Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

11-06-2021 | Año 3 | N°101

Boletín de Seguridad Cibernética

Semana del 04 al 10 de junio de 2021

La semana en cifras

Hash

12

SHA

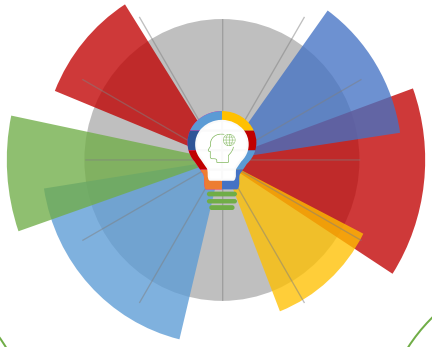
Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron

6

URL

Asociadas a sitios fraudulentos y campañas de phishing



Parches

59

para vulnerabilidades

Las mitigaciones son útiles en productos de Microsoft y Google.

IP

12

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.

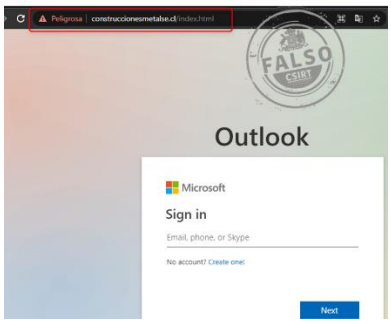
Contenido

Malware

CSIRT alerta de campaña de malware que suplanta a Sodimac	
Alerta de seguridad cibernética	2CMV21-00192-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de junio de 2021
Última revisión	10 de junio de 2021
Indicadores de compromiso	
SHA256	
B64B2AFDCF32D3FC94A528A988E814C33FC99BB934ADF70181C7F6322403C43B 99D45C44F4DDBA585C9773157BCAF3ED4897C6ADC0BB46F8C141D5D09A6C05E9	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00192-01/	
https://csirt.gob.cl/media/2021/06/2CMV21-00192-01.pdf	

Sitios fraudulentos

Imagen del sitio



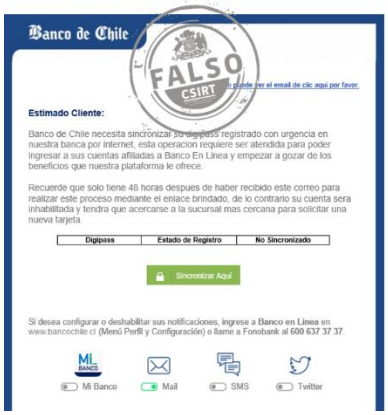
CSIRT advierte de página fraudulenta que suplanta a Outlook	
Alerta de seguridad cibernética	8FFR21-00960-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de junio de 2021
Última revisión	09 de junio de 2021
Indicadores de compromiso	
URL sitio falso	
http://construccionesmetalse[.]cl/index.html	
IP	
[200.63.97.52]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00960-01/	
https://www.csirt.gob.cl/media/2021/06/8FFR21-00960-01.pdf	

Imagen del sitio

CSIRT advierte de página fraudulenta que suplanta a Wells Fargo	
Alerta de seguridad cibernética	8FFR21-00961-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de junio de 2021
Última revisión	10 de junio de 2021
Indicadores de compromiso	
URL sitio falso	
http://www.bikeworld[.]cl/home/	
IP	
[192.140.56.106]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00961-01/	
https://www.csirt.gob.cl/media/2021/06/8FFR21-00961-01.pdf	

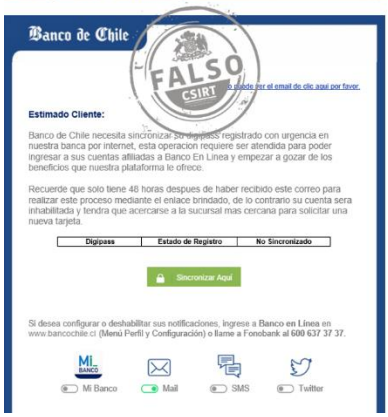
Phishing

Imagen del mensaje



CSIRT alerta de campaña de phishing que suplanta al Banco de Chile	
Alerta de seguridad cibernética	8FPH21-00406-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de junio de 2021
Última revisión	07 de junio de 2021
Indicadores de compromiso	
URL sitio redirección	
http://shyamalaenterprises[.]com/b58980a340f42863d0858b69ffc09b53	
URL sitio falso	
https://portalpersonasbchle.cl-mlx[.]com/1623077009/persona/login	
IP	
[63.250.38.217]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00406-01/	
https://www.csirt.gob.cl/media/2021/06/8FPH21-00406-01.pdf	

Imagen del mensaje



CSIRT advierte de campaña de phishing que suplanta al Banco de Chile	
Alerta de seguridad cibernética	8FPH21-00407-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de junio de 2021
Última revisión	10 de junio de 2021
Indicadores de compromiso	
URL sitio dirección	
http://shyamalaenterprises[.]com/b412496fa5c1181bd0a036332f89df69	
URL sitio falso	
https://portalpersonaslbchle.cl-jsp[.]com/1623351245/persona/login	
IP	
[68.65.122.47]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00407-01/	
https://www.csirt.gob.cl/media/2021/06/8FPH21-00407-01.pdf	

Vulnerabilidades

CSIRT alerta de vulnerabilidad crítica en Google Chrome	
Alerta de seguridad cibernética	9VSA21-00453-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de junio de 2021
Última revisión	10 de junio de 2021

CVE

CVE-2021-30544	CVE-2021-30548	CVE-2021-30551
CVE-2021-30545	CVE-2021-30549	CVE-2021-30552
CVE-2021-30546	CVE-2021-30550	CVE-2021-30553
CVE-2021-30547		

Fabricante

Google Chrome

Productos afectados

Google Chrome: 87.0.4280.66 a 91.0.4472.77

Enlaces para revisar el informe:

https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00453-01
https://www.csirt.gob.cl/media/2021/06/9VSA21-00453-01.pdf

CSIRT advierte de vulnerabilidades críticas en productos de Microsoft	
Alerta de seguridad cibernética	9VSA21-00454-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de junio de 2021
Última revisión	10 de junio de 2021

CVE

CVE-2021-33739	CVE-2021-31966	CVE-2021-31945
CVE-2021-31985	CVE-2021-31965	CVE-2021-31955
CVE-2021-31978	CVE-2021-31964	CVE-2021-1675
CVE-2021-31957	CVE-2021-31963	CVE-2021-31952
CVE-2021-31959	CVE-2021-31950	CVE-2021-31958
CVE-2021-31971	CVE-2021-31949	CVE-2021-31960
CVE-2021-31980	CVE-2021-31948	CVE-2021-31956
CVE-2021-31977	CVE-2021-31944	CVE-2021-31954
CVE-2021-31976	CVE-2021-31943	CVE-2021-31201
CVE-2021-31975	CVE-2021-31942	CVE-2021-31199
CVE-2021-31974	CVE-2021-31941	CVE-2021-31951
CVE-2021-31973	CVE-2021-31940	CVE-2021-31953
CVE-2021-31972	CVE-2021-31939	CVE-2021-26414
CVE-2021-31970	CVE-2021-26420	CVE-2021-31962
CVE-2021-31968	CVE-2021-31983	CVE-2021-33742
CVE-2021-31969	CVE-2021-31946	CVE-2021-31938
CVE-2021-31967		

Fabricante
Microsoft
Productos afectados
Microsoft Windows .NET Core Visual Studio Microsoft Office Microsoft Edge (Chromium-based y EdgeHTML) Microsoft SharePoint Server Hyper-V Visual Studio Code – Kubernetes Tools Windows HTML Platform Windows Remote Desktop
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00454-01
https://www.csirt.gob.cl/media/2021/06/9VSA21-00454-01.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	Tipo Malware	Documento web
48e5957d0051766804f0f0a6503e08ad1748404621e2cc40000a351acb7bf049	MSOffice/Agent.GV!tr	2CMV21-00191-01
de7aa2a14d5e0f7c115416ca88f33b2aefac4e4d9dfb941643a64db60b6f45eb	MSIL/Kryptik.ABHT!tr	2CMV21-00191-01
e479cc72a5c8500bef39e159b9f3b90ba9629a180028f0f80a02274b17a3801c	MSOffice/Agent.GV!tr	2CMV21-00191-01
2f7f1a43ce097e9b4ffaae162eaa6b20f87b4f7b873d7951864978636eedf421	MSOffice/CVE_2017_11882.C!exploit	2CMV21-00191-01
0cd70fd04a01dcb095dac96b68bbffc6a47dc6651030656893f6744278c8926f	Malicious_Behavior.SB	2CMV21-00191-01
8b3499872ce31886294713b699a5c3051ba3ede9bcaaf2a8e54df114725d6308	HTML/Phish.D799!tr	2CMV21-00191-01
c3e1008f5f5bdaa71c41e8fe0ae9615b0de342ddbeac28a0d409b5b004b84a68	Malicious_Behavior.SB	2CMV21-00191-01
07ffbabb575117c731872d2d6cda388f2343fdee55d700f8357263a48c0edabc	HTML/Agent.TA!tr	2CMV21-00191-01
5b52135e0a170eafb2b9479fecbe0591cc14fc3d7cbe6e10d69ab4dd15637dfb	HTML/Phish.BJQ!tr	2CMV21-00191-01
857a20f05d51fb0346fa09c106e7eadb4037f27888e65c56f9688b7cdd00b71f	Malicious_Behavior.SB	2CMV21-00191-01

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
143.244.159.175	DigitalOcean, LLC	2CMV21-00191-01
143.244.159.163	DigitalOcean, LLC	2CMV21-00191-01
103.232.53.185	VietServer Services technology company limited	2CMV21-00191-01
185.222.57.86	RootLayer Web Services Ltd.	2CMV21-00191-01
128.199.119.198	DigitalOcean, LLC	2CMV21-00191-01
165.232.146.180	DigitalOcean, LLC	2CMV21-00191-01
188.166.113.55	DigitalOcean, LLC	2CMV21-00191-01
162.245.190.75	Quadranet-Global	2CMV21-00191-01

Actualidad

Ciberguía | Medidas preventivas de conductas abusivas en RRSS

El internet y las redes sociales son muy útiles y tienen múltiples beneficios, pero también tienen un lado negativo que es importante conocer. Uno de ellos son los programas maliciosos que pueden infectar tu computadora, pero también existen otros riesgos que provienen directamente de personas que hacen uso de las redes sociales para acosar y hacer daño a otros.

Por esta razón, el CSIRT de Gobierno ha creado esta guía con el fin de exponer en un solo lugar las herramientas, métodos más importantes y útiles para prevenir ser víctima del ciberacoso u otros peligros que están presentes hoy en día en las redes sociales.

La guía completa puede verse aquí: https://www.csirt.gob.cl/recomendaciones/ciberguia-medidas-preventivas-de-conductas-abusivas-en-rrss/.

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.

- Juan Pablo Berríos
- Ricardo Rojas Zurita
- Francisco Flefil
- Julián Andrés Palacios
- Osvaldo Simón Carrasco Sepúlveda

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.06.11 20:05:56 -04'00'