	09 de Septiembre de 2020	
Última revisión	09 de Septiembre de 2020	
CVE		
CVE-2020-0664	CVE-2020-1097	CVE-2020-1592
CVE-2020-0856	CVE-2020-1119	CVE-2020-1594
CVE-2020-0875	CVE-2020-1193	CVE-2020-1596
CVE-2020-0914	CVE-2020-1210	CVE-2020-16851
CVE-2020-0921	CVE-2020-1218	CVE-2020-16852
CVE-2020-0928	CVE-2020-1224	CVE-2020-16853
CVE-2020-0941	CVE-2020-1250	CVE-2020-16854
CVE-2020-0989	CVE-2020-1256	CVE-2020-16855
CVE-2020-1031	CVE-2020-1332	CVE-2020-16879
CVE-2020-1033	CVE-2020-1335	CVE-2020-16884
CVE-2020-1083	CVE-2020-1338	CVE-2020-1091
CVE-2020-1589		
Vulnerabilidades adicionales informadas		
CVE-2020-0648	CVE-2020-1053	CVE-2020-1460
CVE-2020-0718	CVE-2020-1057	CVE-2020-1471
CVE-2020-0761	CVE-2020-1074	CVE-2020-1482
CVE-2020-0766	CVE-2020-1098	CVE-2020-1491
CVE-2020-0782	CVE-2020-1115	CVE-2020-1506
CVE-2020-0790	CVE-2020-1122	CVE-2020-1507

CVE-2020-0805	CVE-2020-1129	CVE-2020-1508
CVE-2020-0836	CVE-2020-1130	CVE-2020-1514
CVE-2020-0837	CVE-2020-1133	CVE-2020-1523
CVE-2020-0838	CVE-2020-1146	CVE-2020-1532
CVE-2020-0839	CVE-2020-1152	CVE-2020-1559
CVE-2020-0870	CVE-2020-1159	CVE-2020-1575
CVE-2020-0878	CVE-2020-1169	CVE-2020-1576
CVE-2020-0886	CVE-2020-1172	CVE-2020-1590
CVE-2020-0890	CVE-2020-1180	CVE-2020-1593
CVE-2020-0904	CVE-2020-1182	CVE-2020-1595
CVE-2020-0908	CVE-2020-1198	CVE-2020-1598
CVE-2020-0911	CVE-2020-1200	CVE-2020-16856
CVE-2020-0912	CVE-2020-1205	CVE-2020-16857
CVE-2020-0922	CVE-2020-1227	CVE-2020-16858
CVE-2020-0951	CVE-2020-1228	CVE-2020-16859
CVE-2020-0997	CVE-2020-1245	CVE-2020-16860
CVE-2020-0998	CVE-2020-1252	CVE-2020-16861
CVE-2020-1012	CVE-2020-1285	CVE-2020-16862
CVE-2020-1013	CVE-2020-1303	CVE-2020-16864
CVE-2020-1030	CVE-2020-1308	CVE-2020-16871
CVE-2020-1034	CVE-2020-1319	CVE-2020-16872
CVE-2020-1038	CVE-2020-1345	CVE-2020-16873
CVE-2020-1039	CVE-2020-1376	CVE-2020-16874
CVE-2020-1044	CVE-2020-1440	CVE-2020-16875
CVE-2020-1045	CVE-2020-1452	CVE-2020-16878
CVE-2020-1052	CVE-2020-1453	CVE-2020-16881

Fabricante

Microsoft

Productos afectados

ASP.NET Core 2.1
ASP.NET Core 3.1
ChakraCore
Internet Explorer 9, 11
Microsoft 365 Apps for Enterprise (32-bit y 64-bit)
Microsoft Business Productivity Servers 2010 Service Pack 2
Microsoft Dynamics 365 (on-premises) version 9.0
Microsoft Edge (Chromium-based y EdgeHTML-based)
Microsoft Excel2010 Service Pack 2 (32-bit y 64-bit)
2013 RT Service Pack 1
2013 Service Pack 2 (32-bit y 64-bit)
2016 (32-bit y 64-bit)
Microsoft Exchange Server
2016 Cumulative Update 16
2016 Cumulative Update 17
2019 Cumulative Update 5
2019 Cumulative Update 6
Microsoft Office
2010 Service Pack 2 (32-bit y 64-bit editions)
2013 RT Service Pack 1
2013 Service Pack 1 (32-bit y 64-bit editions)
2016 (32-bit y 64-bit editions)

2016 for Mac
2019 (32-bit y 64-bit editions)
2019 for Mac
Online Server
Web Apps 2013 Service Pack 1
Web Apps 2010 Service Pack 2
Microsoft SharePoint
Enterprise Server 2013 Service Pack 1
Enterprise Server 2016
Foundation 2010 Service Pack 2
Foundation 2013 Service Pack 1
Server 2010 Service Pack 2
Server 2019
Microsoft Visual Studio
2012 Update 5
2013 Update 5
2015 Update 3
2017 version 15.9 (incluidos 15.1 – 15.8)
2019 version 16.0
2019 version 16.4 (incluidos 16.0 – 16.3)
2019 version 16.7 (incluidos 16.0 – 16.6)
Microsoft Word
2010 Service Pack 2 (32-bit y 64-bit editions)
2013 RT Service Pack 1
2013 Service Pack 1 (32-bit y 64-bit editions)
2016 (32-bit y 64-bit editions)
OneDrive for Windows
SQL Server
2017 Reporting Services
2019 Reporting Services
Visual Studio Code
Windows 10 (32-bit y 64-bit)
Version 1607, 1709, 1803, 1809, 1903, 1909, 2004, para 32 bit, 64 bit y ARM64-based
Windows 7
32-bit Systems Service Pack 1
x64-based Systems Service Pack 1
Windows 8.1
32-bit systems
x64-based systems
Windows RT 8.1
Windows Server 2008
32-bit Systems Service Pack 2
32-bit Systems Service Pack 2 (Server Core installation)
x64-based Systems Service Pack 2
x64-based Systems Service Pack 2 (Server Core installation)
R2 for x64-based Systems Service Pack 1
R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Server 2012
2012
Server Core installation

R2 y R2 (Server Core installation) Windows Server 2016 2016 Server Core installation Windows Server 2019 2019 Server Core installation Windows Server version 1903 (Server Core installation) version 1909 (Server Core installation) version 2004 (Server Core installation) xamarin.forms
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00297-01/
https://www.csirt.gob.cl/media/2020/09/9VSA20-00297-01.pdf

Indicadores de Compromisos

Se comparte a continuación el listado de IPs que fueron detectadas durante la pasada semana por el Equipo del CSIRT intentando ejecutar escaneaos puertos, ataques de denegación de servicios o tratando de infectar con códigos maliciosos, entre otros ataques, para el conocimiento de la comunidad.

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 reportados (se recomienda bloquear)

019c37268b08ec8bdf64efc52f889ef1cc2e39d7fd45aa69fd2d22cb27e6b581	ddb867fccaecd7085462b092e5dacff90d666301868981d35ce4cf6a994c4537
0d50239f78bb312fb2c0bea2628104db8e45fea2cb31208b18782b950e0befa1	f380bc34e4d8bed89782b5d6d81c176586c2b34e95efefcb30687220d03e3485
15de7545c8d13285e5cb83c314b0f47ad6428d10169a8d82ab09ab7d7b16bef3	f42309e5bfad3404989189b18254dd8157ec5f170544081a5dc8e4607fe364d1
168b5da0b0b11a0bfb519c5efdce6d03fa2c2e576a7e7cdeffda1c09641f7556	12b128d3cdcbccc9ac0182be91483112605db5d0cf9255df84747701c079596e
1f5b6b69bba1de252b6f92057b798a07be36fc8cbf6f0425d9527e7729a2ab3d	156767e83da4c0d2ccb7d68f48d24c19ae0a47bad182946a7228d2d90de36c5c
2127c6d9a336fa4b6fc48dae6590bdf9604ad60d073aa74355949e5378f0270e	241d87dd58e6021fc9416533b7f9e904f50403906c7861189bec361e3689e653
251a3ce3e3b69e991f5a1e8d1d10b493111e9e2215fb4e4dde32281778a056b9	317984f61950a1dd483b10cac80ba3b66689b0c8ba6ce2a59e2262c5043c7a75
25c4930127bd03f5272a817b8337b5f08f195807fd7cade11011599d2eee99b3	39097a208fc44653546ca6f01bd6af471c01b045da19c6f54cdf97d03cfc6c77
2da3cafc45a2fd98c91b3f1bea2a48e5dd01c09713454be8ef98e2d16d3af8e7	5b310538477685ed729a7821eafbb212b766bacb7fda3154c920c5b5a06cf896
36337c45a233dbc9f106b4415584520ea6e50712417d9b1fdd7751d1cd5b8780	98a208893021fd62a429c88ba79368c66518be6a974814975545e12da2e84950
3768bc365b9b7d45afe4cb30adeda81e1a20fcea35de8ff0af38a226b65e52af	99fed4907368d302e4c5e0b57dd6496cfc09df0a9107f3a3042210d9a637612b
3ac12d0795612fc72b1a0a9e732d2effbf4d9c967be20dd2a76539cd75591529	b696ea1e0be03bdbe2fefec156e3b45c10f33d3335d60e0aa84b03faec97b02d
3be6d0fac78c13868de42d0d8ebdc679fde81153ceff09df7cda34cd0dff9cf6	ea1c23b967f0f98f68d6e7303e3e0cd5ccce0cfe469df5a2bcfe51e06d309c14
46037857291f877b0c4b8eee55a142aee04c2bd94c7545af5123e22985c3ffaf	01d9362710b1782bd7867601e5a4966d227b3dac790433029c5c1237d81027f6
4a9633ecae342b013bcc0c34fc1709600e70e90a43701c9f3218bf80916b6d43	026b46ce13b69a6e48fea6e47360d4680d61dbd075a10c52f4d48591af113bb1
4eb0be1c1604bdc56352f0550ced01ff198d7d1455b56b35ea8e16ef026e842c	03f2e0a14621b7cb6d905929eb44cfd3322fb9b8d4402525d0fa89cc326b7ad3
4f696d59be410a76e8a6c89b400d7aa032d623c362454caccbf322bd400f0a73	06132fc769ac7a487bb873ccfe40806aa32c692543097cf319b8c3c33481cb9b
565956a11acdd3a7c41d291dec85e0e394b70f0d7244497986482d778fdc012d	192a7f545cde03fc0866b274871b4aced624a4a0503cd4e8347eb43f82da39ed
566d866fb7d9577cd92837143d13ee122a5a3a0ba3464d1e75a8f2d095309be7	3588580a33396c90cdea430400aa821c515b0793baeec90845715a1edf8397d5
599a861ba05b57347331fbb180078cc4074c60d71c1e24c6b1469d18f139c4e7	26fd9a48af8ea51c85bd4594f162540d9c1f747c8a51ef2a743e11390011df6f
60016b594d0f144e6af1160157ac8185fa8de5b6c76e9e45ad71ce13adb9b15f	2ce42c9375b8c8baacb0967eeeb05f314786bf3d3fbe4db8c9dae9df34023303
60ad914d6efd04baf8fbc5b0b6448042d688bc49352930fba4cc4c4370221d32	3dc2399972e1602f3b246bf255a1bf07b5e33fdc1f0b313209e7f72328dbb297
65565c13a250f72a089b0306c372d4bc3dc778c6ab9d1b1825e5d505e8c8e306	48ec4a1c85dcaf8025008a81f0a9b4a7ec56f68ecb4d9b8f04c60024bc924f1f
6b6ee7c3eebce87fbf093253a28ca90fb94e7c53134722d7c285b52dbf2f51c7	04bc0c7c9db38c481eccac2dd0b5fbe7b04968312c316b944219f8a4f8008963
6d172d720cf3f98f6ba22e6a6b4e813f2c2300d8a30591b831d75ea628adacfb	50d3e1fecfeb0871cef16d9f3a3b1d904cb9814a67988025605b6421cb3e8239
70acca94041bb5834f3948f6ad9f87d4e0e9339c393774e4b9452af0b85ef537	603e2360c34816cf216def981a1b3aa21ed41c9dc278445eefe85b79311cd406
71595cc89b180dbd13282860b351ca4fb2859e46b72a75126c3976ea16fa46f9	68ff6304a7e84965b7d175ae14428594023db93e6933be3e7f98052b971cd64c
74ff45732723b71e80c075cab3d3a0c776234c8b0cddd41260691581365150ea	71637f20eb65c438460dc30d6885edc9fbf212acb07690a068f938bf3a467265
7c178f6f73eda5a5e0a4de819f092772ad4cb0ac2f6d996f7b9b072883b04bc0	736705e6d0f287c58d87fc7155bd5bc92f5f199111c5beea155be49e5c8a9187
83a608a684d531170d1d962a923ec80ff882ad17ac5a24ce4477d634e575c74e	676f179bee2368ddad94caa8ecbc409ebca984ec8b01b53d5e2e8e7c4660d79b
8a4c384c2f0e89b7a1561aae298715c3981e9ade62e7d41b4acf6f6138af0caf	862ee4cb0fce9735028da42d638c2c657638fc782f7cd4054f5d78b853cac678
95e06de334578875b8a103e5ceb5befc765c081e75bf39907b2c8f910b8b1eb3	7337dc6d871ef01de0342134fb584670dbdbc0e50181f7219abd26225b837ad0
9e0b617d1f1079cb339de903f320274b428c1e8723580e2152f8b5af88563c20	bf9e369af8e87627b319f6acafa3d9ed53e5b834ca16b295b3bfe9c27770588d

a32e3083bd066fd21f716cbb3063fd0daf6cc2644c4ff7630d831f06f7eb6553	c2cbf0f3fe5ecfeb1dca0ae514203c7560968edbaef3de13340d2c724c2a08b0
a4742aa9bc3444d4d3406dd0006e62ccbe08a89589e023fd842629208a3127f9	e0b66f439651029c988f98e99862e25978c36d31ffdd7a934d8a1a86db29e84a
aded839540bb039ff325a997f2bb52dd495ca8aa6cf458e81d408fb942df6218	06132fc769ac7a487bb873ccfe40806aa32c692543097cf319b8c3c33481cb9b
b8b883d714658e0a4974d4356dfebdb2e628ae3e7355d42a15ccc6034b01a0d4	e0b66f439651029c988f98e99862e25978c36d31ffdd7a934d8a1a86db29e84a
d4abe10db55578ef5df589545e27e8e8a008f9a1744d8c6112b57215e4cd86da	e3bea2c996c8d221188e782285c015b049aae6d6e86af24d1cfae0ab4b3883f9
d6d2ca7a33955eb437bd4f529e9768eab28715aa30332737f94151c223f9a851	15caa31c1af89e1d255853f9f1037fae20d9068d74dc26d040a16988c948840b

Archivos reportados (se recomienda mantener en monitoreo)

23.106.122.108	37.48.85.217
103.125.191.128	173.0.139.104
103.125.191.208	45.137.22.107
103.133.108.114	206.183.108.197
103.141.138.124	110.4.43.200
195.200.252.120	110.4.41.14
201.163.211.245	168.245.18.217
103.150.8.29	51.81.143.195
103.254.13.91	185.83.252.40
103.53.172.9	149.72.62.218
139.138.58.70	5.206.224.202
159.148.73.55	192.155.250.195
199.40.206.35	103.225.25.3
199.40.206.35	116.50.58.190
212.114.52.195	128.199.27.192
37.48.85.220	179.61.152.133
38.64.1.164	179.61.152.134
45.137.22.133	185.222.57.240
45.137.22.158	185.222.57.85
45.137.22.76	185.222.57.88
45.147.228.64	45.137.22.108
95.211.208.25	45.88.3.61
51.68.128.161	

Correo electrónico (Se recomienda mantener monitoreo)

umjhy@hpmm.com.ar	info@zzcontrols.com
accounts@pinkmondo.com	ipm@ipm-korea.co.kr
admin@uchile.cl	kajiriart@gmail.com
craiggoodman@greatplainsfire.com	Kelvin.Tan@fendercare.com
dien.nd@nsets.com.vn	krfijc@libreriapaniagua.com.ar
facturacion@ddsm.mx	maheshwariviresh87@gmail.com
gguzman@tratausa.com	MBagnara@freshdelmonte.com
heeyoung.youn@kuehne-nagel.com	nfe@sigmametais.com.br
info@antaisolar.com	noliktava@zdkrava.lv
info@teyseergroup.com	odds.f12@gmail.com
info@zzcontrols.com	ovy.kurnia14@pgascom.co.id
ipm@ipm-korea.co.kr	purchase@cenerg.in
spam@bfs.barracudanetworks.com	recibos@cafsa.com
stanko@green.net.ua	sales.dhl@bitisgroup.vn

tec.deckel@globalpack.com.br	Sales@Lisungroup.com
umjhy@hpmm.com.ar	sales@yingdapc.com
krfijc@libreriapaniagua.com.ar	spam@bfs.barracudanetworks.com
maheshwariviresh87@gmail.com	stanko@green.net.ua
MBagnara@freshdelmonte.com	tec.deckel@globalpack.com.br
nfe@sigmametais.com.br	twokings992@gmail.com
noliktava@zdkrava.lv	unitedstatecustom@gmail.com
odds.f12@gmail.com	umjhy@hpmm.com.ar
ovy.kurnia14@pgascom.co.id	esrakennedy@gracecole.co.uk
purchase@cenerg.in	accounts@rust.com
recibos@cafsa.com	accounts@tpflogistics.in
sales.dhl@bitisgroup.vn	adrian@bestwaycargo.es
Sales@Lisungroup.com	dicki@ramencoa.ga
sales@yingdapc.com	esrakennedy@gracecole.co.uk
twokings992@gmail.com	jeff@alrawdha.bh
unitedstatecustom@gmail.com	josephine.wong@sc.com
kajiriart@gmail.com	mail@akbartrading.com
Kelvin.Tan@fendercare.com	michael.kwong@seapinepower.com
umjhy@hpmm.com.ar	ngocmy.ta@bitisgroup.vn
accounts@pinkmondo.com	reply@indusdrills.org
admin@uchile.cl	rsalazar@gpikoz.com
craiggoodman@greatplainsfire.com	sales.in@alliancecomm.com
dien.nd@nsets.com.vn	sales@cnpc.com.cn
facturacion@ddsm.mx	Sales@ecandes.de
gguzman@tratausa.com	sales@fengqi.sh.cn
heeyoung.youn@kuehne-nagel.com	sales02@cysmodel.com
info@antaisolar.com	shevchenko@badger.ru
info@teyseergroup.com	teodora.Dinca@garettmoion.com
www-data@consider.vps-ams1.blazingfast.io	

URL (Se recomienda mantener monitoreo)

hxxp://vermasiyaahi[.]com/wp-content/8/
hxxps://bauzeichnung[.]com/cgi-bin/8V/
hxxp://bobenstetter[.]net/cgi-bin/V/
hxxps://bosonit[.]com/wp-includes/We/
hxxp://chinese-photography[.]net/books/T7/
hxxp://compartirwifi[.]com/WordPress_01/ZAa/
hxxp://asn-espirulina[.]com/wp-admin/6hU/
hxxp://accemarbeyal[.]com/wp-includes/meR/
hxxp://somosdrucken[.]com/upload/Wvv/
hxxp://ballatstone[.]com/ballatstone[.]com/Dy0/
hxxp://marmi[.]seoper[.]beget[.]tech/fonts/Aoa/
hxxps://aselsa[.]com/wp-includes/0T/

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.

Actualidad

El malware es un programa o código malicioso diseñado intencionalmente para causar daño a cualquier clase de dispositivos, por ejemplo, computadoras, teléfonos móviles, dispositivos IoT y a toda una infraestructura de red. Existen distintos tipos de malware, por ejemplo, el ransomware, y cada uno ellos tienen una característica y una forma de propagarse diferente.

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 del mismo.

- Javier Valdivia
- Nicole Corsanigo
- Eduardo Romero

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.09.11 13:11:44 -03'00'