Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

09-07-2021 | Año 3 | N°105

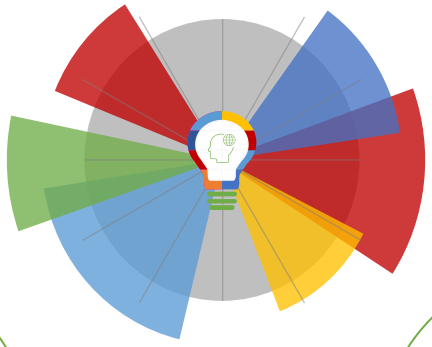
Boletín de Seguridad Cibernética

Semana del 2 al 8 de julio de 2021

La semana en cifras

Hash
22
SHA
Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron
44
URL
Asociadas a sitios fraudulentos y campañas de phishing



Parches
6
para vulnerabilidades
Las mitigaciones son útiles en productos de Kaseya, Windows y Sage.

IP
22
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.

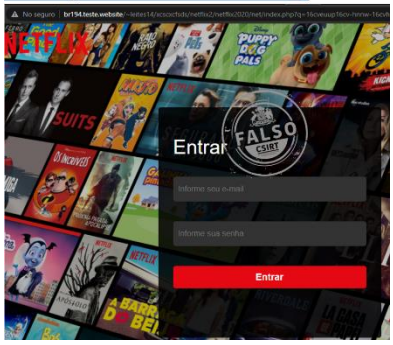
Contenido

Sitios fraudulentos

Imagen del sitio

CSIRT alerta ante página fraudulenta que suplanta a DHL	
Alerta de seguridad cibernética	8FFR21-00987-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de julio de 2021
Última revisión	7 de julio de 2021
Indicadores de compromiso	
URL sitio falso	
https://mail.cabconnect.com[.]au/images/wet/2020dhl_topscript/dhl_topscript/cmd-login=cd01efe09a3c34091edcbd69433f3bbc/?reff=MDg1ODI4MGI1NTA4ZWUxMDk1OGE3NWVkNTExOGE3Nzg=	
IP	
[162.222.226.104]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00987-01/	
https://www.csirt.gob.cl/media/2021/07/8FFR21-00987-01.pdf	

Imagen del sitio



CSIRT alerta ante sitio fraudulento que suplanta a Netflix	
Alerta de seguridad cibernética	8FFR21-00988-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de julio de 2021
Última revisión	7 de julio de 2021
Indicadores de compromiso	
URL sitio falso	
http://br194.teste[.]website/~leites14/xcscxcfsds/netflix2/netflix2020/net/index.php	
IP	
[192.185.176.17]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00988-01/	
https://www.csirt.gob.cl/media/2021/07/8FFR21-00988-01.pdf	

Phishing

CSIRT alerta ante campaña de phishing que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FPH21-00417-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de julio de 2021
Última revisión	7 de julio de 2021
Indicadores de compromiso	
URL de redirección	
https://seguimiento-correos-cl-info[.]com/Tracking2021/	
URL sitio falso	
https://seguimiento-correos-cl-info[.]com/empresas-sep/servicios/V2/f5bac/	
IP	
[192.232.218.213]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00417-01/	
https://www.csirt.gob.cl/media/2021/07/8FPH21-00417-01.pdf	

Vulnerabilidades

CSIRT alerta ante vulnerabilidad crítica que afecta a Kaseya VSA	
Alerta de seguridad cibernética	9VSA21-00462-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de julio de 2021
Última revisión	6 de julio de 2021
CVE	
CVE-2021-30116	
Fabricante	
Kaseya	
Productos afectados	
Kaseya VSA: Todas las versiones	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00462-01	
https://www.csirt.gob.cl/media/2021/07/9VSA21-00462-01.pdf	

CSIRT alerta ante vulnerabilidad crítica que afecta a Windows Print	
Alerta de seguridad cibernética	9VSA21-00463-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de julio de 2021
Última revisión	6 de julio de 2021
CVE	
CVE-2021-34527	
Fabricante	
Windows	
Productos afectados	
Todas las versiones de Windows para clientes y servidores, incluyendo Windows 7, 8.1 y 10, además de Windows Server 2004 a 2019.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00463-01	
https://www.csirt.gob.cl/media/2021/07/9VSA21-00463-01.pdf	

CSIRT alerta por vulnerabilidades en Sage X3	
Alerta de seguridad cibernética	9VSA21-00464-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de julio de 2021
Última revisión	7 de julio de 2021
CVE	
CVE-2020-7387 CVE-2020-7388 CVE-2020-7389 CVE-2020-7390	
Fabricante	
Sage	
Productos afectados	
Sage X3 9, X3 HR & Payroll Version 9, X3 11, y X3 12.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00464-01	
https://www.csirt.gob.cl/media/2021/07/9VSA21-00464-01.pdf	

IoC Malware

A continuación, se comparten los Indicadores de Compromisos que fueron detectados durante la semana pasada por el CSIRT de Gobierno.

Recomendamos a los administradores y usuarios bloquear los hash publicados en este informe, y mantener un permanente monitoreo sobre el resto de los Indicadores de Compromiso.

Hash de archivos maliciosos	Tipo de malware	Documento web
b210c1d75ecf14c15990acd5524688680b99c5f7284f8a14d3a42458e9bc737d	MSIL/CoinMiner.YII!tr	2CMV21-00201-01
b6841eaa5efc709cf762532ec8af2daa90cf08a4a8cda12edd2adb10001bc31a	MSIL/Kryptik.DLO!tr	2CMV21-00201-01
9d8eec2a5899f9d9d0a14bd7e7b6a39aa582cbbf60db5b5043648d2696b0a319	MSIL/Zmutzy.10!tr	2CMV21-00201-01
3c2a5d950317aa50d37b191ba295162c02d14a6ff3c025af487bc99783eff414	MSIL/Kryptik.ABSN!tr	2CMV21-00201-01
0fd6652f7c270e1305795106182c94dd053ba35c2f3e3f418ddf4d778015f569	MSIL/CoinMiner.YII!tr	2CMV21-00201-01
af3d79e42de3f8759ad4ada86a8952a4aae9250b56779465bac4c5764adb0dcd	MSIL/GenKryptik.FHHH!tr	2CMV21-00201-01
a9b03983f5a4ee070a257b4abceb58ad40100b0222d4a16b13eecdb376d9e119	MSIL/Zmutzy.10!tr	2CMV21-00201-01
cd12a0dfbfcc5d7722934554a45661900dcb2b516b802e092d1a4bff2e53d8c7	MSIL/Zmutzy.10!tr	2CMV21-00201-01
72b2e3c62ce309dc3ad54629be509aeb8c7b3e641cc2b20e773875102a355f72	MSIL/Zmutzy.10!tr	2CMV21-00201-01
e417a3467627ffc0faf36de78a5a4157dd03221f6acdf991cbf12aadf8b4c032	Malicious_Behavior.SB	2CMV21-00201-01
02849d08315cde8a0b40ef84efa6a124335b8cc3059e62cc6276c396716afd48	MSExcel/Agent.1C28!tr	2CMV21-00201-01
c0ab2eba9b259d824d95faf3402e25a2166bfa3abf8b05ae13ddd45db10c89fd	MSIL/Zmutzy.10!tr	2CMV21-00201-01
98241126288b257ea140884e7c4f0f88f4694d8fe2f1a7bc0b006db35644e3be	W32/Injector.EPMJ!tr	2CMV21-00201-01
f785d92c7dc3988cc720cd0b75d2d7ffb55fe22c972b85ca2ce6e0cd9a7b393d	MSIL/Zmutzy.10!tr	2CMV21-00201-01
e643cd12513d5b497dc929f3b9bcc4ced2dba43c572854fdab3f9191b2d42d2c	MSIL/CoinMiner.YII!tr	2CMV21-00201-01
9ab06dad5958032d92be8b54abfd84e4a782	Malware_Generic.P0	2CMV21-00201-01

8df3accffca30a459ad3a87ff4ec		
829bf6c033b2eb64533471fe8b10a3681219afcdaf61ab47efa30133098db6b1	MSIL/Zmutzy.10!tr	2CMV21-00201-01
c8b2192f933e3b3124abbf20d43e8de51cfceea1469ef40413d3fc83d98c8d03	W32/Malicious_Behavior	2CMV21-00201-01
9627f98b6a50fed8620dae19198edfce38b9ac6e405431ef3b02f90a3904aaa2	MSIL/Zmutzy.10!tr	2CMV21-00201-01
1e4a78b8b23dadfd585b80f8cb12431e6b6b56a0d858c37274dfec5362ebde40	Malicious_Behavior.SB	2CMV21-00201-01
72eebffcbd8b447b411063c73c3de336ac6c7f924451ca701ff66ac4087ec875	MSIL/Kryptik.DLO!tr	2CMV21-00201-01
4092cc3841bc5e1377fb65e343cb837f0255e33d2194c3b24c8dde82a28511ba	Malicious_Behavior.SB	2CMV21-00201-01

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
45.35.196.146	Psychz Networks	2CMV21-00201-01
23.254.230.107	Hostwinds LLC.	2CMV21-00201-01
77.247.110.72	Myweb Limited	2CMV21-00201-01
70.35.201.40	Fasthosts Internet Inc	2CMV21-00201-01
185.222.57.78	Data Center/Web Hosting/Transit	2CMV21-00201-01
185.222.57.135	RootLayer Web Services Ltd	2CMV21-00201-01
103.155.83.165	Vietspeed Service Company Limited	2CMV21-00201-01
135.148.114.42	OVH US LLC	2CMV21-00201-01
103.139.44.229	Trung Hieu Services Trading Investment Company Limited	2CMV21-00201-01
103.155.80.68	Viet Speed Service Company Limited	2CMV21-00201-01
103.133.106.175	NOCIX Trading and Service Limited Company	2CMV21-00201-01
185.244.38.120	Hyonix LLC	2CMV21-00201-01
203.146.21.245	CSLOXINFO IDC	2CMV21-00201-01
165.22.8.198	DigitalOcean LLC	2CMV21-00201-01
103.141.137.99	Echip Service Trading Company Limited	2CMV21-00201-01
185.222.57.89	RootLayer Web Services Ltd.	2CMV21-00201-01
77.247.110.249	Myweb Limited	2CMV21-00201-01

209.126.124.211	GoDaddy.com LLC	2CMV21-00201-01
185.222.57.72	RootLayer Web Services Ltd.	2CMV21-00201-01

Actualidad

Exitosa cuarta versión del OEA Cyberwomen Challenge premia cuatro chilenas que disputarán final regional

Este jueves se realizó en Chile la primera fecha de la cuarta edición del Cyberwomen Challenge, clasificatoria para la final americana. Como cada año, mujeres de todo el país se inscribieron para participar, organizadas en equipos y compitiendo en una serie de realistas simulaciones de ataques informáticos.

Las ganadoras fueron Leticia Palazuelos, Margarita Vargas, Alejandra Rojas y Montserrat Rodríguez. Los detalles, aquí: https://www.csirt.gob.cl/noticias/exitosa-cuarta-version-del-oea-cyberwomen-challenge-premia-cuatro-chilenas-que-disputaran-final-regional/.

Ataques a repositorios git | Características y mitigación

Los ataques a los repositorios git, el sistema de control de versiones de código más usado en el mundo, protagonizan una investigación de Juan Sanhueza, experto del CSIRT de Gobierno, quien elaboró un informe para conocer cómo funcionan estos ataques y como mitigarlos. Este documento en PDF lo pueden descargar aquí: https://www.csirt.gob.cl/reportes/ataques-a-repositorios-git-caracteristicas-y-mitigacion/.

Informe de Gestión CSIRT de Gobierno Junio 2021

Durante esta semana, el CSIRT de Gobierno entregó su Informe de Gestión mensual correspondiente a junio, el que puede ser revisado aquí: https://www.csirt.gob.cl/estadisticas/informe-de-gestion-csirt-de-gobierno-junio-2021/.

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 del Estado, al informar problemas de seguridad y vulnerabilidades descubiertas.

El CSIRT de Gobierno destaca en este segmento a quienes reportaron incidentes utilizando canales formales (https://www.csirt.gob.cl o al teléfono +(562) 2486 3850) siempre que hayan aportado información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- José Francisco Lagos Alvear
- Miguel Carvajal Franco
- Andrés Aldana
- Mónica María Palma Viganego
- Camila Isabel Donoso Urrutia
- Leonardo Guerra
- Víctor Ulloa
- Laura Andrea Riveros Araya
- German E. Navarro Navarrete
- Rodrigo Herrera Vergara
- Ximena Fernández

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.07.09 14:46:15 -04'00'